```
pre-rule  THM

⊢  ∀i,a:Id, T:Type, ds:x:Id fp-> Type, P:(State(ds)→T→Prop).
|  @i (with ds: ds
|     action a:T
|     precondition a(v) is
|     P s v)
|  realizes es.(∀x:Id. vartype(i;x) ⊆r ds(x)?Top)
|              & (∀e:E.
|                 loc(e) = i
|                 ⇒
|                 kind(e) = locl(a) ⇒ (valtype(e) ⊆r T))
|              & (∀e:E.
|                 loc(e) = i
|                 ⇒
|                 (kind(e) = locl(a) ⇒ P((λz.(z when e)),val(e)))
|                 & (∃e':E.
|                    (e <loc e') ∨ e = e'
|                    & kind(e') = locl(a)
|                      ∨ (∀v:T. ¬P((λz.(z after e')),v))))
| by Auto
|    THEN
|    BackThru
|    Thm* ∀D:Dsys, P:({es:ES| es is an event system of D }→Prop{i'}).
|         D realizes2 es.P(es) ⇒ D realizes es.P(es)
|    {d_DASH_realizes2_DASH_implies_DASH_realizes}
|    THENA
|    Try (Complete Auto)
|
|\
| .....wf .....
| 1. i : Id
| 2. a : Id
| 3. T : Type
| 4. ds : x:Id fp-> Type
| 5. P : State(ds)→T→Prop
| ⊢  (λes.(∀x:Id. vartype(i;x) ⊆r ds(x)?Top)
|     & (∀e:E. loc(e) = i ⇒ kind(e) = locl(a) ⇒ (valtype(e) ⊆r T))
|     & (∀e:E.
|        loc(e) = i
|        ⇒
|        (kind(e) = locl(a) ⇒ P((λz.(z when e)),val(e)))
|        & (∃e':E.
|           (e <loc e') ∨ e = e'
|           & kind(e') = locl(a) ∨ (∀v:T. ¬P((λz.(z after e')),v)))))
|    ∈ {es:ES
|       | es is an event system of @i (with ds: ds
|                                       action a:T
|                                       precondition a(v) is
|                                       P s v) }
|      →Prop
|   by Analyze THEN Analyze -1 THEN Analyze -1 THEN ExRepD
|      THEN
|      Try (Unfold `ma-state` 0)
|      THEN
```

```
|      DoSubsume
|      THEN
|      Subst (loc(e) = i) 0
|      THEN
|      Try BackThruSomeHyp
|      THEN
|      Subst (loc(e') = i) 0
|      THEN
|      Try BackThruSomeHyp
|      THEN
|      SplitOrHyps
|      THEN
|      AllHyps (Unfold `es-locl`)
|      THEN
|      Subst (e' = e) 0
|
.\
. 1. i : Id
. 2. a : Id
. 3. T : Type
. 4. ds : x:Id fp-> Type
. 5. P : State(ds)→T→Prop
. ⊢  @i (with ds: ds
. |     action a:T
. |     precondition a(v) is
. |     P s v) realizes2 es.(∀x:Id. vartype(i;x) ⊆r ds(x)?Top)
. |  & (∀e:E. loc(e) = i ⇒ kind(e) = locl(a) ⇒ (valtype(e) ⊆r T))
. |  & (∀e:E.
. |     loc(e) = i
. |     ⇒
. |     (kind(e) = locl(a) ⇒ P((λz.(z when e)),val(e)))
. |     & (∃e':E.
. |        (e <loc e') ∨ e = e'
. |        & kind(e') = locl(a) ∨ (∀v:T. ¬P((λz.(z after e')),v))))
. | by let maops
. |        ≡ [`ma-ds`
. |          ;`ma-da`
. |          ;`ma-din`
. |          ;`ma-dout`
. |          ;`ma-pre`
. |          ;`ma-npre`
. |          ;`ma-ef`
. |          ;`ma-init`
. |          ;`ma-decla`] in
. |    RepeatFor 3 (Analyze 0 THENA Complete Auto)
. |    THEN
. |    AssertBY ((eqof(IdDeq)(i,i)) ∼ true2)
. |    (BackThru
. |     Thm* ∀d:EqDecider(A), i:A. (eqof(d)(i,i)) ∼ true2
. |     {eqof_eq_btrue})
. |    THEN
. |    ES_Reduce
. |    THEN
. |    PW_Reduce -2
. |    THEN
```

```
. |    AllHyps
. |    (λh.
. |     InstHyp [i] h THENA Complete Auto
. |     THEN
. |     Subst ((eqof(IdDeq)(i,i)) ∼ true₂) -1
. |     THENL
. |     [Trivial
. |     ;Thin h THEN Reduce -1
. |      THEN
. |      Repeat (Unfolds maops -1 THEN Reduce -1)])
. |
. 1. i : Id
. 2. a : Id
. 3. T : Type
. 4. ds : x:Id fp-> Type
. 5. P : State(ds)→T→Prop
. 6. w : World
. 7. p : FairFifo
. 8. FairFifo
. 9. ∀l:IdLnk, tg:Id.
. |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. |                    <ds,<[locl(a)],λx.T>,,<[a],λx.P>,,,,,•>
. |                 else  fi.da(rcv(l; tg))
. 10. (eqof(IdDeq)(i,i)) ∼ true₂
. 11. ∀a@0:Id, t:ℕ.
. |   ∃t':ℕ.
. |   t≤t'
. |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. |     ∨ P@0 != <[a],λx.P>(a@0) ==> ∀v:<[locl(a)]
. |                                     ,λx.T>(locl(a@0))?Top.
. |       ¬P@0((λx.s(i;t').x),v)
. 12. ∀t:ℕ.
. |   ¬isnull(a(i;t))
. |   ⇒
. |   (islocal(kind(a(i;t)))
. |    ⇒
. |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. |    ⇒
. |    P((λx.s(i;t).x),val(a(i;t))))
. |   & (∀x:Id.
. |      deq-member(product-deq(Knd;Id;KindDeq;IdDeq);...;1of())
. |      ⇒
. |      s(i;t+1).x = 2of()(<kind(a(i;t)),x>,λx.s(i;t).x,val(a(i;t))))
. |   & (∀l:IdLnk.
. |      deq-member(product-deq(Knd;IdLnk;KindDeq;IdLnkDeq);<kind(...)
. |                                                          ,l>;1of())
. |      ⇒
. |      withlnk(l;m(i;t))
. |      =
. |      if source(l) = i→
. |         concat(map(λtgf.map(λx.<1of(tgf)
. |                                 ,x>;2of(tgf)
. |                                     ((λx.s(i;t).x)
. |                                     ,val(a(i;t))));2of()
```

```
. |                                                    (<kind(a(i;t))
. |                                                     ,l>)))
. |      else nil fi)
. |   & (∀x:Id.
. |      ¬(deq-member(IdDeq;x;1of())
. |        ⇒
. |        deq-member(KindDeq;kind(a(i;t));2of()(x)))
. |      ⇒
. |      s(i;t).x = s(i;t+1).x)
. |   & (∀l:IdLnk, tg:Id.
. |      ¬(deq-member(product-deq(IdLnk;Id;IdLnkDeq;IdDeq);<l,tg>;1of(
. |                                                                 ))
. |        ⇒
. |        deq-member(KindDeq;kind(a(i;t));2of()(<l,tg>)))
. |      ⇒
. |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. 13. ∀x:Id. deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. 14. ∀a@0:Action(i).
. |   ¬isnull(a@0)
. |   ⇒
. |   (valtype(i;a@0) ⊆r <[locl(a)],λx.T>(kind(a@0))?Top)
. 15. ∀x:Id.
. |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→ 2of(ds)(x)
. |                  else Top fi
. ⊢  (∀x:Id. vartype(i;x) ⊆r ds(x)?Top)
. |  & (∀e:E. loc(e) = i ⇒ kind(e) = locl(a) ⇒ (valtype(e) ⊆r T))
. |  & (∀e:E.
. |     loc(e) = i
. |     ⇒
. |     (kind(e) = locl(a) ⇒ P((λz.(z when e)),val(e)))
. |     & (∃e':E.
. |        (e <loc e') ∨ e = e'
. |        & kind(e') = locl(a) ∨ (∀v:T. ¬P((λz.(z after e')),v))))
. | by Assert (IdDeq ∈ EqDecider(Id))
. |
. |\
. | .....assertion .....
. | 1. i : Id
. | 2. a : Id
. | 3. T : Type
. | 4. ds : x:Id fp-> Type
. | 5. P : State(ds)→T→Prop
. | 6. w : World
. | 7. FairFifo
. | 8. FairFifo
. | 9. ∀l:IdLnk, tg:Id.
. |    (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. |                      <ds,<[locl(a)],λx.T>,,<[a],λx.P>,,,,,·>
. |                   else  fi.da(rcv(l; tg))
. | 10. (eqof(IdDeq)(i,i)) ∼ true₂
. | 11. ∀a@0:Id, t:ℕ.
. |     ∃t':ℕ.
. |     t≤t'
. |     & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. |       ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
```

```
. |       ∨ P@0 != <[a],λx.P>(a@0) ==> ∀v:<[locl(a)]
. |                                      ,λx.T>(locl(a@0))?Top.
. |         ¬P@0((λx.s(i;t').x),v)
. | 12. ∀t:ℕ.
. |     ¬isnull(a(i;t))
. |     ⇒
. |     (islocal(kind(a(i;t)))
. |      ⇒
. |      (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. |      ⇒
. |      P((λx.s(i;t).x),val(a(i;t))))
. |     & (∀x:Id.
. |        deq-member(product-deq(Knd;Id;KindDeq;IdDeq);<kind(a(i;t))
. |                                                     ,x>;1of())
. |        ⇒
. |        s(i;t+1).x
. |        =
. |        2of()(<kind(a(i;t)),x>,λx.s(i;t).x,val(a(i;t))))
. |     & (∀l:IdLnk.
. |        deq-member(product-deq(Knd;IdLnk;KindDeq;IdLnkDeq);<...
. |                                                          ,l>;1of(
. |                                                              ))
. |        ⇒
. |        withlnk(l;m(i;t))
. |        =
. |        if source(l) = i→
. |           concat(map(λtgf.map(λx.<1of(tgf)
. |                                  ,x>;2of(tgf)
. |                                      ((λx.s(i;t).x)
. |                                      ,val(a(i;t))));2of()
. |                                                     (<kind(a(i;t))
. |                                                      ,l>)))
. |        else nil fi)
. |     & (∀x:Id.
. |        ¬(deq-member(IdDeq;x;1of())
. |          ⇒
. |          deq-member(KindDeq;kind(a(i;t));2of()(x)))
. |        ⇒
. |        s(i;t).x = s(i;t+1).x)
. |     & (∀l:IdLnk, tg:Id.
. |        ¬(deq-member(product-deq(IdLnk;Id;IdLnkDeq;IdDeq);...;1of(
. |                                                             ))
. |          ⇒
. |          deq-member(KindDeq;kind(a(i;t));2of()(<l,tg>)))
. |        ⇒
. |        w-tagged(tg; onlnk(l;m(i;t))) = nil)
. | 13. ∀x:Id. deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. | 14. ∀a@0:Action(i).
. |     ¬isnull(a@0)
. |     ⇒
. |     (valtype(i;a@0) ⊆r <[locl(a)],λx.T>(kind(a@0))?Top)
. | 15. ∀x:Id.
. |     vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→ 2of(ds)(x)
. |                      else Top fi
. | ⊢  IdDeq ∈ EqDecider(Id)  by Auto
```

```
. |
. .\
. . 1. i : Id
. . 2. a : Id
. . 3. T : Type
. . 4. ds : x:Id fp-> Type
. . 5. P : State(ds)→T→Prop
. . 6. w : World
. . 7. p : FairFifo
. . 8. FairFifo
. . 9. ∀l:IdLnk, tg:Id.
. . |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . |                    <ds,<[locl(a)],λx.T>,,<[a],λx.P>,,,,,•>
. . |                 else  fi.da(rcv(l; tg))
. . 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . 11. ∀a@0:Id, t:ℕ.
. . |   ∃t':ℕ.
. . |   t≤t'
. . |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . |     ∨ P@0 != <[a],λx.P>(a@0) ==> ∀v:<[locl(a)]
. . |                                     ,λx.T>(locl(a@0))?Top.
. . |       ¬P@0((λx.s(i;t').x),v)
. . 12. ∀t:ℕ.
. . |   ¬isnull(a(i;t))
. . |   ⇒
. . |   (islocal(kind(a(i;t)))
. . |    ⇒
. . |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . |    ⇒
. . |    P((λx.s(i;t).x),val(a(i;t))))
. . |   & (∀x:Id.
. . |      deq-member(product-deq(Knd;Id;KindDeq;IdDeq);<kind(a(i;t))
. . |                                                  ,x>;1of())
. . |      ⇒
. . |      s(i;t+1).x
. . |      =
. . |      2of()(<kind(a(i;t)),x>,λx.s(i;t).x,val(a(i;t))))
. . |   & (∀l:IdLnk.
. . |      deq-member(product-deq(Knd;IdLnk;KindDeq;IdLnkDeq);<...
. . |                                                        ,l>;1of(
. . |                                                            ))
. . |      ⇒
. . |      withlnk(l;m(i;t))
. . |      =
. . |      if source(l) = i→
. . |         concat(map(λtgf.map(λx.<1of(tgf)
. . |                                 ,x>;2of(tgf)
. . |                                     ((λx.s(i;t).x)
. . |                                     ,val(a(i;t))));2of()
. . |                                                  (<kind(a(i;t))
. . |                                                   ,l>)))
. . |      else nil fi)
. . |   & (∀x:Id.
. . |      ¬(deq-member(IdDeq;x;1of())
```

```
. . |        ⇒
. . |        deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . |      ⇒
. . |      s(i;t).x = s(i;t+1).x)
. . |   & (∀l:IdLnk, tg:Id.
. . |      ¬(deq-member(product-deq(IdLnk;Id;IdLnkDeq;IdDeq);...;1of(
. . |                                                          ))
. . |        ⇒
. . |        deq-member(KindDeq;kind(a(i;t));2of()(<l,tg>)))
. . |      ⇒
. . |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . 13. ∀x:Id. deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . 14. ∀a@0:Action(i).
. . |   ¬isnull(a@0)
. . |   ⇒
. . |   (valtype(i;a@0) ⊆r <[locl(a)],λx.T>(kind(a@0))?Top)
. . 15. ∀x:Id.
. . |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→ 2of(ds)(x)
. . |                  else Top fi
. . 16. IdDeq ∈ EqDecider(Id)
. . ⊢  (∀x:Id. vartype(i;x) ⊆r ds(x)?Top)
. . |  & (∀e:E. loc(e) = i ⇒ kind(e) = locl(a) ⇒ (valtype(e) ⊆r T))
. . |  & (∀e:E.
. . |     loc(e) = i
. . |     ⇒
. . |     (kind(e) = locl(a) ⇒ P((λz.(z when e)),val(e)))
. . |     & (∃e':E.
. . |        (e <loc e') ∨ e = e'
. . |        & kind(e') = locl(a) ∨ (∀v:T. ¬P((λz.(z after e')),v))))
. . | by Analyze 0
. . |
. . |\
. . | 1. i : Id
. . | 2. a : Id
. . | 3. T : Type
. . | 4. ds : x:Id fp-> Type
. . | 5. P : State(ds)→T→Prop
. . | 6. w : World
. . | 7. p : FairFifo
. . | 8. FairFifo
. . | 9. ∀l:IdLnk, tg:Id.
. . | |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . | |                    <ds,<[locl(a)],λx.T>,,<[a],λx.P>,,,,,•>
. . | |                 else  fi.da(rcv(l; tg))
. . | 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . | 11. ∀a@0:Id, t:ℕ.
. . | |   ∃t':ℕ.
. . | |   t≤t'
. . | |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . | |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . | |     ∨ P@0 != <[a],λx.P>(a@0) ==> ∀v:<[locl(a)]
. . | |                                    ,λx.T>(locl(a@0))?Top.
. . | |       ¬P@0((λx.s(i;t').x),v)
. . | 12. ∀t:ℕ.
. . | |   ¬isnull(a(i;t))
```

```
. . | |   ⇒
. . | |   (islocal(kind(a(i;t)))
. . | |    ⇒
. . | |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . | |    ⇒
. . | |    P((λx.s(i;t).x),val(a(i;t))))
. . | |   & (∀x:Id.
. . | |      deq-member(product-deq(Knd;Id;KindDeq;IdDeq);<kind(...)
. . | |                                                  ,x>;1of())
. . | |      ⇒
. . | |      s(i;t+1).x
. . | |      =
. . | |      2of()(<kind(a(i;t)),x>,λx.s(i;t).x,val(a(i;t))))
. . | |   & (∀l:IdLnk.
. . | |      deq-member(product-deq(Knd;IdLnk;KindDeq;...);<kind(...)
. . | |                                                   ,l>;1of())
. . | |      ⇒
. . | |      withlnk(l;m(i;t))
. . | |      =
. . | |      if source(l) = i→
. . | |         concat(map(λtgf.map(λx.
. . | |         <1of(tgf),x>;2of(tgf)
. . | |                      ((λx.s(i;t).x)
. . | |                      ,val(a(i;t))));2of()(<kind(a(i;t)),l>)))
. . | |      else nil fi)
. . | |   & (∀x:Id.
. . | |      ¬(deq-member(IdDeq;x;1of())
. . | |        ⇒
. . | |        deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . | |      ⇒
. . | |      s(i;t).x = s(i;t+1).x)
. . | |   & (∀l:IdLnk, tg:Id.
. . | |      ¬(deq-member(product-deq(IdLnk;Id;IdLnkDeq;...);...;1of(
. . | |                                                        ))
. . | |        ⇒
. . | |        deq-member(KindDeq;kind(a(i;t));2of()(<l,tg>)))
. . | |      ⇒
. . | |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . | 13. ∀x:Id. deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . | 14. ∀a@0:Action(i).
. . | |   ¬isnull(a@0)
. . | |   ⇒
. . | |   (valtype(i;a@0) ⊆r <[locl(a)],λx.T>(kind(a@0))?Top)
. . | 15. ∀x:Id.
. . | |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→ 2of(ds)(x)
. . | |                  else Top fi
. . | 16. IdDeq ∈ EqDecider(Id)
. . | ⊢  (∀x:Id. vartype(i;x) ⊆r ds(x)?Top)
. . | |  & (∀e:E.
. . | |     loc(e) = i ⇒ kind(e) = locl(a) ⇒ (valtype(e) ⊆r T))
. . | | by Analyze 0
. . | |
. . | |\
. . | | 1. i : Id
. . | | 2. a : Id
```

```
. . | | 3. T : Type
. . | | 4. ds : x:Id fp-> Type
. . | | 5. P : State(ds)→T→Prop
. . | | 6. w : World
. . | | 7. FairFifo
. . | | 8. FairFifo
. . | | 9. ∀l:IdLnk, tg:Id.
. . | | |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . | | |                    <ds,<[locl(a)],λx.T>,,<[a],λx.P>,,,,,•>
. . | | |                 else  fi.da(rcv(l; tg))
. . | | 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . | | 11. ∀a@0:Id, t:ℕ.
. . | | |   ∃t':ℕ.
. . | | |   t≤t'
. . | | |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . | | |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . | | |     ∨ P@0 != <[a],λx.P>(a@0) ==> ∀v:<[locl(a)]
. . | | |                                    ,λx.T>(locl(a@0))?Top.
. . | | |       ¬P@0((λx.s(i;t').x),v)
. . | | 12. ∀t:ℕ.
. . | | |   ¬isnull(a(i;t))
. . | | |   ⇒
. . | | |   (islocal(kind(a(i;t)))
. . | | |    ⇒
. . | | |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . | | |    ⇒
. . | | |    P((λx.s(i;t).x),val(a(i;t))))
. . | | |   & (∀x:Id.
. . | | |      deq-member(product-deq(Knd;Id;KindDeq;IdDeq);<kind(...)
. . | | |                                                  ,x>;1of())
. . | | |      ⇒
. . | | |      s(i;t+1).x
. . | | |      =
. . | | |      2of()(<kind(a(i;t)),x>,λx.s(i;t).x,val(a(i;t))))
. . | | |   & (∀l:IdLnk.
. . | | |      deq-member(product-deq(Knd;IdLnk;KindDeq;...);<...
. . | | |                                                   ,l>;1of(
. . | | |                                                       ))
. . | | |      ⇒
. . | | |      withlnk(l;m(i;t))
. . | | |      =
. . | | |      if source(l) = i→
. . | | |         concat(map(λtgf.map(λx.
. . | | |         <1of(tgf),x>;2of(tgf)
. . | | |                     ((λx.s(i;t).x)
. . | | |                     ,val(a(i;t))));2of()
. . | | |                                   (<kind(a(i;t)),l>)))
. . | | |      else nil fi)
. . | | |   & (∀x:Id.
. . | | |      ¬(deq-member(IdDeq;x;1of())
. . | | |        ⇒
. . | | |        deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . | | |      ⇒
. . | | |      s(i;t).x = s(i;t+1).x)
. . | | |   & (∀l:IdLnk, tg:Id.
```

```
. . | | |      ¬(deq-member(product-deq(IdLnk;Id;...;IdDeq);...;1of())
. . | | |        ⇒
. . | | |        deq-member(KindDeq;kind(a(i;t));2of()(<l,tg>)))
. . | | |      ⇒
. . | | |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . | | 13. ∀x:Id. deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . | | 14. ∀a@0:Action(i).
. . | | |   ¬isnull(a@0)
. . | | |   ⇒
. . | | |   (valtype(i;a@0) ⊆r <[locl(a)],λx.T>(kind(a@0))?Top)
. . | | 15. ∀x:Id.
. . | | |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→ 2of(ds)(x)
. . | | |                   else Top fi
. . | | 16. IdDeq ∈ EqDecider(Id)
. . | | ⊢  ∀x:Id. vartype(i;x) ⊆r ds(x)?Top  by Analyze 0
. . | | |
. . | | 1. i : Id
. . | | 2. a : Id
. . | | 3. T : Type
. . | | 4. ds : x:Id fp-> Type
. . | | 5. P : State(ds)→T→Prop
. . | | 6. w : World
. . | | 7. FairFifo
. . | | 8. FairFifo
. . | | 9. ∀l:IdLnk, tg:Id.
. . | | |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . | | |                   <ds,<[locl(a)],λx.T>,,<[a],λx.P>,,,,,•>
. . | | |                 else  fi.da(rcv(l; tg))
. . | | 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . | | 11. ∀a@0:Id, t:ℕ.
. . | | |   ∃t':ℕ.
. . | | |   t≤t'
. . | | |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . | | |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . | | |     ∨ P@0 != <[a],λx.P>(a@0) ==> ∀v:<[locl(a)]
. . | | |                                   ,λx.T>(locl(a@0))?Top.
. . | | |       ¬P@0((λx.s(i;t').x),v)
. . | | 12. ∀t:ℕ.
. . | | |   ¬isnull(a(i;t))
. . | | |   ⇒
. . | | |   (islocal(kind(a(i;t)))
. . | | |    ⇒
. . | | |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . | | |    ⇒
. . | | |    P((λx.s(i;t).x),val(a(i;t))))
. . | | |   & (∀x:Id.
. . | | |      deq-member(product-deq(Knd;Id;KindDeq;IdDeq);<kind(...)
. . | | |                                                   ,x>;1of())
. . | | |      ⇒
. . | | |      s(i;t+1).x
. . | | |      =
. . | | |      2of()(<kind(a(i;t)),x>,λx.s(i;t).x,val(a(i;t))))
. . | | |   & (∀l:IdLnk.
. . | | |      deq-member(product-deq(Knd;IdLnk;KindDeq;...);<...
. . | | |                                                  ,l>;1of(
```

```
. . | | |                                                          ))
. . | | |      ⇒
. . | | |      withlnk(l;m(i;t))
. . | | |      =
. . | | |      if source(l) = i→
. . | | |         concat(map(λtgf.map(λx.
. . | | |         <1of(tgf),x>;2of(tgf)
. . | | |                     ((λx.s(i;t).x)
. . | | |                     ,val(a(i;t))));2of()
. . | | |                                  (<kind(a(i;t)),l>)))
. . | | |      else nil fi)
. . | | |   & (∀x:Id.
. . | | |      ¬(deq-member(IdDeq;x;1of())
. . | | |        ⇒
. . | | |        deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . | | |      ⇒
. . | | |      s(i;t).x = s(i;t+1).x)
. . | | |   & (∀l:IdLnk, tg:Id.
. . | | |      ¬(deq-member(product-deq(IdLnk;Id;...;IdDeq);...;1of())
. . | | |        ⇒
. . | | |        deq-member(KindDeq;kind(a(i;t));2of()(<l,tg>)))
. . | | |      ⇒
. . | | |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . | | 13. ∀x:Id. deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . | | 14. ∀a@0:Action(i).
. . | | |   ¬isnull(a@0)
. . | | |   ⇒
. . | | |   (valtype(i;a@0) ⊆r <[locl(a)],λx.T>(kind(a@0))?Top)
. . | | 15. ∀x:Id.
. . | | |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→ 2of(ds)(x)
. . | | |                   else Top fi
. . | | 16. IdDeq ∈ EqDecider(Id)
. . | | 17. x : Id
. . | | ⊢  vartype(i;x) ⊆r ds(x)?Top
. . | | | by Assert (IdDeq ∈ EqDecider(Id))
. . | | |
. . | | |\
. . | | | .....assertion .....
. . | | | 1. i : Id
. . | | | 2. a : Id
. . | | | 3. T : Type
. . | | | 4. ds : x:Id fp-> Type
. . | | | 5. P : State(ds)→T→Prop
. . | | | 6. w : World
. . | | | 7. FairFifo
. . | | | 8. FairFifo
. . | | | 9. ∀l:IdLnk, tg:Id.
. . | | |    (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . | | |                    <ds,<[locl(a)],λx.T>,,<[a],λx.P>,,,,,•>
. . | | |                  else  fi.da(rcv(l; tg))
. . | | | 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . | | | 11. ∀a@0:Id, t:ℕ.
. . | | |     ∃t':ℕ.
. . | | |     t≤t'
. . | | |     & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
```

```
. . | | |       ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . | | |       ∨ P@0 != <[a],λx.P>(a@0) ==> ∀v:<[locl(a)]
. . | | |                                      ,λx.T>(locl(a@0))?Top.
. . | | |         ¬P@0((λx.s(i;t').x),v)
. . | | | 12. ∀t:ℕ.
. . | | |     ¬isnull(a(i;t))
. . | | |     ⇒
. . | | |     (islocal(kind(a(i;t)))
. . | | |      ⇒
. . | | |      (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . | | |      ⇒
. . | | |      P((λx.s(i;t).x),val(a(i;t))))
. . | | |     & (∀x:Id.
. . | | |        deq-member(product-deq(Knd;Id;KindDeq;IdDeq);<...
. . | | |                                                    ,x>;1of(
. . | | |                                                        ))
. . | | |        ⇒
. . | | |        s(i;t+1).x
. . | | |        =
. . | | |        2of()(<kind(a(i;t)),x>,λx.s(i;t).x,val(a(i;t))))
. . | | |     & (∀l:IdLnk.
. . | | |        deq-member(product-deq(Knd;IdLnk;...;...);<kind(...)
. . | | |                                                ,l>;1of())
. . | | |        ⇒
. . | | |        withlnk(l;m(i;t))
. . | | |        =
. . | | |        if source(l) = i→
. . | | |           concat(map(λtgf.map(λx.
. . | | |           <1of(tgf),x>;2of(tgf)
. . | | |                       ((λx.s(i;t).x)
. . | | |                       ,val(a(i;t))));2of()
. . | | |                                    (<kind(a(i;t)),l>)))
. . | | |        else nil fi)
. . | | |     & (∀x:Id.
. . | | |        ¬(deq-member(IdDeq;x;1of())
. . | | |          ⇒
. . | | |          deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . | | |        ⇒
. . | | |        s(i;t).x = s(i;t+1).x)
. . | | |     & (∀l:IdLnk, tg:Id.
. . | | |        ¬(deq-member(product-deq(IdLnk;Id;...;IdDeq);...;1of(
. . | | |                                                        ))
. . | | |          ⇒
. . | | |          deq-member(KindDeq;kind(a(i;t));2of()(<l,tg>)))
. . | | |        ⇒
. . | | |        w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . | | | 13. ∀x:Id. deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . | | | 14. ∀a@0:Action(i).
. . | | |     ¬isnull(a@0)
. . | | |     ⇒
. . | | |     (valtype(i;a@0) ⊆r <[locl(a)],λx.T>(kind(a@0))?Top)
. . | | | 15. ∀x:Id.
. . | | |     vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . | | |                        2of(ds)(x)
. . | | |                     else Top fi
```

```
. . | | | 16. IdDeq ∈ EqDecider(Id)
. . | | | 17. Id
. . | | | ⊢  IdDeq ∈ EqDecider(Id)  by Auto
. . | | |
. . | | .\
. . | | . 1. i : Id
. . | | . 2. a : Id
. . | | . 3. T : Type
. . | | . 4. ds : x:Id fp-> Type
. . | | . 5. P : State(ds)→T→Prop
. . | | . 6. w : World
. . | | . 7. FairFifo
. . | | . 8. FairFifo
. . | | . 9. ∀l:IdLnk, tg:Id.
. . | | . |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . | | . |                    <ds,<[locl(a)],λx.T>,,<[a],λx.P>,,,,,•>
. . | | . |                 else  fi.da(rcv(l; tg))
. . | | . 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . | | . 11. ∀a@0:Id, t:ℕ.
. . | | . |   ∃t':ℕ.
. . | | . |   t≤t'
. . | | . |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . | | . |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . | | . |     ∨ P@0 != <[a],λx.P>(a@0) ==> ∀v:<[locl(a)]
. . | | . |                                    ,λx.T>(locl(a@0))?Top.
. . | | . |       ¬P@0((λx.s(i;t').x),v)
. . | | . 12. ∀t:ℕ.
. . | | . |   ¬isnull(a(i;t))
. . | | . |   ⇒
. . | | . |   (islocal(kind(a(i;t)))
. . | | . |    ⇒
. . | | . |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . | | . |    ⇒
. . | | . |    P((λx.s(i;t).x),val(a(i;t))))
. . | | . |   & (∀x:Id.
. . | | . |      deq-member(product-deq(Knd;Id;KindDeq;IdDeq);<...
. . | | . |                                                  ,x>;1of(
. . | | . |                                                      ))
. . | | . |      ⇒
. . | | . |      s(i;t+1).x
. . | | . |      =
. . | | . |      2of()(<kind(a(i;t)),x>,λx.s(i;t).x,val(a(i;t))))
. . | | . |   & (∀l:IdLnk.
. . | | . |      deq-member(product-deq(Knd;IdLnk;...;...);<kind(...)
. . | | . |                                               ,l>;1of())
. . | | . |      ⇒
. . | | . |      withlnk(l;m(i;t))
. . | | . |      =
. . | | . |      if source(l) = i→
. . | | . |         concat(map(λtgf.map(λx.
. . | | . |         <1of(tgf),x>;2of(tgf)
. . | | . |                      ((λx.s(i;t).x)
. . | | . |                      ,val(a(i;t))));2of()
. . | | . |                                    (<kind(a(i;t)),l>)))
. . | | . |      else nil fi)
```

```
. . | | . |   & (∀x:Id.
. . | | . |      ¬(deq-member(IdDeq;x;1of())
. . | | . |        ⇒
. . | | . |        deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . | | . |      ⇒
. . | | . |      s(i;t).x = s(i;t+1).x)
. . | | . |   & (∀l:IdLnk, tg:Id.
. . | | . |      ¬(deq-member(product-deq(IdLnk;Id;...;IdDeq);...;1of(
. . | | . |                                                      ))
. . | | . |        ⇒
. . | | . |        deq-member(KindDeq;kind(a(i;t));2of()(<l,tg>)))
. . | | . |      ⇒
. . | | . |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . | | . 13. ∀x:Id. deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . | | . 14. ∀a@0:Action(i).
. . | | . |   ¬isnull(a@0)
. . | | . |   ⇒
. . | | . |   (valtype(i;a@0) ⊆r <[locl(a)],λx.T>(kind(a@0))?Top)
. . | | . 15. ∀x:Id.
. . | | . |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . | | . |                      2of(ds)(x)
. . | | . |                   else Top fi
. . | | . 16. IdDeq ∈ EqDecider(Id)
. . | | . 17. x : Id
. . | | . 18. IdDeq ∈ EqDecider(Id)
. . | | . ⊢  vartype(i;x) ⊆r ds(x)?Top
. . | | . | by InstHyp [x] -4
. . | | . |    THENA
. . | | . |    (Auto THEN All (Unfold `dstype`) THEN All Reduce
. . | | . |     THEN
. . | | . |     Trivial)
. . | | . |
. . | | . 1. i : Id
. . | | . 2. a : Id
. . | | . 3. T : Type
. . | | . 4. ds : x:Id fp-> Type
. . | | . 5. P : State(ds)→T→Prop
. . | | . 6. w : World
. . | | . 7. FairFifo
. . | | . 8. FairFifo
. . | | . 9. ∀l:IdLnk, tg:Id.
. . | | . |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . | | . |                    <ds,<[locl(a)],λx.T>,,<[a],λx.P>,,,,,•>
. . | | . |                 else  fi.da(rcv(l; tg))
. . | | . 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . | | . 11. ∀a@0:Id, t:ℕ.
. . | | . |   ∃t':ℕ.
. . | | . |   t≤t'
. . | | . |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . | | . |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . | | . |     ∨ P@0 != <[a],λx.P>(a@0) ==> ∀v:<[locl(a)]
. . | | . |                                    ,λx.T>(locl(a@0))?Top.
. . | | . |       ¬P@0((λx.s(i;t').x),v)
. . | | . 12. ∀t:ℕ.
. . | | . |   ¬isnull(a(i;t))
```

```
. . | | . |   ⇒
. . | | . |   (islocal(kind(a(i;t)))
. . | | . |    ⇒
. . | | . |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . | | . |    ⇒
. . | | . |    P((λx.s(i;t).x),val(a(i;t))))
. . | | . |   & (∀x:Id.
. . | | . |      deq-member(product-deq(Knd;Id;KindDeq;IdDeq);<...
. . | | . |                                                  ,x>;1of(
. . | | . |                                                      ))
. . | | . |      ⇒
. . | | . |      s(i;t+1).x
. . | | . |      =
. . | | . |      2of()(<kind(a(i;t)),x>,λx.s(i;t).x,val(a(i;t))))
. . | | . |   & (∀l:IdLnk.
. . | | . |      deq-member(product-deq(Knd;IdLnk;...;...);<kind(...)
. . | | . |                                               ,l>;1of())
. . | | . |      ⇒
. . | | . |      withlnk(l;m(i;t))
. . | | . |      =
. . | | . |      if source(l) = i→
. . | | . |         concat(map(λtgf.map(λx.
. . | | . |         <1of(tgf),x>;2of(tgf)
. . | | . |                     ((λx.s(i;t).x)
. . | | . |                     ,val(a(i;t))));2of()
. . | | . |                                    (<kind(a(i;t)),l>)))
. . | | . |      else nil fi)
. . | | . |   & (∀x:Id.
. . | | . |      ¬(deq-member(IdDeq;x;1of())
. . | | . |        ⇒
. . | | . |        deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . | | . |      ⇒
. . | | . |      s(i;t).x = s(i;t+1).x)
. . | | . |   & (∀l:IdLnk, tg:Id.
. . | | . |      ¬(deq-member(product-deq(IdLnk;Id;...;IdDeq);...;1of(
. . | | . |                                                      ))
. . | | . |        ⇒
. . | | . |        deq-member(KindDeq;kind(a(i;t));2of()(<l,tg>)))
. . | | . |      ⇒
. . | | . |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . | | . 13. ∀x:Id. deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . | | . 14. ∀a@0:Action(i).
. . | | . |   ¬isnull(a@0)
. . | | . |   ⇒
. . | | . |   (valtype(i;a@0) ⊆r <[locl(a)],λx.T>(kind(a@0))?Top)
. . | | . 15. ∀x:Id.
. . | | . |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . | | . |                     2of(ds)(x)
. . | | . |                  else Top fi
. . | | . 16. IdDeq ∈ EqDecider(Id)
. . | | . 17. x : Id
. . | | . 18. IdDeq ∈ EqDecider(Id)
. . | | . 19. vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . | | . |                     2of(ds)(x)
. . | | . |                  else Top fi
```

```
. . | | . ⊢  vartype(i;x) ⊆r ds(x)?Top
. . | | . | by Subst
. . | | . |    (if deq-member(IdDeq;x;1of(ds))→ 2of(ds)(x) else Top fi
. . | | . |     =
. . | | . |     ds(x)?Top)
. . | | . |    -1
. . | | . |    THENA
. . | | . |    (Auto THEN Try D_ES_Subtype)
. . | | . |    THEN
. . | | . |    Try Trivial
. . | | . |
. . | | . .....equality .....
. . | | . 1. i : Id
. . | | . 2. a : Id
. . | | . 3. T : Type
. . | | . 4. ds : x:Id fp-> Type
. . | | . 5. P : State(ds)→T→Prop
. . | | . 6. w : World
. . | | . 7. FairFifo
. . | | . 8. FairFifo
. . | | . 9. ∀l:IdLnk, tg:Id.
. . | | . |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . | | . |                    <ds,<[locl(a)],λx.T>,,<[a],λx.P>,,,,,•>
. . | | . |                 else  fi.da(rcv(l; tg))
. . | | . 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . | | . 11. ∀a@0:Id, t:ℕ.
. . | | . |   ∃t':ℕ.
. . | | . |   t≤t'
. . | | . |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . | | . |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . | | . |     ∨ P@0 != <[a],λx.P>(a@0) ==> ∀v:<[locl(a)]
. . | | . |                                    ,λx.T>(locl(a@0))?Top.
. . | | . |       ¬P@0((λx.s(i;t').x),v)
. . | | . 12. ∀t:ℕ.
. . | | . |   ¬isnull(a(i;t))
. . | | . |   ⇒
. . | | . |   (islocal(kind(a(i;t)))
. . | | . |    ⇒
. . | | . |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . | | . |    ⇒
. . | | . |    P((λx.s(i;t).x),val(a(i;t))))
. . | | . |   & (∀x:Id.
. . | | . |      deq-member(product-deq(Knd;Id;KindDeq;IdDeq);<...
. . | | . |                                                  ,x>;1of(
. . | | . |                                                      ))
. . | | . |      ⇒
. . | | . |      s(i;t+1).x
. . | | . |      =
. . | | . |      2of()(<kind(a(i;t)),x>,λx.s(i;t).x,val(a(i;t))))
. . | | . |   & (∀l:IdLnk.
. . | | . |      deq-member(product-deq(Knd;IdLnk;...;...);<kind(...)
. . | | . |                                               ,l>;1of())
. . | | . |      ⇒
. . | | . |      withlnk(l;m(i;t))
. . | | . |      =
```

```
. . | | . |      if source(l) = i→
. . | | . |         concat(map(λtgf.map(λx.
. . | | . |         <1of(tgf),x>;2of(tgf)
. . | | . |                      ((λx.s(i;t).x)
. . | | . |                      ,val(a(i;t))));2of()
. . | | . |                                    (<kind(a(i;t)),l>)))
. . | | . |      else nil fi)
. . | | . |   & (∀x:Id.
. . | | . |      ¬(deq-member(IdDeq;x;1of())
. . | | . |        ⇒
. . | | . |        deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . | | . |      ⇒
. . | | . |      s(i;t).x = s(i;t+1).x)
. . | | . |   & (∀l:IdLnk, tg:Id.
. . | | . |      ¬(deq-member(product-deq(IdLnk;Id;...;IdDeq);...;1of(
. . | | . |                                                        ))
. . | | . |        ⇒
. . | | . |        deq-member(KindDeq;kind(a(i;t));2of()(<l,tg>)))
. . | | . |      ⇒
. . | | . |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . | | . 13. ∀x:Id. deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . | | . 14. ∀a@0:Action(i).

. . | | . |   ¬isnull(a@0)
. . | | . |   ⇒
. . | | . |   (valtype(i;a@0) ⊆r <[locl(a)],λx.T>(kind(a@0))?Top)
. . | | . 15. ∀x:Id.
. . | | . |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . | | . |                      2of(ds)(x)
. . | | . |                   else Top fi
. . | | . 16. IdDeq ∈ EqDecider(Id)
. . | | . 17. x : Id
. . | | . 18. IdDeq ∈ EqDecider(Id)
. . | | . 19. vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . | | . |                      2of(ds)(x)
. . | | . |                   else Top fi
. . | | . ⊢  if deq-member(IdDeq;x;1of(ds))→ 2of(ds)(x) else Top fi
. . | | . |  =
. . | | . |  ds(x)?Top  by Assert (deq-member(IdDeq;x;1of(ds)) ∈ 𝔹)
. . | | . |
. . | | . |\
. . | | . | .....assertion .....
. . | | . | 1. i : Id
. . | | . | 2. a : Id
. . | | . | 3. T : Type
. . | | . | 4. ds : x:Id fp-> Type
. . | | . | 5. P : State(ds)→T→Prop
. . | | . | 6. w : World
. . | | . | 7. FairFifo
. . | | . | 8. FairFifo
. . | | . | 9. ∀l:IdLnk, tg:Id.
. . | | . |    (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . | | . |                      <ds
. . | | . |                      ,<[locl(a)],λx.T>
. . | | . |                      ,
. . | | . |                      ,<[a],λx.P>
```

```
. . | | . |                      ,
. . | | . |                      ,
. . | | . |                      ,
. . | | . |                      ,
. . | | . |                      ,·>
. . | | . |                  else  fi.da(rcv(l; tg))
. . | | . | 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . | | . | 11. ∀a@0:Id, t:ℕ.
. . | | . |     ∃t':ℕ.
. . | | . |     t≤t'
. . | | . |     & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . | | . |       ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . | | . |       ∨ P@0 != <[a],λx.P>(a@0) ==> ∀v:<[locl(a)]
. . | | . |                                      ,λx.
. . | | . |                                       T>(locl(a@0))?Top.
. . | | . |         ¬P@0((λx.s(i;t').x),v)
. . | | . | 12. ∀t:ℕ.
. . | | . |     ¬isnull(a(i;t))
. . | | . |     ⇒
. . | | . |     (islocal(kind(a(i;t)))
. . | | . |      ⇒
. . | | . |      (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . | | . |      ⇒
. . | | . |      P((λx.s(i;t).x),val(a(i;t))))
. . | | . |     & (∀x:Id.
. . | | . |        deq-member(product-deq(Knd;Id;KindDeq;...);<...
. . | | . |                                                  ,x>;1of(
. . | | . |                                                      ))
. . | | . |        ⇒
. . | | . |        s(i;t+1).x
. . | | . |        =
. . | | . |        2of()(<kind(a(i;t)),x>,λx.s(i;t).x,val(a(i;t))))
. . | | . |     & (∀l:IdLnk.
. . | | . |        deq-member(product-deq(Knd;IdLnk;...;...);<...
. . | | . |                                                ,l>;1of(
. . | | . |                                                    ))
. . | | . |        ⇒
. . | | . |        withlnk(l;m(i;t))
. . | | . |        =
. . | | . |        if source(l) = i→
. . | | . |           concat(map(λtgf.map(λx.
. . | | . |           <1of(tgf),x>;2of(tgf)
. . | | . |                       ((λx.s(i;t).x)
. . | | . |                       ,val(a(i;t))));2of()
. . | | . |                                      (<kind(a(i;t)),l>)))
. . | | . |        else nil fi)
. . | | . |     & (∀x:Id.
. . | | . |        ¬(deq-member(IdDeq;x;1of())
. . | | . |          ⇒
. . | | . |          deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . | | . |        ⇒
. . | | . |        s(i;t).x = s(i;t+1).x)
. . | | . |     & (∀l:IdLnk, tg:Id.
. . | | . |        ¬(deq-member(product-deq(IdLnk;Id;...;...);...;1of(
. . | | . |                                                      ))
```

```
. . | | . |          ⇒
. . | | . |          deq-member(KindDeq;kind(a(i;t));2of()(<l,tg>)))
. . | | . |        ⇒
. . | | . |        w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . | | . | 13. ∀x:Id.
. . | | . |     deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . | | . | 14. ∀a@0:Action(i).
. . | | . |     ¬isnull(a@0)
. . | | . |     ⇒
. . | | . |     (valtype(i;a@0) ⊆r <[locl(a)],λx.T>(kind(a@0))?Top)
. . | | . | 15. ∀x:Id.
. . | | . |     vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . | | . |                        2of(ds)(x)
. . | | . |                    else Top fi
. . | | . | 16. IdDeq ∈ EqDecider(Id)
. . | | . | 17. x : Id
. . | | . | 18. IdDeq ∈ EqDecider(Id)
. . | | . | 19. vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . | | . |                        2of(ds)(x)
. . | | . |                    else Top fi
. . | | . | ⊢  deq-member(IdDeq;x;1of(ds)) ∈ 𝔹
. . | | . |   by DVar 'ds' THEN Reduce 0
. . | | . |
. . | | . .\
. . | | . . 1. i : Id
. . | | . . 2. a : Id
. . | | . . 3. T : Type
. . | | . . 4. ds : x:Id fp-> Type
. . | | . . 5. P : State(ds)→T→Prop
. . | | . . 6. w : World
. . | | . . 7. FairFifo
. . | | . . 8. FairFifo
. . | | . . 9. ∀l:IdLnk, tg:Id.
. . | | . .  | (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . | | . .  |                   <ds
. . | | . .  |                   ,<[locl(a)],λx.T>
. . | | . .  |                   ,
. . | | . .  |                   ,<[a],λx.P>
. . | | . .  |                   ,
. . | | . .  |                   ,
. . | | . .  |                   ,
. . | | . .  |                   ,
. . | | . .  |                   ,·>
. . | | . .  |                else  fi.da(rcv(l; tg))
. . | | . . 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . | | . . 11. ∀a@0:Id, t:ℕ.
. . | | . .  |   ∃t':ℕ.
. . | | . .  |   t≤t'
. . | | . .  |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . | | . .  |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . | | . .  |     ∨ P@0 != <[a],λx.P>(a@0) ==> ∀v:<[locl(a)]
. . | | . .  |                                    ,λx.
. . | | . .  |                                     T>(locl(a@0))?Top.
. . | | . .  |       ¬P@0((λx.s(i;t').x),v)
. . | | . . 12. ∀t:ℕ.
```

```
. . | | . . |   ¬isnull(a(i;t))
. . | | . . |   ⇒
. . | | . . |   (islocal(kind(a(i;t)))
. . | | . . |    ⇒
. . | | . . |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . | | . . |    ⇒
. . | | . . |    P((λx.s(i;t).x),val(a(i;t))))
. . | | . . |   & (∀x:Id.
. . | | . . |      deq-member(product-deq(Knd;Id;KindDeq;...);<...
. . | | . . |                                                ,x>;1of(
. . | | . . |                                                    ))
. . | | . . |      ⇒
. . | | . . |      s(i;t+1).x
. . | | . . |      =
. . | | . . |      2of()(<kind(a(i;t)),x>,λx.s(i;t).x,val(a(i;t))))
. . | | . . |   & (∀l:IdLnk.
. . | | . . |      deq-member(product-deq(Knd;IdLnk;...;...);<...
. . | | . . |                                              ,l>;1of(
. . | | . . |                                                  ))
. . | | . . |      ⇒
. . | | . . |      withlnk(l;m(i;t))
. . | | . . |      =
. . | | . . |      if source(l) = i→
. . | | . . |         concat(map(λtgf.map(λx.
. . | | . . |         <1of(tgf),x>;2of(tgf)
. . | | . . |                     ((λx.s(i;t).x)
. . | | . . |                     ,val(a(i;t))));2of()
. . | | . . |                                   (<kind(a(i;t)),l>)))
. . | | . . |      else nil fi)
. . | | . . |   & (∀x:Id.
. . | | . . |      ¬(deq-member(IdDeq;x;1of())
. . | | . . |        ⇒
. . | | . . |        deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . | | . . |      ⇒
. . | | . . |      s(i;t).x = s(i;t+1).x)
. . | | . . |   & (∀l:IdLnk, tg:Id.
. . | | . . |      ¬(deq-member(product-deq(IdLnk;Id;...;...);...;1of(
. . | | . . |                                                    ))
. . | | . . |        ⇒
. . | | . . |        deq-member(KindDeq;kind(a(i;t));2of()(<l,tg>)))
. . | | . . |      ⇒
. . | | . . |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . | | . . 13. ∀x:Id.
. . | | . . |   deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . | | . . 14. ∀a@0:Action(i).
. . | | . . |   ¬isnull(a@0)
. . | | . . |   ⇒
. . | | . . |   (valtype(i;a@0) ⊆r <[locl(a)],λx.T>(kind(a@0))?Top)
. . | | . . 15. ∀x:Id.
. . | | . . |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . | | . . |                      2of(ds)(x)
. . | | . . |                  else Top fi
. . | | . . 16. IdDeq ∈ EqDecider(Id)
. . | | . . 17. x : Id
. . | | . . 18. IdDeq ∈ EqDecider(Id)
```

```
. . | | . . 19. vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . | | . . |                      2of(ds)(x)

. . | | . . |                   else Top fi
. . | | . . 20. deq-member(IdDeq;x;1of(ds)) ∈ 𝔹
. . | | . . ⊢  if deq-member(IdDeq;x;1of(ds))→ 2of(ds)(x) else Top fi
. . | | . . |  =
. . | | . . |  ds(x)?Top
. . | | . . | by AssertBY (x ∈ dom(ds) ∈ 𝔹) (Auto THEN FpfSubtype)
. . | | . . |
. . | | . . 1. i : Id
. . | | . . 2. a : Id
. . | | . . 3. T : Type
. . | | . . 4. ds : x:Id fp-> Type
. . | | . . 5. P : State(ds)→T→Prop
. . | | . . 6. w : World
. . | | . . 7. FairFifo
. . | | . . 8. FairFifo
. . | | . . 9. ∀l:IdLnk, tg:Id.
. . | | . . |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . | | . . |                    <ds
. . | | . . |                    ,<[locl(a)],λx.T>
. . | | . . |                    ,
. . | | . . |                    ,<[a],λx.P>
. . | | . . |                    ,
. . | | . . |                    ,
. . | | . . |                    ,
. . | | . . |                    ,
. . | | . . |                    ,•>
. . | | . . |                 else  fi.da(rcv(l; tg))
. . | | . . 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . | | . . 11. ∀a@0:Id, t:ℕ.
. . | | . . |   ∃t':ℕ.
. . | | . . |   t≤t'
. . | | . . |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . | | . . |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . | | . . |     ∨ P@0 != <[a],λx.P>(a@0) ==> ∀v:<[locl(a)]
. . | | . . |                                    ,λx.
. . | | . . |                                     T>(locl(a@0))?Top.
. . | | . . |       ¬P@0((λx.s(i;t').x),v)
. . | | . . 12. ∀t:ℕ.
. . | | . . |   ¬isnull(a(i;t))
. . | | . . |   ⇒
. . | | . . |   (islocal(kind(a(i;t)))
. . | | . . |    ⇒
. . | | . . |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . | | . . |    ⇒
. . | | . . |    P((λx.s(i;t).x),val(a(i;t))))
. . | | . . |   & (∀x:Id.
. . | | . . |      deq-member(product-deq(Knd;Id;KindDeq;...);<...
. . | | . . |                                                ,x>;1of(
. . | | . . |                                                    ))
. . | | . . |      ⇒
. . | | . . |      s(i;t+1).x
. . | | . . |      =
. . | | . . |      2of()(<kind(a(i;t)),x>,λx.s(i;t).x,val(a(i;t))))
```

```
. . | | . . |   & (∀l:IdLnk.
. . | | . . |      deq-member(product-deq(Knd;IdLnk;...;...);<...
. . | | . . |                                                ,l>;1of(
. . | | . . |                                                    ))
. . | | . . |      ⇒
. . | | . . |      withlnk(l;m(i;t))
. . | | . . |      =
. . | | . . |      if source(l) = i→
. . | | . . |         concat(map(λtgf.map(λx.
. . | | . . |         <1of(tgf),x>;2of(tgf)
. . | | . . |                     ((λx.s(i;t).x)
. . | | . . |                     ,val(a(i;t))));2of()
. . | | . . |                                   (<kind(a(i;t)),l>)))
. . | | . . |      else nil fi)
. . | | . . |   & (∀x:Id.
. . | | . . |      ¬(deq-member(IdDeq;x;1of())
. . | | . . |        ⇒
. . | | . . |        deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . | | . . |      ⇒
. . | | . . |      s(i;t).x = s(i;t+1).x)
. . | | . . |   & (∀l:IdLnk, tg:Id.
. . | | . . |      ¬(deq-member(product-deq(IdLnk;Id;...;...);...;1of(
. . | | . . |                                                    ))
. . | | . . |        ⇒
. . | | . . |        deq-member(KindDeq;kind(a(i;t));2of()(<l,tg>)))
. . | | . . |      ⇒
. . | | . . |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . | | . . 13. ∀x:Id.
. . | | . . |   deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . | | . . 14. ∀a@0:Action(i).
. . | | . . |   ¬isnull(a@0)
. . | | . . |   ⇒
. . | | . . |   (valtype(i;a@0) ⊆r <[locl(a)],λx.T>(kind(a@0))?Top)
. . | | . . 15. ∀x:Id.
. . | | . . |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . | | . . |                      2of(ds)(x)
. . | | . . |                   else Top fi
. . | | . . 16. IdDeq ∈ EqDecider(Id)
. . | | . . 17. x : Id
. . | | . . 18. IdDeq ∈ EqDecider(Id)
. . | | . . 19. vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . | | . . |                      2of(ds)(x)
. . | | . . |                   else Top fi
. . | | . . 20. deq-member(IdDeq;x;1of(ds)) ∈ 𝔹
. . | | . . 21. x ∈ dom(ds) ∈ 𝔹
. . | | . . ⊢  if deq-member(IdDeq;x;1of(ds))→ 2of(ds)(x) else Top fi
. . | | . . |  =

. . | | . . |  ds(x)?Top
. . | | . . | by Unfold ‘fpf-cap‘ 0 THEN RepeatFor 2 SplitOnConclITE
. . | | . . |    THEN
. . | | . . |    Try (Fold ‘member‘ 0)
. . | | . . |
. . | | . . |\
. . | | . . | .....truecase .....
. . | | . . | 1. i : Id
```

```
. . | | . . | 2. a : Id
. . | | . . | 3. T : Type
. . | | . . | 4. ds : x:Id fp-> Type
. . | | . . | 5. P : State(ds)→T→Prop
. . | | . . | 6. w : World
. . | | . . | 7. FairFifo
. . | | . . | 8. FairFifo
. . | | . . | 9. ∀l:IdLnk, tg:Id.
. . | | . . |    (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . | | . . |                       <ds
. . | | . . |                       ,<[locl(a)],λx.T>
. . | | . . |                       ,
. . | | . . |                       ,<[a],λx.P>
. . | | . . |                       ,
. . | | . . |                       ,
. . | | . . |                       ,
. . | | . . |                       ,
. . | | . . |                       ,·>
. . | | . . |                    else  fi.da(rcv(l; tg))
. . | | . . | 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . | | . . | 11. ∀a@0:Id, t:ℕ.
. . | | . . |     ∃t':ℕ.
. . | | . . |     t≤t'
. . | | . . |     & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . | | . . |       ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . | | . . |       ∨ P@0 != <[a]
. . | | . . |                ,λx.P>(a@0) ==> ∀v:<[locl(a)]
. . | | . . |                                  ,λx.T>(locl(a@0))?Top.
. . | | . . |         ¬P@0((λx.s(i;t').x),v)
. . | | . . | 12. ∀t:ℕ.
. . | | . . |     ¬isnull(a(i;t))
. . | | . . |     ⇒
. . | | . . |     (islocal(kind(a(i;t)))
. . | | . . |      ⇒
. . | | . . |      (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . | | . . |      ⇒
. . | | . . |      P((λx.s(i;t).x),val(a(i;t))))
. . | | . . |     & (∀x:Id.
. . | | . . |        deq-member(product-deq(Knd;Id;...;IdDeq);<...
. . | | . . |                                                ,x>;1of(
. . | | . . |                                                    ))
. . | | . . |        ⇒
. . | | . . |        s(i;t+1).x
. . | | . . |        =
. . | | . . |        2of()(<kind(a(i;t)),x>,λx.s(i;t).x,val(a(i;t))))
. . | | . . |     & (∀l:IdLnk.
. . | | . . |        deq-member(product-deq(Knd;...;...;...);<...
. . | | . . |                                                ,l>;1of(
. . | | . . |                                                    ))
. . | | . . |        ⇒
. . | | . . |        withlnk(l;m(i;t))
. . | | . . |        =
. . | | . . |        if source(l) = i→
. . | | . . |           concat(map(λtgf.map(λx.
. . | | . . |           <1of(tgf)
```

```
. . | | . . |           ,x>;2of(tgf)
. . | | . . |               ((λx.s(i;t).x)
. . | | . . |               ,val(a(i;t))));2of()(<kind(a(i;t)),l>)))
. . | | . . |       else nil fi)
. . | | . . |    & (∀x:Id.
. . | | . . |       ¬(deq-member(IdDeq;x;1of())
. . | | . . |         ⇒
. . | | . . |         deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . | | . . |       ⇒
. . | | . . |       s(i;t).x = s(i;t+1).x)
. . | | . . |    & (∀l:IdLnk, tg:Id.
. . | | . . |       ¬(deq-member(product-deq(...;Id;...;...);...;1of(
. . | | . . |                                                    ))
. . | | . . |         ⇒
. . | | . . |         deq-member(KindDeq;kind(a(i;t));2of()(<l,tg>)))
. . | | . . |       ⇒
. . | | . . |       w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . | | . . | 13. ∀x:Id.
. . | | . . |     deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . | | . . | 14. ∀a@0:Action(i).
. . | | . . |     ¬isnull(a@0)
. . | | . . |     ⇒
. . | | . . |     (valtype(i;a@0) ⊆r <[locl(a)],λx.T>(kind(a@0))?Top)
. . | | . . | 15. ∀x:Id.
. . | | . . |     vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . | | . . |                        2of(ds)(x)
. . | | . . |                     else Top fi
. . | | . . | 16. IdDeq ∈ EqDecider(Id)
. . | | . . | 17. x : Id
. . | | . . | 18. IdDeq ∈ EqDecider(Id)
. . | | . . | 19. vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . | | . . |                        2of(ds)(x)
. . | | . . |                     else Top fi
. . | | . . | 20. deq-member(IdDeq;x;1of(ds)) ∈ ℙ
. . | | . . | 21. x ∈ dom(ds) ∈ ℙ
. . | | . . | 22. deq-member(IdDeq;x;1of(ds))
. . | | . . | 23. x ∈ dom(ds)
. . | | . . | ⊢  2of(ds)(x) = ds(x)
. . | | . . |   by Subst ((2of(ds)(x)) ∼ ds(x)) 0
. . | | . . |      THEN
. . | | . . |      Try (Unfold `fpf-ap` 0 THEN Trivial)
. . | | . . |      THEN
. . | | . . |      FpfSubtype
. . | | . . |
. . | | . . |\
. . | | . . | .....falsecase .....
. . | | . . | 1. i : Id
. . | | . . | 2. a : Id
. . | | . . | 3. T : Type
. . | | . . | 4. ds : x:Id fp-> Type
. . | | . . | 5. P : State(ds)→T→Prop
. . | | . . | 6. w : World
. . | | . . | 7. FairFifo
. . | | . . | 8. FairFifo
. . | | . . | 9. ∀l:IdLnk, tg:Id.
```

```
. . | | . . |    (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . | | . . |                      <ds
. . | | . . |                      ,<[locl(a)],λx.T>
. . | | . . |                      ,
. . | | . . |                      ,<[a],λx.P>
. . | | . . |                      ,
. . | | . . |                      ,
. . | | . . |                      ,
. . | | . . |                      ,
. . | | . . |                      ,·>
. . | | . . |                    else  fi.da(rcv(l; tg))
. . | | . . | 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . | | . . | 11. ∀a@0:Id, t:ℕ.
. . | | . . |     ∃t':ℕ.
. . | | . . |     t≤t'
. . | | . . |     & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . | | . . |       ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . | | . . |       ∨ P@0 != <[a]
. . | | . . |                ,λx.P>(a@0) ==> ∀v:<[locl(a)]
. . | | . . |                                ,λx.T>(locl(a@0))?Top.
. . | | . . |         ¬P@0((λx.s(i;t').x),v)
. . | | . . | 12. ∀t:ℕ.
. . | | . . |     ¬isnull(a(i;t))
. . | | . . |     ⇒
. . | | . . |     (islocal(kind(a(i;t)))
. . | | . . |      ⇒
. . | | . . |      (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . | | . . |      ⇒
. . | | . . |      P((λx.s(i;t).x),val(a(i;t))))
. . | | . . |     & (∀x:Id.
. . | | . . |        deq-member(product-deq(Knd;Id;...;IdDeq);<...
. . | | . . |                                                 ,x>;1of(
. . | | . . |                                                     ))
. . | | . . |        ⇒
. . | | . . |        s(i;t+1).x
. . | | . . |        =
. . | | . . |        2of()(<kind(a(i;t)),x>,λx.s(i;t).x,val(a(i;t))))
. . | | . . |     & (∀l:IdLnk.
. . | | . . |        deq-member(product-deq(Knd;...;...;...);<...
. . | | . . |                                                ,l>;1of(
. . | | . . |                                                    ))
. . | | . . |        ⇒
. . | | . . |        withlnk(l;m(i;t))
. . | | . . |        =
. . | | . . |        if source(l) = i→
. . | | . . |           concat(map(λtgf.map(λx.
. . | | . . |           <1of(tgf)
. . | | . . |           ,x>;2of(tgf)
. . | | . . |               ((λx.s(i;t).x)
. . | | . . |               ,val(a(i;t))));2of()(<kind(a(i;t)),l>)))
. . | | . . |        else nil fi)
. . | | . . |     & (∀x:Id.
. . | | . . |        ¬(deq-member(IdDeq;x;1of())
. . | | . . |          ⇒
. . | | . . |          deq-member(KindDeq;kind(a(i;t));2of()(x)))
```

```
. . | | . . |        ⇒
. . | | . . |        s(i;t).x = s(i;t+1).x)
. . | | . . |     & (∀l:IdLnk, tg:Id.
. . | | . . |        ¬(deq-member(product-deq(...;Id;...;...);...;1of(
. . | | . . |                                                    ))
. . | | . . |          ⇒
. . | | . . |          deq-member(KindDeq;kind(a(i;t));2of()(<l,tg>)))
. . | | . . |        ⇒
. . | | . . |        w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . | | . . | 13. ∀x:Id.
. . | | . . |     deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . | | . . | 14. ∀a@0:Action(i).
. . | | . . |     ¬isnull(a@0)
. . | | . . |     ⇒
. . | | . . |     (valtype(i;a@0) ⊆r <[locl(a)],λx.T>(kind(a@0))?Top)
. . | | . . | 15. ∀x:Id.
. . | | . . |     vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . | | . . |                        2of(ds)(x)
. . | | . . |                     else Top fi
. . | | . . | 16. IdDeq ∈ EqDecider(Id)
. . | | . . | 17. x : Id
. . | | . . | 18. IdDeq ∈ EqDecider(Id)
. . | | . . | 19. vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . | | . . |                        2of(ds)(x)
. . | | . . |                     else Top fi
. . | | . . | 20. deq-member(IdDeq;x;1of(ds)) ∈ 𝔹
. . | | . . | 21. x ∈ dom(ds) ∈ 𝔹

. . | | . . | 22. deq-member(IdDeq;x;1of(ds))
. . | | . . | 23. ¬x ∈ dom(ds)
. . | | . . | ⊢  2of(ds)(x) = Top
. . | | . . |   by Analyze -1 THEN Unfold ‘fpf-dom‘ 0 THEN Analyze 8
. . | | . . |      THEN
. . | | . . |      All Reduce
. . | | . . |      THEN
. . | | . . |      RWO
. . | | . . |      Thm* ∀eq:EqDecider(A), L:A List, x:A.
. . | | . . |           deq-member(eq;x;L) ⟺ (x ∈ L)
. . | | . . |      {assert_DASH_deq_DASH_member}
. . | | . . |      0
. . | | . . |      THEN
. . | | . . |      RWO
. . | | . . |      Thm* ∀eq:EqDecider(A), L:A List, x:A.
. . | | . . |           deq-member(eq;x;L) ⟺ (x ∈ L)
. . | | . . |      {assert_DASH_deq_DASH_member}
. . | | . . |      -1
. . | | . . |      THEN
. . | | . . |      DVar ‘ds’
. . | | . . |      THEN
. . | | . . |      Reduce 0
. . | | . . |
. . | | . .\
. . | | . . . .....truecase .....
. . | | . . . 1. i : Id
. . | | . . . 2. a : Id
. . | | . . . 3. T : Type
```

```
. . | | . . . 4. ds : x:Id fp-> Type
. . | | . . . 5. P : State(ds)→T→Prop
. . | | . . . 6. w : World
. . | | . . . 7. FairFifo
. . | | . . . 8. FairFifo
. . | | . . . 9. ∀l:IdLnk, tg:Id.
. . | | . . .    (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . | | . . .                      <ds
. . | | . . .                      ,<[locl(a)],λx.T>
. . | | . . .                      ,
. . | | . . .                      ,<[a],λx.P>
. . | | . . .                      ,
. . | | . . .                      ,
. . | | . . .                      ,
. . | | . . .                      ,
. . | | . . .                      ,·>
. . | | . . .                  else  fi.da(rcv(l; tg))
. . | | . . . 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . | | . . . 11. ∀a@0:Id, t:ℕ.
. . | | . . .     ∃t':ℕ.
. . | | . . .     t≤t'
. . | | . . .     & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . | | . . .       ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . | | . . .       ∨ P@0 != <[a]
. . | | . . .                ,λx.P>(a@0) ==> ∀v:<[locl(a)]
. . | | . . .                                  ,λx.T>(locl(a@0))?Top.
. . | | . . .         ¬P@0((λx.s(i;t').x),v)
. . | | . . . 12. ∀t:ℕ.
. . | | . . .     ¬isnull(a(i;t))
. . | | . . .     ⇒
. . | | . . .     (islocal(kind(a(i;t)))
. . | | . . .      ⇒
. . | | . . .      (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . | | . . .      ⇒
. . | | . . .      P((λx.s(i;t).x),val(a(i;t))))
. . | | . . .     & (∀x:Id.
. . | | . . .        deq-member(product-deq(Knd;Id;...;IdDeq);<...
. . | | . . .                                                ,x>;1of(
. . | | . . .                                                    ))
. . | | . . .        ⇒
. . | | . . .        s(i;t+1).x
. . | | . . .        =
. . | | . . .        2of()(<kind(a(i;t)),x>,λx.s(i;t).x,val(a(i;t))))
. . | | . . .     & (∀l:IdLnk.
. . | | . . .        deq-member(product-deq(Knd;...;...;...);<...
. . | | . . .                                              ,l>;1of(
. . | | . . .                                                  ))
. . | | . . .        ⇒
. . | | . . .        withlnk(l;m(i;t))
. . | | . . .        =
. . | | . . .        if source(l) = i→
. . | | . . .           concat(map(λtgf.map(λx.
. . | | . . .           <1of(tgf)
. . | | . . .           ,x>;2of(tgf)
. . | | . . .               ((λx.s(i;t).x)
```

```
. . | | . . .              ,val(a(i;t))));2of()(<kind(a(i;t)),l>)))
. . | | . . .       else nil fi)
. . | | . . .    & (∀x:Id.
. . | | . . .       ¬(deq-member(IdDeq;x;1of())
. . | | . . .         ⇒
. . | | . . .         deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . | | . . .       ⇒
. . | | . . .       s(i;t).x = s(i;t+1).x)
. . | | . . .    & (∀l:IdLnk, tg:Id.
. . | | . . .       ¬(deq-member(product-deq(...;Id;...;...);...;1of(
. . | | . . .                                                  ))
. . | | . . .         ⇒
. . | | . . .         deq-member(KindDeq;kind(a(i;t));2of()(<l,tg>)))
. . | | . . .       ⇒
. . | | . . .       w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . | | . . 13. ∀x:Id.
. . | | . . .    deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . | | . . 14. ∀a@0:Action(i).
. . | | . . .    ¬isnull(a@0)
. . | | . . .    ⇒
. . | | . . .    (valtype(i;a@0) ⊆r <[locl(a)],λx.T>(kind(a@0))?Top)
. . | | . . 15. ∀x:Id.
. . | | . . .    vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . | | . . .                       2of(ds)(x)
. . | | . . .                    else Top fi
. . | | . . 16. IdDeq ∈ EqDecider(Id)
. . | | . . 17. x : Id
. . | | . . 18. IdDeq ∈ EqDecider(Id)
. . | | . . 19. vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . | | . . .                       2of(ds)(x)
. . | | . . .                    else Top fi
. . | | . . 20. deq-member(IdDeq;x;1of(ds)) ∈ 𝔹
. . | | . . 21. x ∈ dom(ds) ∈ 𝔹
. . | | . . 22. ¬deq-member(IdDeq;x;1of(ds))
. . | | . . 23. x ∈ dom(ds)
. . | | . . ⊢  Top = ds(x)
. . | | . .   by Analyze -2 THEN Unfold `fpf-dom` -1 THEN Analyze 8
. . | | . .      THEN
. . | | . .      All Reduce
. . | | . .      THEN
. . | | . .      RWO
. . | | . .      Thm* ∀eq:EqDecider(A), L:A List, x:A.
. . | | . .           deq-member(eq;x;L) ⟺ (x ∈ L)
. . | | . .      {assert_DASH_deq_DASH_member}
. . | | . .      0
. . | | . .      THEN
. . | | . .      RWO
. . | | . .      Thm* ∀eq:EqDecider(A), L:A List, x:A.
. . | | . .           deq-member(eq;x;L) ⟺ (x ∈ L)
. . | | . .      {assert_DASH_deq_DASH_member}
. . | | . .      -1
. . | | . .      THEN
. . | | . .      DVar `ds`
. . | | . .      THEN
. . | | . .      Reduce 0
```

```
. . | |
. . | .\
. . | . 1. i : Id
. . | . 2. a : Id
. . | . 3. T : Type
. . | . 4. ds : x:Id fp-> Type
. . | . 5. P : State(ds)→T→Prop
. . | . 6. w : World
. . | . 7. p : FairFifo
. . | . 8. FairFifo
. . | . 9. ∀l:IdLnk, tg:Id.
. . | . |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . | . |                    <ds,<[locl(a)],λx.T>,,<[a],λx.P>,,,,,•>
. . | . |                 else  fi.da(rcv(l; tg))
. . | . 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . | . 11. ∀a@0:Id, t:ℕ.
. . | . |   ∃t':ℕ.
. . | . |   t≤t'
. . | . |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . | . |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . | . |     ∨ P@0 != <[a],λx.P>(a@0) ==> ∀v:<[locl(a)]
. . | . |                                      ,λx.T>(locl(a@0))?Top.
. . | . |       ¬P@0((λx.s(i;t').x),v)
. . | . 12. ∀t:ℕ.
. . | . |   ¬isnull(a(i;t))
. . | . |   ⇒
. . | . |   (islocal(kind(a(i;t)))
. . | . |    ⇒
. . | . |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . | . |    ⇒
. . | . |    P((λx.s(i;t).x),val(a(i;t))))
. . | . |   & (∀x:Id.
. . | . |      deq-member(product-deq(Knd;Id;KindDeq;IdDeq);<kind(...)
. . | . |                                                  ,x>;1of())
. . | . |      ⇒
. . | . |      s(i;t+1).x
. . | . |      =
. . | . |      2of()(<kind(a(i;t)),x>,λx.s(i;t).x,val(a(i;t))))
. . | . |   & (∀l:IdLnk.
. . | . |      deq-member(product-deq(Knd;IdLnk;KindDeq;...);<...
. . | . |                                                   ,l>;1of(
. . | . |                                                       ))
. . | . |      ⇒
. . | . |      withlnk(l;m(i;t))
. . | . |      =
. . | . |      if source(l) = i→
. . | . |         concat(map(λtgf.map(λx.
. . | . |         <1of(tgf),x>;2of(tgf)
. . | . |                      ((λx.s(i;t).x)
. . | . |                      ,val(a(i;t))));2of()
. . | . |                                    (<kind(a(i;t)),l>)))
. . | . |      else nil fi)
. . | . |   & (∀x:Id.
. . | . |      ¬(deq-member(IdDeq;x;1of())
. . | . |        ⇒
```

```
. . | . |       deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . | . |     ⇒
. . | . |     s(i;t).x = s(i;t+1).x)
. . | . |   & (∀l:IdLnk, tg:Id.
. . | . |     ¬(deq-member(product-deq(IdLnk;Id;...;IdDeq);...;1of())
. . | . |       ⇒
. . | . |       deq-member(KindDeq;kind(a(i;t));2of()(<l,tg>)))
. . | . |     ⇒
. . | . |     w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . | . 13. ∀x:Id. deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . | . 14. ∀a@0:Action(i).
. . | . |   ¬isnull(a@0)
. . | . |   ⇒
. . | . |   (valtype(i;a@0) ⊆r <[locl(a)],λx.T>(kind(a@0))?Top)
. . | . 15. ∀x:Id.
. . | . |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→ 2of(ds)(x)
. . | . |                  else Top fi
. . | . 16. IdDeq ∈ EqDecider(Id)
. . | . ⊢  ∀e:E. loc(e) = i ⇒ kind(e) = locl(a) ⇒ (valtype(e) ⊆r T)
. . | . | by Auto
. . | . |
. . | . 1. i : Id
. . | . 2. a : Id
. . | . 3. T : Type
. . | . 4. ds : x:Id fp-> Type
. . | . 5. P : State(ds)→T→Prop
. . | . 6. w : World
. . | . 7. p : FairFifo
. . | . 8. FairFifo
. . | . 9. ∀l:IdLnk, tg:Id.
. . | . |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . | . |                   <ds,<[locl(a)],λx.T>,,<[a],λx.P>,,,,,•>
. . | . |                else  fi.da(rcv(l; tg))
. . | . 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . | . 11. ∀a@0:Id, t:ℕ.
. . | . |   ∃t':ℕ.
. . | . |   t≤t'
. . | . |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . | . |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . | . |     ∨ P@0 != <[a],λx.P>(a@0) ==> ∀v:<[locl(a)]
. . | . |                                    ,λx.T>(locl(a@0))?Top.
. . | . |       ¬P@0((λx.s(i;t').x),v)
. . | . 12. ∀t:ℕ.
. . | . |   ¬isnull(a(i;t))
. . | . |   ⇒
. . | . |   (islocal(kind(a(i;t)))
. . | . |    ⇒
. . | . |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . | . |    ⇒
. . | . |    P((λx.s(i;t).x),val(a(i;t))))
. . | . |   & (∀x:Id.
. . | . |     deq-member(product-deq(Knd;Id;KindDeq;IdDeq);<kind(...)
. . | . |                                                  ,x>;1of())
. . | . |     ⇒
. . | . |     s(i;t+1).x
```

```
. . | . |      =
. . | . |      2of()(<kind(a(i;t)),x>,λx.s(i;t).x,val(a(i;t))))
. . | . |   & (∀l:IdLnk.
. . | . |      deq-member(product-deq(Knd;IdLnk;KindDeq;...);<...
. . | . |                                                  ,l>;1of(
. . | . |                                                      ))
. . | . |      ⇒
. . | . |      withlnk(l;m(i;t))
. . | . |      =
. . | . |      if source(l) = i→
. . | . |         concat(map(λtgf.map(λx.
. . | . |         <1of(tgf),x>;2of(tgf)
. . | . |                      ((λx.s(i;t).x)
. . | . |                      ,val(a(i;t))));2of()
. . | . |                                   (<kind(a(i;t)),l>)))
. . | . |      else nil fi)
. . | . |   & (∀x:Id.
. . | . |      ¬(deq-member(IdDeq;x;1of())
. . | . |        ⇒
. . | . |        deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . | . |      ⇒
. . | . |      s(i;t).x = s(i;t+1).x)
. . | . |   & (∀l:IdLnk, tg:Id.
. . | . |      ¬(deq-member(product-deq(IdLnk;Id;...;IdDeq);...;1of())
. . | . |        ⇒
. . | . |        deq-member(KindDeq;kind(a(i;t));2of()(<l,tg>)))
. . | . |      ⇒
. . | . |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . | . 13. ∀x:Id. deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . | . 14. ∀a@0:Action(i).
. . | . |   ¬isnull(a@0)
. . | . |   ⇒
. . | . |   (valtype(i;a@0) ⊆r <[locl(a)],λx.T>(kind(a@0))?Top)
. . | . 15. ∀x:Id.
. . | . |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→ 2of(ds)(x)
. . | . |                   else Top fi
. . | . 16. IdDeq ∈ EqDecider(Id)
. . | . 17. e : E
. . | . 18. loc(e) = i
. . | . 19. kind(e) = locl(a)
. . | . ⊢  valtype(e) ⊆r T
. . | . | by DVar ‘e’ THEN DVar ‘e’ THEN RenameTo ‘j’ ‘e1’
. . | . |    THEN
. . | . |    RenameTo ‘t’ ‘e2’
. . | . |    THEN
. . | . |    All Reduce
. . | . |    THEN
. . | . |    Decide isnull(a(j;t))
. . | . |    THEN
. . | . |    Try (Assert False THEN Unhide THEN Complete Auto)
. . | . |
. . | . 1. i : Id
. . | . 2. a : Id
. . | . 3. T : Type
. . | . 4. ds : x:Id fp-> Type
```

```
. . | . 5. P : State(ds)→T→Prop
. . | . 6. w : World
. . | . 7. p : FairFifo
. . | . 8. FairFifo
. . | . 9. ∀l:IdLnk, tg:Id.
. . | . |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . | . |                    <ds,<[locl(a)],λx.T>,,<[a],λx.P>,,,,,•>
. . | . |                 else  fi.da(rcv(l; tg))
. . | . 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . | . 11. ∀a@0:Id, t:ℕ.
. . | . |   ∃t':ℕ.
. . | . |   t≤t'
. . | . |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . | . |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . | . |     ∨ P@0 != <[a],λx.P>(a@0) ==> ∀v:<[locl(a)]
. . | . |                                      ,λx.T>(locl(a@0))?Top.
. . | . |       ¬P@0((λx.s(i;t').x),v)
. . | . 12. ∀t:ℕ.
. . | . |   ¬isnull(a(i;t))
. . | . |   ⇒
. . | . |   (islocal(kind(a(i;t)))
. . | . |    ⇒
. . | . |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . | . |    ⇒
. . | . |    P((λx.s(i;t).x),val(a(i;t))))
. . | . |   & (∀x:Id.
. . | . |      deq-member(product-deq(Knd;Id;KindDeq;IdDeq);<kind(...)
. . | . |                                                  ,x>;1of())
. . | . |      ⇒
. . | . |      s(i;t+1).x
. . | . |      =
. . | . |      2of()(<kind(a(i;t)),x>,λx.s(i;t).x,val(a(i;t))))
. . | . |   & (∀l:IdLnk.
. . | . |      deq-member(product-deq(Knd;IdLnk;KindDeq;...);<...
. . | . |                                                   ,l>;1of(
. . | . |                                                       ))
. . | . |      ⇒
. . | . |      withlnk(l;m(i;t))
. . | . |      =
. . | . |      if source(l) = i→
. . | . |         concat(map(λtgf.map(λx.
. . | . |         <1of(tgf),x>;2of(tgf)
. . | . |                      ((λx.s(i;t).x)
. . | . |                      ,val(a(i;t))));2of()
. . | . |                                   (<kind(a(i;t)),l>)))
. . | . |      else nil fi)
. . | . |   & (∀x:Id.
. . | . |      ¬(deq-member(IdDeq;x;1of())
. . | . |        ⇒
. . | . |        deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . | . |      ⇒
. . | . |      s(i;t).x = s(i;t+1).x)
. . | . |   & (∀l:IdLnk, tg:Id.
. . | . |      ¬(deq-member(product-deq(IdLnk;Id;...;IdDeq);...;1of())
. . | . |        ⇒
```

```
. . | . |        deq-member(KindDeq;kind(a(i;t));2of()(<l,tg>)))
. . | . |      ⇒
. . | . |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . | . 13. ∀x:Id. deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . | . 14. ∀a@0:Action(i).
. . | . |   ¬isnull(a@0)
. . | . |   ⇒
. . | . |   (valtype(i;a@0) ⊆r <[locl(a)],λx.T>(kind(a@0))?Top)
. . | . 15. ∀x:Id.
. . | . |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→ 2of(ds)(x)
. . | . |                  else Top fi
. . | . 16. IdDeq ∈ EqDecider(Id)
. . | . 17. j : Id
. . | . 18. t : ℕ
. . | . 19. ¬isnull(a(j;t))  [not for witness]
. . | . 20. j = i
. . | . 21. kind(<j,t>) = locl(a)
. . | . 22. ¬isnull(a(j;t))
. . | . ⊢  valtype(<j,t>) ⊆r T
. . | . | by Repeat
. . | . |    (Unfolds
. . | . |     [‘es-kind‘
. . | . |     ;‘es-loc‘
. . | . |     ;‘es-act‘
. . | . |     ;‘es-isrcv‘
. . | . |     ;‘es-valtype‘
. . | . |     ;‘es-acttype‘]
. . | . |     0
. . | . |     THEN
. . | . |     Reduce 0)
. . | . |    THEN
. . | . |    StrongHypSubst -2 0
. . | . |
. . | . |\
. . | . | 1. i : Id
. . | . | 2. a : Id
. . | . | 3. T : Type
. . | . | 4. ds : x:Id fp-> Type
. . | . | 5. P : State(ds)→T→Prop
. . | . | 6. w : World
. . | . | 7. p : FairFifo
. . | . | 8. FairFifo
. . | . | 9. ∀l:IdLnk, tg:Id.
. . | . | |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . | . | |                   <ds,<[locl(a)],λx.T>,,<[a],λx.P>,,,,,•>
. . | . | |                else  fi.da(rcv(l; tg))
. . | . | 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . | . | 11. ∀a@0:Id, t:ℕ.
. . | . | |   ∃t':ℕ.
. . | . | |   t≤t'
. . | . | |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . | . | |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . | . | |     ∨ P@0 != <[a],λx.P>(a@0) ==> ∀v:<[locl(a)]
. . | . | |                                    ,λx.T>(locl(a@0))?Top.
. . | . | |       ¬P@0((λx.s(i;t').x),v)
```

```
. . | . | 12. ∀t:ℕ.
. . | . | |   ¬isnull(a(i;t))
. . | . | |   ⇒
. . | . | |   (islocal(kind(a(i;t)))
. . | . | |    ⇒
. . | . | |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . | . | |    ⇒
. . | . | |    P((λx.s(i;t).x),val(a(i;t))))
. . | . | |   & (∀x:Id.
. . | . | |      deq-member(product-deq(Knd;Id;KindDeq;IdDeq);<...
. . | . | |                                                  ,x>;1of(
. . | . | |                                                      ))
. . | . | |      ⇒
. . | . | |      s(i;t+1).x
. . | . | |      =
. . | . | |      2of()(<kind(a(i;t)),x>,λx.s(i;t).x,val(a(i;t))))
. . | . | |   & (∀l:IdLnk.
. . | . | |      deq-member(product-deq(Knd;IdLnk;...;...);<kind(...)
. . | . | |                                                ,l>;1of())
. . | . | |      ⇒
. . | . | |      withlnk(l;m(i;t))
. . | . | |      =
. . | . | |      if source(l) = i→
. . | . | |         concat(map(λtgf.map(λx.
. . | . | |         <1of(tgf),x>;2of(tgf)
. . | . | |                      ((λx.s(i;t).x)
. . | . | |                      ,val(a(i;t))));2of()
. . | . | |                                    (<kind(a(i;t)),l>)))
. . | . | |      else nil fi)
. . | . | |   & (∀x:Id.
. . | . | |      ¬(deq-member(IdDeq;x;1of())
. . | . | |        ⇒
. . | . | |        deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . | . | |      ⇒
. . | . | |      s(i;t).x = s(i;t+1).x)
. . | . | |   & (∀l:IdLnk, tg:Id.
. . | . | |      ¬(deq-member(product-deq(IdLnk;Id;...;IdDeq);...;1of(
. . | . | |                                                      ))
. . | . | |        ⇒
. . | . | |        deq-member(KindDeq;kind(a(i;t));2of()(<l,tg>)))
. . | . | |      ⇒
. . | . | |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . | . | 13. ∀x:Id. deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . | . | 14. ∀a@0:Action(i).
. . | . | |   ¬isnull(a@0)
. . | . | |   ⇒
. . | . | |   (valtype(i;a@0) ⊆r <[locl(a)],λx.T>(kind(a@0))?Top)
. . | . | 15. ∀x:Id.
. . | . | |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . | . | |                      2of(ds)(x)
. . | . | |                  else Top fi
. . | . | 16. IdDeq ∈ EqDecider(Id)
. . | . | 17. j : Id
. . | . | 18. t : ℕ
. . | . | 19. ¬isnull(a(j;t))  [not for witness]
```

```
. . | . | 20. j = i
. . | . | 21. kind(<j,t>) = locl(a)
. . | . | 22. ¬isnull(a(j;t))
. . | . | ⊢  if isrcv(locl(a))→ rcvtype(<j,t>)
. . | . | |  else V(j;locl(act(locl(a)))) fi ⊆r T
. . | . | | by Unfolds [‘isrcv‘;‘locl‘;‘actof‘] 0 THEN Reduce 0
. . | . | |    THEN
. . | . | |    Fold ‘locl‘ 0
. . | . | |
. . | . | 1. i : Id
. . | . | 2. a : Id
. . | . | 3. T : Type
. . | . | 4. ds : x:Id fp-> Type
. . | . | 5. P : State(ds)→T→Prop
. . | . | 6. w : World
. . | . | 7. FairFifo
. . | . | 8. FairFifo
. . | . | 9. ∀l:IdLnk, tg:Id.
. . | . | |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . | . | |                    <ds,<[locl(a)],λx.T>,,<[a],λx.P>,,,,,·>
. . | . | |                 else  fi.da(rcv(l; tg))
. . | . | 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . | . | 11. ∀a@0:Id, t:ℕ.
. . | . | |   ∃t':ℕ.
. . | . | |   t≤t'
. . | . | |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . | . | |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . | . | |     ∨ P@0 != <[a],λx.P>(a@0) ==> ∀v:<[locl(a)]
. . | . | |                                    ,λx.T>(locl(a@0))?Top.
. . | . | |       ¬P@0((λx.s(i;t').x),v)
. . | . | 12. ∀t:ℕ.
. . | . | |   ¬isnull(a(i;t))

. . | . | |   ⇒
. . | . | |   (islocal(kind(a(i;t)))
. . | . | |    ⇒
. . | . | |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . | . | |    ⇒
. . | . | |    P((λx.s(i;t).x),val(a(i;t))))
. . | . | |   & (∀x:Id.
. . | . | |      deq-member(product-deq(Knd;Id;KindDeq;IdDeq);<...
. . | . | |                                                ,x>;1of(
. . | . | |                                                    ))
. . | . | |      ⇒
. . | . | |      s(i;t+1).x
. . | . | |      =
. . | . | |      2of()(<kind(a(i;t)),x>,λx.s(i;t).x,val(a(i;t))))
. . | . | |   & (∀l:IdLnk.
. . | . | |      deq-member(product-deq(Knd;IdLnk;...;...);<kind(...)
. . | . | |                                              ,l>;1of())
. . | . | |      ⇒
. . | . | |      withlnk(l;m(i;t))
. . | . | |      =
. . | . | |      if source(l) = i→
. . | . | |         concat(map(λtgf.map(λx.
. . | . | |         <1of(tgf),x>;2of(tgf)
```

```
. . | . | |                      ((λx.s(i;t).x)
. . | . | |                      ,val(a(i;t))));2of()
. . | . | |                                    (<kind(a(i;t)),l>)))
. . | . | |      else nil fi)
. . | . | |   & (∀x:Id.
. . | . | |      ¬(deq-member(IdDeq;x;1of())
. . | . | |        ⇒
. . | . | |        deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . | . | |      ⇒
. . | . | |      s(i;t).x = s(i;t+1).x)
. . | . | |   & (∀l:IdLnk, tg:Id.
. . | . | |      ¬(deq-member(product-deq(IdLnk;Id;...;IdDeq);...;1of(
. . | . | |                                                      ))
. . | . | |        ⇒
. . | . | |        deq-member(KindDeq;kind(a(i;t));2of()(<l,tg>)))
. . | . | |      ⇒
. . | . | |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . | . | 13. ∀x:Id. deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . | . | 14. ∀a@0:Action(i).
. . | . | |   ¬isnull(a@0)
. . | . | |   ⇒
. . | . | |   (valtype(i;a@0) ⊆r <[locl(a)],λx.T>(kind(a@0))?Top)
. . | . | 15. ∀x:Id.
. . | . | |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . | . | |                     2of(ds)(x)
. . | . | |                  else Top fi
. . | . | 16. IdDeq ∈ EqDecider(Id)
. . | . | 17. j : Id
. . | . | 18. t : ℕ
. . | . | 19. ¬isnull(a(j;t))  [not for witness]
. . | . | 20. j = i
. . | . | 21. kind(<j,t>) = locl(a)
. . | . | 22. ¬isnull(a(j;t))
. . | . | ⊢  V(j;locl(a)) ⊆r T
. . | . | | by AssertBY (Action(j) = Action(i)) (Subst (j = i) 0)
. . | . | |    THEN
. . | . | |    AllHyps (λh.InstHyp [a(j;t)] h THENA Complete Auto)
. . | . | |
. . | . | 1. i : Id
. . | . | 2. a : Id
. . | . | 3. T : Type
. . | . | 4. ds : x:Id fp-> Type
. . | . | 5. P : State(ds)→T→Prop
. . | . | 6. w : World
. . | . | 7. FairFifo
. . | . | 8. FairFifo
. . | . | 9. ∀l:IdLnk, tg:Id.
. . | . | |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . | . | |                    <ds,<[locl(a)],λx.T>,,<[a],λx.P>,,,,,•>
. . | . | |                 else  fi.da(rcv(l; tg))
. . | . | 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . | . | 11. ∀a@0:Id, t:ℕ.
. . | . | |   ∃t':ℕ.
. . | . | |   t≤t'
. . | . | |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
```

```
. . | . | |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . | . | |     ∨ P@0 != <[a],λx.P>(a@0) ==> ∀v:<[locl(a)]
. . | . | |                                    ,λx.T>(locl(a@0))?Top.
. . | . | |       ¬P@0((λx.s(i;t').x),v)
. . | . | 12. ∀t:ℕ.
. . | . | |   ¬isnull(a(i;t))
. . | . | |   ⇒
. . | . | |   (islocal(kind(a(i;t)))
. . | . | |    ⇒
. . | . | |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . | . | |    ⇒
. . | . | |    P((λx.s(i;t).x),val(a(i;t))))
. . | . | |   & (∀x:Id.
. . | . | |      deq-member(product-deq(Knd;Id;KindDeq;IdDeq);<...
. . | . | |                                                  ,x>;1of(
. . | . | |                                                      ))
. . | . | |      ⇒
. . | . | |      s(i;t+1).x
. . | . | |      =
. . | . | |      2of()(<kind(a(i;t)),x>,λx.s(i;t).x,val(a(i;t))))
. . | . | |   & (∀l:IdLnk.
. . | . | |      deq-member(product-deq(Knd;IdLnk;...;...);<kind(...)
. . | . | |                                                 ,l>;1of())
. . | . | |      ⇒
. . | . | |      withlnk(l;m(i;t))
. . | . | |      =
. . | . | |      if source(l) = i→
. . | . | |         concat(map(λtgf.map(λx.
. . | . | |         <1of(tgf),x>;2of(tgf)
. . | . | |                      ((λx.s(i;t).x)
. . | . | |                      ,val(a(i;t))));2of()
. . | . | |                                    (<kind(a(i;t)),l>)))
. . | . | |      else nil fi)
. . | . | |   & (∀x:Id.
. . | . | |      ¬(deq-member(IdDeq;x;1of())
. . | . | |        ⇒
. . | . | |        deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . | . | |      ⇒
. . | . | |      s(i;t).x = s(i;t+1).x)
. . | . | |   & (∀l:IdLnk, tg:Id.
. . | . | |      ¬(deq-member(product-deq(IdLnk;Id;...;IdDeq);...;1of(
. . | . | |                                                      ))
. . | . | |        ⇒
. . | . | |        deq-member(KindDeq;kind(a(i;t));2of()(<l,tg>)))
. . | . | |      ⇒
. . | . | |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . | . | 13. ∀x:Id. deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . | . | 14. ∀a@0:Action(i).
. . | . | |   ¬isnull(a@0)
. . | . | |   ⇒
. . | . | |   (valtype(i;a@0) ⊆r <[locl(a)],λx.T>(kind(a@0))?Top)
. . | . | 15. ∀x:Id.
. . | . | |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . | . | |                      2of(ds)(x)
. . | . | |                  else Top fi
```

```
. . | . | 16. IdDeq ∈ EqDecider(Id)
. . | . | 17. j : Id
. . | . | 18. t : ℕ
. . | . | 19. ¬isnull(a(j;t))  [not for witness]
. . | . | 20. j = i
. . | . | 21. kind(<j,t>) = locl(a)
. . | . | 22. ¬isnull(a(j;t))
. . | . | 23. Action(j) = Action(i)
. . | . | 24. valtype(i;a(j;t)) ⊆r <[locl(a)],λx.T>(kind(a(j;t)))?Top
. . | . | ⊢  V(j;locl(a)) ⊆r T
. . | . | | by Repeat (Unfolds [‘w-act‘;‘w-ekind‘] -4 THEN Reduce -4)
. . | . | |
. . | . | 1. i : Id
. . | . | 2. a : Id
. . | . | 3. T : Type
. . | . | 4. ds : x:Id fp-> Type
. . | . | 5. P : State(ds)→T→Prop
. . | . | 6. w : World
. . | . | 7. FairFifo
. . | . | 8. FairFifo
. . | . | 9. ∀l:IdLnk, tg:Id.
. . | . | |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . | . | |                    <ds,<[locl(a)],λx.T>,,<[a],λx.P>,,,,,•>
. . | . | |                else  fi.da(rcv(l; tg))
. . | . | 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . | . | 11. ∀a@0:Id, t:ℕ.
. . | . | |   ∃t':ℕ.
. . | . | |   t≤t'
. . | . | |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . | . | |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . | . | |     ∨ P@0 != <[a],λx.P>(a@0) ==> ∀v:<[locl(a)]
. . | . | |                                    ,λx.T>(locl(a@0))?Top.
. . | . | |       ¬P@0((λx.s(i;t').x),v)
. . | . | 12. ∀t:ℕ.
. . | . | |   ¬isnull(a(i;t))
. . | . | |   ⇒
. . | . | |   (islocal(kind(a(i;t)))
. . | . | |    ⇒
. . | . | |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . | . | |    ⇒
. . | . | |    P((λx.s(i;t).x),val(a(i;t))))
. . | . | |   & (∀x:Id.
. . | . | |      deq-member(product-deq(Knd;Id;KindDeq;IdDeq);<...
. . | . | |                                                  ,x>;1of(
. . | . | |                                                      ))
. . | . | |      ⇒
. . | . | |      s(i;t+1).x
. . | . | |      =
. . | . | |      2of()(<kind(a(i;t)),x>,λx.s(i;t).x,val(a(i;t))))
. . | . | |   & (∀l:IdLnk.
. . | . | |      deq-member(product-deq(Knd;IdLnk;...;...);<kind(...)
. . | . | |                                               ,l>;1of())
. . | . | |      ⇒
. . | . | |      withlnk(l;m(i;t))
. . | . | |      =
```

```
. . | . | |      if source(l) = i→
. . | . | |         concat(map(λtgf.map(λx.
. . | . | |         <1of(tgf),x>;2of(tgf)
. . | . | |                      ((λx.s(i;t).x)
. . | . | |                      ,val(a(i;t))));2of()
. . | . | |                                    (<kind(a(i;t)),l>)))
. . | . | |      else nil fi)
. . | . | |   & (∀x:Id.
. . | . | |      ¬(deq-member(IdDeq;x;1of())
. . | . | |        ⇒
. . | . | |        deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . | . | |      ⇒
. . | . | |      s(i;t).x = s(i;t+1).x)
. . | . | |   & (∀l:IdLnk, tg:Id.
. . | . | |      ¬(deq-member(product-deq(IdLnk;Id;...;IdDeq);...;1of(
. . | . | |                                                       ))
. . | . | |        ⇒
. . | . | |        deq-member(KindDeq;kind(a(i;t));2of()(<l,tg>)))
. . | . | |      ⇒
. . | . | |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . | . | 13. ∀x:Id. deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . | . | 14. ∀a@0:Action(i).
. . | . | |   ¬isnull(a@0)
. . | . | |   ⇒
. . | . | |   (valtype(i;a@0) ⊆r <[locl(a)],λx.T>(kind(a@0))?Top)
. . | . | 15. ∀x:Id.
. . | . | |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . | . | |                      2of(ds)(x)
. . | . | |                   else Top fi
. . | . | 16. IdDeq ∈ EqDecider(Id)
. . | . | 17. j : Id
. . | . | 18. t : ℕ
. . | . | 19. ¬isnull(a(j;t))  [not for witness]
. . | . | 20. j = i
. . | . | 21. kind(a(j;t)) = locl(a)
. . | . | 22. ¬isnull(a(j;t))
. . | . | 23. Action(j) = Action(i)
. . | . | 24. valtype(i;a(j;t)) ⊆r <[locl(a)],λx.T>(kind(a(j;t)))?Top
. . | . | ⊢  V(j;locl(a)) ⊆r T  by HypSubst -4 -1
. . | . | |
. . | . | |\
. . | . | | .....wf .....
. . | . | | 1. i : Id
. . | . | | 2. a : Id
. . | . | | 3. T : Type
. . | . | | 4. ds : x:Id fp-> Type
. . | . | | 5. P : State(ds)→T→Prop
. . | . | | 6. w : World
. . | . | | 7. FairFifo
. . | . | | 8. FairFifo
. . | . | | 9. ∀l:IdLnk, tg:Id.
. . | . | | |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . | . | | |                    <ds
. . | . | | |                    ,<[locl(a)],λx.T>
. . | . | | |                    ,
```

```
. . | . | | |                    ,<[a],λx.P>
. . | . | | |                    ,
. . | . | | |                    ,
. . | . | | |                    ,
. . | . | | |                    ,
. . | . | | |                    ,.>
. . | . | | |                 else  fi.da(rcv(l; tg))
. . | . | | 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . | . | | 11. ∀a@0:Id, t:ℕ.
. . | . | | |   ∃t':ℕ.
. . | . | | |   t≤t'
. . | . | | |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . | . | | |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . | . | | |     ∨ P@0 != <[a],λx.P>(a@0) ==> ∀v:<[locl(a)]
. . | . | | |                                    ,λx.
. . | . | | |                                     T>(locl(a@0))?Top.
. . | . | | |       ¬P@0((λx.s(i;t').x),v)
. . | . | | 12. ∀t:ℕ.
. . | . | | |   ¬isnull(a(i;t))
. . | . | | |   ⇒
. . | . | | |   (islocal(kind(a(i;t)))
. . | . | | |    ⇒
. . | . | | |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . | . | | |    ⇒
. . | . | | |    P((λx.s(i;t).x),val(a(i;t))))
. . | . | | |   & (∀x:Id.
. . | . | | |      deq-member(product-deq(Knd;Id;KindDeq;...);<...
. . | . | | |                                                ,x>;1of(
. . | . | | |                                                    ))
. . | . | | |      ⇒
. . | . | | |      s(i;t+1).x
. . | . | | |      =
. . | . | | |      2of()(<kind(a(i;t)),x>,λx.s(i;t).x,val(a(i;t))))
. . | . | | |   & (∀l:IdLnk.
. . | . | | |      deq-member(product-deq(Knd;IdLnk;...;...);<...
. . | . | | |                                               ,l>;1of(
. . | . | | |                                                   ))
. . | . | | |      ⇒
. . | . | | |      withlnk(l;m(i;t))
. . | . | | |      =
. . | . | | |      if source(l) = i→
. . | . | | |         concat(map(λtgf.map(λx.
. . | . | | |         <1of(tgf),x>;2of(tgf)
. . | . | | |                     ((λx.s(i;t).x)
. . | . | | |                     ,val(a(i;t))));2of()
. . | . | | |                                    (<kind(a(i;t)),l>)))
. . | . | | |      else nil fi)
. . | . | | |   & (∀x:Id.
. . | . | | |      ¬(deq-member(IdDeq;x;1of())
. . | . | | |        ⇒
. . | . | | |        deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . | . | | |      ⇒
. . | . | | |      s(i;t).x = s(i;t+1).x)
. . | . | | |   & (∀l:IdLnk, tg:Id.
. . | . | | |      ¬(deq-member(product-deq(IdLnk;Id;...;...);...;1of(
```

```
. . | . | | |                                                    ))
. . | . | | |        ⇒
. . | . | | |        deq-member(KindDeq;kind(a(i;t));2of()(<l,tg>)))
. . | . | | |      ⇒
. . | . | | |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . | . | | 13. ∀x:Id.
. . | . | | |   deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . | . | | 14. ∀a@0:Action(i).
. . | . | | |   ¬isnull(a@0)
. . | . | | |   ⇒
. . | . | | |   (valtype(i;a@0) ⊆r <[locl(a)],λx.T>(kind(a@0))?Top)
. . | . | | 15. ∀x:Id.
. . | . | | |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . | . | | |                      2of(ds)(x)
. . | . | | |                   else Top fi
. . | . | | 16. IdDeq ∈ EqDecider(Id)
. . | . | | 17. j : Id
. . | . | | 18. t : ℕ
. . | . | | 19. ¬isnull(a(j;t))
. . | . | | 20. j = i
. . | . | | 21. kind(a(j;t)) = locl(a)
. . | . | | 22. ¬isnull(a(j;t))
. . | . | | 23. Action(j) = Action(i)
. . | . | | 24. valtype(i;a(j;t)) ⊆r <[locl(a)]
. . | . | | |                        ,λx.T>(kind(a(j;t)))?Top
. . | . | | 25. z : Knd
. . | . | | ⊢  (valtype(i;a(j;t)) ⊆r <[locl(a)],λx.T>(z)?Top) ∈ Type
. . | . | | | by Auto
. . | . | | |
. . | . | | 1. i : Id
. . | . | | 2. a : Id
. . | . | | 3. T : Type
. . | . | | 4. ds : x:Id fp-> Type
. . | . | | 5. P : State(ds)→T→Prop
. . | . | | 6. w : World
. . | . | | 7. FairFifo
. . | . | | 8. FairFifo
. . | . | | 9. ∀l:IdLnk, tg:Id.
. . | . | | |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . | . | | |                    <ds
. . | . | | |                    ,<[locl(a)],λx.T>
. . | . | | |                    ,
. . | . | | |                    ,<[a],λx.P>
. . | . | | |                    ,
. . | . | | |                    ,
. . | . | | |                    ,
. . | . | | |                    ,
. . | . | | |                    ,.>
. . | . | | |                 else  fi.da(rcv(l; tg))
. . | . | | 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . | . | | 11. ∀a@0:Id, t:ℕ.
. . | . | | |   ∃t':ℕ.
. . | . | | |   t≤t'
. . | . | | |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . | . | | |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
```

```
. . | . | | |     ∨ P@0 != <[a],λx.P>(a@0) ==> ∀v:<[locl(a)]
. . | . | | |                                  ,λx.
. . | . | | |                                   T>(locl(a@0))?Top.
. . | . | | |       ¬P@0((λx.s(i;t').x),v)
. . | . | | 12. ∀t:ℕ.
. . | . | | |   ¬isnull(a(i;t))
. . | . | | |   ⇒
. . | . | | |   (islocal(kind(a(i;t)))
. . | . | | |    ⇒
. . | . | | |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . | . | | |    ⇒
. . | . | | |    P((λx.s(i;t).x),val(a(i;t))))
. . | . | | |   & (∀x:Id.
. . | . | | |      deq-member(product-deq(Knd;Id;KindDeq;...);<...
. . | . | | |                                                 ,x>;1of(
. . | . | | |                                                     ))
. . | . | | |      ⇒
. . | . | | |      s(i;t+1).x
. . | . | | |      =
. . | . | | |      2of()(<kind(a(i;t)),x>,λx.s(i;t).x,val(a(i;t))))
. . | . | | |   & (∀l:IdLnk.
. . | . | | |      deq-member(product-deq(Knd;IdLnk;...;...);<...
. . | . | | |                                               ,l>;1of(
. . | . | | |                                                   ))
. . | . | | |      ⇒
. . | . | | |      withlnk(l;m(i;t))
. . | . | | |      =
. . | . | | |      if source(l) = i→
. . | . | | |         concat(map(λtgf.map(λx.
. . | . | | |         <1of(tgf),x>;2of(tgf)
. . | . | | |                     ((λx.s(i;t).x)
. . | . | | |                     ,val(a(i;t))));2of()
. . | . | | |                                    (<kind(a(i;t)),l>)))
. . | . | | |      else nil fi)
. . | . | | |   & (∀x:Id.
. . | . | | |      ¬(deq-member(IdDeq;x;1of())
. . | . | | |        ⇒
. . | . | | |        deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . | . | | |      ⇒
. . | . | | |      s(i;t).x = s(i;t+1).x)
. . | . | | |   & (∀l:IdLnk, tg:Id.
. . | . | | |      ¬(deq-member(product-deq(IdLnk;Id;...;...);...;1of(
. . | . | | |                                                   ))
. . | . | | |        ⇒
. . | . | | |        deq-member(KindDeq;kind(a(i;t));2of()(<l,tg>)))
. . | . | | |      ⇒
. . | . | | |      w-tagged(tg; onlnk(l;m(i;t))) = nil)

. . | . | | 13. ∀x:Id.
. . | . | | |   deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . | . | | 14. ∀a@0:Action(i).
. . | . | | |   ¬isnull(a@0)
. . | . | | |   ⇒
. . | . | | |   (valtype(i;a@0) ⊆r <[locl(a)],λx.T>(kind(a@0))?Top)
. . | . | | 15. ∀x:Id.
. . | . | | |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
```

```
. . | . | | |                      2of(ds)(x)
. . | . | | |                   else Top fi
. . | . | | 16. IdDeq ∈ EqDecider(Id)
. . | . | | 17. j : Id
. . | . | | 18. t : ℕ
. . | . | | 19. ¬isnull(a(j;t))
. . | . | | 20. j = i
. . | . | | 21. kind(a(j;t)) = locl(a)
. . | . | | 22. ¬isnull(a(j;t))
. . | . | | 23. Action(j) = Action(i)
. . | . | | 24. valtype(i;a(j;t)) ⊆r <[locl(a)]
. . | . | | |                        ,λx.T>(kind(a(j;t)))?Top
. . | . | | 25. z : Knd
. . | . | | ⊢  <[locl(a)],λx.T>(z)?Top ∈ Type
. . | . | | | by GenConcl (<[locl(a)],λx.T> = f)
. . | . | | |
. . | . | | .....wf .....
. . | . | | 1. i : Id
. . | . | | 2. a : Id
. . | . | | 3. T : Type
. . | . | | 4. ds : x:Id fp-> Type
. . | . | | 5. P : State(ds)→T→Prop
. . | . | | 6. w : World
. . | . | | 7. FairFifo
. . | . | | 8. FairFifo
. . | . | | 9. ∀l:IdLnk, tg:Id.
. . | . | |    (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . | . | |                      <ds
. . | . | |                      ,<[locl(a)],λx.T>
. . | . | |                      ,
. . | . | |                      ,<[a],λx.P>
. . | . | |                      ,
. . | . | |                      ,
. . | . | |                      ,
. . | . | |                      ,
. . | . | |                      ,•>
. . | . | |                  else  fi.da(rcv(l; tg))
. . | . | | 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . | . | | 11. ∀a@0:Id, t:ℕ.
. . | . | |     ∃t':ℕ.
. . | . | |     t≤t'
. . | . | |     & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . | . | |       ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . | . | |       ∨ P@0 != <[a],λx.P>(a@0) ==> ∀v:<[locl(a)]
. . | . | |                                      ,λx.
. . | . | |                                       T>(locl(a@0))?Top.
. . | . | |         ¬P@0((λx.s(i;t').x),v)
. . | . | | 12. ∀t:ℕ.
. . | . | |     ¬isnull(a(i;t))
. . | . | |     ⇒
. . | . | |     (islocal(kind(a(i;t)))
. . | . | |      ⇒
. . | . | |      (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . | . | |      ⇒
. . | . | |      P((λx.s(i;t).x),val(a(i;t))))
```

```
. . | . | |     & (∀x:Id.
. . | . | |        deq-member(product-deq(Knd;Id;KindDeq;...);<...
. . | . | |                                                  ,x>;1of(
. . | . | |                                                      ))
. . | . | |        ⇒
. . | . | |        s(i;t+1).x
. . | . | |        =
. . | . | |        2of()(<kind(a(i;t)),x>,λx.s(i;t).x,val(a(i;t))))
. . | . | |     & (∀l:IdLnk.
. . | . | |        deq-member(product-deq(Knd;IdLnk;...;...);<...
. . | . | |                                                ,l>;1of(
. . | . | |                                                    ))
. . | . | |        ⇒
. . | . | |        withlnk(l;m(i;t))
. . | . | |        =
. . | . | |        if source(l) = i→
. . | . | |           concat(map(λtgf.map(λx.
. . | . | |           <1of(tgf),x>;2of(tgf)
. . | . | |                       ((λx.s(i;t).x)
. . | . | |                       ,val(a(i;t))));2of()
. . | . | |                                    (<kind(a(i;t)),l>)))
. . | . | |        else nil fi)
. . | . | |     & (∀x:Id.
. . | . | |        ¬(deq-member(IdDeq;x;1of())
. . | . | |          ⇒
. . | . | |          deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . | . | |        ⇒
. . | . | |        s(i;t).x = s(i;t+1).x)
. . | . | |     & (∀l:IdLnk, tg:Id.
. . | . | |        ¬(deq-member(product-deq(IdLnk;Id;...;...);...;1of(
. . | . | |                                                      ))
. . | . | |          ⇒
. . | . | |          deq-member(KindDeq;kind(a(i;t));2of()(<l,tg>)))
. . | . | |        ⇒
. . | . | |        w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . | . | | 13. ∀x:Id.
. . | . | |     deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . | . | | 14. ∀a@0:Action(i).
. . | . | |     ¬isnull(a@0)
. . | . | |     ⇒
. . | . | |     (valtype(i;a@0) ⊆r <[locl(a)],λx.T>(kind(a@0))?Top)
. . | . | | 15. ∀x:Id.
. . | . | |     vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . | . | |                        2of(ds)(x)
. . | . | |                     else Top fi
. . | . | | 16. IdDeq ∈ EqDecider(Id)
. . | . | | 17. j : Id
. . | . | | 18. t : ℕ
. . | . | | 19. ¬isnull(a(j;t))
. . | . | | 20. j = i
. . | . | | 21. kind(a(j;t)) = locl(a)
. . | . | | 22. ¬isnull(a(j;t))
. . | . | | 23. Action(j) = Action(i)
. . | . | | 24. valtype(i;a(j;t)) ⊆r <[locl(a)]
. . | . | |                          ,λx.T>(kind(a(j;t)))?Top
```

```
. . | . | | 25. Knd
. . | . | | ⊢  <[locl(a)],λx.T> ∈ a:Knd fp-> Type
. . | . | |   by Fold ‘fpf-single‘ 0
. . | . | |
. . | . | .\
. . | . | . 1. i : Id
. . | . | . 2. a : Id
. . | . | . 3. T : Type
. . | . | . 4. ds : x:Id fp-> Type
. . | . | . 5. P : State(ds)→T→Prop
. . | . | . 6. w : World
. . | . | . 7. FairFifo
. . | . | . 8. FairFifo
. . | . | . 9. ∀l:IdLnk, tg:Id.
. . | . | . |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . | . | . |                    <ds
. . | . | . |                    ,<[locl(a)],λx.T>
. . | . | . |                    ,
. . | . | . |                    ,<[a],λx.P>
. . | . | . |                    ,
. . | . | . |                    ,
. . | . | . |                    ,
. . | . | . |                    ,
. . | . | . |                    ,.>
. . | . | . |                else  fi.da(rcv(l; tg))
. . | . | . 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . | . | . 11. ∀a@0:Id, t:ℕ.
. . | . | . |   ∃t':ℕ.
. . | . | . |   t≤t'
. . | . | . |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . | . | . |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . | . | . |     ∨ P@0 != <[a],λx.P>(a@0) ==> ∀v:<[locl(a)]
. . | . | . |                                    ,λx.
. . | . | . |                                     T>(locl(a@0))?Top.
. . | . | . |       ¬P@0((λx.s(i;t').x),v)
. . | . | . 12. ∀t:ℕ.
. . | . | . |   ¬isnull(a(i;t))
. . | . | . |   ⇒
. . | . | . |   (islocal(kind(a(i;t)))
. . | . | . |    ⇒
. . | . | . |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . | . | . |    ⇒
. . | . | . |    P((λx.s(i;t).x),val(a(i;t))))
. . | . | . |   & (∀x:Id.
. . | . | . |      deq-member(product-deq(Knd;Id;KindDeq;...);<...
. . | . | . |                                                ,x>;1of(
. . | . | . |                                                    ))
. . | . | . |      ⇒
. . | . | . |      s(i;t+1).x
. . | . | . |      =
. . | . | . |      2of()(<kind(a(i;t)),x>,λx.s(i;t).x,val(a(i;t))))
. . | . | . |   & (∀l:IdLnk.
. . | . | . |      deq-member(product-deq(Knd;IdLnk;...;...);<...
. . | . | . |                                              ,l>;1of(
. . | . | . |                                                  ))
```

```
. . | . | . |      ⇒
. . | . | . |      withlnk(l;m(i;t))
. . | . | . |      =
. . | . | . |      if source(l) = i→
. . | . | . |         concat(map(λtgf.map(λx.
. . | . | . |         <1of(tgf),x>;2of(tgf)
. . | . | . |                      ((λx.s(i;t).x)
. . | . | . |                      ,val(a(i;t))));2of()
. . | . | . |                                    (<kind(a(i;t)),l>)))
. . | . | . |      else nil fi)
. . | . | . |   & (∀x:Id.
. . | . | . |      ¬(deq-member(IdDeq;x;1of())
. . | . | . |        ⇒
. . | . | . |        deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . | . | . |      ⇒
. . | . | . |      s(i;t).x = s(i;t+1).x)
. . | . | . |   & (∀l:IdLnk, tg:Id.
. . | . | . |      ¬(deq-member(product-deq(IdLnk;Id;...;...);...;1of(
. . | . | . |                                                    ))
. . | . | . |        ⇒
. . | . | . |        deq-member(KindDeq;kind(a(i;t));2of()(<l,tg>)))
. . | . | . |      ⇒
. . | . | . |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . | . | . 13. ∀x:Id.
. . | . | . |   deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . | . | . 14. ∀a@0:Action(i).
. . | . | . |   ¬isnull(a@0)
. . | . | . |   ⇒
. . | . | . |   (valtype(i;a@0) ⊆r <[locl(a)],λx.T>(kind(a@0))?Top)
. . | . | . 15. ∀x:Id.
. . | . | . |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . | . | . |                     2of(ds)(x)
. . | . | . |                  else Top fi
. . | . | . 16. IdDeq ∈ EqDecider(Id)
. . | . | . 17. j : Id
. . | . | . 18. t : ℕ
. . | . | . 19. ¬isnull(a(j;t))  [not for witness]
. . | . | . 20. j = i
. . | . | . 21. kind(a(j;t)) = locl(a)
. . | . | . 22. ¬isnull(a(j;t))
. . | . | . 23. Action(j) = Action(i)
. . | . | . 24. valtype(i;a(j;t)) ⊆r <[locl(a)],λx.T>(locl(a))?Top
. . | . | . ⊢  V(j;locl(a)) ⊆r T
. . | . | . | by ((Repeat
. . | . | . |      (Unfolds
. . | . | . |       [‘fpf-single‘;‘fpf-cap‘;‘fpf-ap‘;‘fpf-dom‘]
. . | . | . |       -1
. . | . | . |       THEN
. . | . | . |       Reduce -1)
. . | . | . |      THEN
. . | . | . |      RWO
. . | . | . |      Thm* ∀d:EqDecider(A), i:A. (eqof(d)(i,i)) ∼ true₂
. . | . | . |      {eqof_eq_btrue}
. . | . | . |      -1)
. . | . | . |     THEN
```

```
. . | . | . |     (Reduce -1))
. . | . | . |    THEN
. . | . | . |    Subst (valtype(i;a(j;t)) = V(j;locl(a))) -1
. . | . | . |
. . | . | . .....equality .....
. . | . | . 1. i : Id
. . | . | . 2. a : Id
. . | . | . 3. T : Type
. . | . | . 4. ds : x:Id fp-> Type
. . | . | . 5. P : State(ds)→T→Prop
. . | . | . 6. w : World
. . | . | . 7. FairFifo
. . | . | . 8. FairFifo
. . | . | . 9. ∀l:IdLnk, tg:Id.
. . | . | .    (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . | . | .                      <ds
. . | . | .                      ,<[locl(a)],λx.T>
. . | . | .                      ,
. . | . | .                      ,<[a],λx.P>
. . | . | .                      ,
. . | . | .                      ,
. . | . | .                      ,
. . | . | .                      ,
. . | . | .                      ,.>
. . | . | .                  else  fi.da(rcv(l; tg))
. . | . | . 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . | . | . 11. ∀a@0:Id, t:ℕ.
. . | . | .     ∃t':ℕ.
. . | . | .     t≤t'
. . | . | .     & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . | . | .       ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . | . | .       ∨ P@0 != <[a],λx.P>(a@0) ==> ∀v:<[locl(a)]
. . | . | .                                    ,λx.
. . | . | .                                     T>(locl(a@0))?Top.
. . | . | .         ¬P@0((λx.s(i;t').x),v)
. . | . | . 12. ∀t:ℕ.
. . | . | .     ¬isnull(a(i;t))
. . | . | .     ⇒
. . | . | .     (islocal(kind(a(i;t)))
. . | . | .      ⇒
. . | . | .      (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . | . | .      ⇒
. . | . | .      P((λx.s(i;t).x),val(a(i;t))))
. . | . | .     & (∀x:Id.
. . | . | .        deq-member(product-deq(Knd;Id;KindDeq;...);<...
. . | . | .                                                  ,x>;1of(
. . | . | .                                                      ))
. . | . | .        ⇒
. . | . | .        s(i;t+1).x
. . | . | .        =
. . | . | .        2of()(<kind(a(i;t)),x>,λx.s(i;t).x,val(a(i;t))))
. . | . | .     & (∀l:IdLnk.
. . | . | .        deq-member(product-deq(Knd;IdLnk;...;...);<...
. . | . | .                                                ,l>;1of(
. . | . | .                                                    ))
```

```
. . | . | .        ⇒
. . | . | .        withlnk(l;m(i;t))
. . | . | .        =
. . | . | .        if source(l) = i→
. . | . | .           concat(map(λtgf.map(λx.
. . | . | .           <1of(tgf),x>;2of(tgf)
. . | . | .                        ((λx.s(i;t).x)
. . | . | .                        ,val(a(i;t))));2of()
. . | . | .                                     (<kind(a(i;t)),l>)))
. . | . | .        else nil fi)
. . | . | .     & (∀x:Id.
. . | . | .        ¬(deq-member(IdDeq;x;1of())
. . | . | .          ⇒
. . | . | .          deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . | . | .        ⇒
. . | . | .        s(i;t).x = s(i;t+1).x)
. . | . | .     & (∀l:IdLnk, tg:Id.

. . | . | .        ¬(deq-member(product-deq(IdLnk;Id;...;...);...;1of(
. . | . | .                                                      ))
. . | . | .          ⇒
. . | . | .          deq-member(KindDeq;kind(a(i;t));2of()(<l,tg>)))
. . | . | .        ⇒
. . | . | .        w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . | . | . 13. ∀x:Id.
. . | . | .     deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . | . | . 14. ∀a@0:Action(i).
. . | . | .     ¬isnull(a@0)
. . | . | .     ⇒
. . | . | .     (valtype(i;a@0) ⊆r <[locl(a)],λx.T>(kind(a@0))?Top)
. . | . | . 15. ∀x:Id.
. . | . | .     vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . | . | .                         2of(ds)(x)
. . | . | .                    else Top fi
. . | . | . 16. IdDeq ∈ EqDecider(Id)
. . | . | . 17. j : Id
. . | . | . 18. t : ℕ
. . | . | . 19. ¬isnull(a(j;t))
. . | . | . 20. j = i
. . | . | . 21. kind(a(j;t)) = locl(a)
. . | . | . 22. ¬isnull(a(j;t))
. . | . | . 23. Action(j) = Action(i)
. . | . | . 24. valtype(i;a(j;t)) ⊆r T
. . | . | . ⊢  valtype(i;a(j;t)) = V(j;locl(a))
. . | . | .   by Unfolds [‘w-V‘;‘w-valtype‘] 0 THEN Analyze
. . | . | .      THEN
. . | . | .      Try (Fold ‘w-M‘ 0)
. . | . | .      THEN
. . | . | .      Try (Fold ‘w-TA‘ 0)
. . | . | .      THEN
. . | . | .      Repeat Analyze
. . | . |
. . | . .\
. . | . . 1. i : Id
. . | . . 2. a : Id
. . | . . 3. T : Type
```

```
. . | . . 4. ds : x:Id fp-> Type
. . | . . 5. P : State(ds)→T→Prop
. . | . . 6. w : World
. . | . . 7. p : FairFifo
. . | . . 8. FairFifo
. . | . . 9. ∀l:IdLnk, tg:Id.
. . | . . |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . | . . |                    <ds,<[locl(a)],λx.T>,,<[a],λx.P>,,,,,•>
. . | . . |                 else  fi.da(rcv(l; tg))
. . | . . 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . | . . 11. ∀a@0:Id, t:ℕ.
. . | . . |   ∃t':ℕ.
. . | . . |   t≤t'
. . | . . |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . | . . |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . | . . |     ∨ P@0 != <[a],λx.P>(a@0) ==> ∀v:<[locl(a)]
. . | . . |                                      ,λx.T>(locl(a@0))?Top.
. . | . . |       ¬P@0((λx.s(i;t').x),v)
. . | . . 12. ∀t:ℕ.
. . | . . |   ¬isnull(a(i;t))
. . | . . |   ⇒
. . | . . |   (islocal(kind(a(i;t)))
. . | . . |    ⇒
. . | . . |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . | . . |    ⇒
. . | . . |    P((λx.s(i;t).x),val(a(i;t))))
. . | . . |   & (∀x:Id.
. . | . . |      deq-member(product-deq(Knd;Id;KindDeq;IdDeq);<...
. . | . . |                                                  ,x>;1of(
. . | . . |                                                      ))
. . | . . |      ⇒
. . | . . |      s(i;t+1).x
. . | . . |      =
. . | . . |      2of()(<kind(a(i;t)),x>,λx.s(i;t).x,val(a(i;t))))
. . | . . |   & (∀l:IdLnk.
. . | . . |      deq-member(product-deq(Knd;IdLnk;...;...);<kind(...)
. . | . . |                                              ,l>;1of())
. . | . . |      ⇒
. . | . . |      withlnk(l;m(i;t))
. . | . . |      =
. . | . . |      if source(l) = i→
. . | . . |         concat(map(λtgf.map(λx.
. . | . . |         <1of(tgf),x>;2of(tgf)
. . | . . |                     ((λx.s(i;t).x)
. . | . . |                     ,val(a(i;t))));2of()
. . | . . |                                    (<kind(a(i;t)),l>)))
. . | . . |      else nil fi)
. . | . . |   & (∀x:Id.
. . | . . |      ¬(deq-member(IdDeq;x;1of())
. . | . . |        ⇒
. . | . . |        deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . | . . |      ⇒
. . | . . |      s(i;t).x = s(i;t+1).x)
. . | . . |   & (∀l:IdLnk, tg:Id.
. . | . . |      ¬(deq-member(product-deq(IdLnk;Id;...;IdDeq);...;1of(
```

```
. . | . . |                                                          ))
. . | . . |        ⇒
. . | . . |        deq-member(KindDeq;kind(a(i;t));2of()(<l,tg>)))
. . | . . |      ⇒
. . | . . |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . | . . 13. ∀x:Id. deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . | . . 14. ∀a@0:Action(i).
. . | . . |   ¬isnull(a@0)
. . | . . |   ⇒
. . | . . |   (valtype(i;a@0) ⊆r <[locl(a)],λx.T>(kind(a@0))?Top)
. . | . . 15. ∀x:Id.
. . | . . |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . | . . |                     2of(ds)(x)
. . | . . |                  else Top fi
. . | . . 16. IdDeq ∈ EqDecider(Id)
. . | . . 17. j : Id
. . | . . 18. t : ℕ
. . | . . 19. ¬isnull(a(j;t))
. . | . . 20. j = i
. . | . . 21. kind(<j,t>) = locl(a)
. . | . . 22. ¬isnull(a(j;t))
. . | . . 23. z : Knd
. . | . . 24. z = locl(a)
. . | . . ⊢  (if isrcv(z)→ rcvtype(<j,t>)
. . | . . |   else V(j;locl(act(z))) fi ⊆r T)
. . | . . |  ∈ Type
. . | . . | by Analyze -2 THEN Unfold `isrcv` 0 THEN Reduce 0
. . | . . |
. . | . . |\
. . | . . | 1. i : Id
. . | . . | 2. a : Id
. . | . . | 3. T : Type
. . | . . | 4. ds : x:Id fp-> Type
. . | . . | 5. P : State(ds)→T→Prop
. . | . . | 6. w : World
. . | . . | 7. p : FairFifo
. . | . . | 8. FairFifo
. . | . . | 9. ∀l:IdLnk, tg:Id.
. . | . . |    (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . | . . |                     <ds
. . | . . |                     ,<[locl(a)],λx.T>
. . | . . |                     ,
. . | . . |                     ,<[a],λx.P>
. . | . . |                     ,
. . | . . |                     ,
. . | . . |                     ,
. . | . . |                     ,
. . | . . |                     ,.>
. . | . . |                  else  fi.da(rcv(l; tg))
. . | . . | 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . | . . | 11. ∀a@0:Id, t:ℕ.
. . | . . |     ∃t':ℕ.
. . | . . |     t≤t'
. . | . . |     & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . | . . |       ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
```

```
. . | . . |       ∨ P@0 != <[a],λx.P>(a@0) ==> ∀v:<[locl(a)]
. . | . . |                                      ,λx.
. . | . . |                                       T>(locl(a@0))?Top.
. . | . . |         ¬P@0((λx.s(i;t').x),v)
. . | . . | 12. ∀t:ℕ.
. . | . . |     ¬isnull(a(i;t))
. . | . . |     ⇒
. . | . . |     (islocal(kind(a(i;t)))
. . | . . |      ⇒
. . | . . |      (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . | . . |      ⇒
. . | . . |      P((λx.s(i;t).x),val(a(i;t))))
. . | . . |     & (∀x:Id.
. . | . . |        deq-member(product-deq(Knd;Id;KindDeq;...);<...
. . | . . |                                                  ,x>;1of(
. . | . . |                                                      ))
. . | . . |        ⇒
. . | . . |        s(i;t+1).x
. . | . . |        =
. . | . . |        2of()(<kind(a(i;t)),x>,λx.s(i;t).x,val(a(i;t))))
. . | . . |     & (∀l:IdLnk.
. . | . . |        deq-member(product-deq(Knd;IdLnk;...;...);<...
. . | . . |                                                ,l>;1of(
. . | . . |                                                    ))
. . | . . |        ⇒
. . | . . |        withlnk(l;m(i;t))
. . | . . |        =
. . | . . |        if source(l) = i→
. . | . . |           concat(map(λtgf.map(λx.
. . | . . |           <1of(tgf),x>;2of(tgf)
. . | . . |                       ((λx.s(i;t).x)
. . | . . |                       ,val(a(i;t))));2of()
. . | . . |                                      (<kind(a(i;t)),l>)))
. . | . . |        else nil fi)
. . | . . |     & (∀x:Id.
. . | . . |        ¬(deq-member(IdDeq;x;1of())
. . | . . |          ⇒
. . | . . |          deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . | . . |        ⇒
. . | . . |        s(i;t).x = s(i;t+1).x)
. . | . . |     & (∀l:IdLnk, tg:Id.
. . | . . |        ¬(deq-member(product-deq(IdLnk;Id;...;...);...;1of(
. . | . . |                                                      ))
. . | . . |          ⇒
. . | . . |          deq-member(KindDeq;kind(a(i;t));2of()(<l,tg>)))
. . | . . |        ⇒
. . | . . |        w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . | . . | 13. ∀x:Id.
. . | . . |     deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . | . . | 14. ∀a@0:Action(i).
. . | . . |     ¬isnull(a@0)
. . | . . |     ⇒
. . | . . |     (valtype(i;a@0) ⊆r <[locl(a)],λx.T>(kind(a@0))?Top)
. . | . . | 15. ∀x:Id.
. . | . . |     vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
```

```
. . | . . |                        2of(ds)(x)
. . | . . |                      else Top fi
. . | . . | 16. IdDeq ∈ EqDecider(Id)
. . | . . | 17. j : Id
. . | . . | 18. t : ℕ
. . | . . | 19. ¬isnull(a(j;t))
. . | . . | 20. j = i
. . | . . | 21. kind(<j,t>) = locl(a)
. . | . . | 22. ¬isnull(a(j;t))
. . | . . | 23. x : IdLnk×Id
. . | . . | 24. inl(x) = locl(a)
. . | . . | ⊢  (rcvtype(<j,t>) ⊆r T) ∈ Type
. . | . . |   by Unfolds [‘Knd‘;‘locl‘] -1
. . | . . |      THEN
. . | . . |      FwdThru
. . | . . |      Thm* ∀x:A, y:B. inl(x) = inr(y) ∈ A+B ⇒ False
. . | . . |      {inl_eq_inr}
. . | . . |      [-1]
. . | . . |      THEN
. . | . . |      PWTrivial
. . | . . |
. . | . .\
. . | . . 1. i : Id
. . | . . 2. a : Id
. . | . . 3. T : Type
. . | . . 4. ds : x:Id fp-> Type
. . | . . 5. P : State(ds)→T→Prop
. . | . . 6. w : World
. . | . . 7. FairFifo
. . | . . 8. FairFifo
. . | . . 9. ∀l:IdLnk, tg:Id.
. . | . .    (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . | . .                      <ds
. . | . .                      ,<[locl(a)],λx.T>
. . | . .                      ,
. . | . .                      ,<[a],λx.P>
. . | . .                      ,
. . | . .                      ,
. . | . .                      ,
. . | . .                      ,
. . | . .                      ,·>
. . | . .                    else  fi.da(rcv(l; tg))
. . | . . 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . | . . 11. ∀a@0:Id, t:ℕ.
. . | . .     ∃t':ℕ.
. . | . .     t≤t'
. . | . .     & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . | . .       ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . | . .       ∨ P@0 != <[a],λx.P>(a@0) ==> ∀v:<[locl(a)]
. . | . .                                     ,λx.
. . | . .                                      T>(locl(a@0))?Top.
. . | . .         ¬P@0((λx.s(i;t').x),v)
. . | . . 12. ∀t:ℕ.
. . | . .     ¬isnull(a(i;t))
. . | . .     ⇒
```

```
. . | . . .     (islocal(kind(a(i;t)))
. . | . . .      ⇒
. . | . . .      (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . | . . .      ⇒
. . | . . .      P((λx.s(i;t).x),val(a(i;t))))
. . | . . .     & (∀x:Id.
. . | . . .        deq-member(product-deq(Knd;Id;KindDeq;...);<...
. . | . . .                                                 ,x>;1of(
. . | . . .                                                     ))
. . | . . .        ⇒
. . | . . .        s(i;t+1).x
. . | . . .        =
. . | . . .        2of()(<kind(a(i;t)),x>,λx.s(i;t).x,val(a(i;t))))
. . | . . .     & (∀l:IdLnk.
. . | . . .        deq-member(product-deq(Knd;IdLnk;...;...);<...
. . | . . .                                               ,l>;1of(
. . | . . .                                                   ))
. . | . . .        ⇒
. . | . . .        withlnk(l;m(i;t))
. . | . . .        =
. . | . . .        if source(l) = i→
. . | . . .           concat(map(λtgf.map(λx.
. . | . . .           <1of(tgf),x>;2of(tgf)
. . | . . .                       ((λx.s(i;t).x)
. . | . . .                       ,val(a(i;t))));2of()
. . | . . .                                     (<kind(a(i;t)),l>)))
. . | . . .        else nil fi)
. . | . . .     & (∀x:Id.
. . | . . .        ¬(deq-member(IdDeq;x;1of())
. . | . . .          ⇒
. . | . . .          deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . | . . .        ⇒
. . | . . .        s(i;t).x = s(i;t+1).x)
. . | . . .     & (∀l:IdLnk, tg:Id.
. . | . . .        ¬(deq-member(product-deq(IdLnk;Id;...;...);...;1of(
. . | . . .                                                     ))
. . | . . .          ⇒
. . | . . .          deq-member(KindDeq;kind(a(i;t));2of()(<l,tg>)))
. . | . . .        ⇒
. . | . . .        w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . | . . . 13. ∀x:Id.
. . | . . .     deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . | . . . 14. ∀a@0:Action(i).
. . | . . .     ¬isnull(a@0)
. . | . . .     ⇒
. . | . . .     (valtype(i;a@0) ⊆r <[locl(a)],λx.T>(kind(a@0))?Top)
. . | . . . 15. ∀x:Id.
. . | . . .     vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . | . . .                        2of(ds)(x)
. . | . . .                     else Top fi
. . | . . . 16. IdDeq ∈ EqDecider(Id)
. . | . . . 17. j : Id
. . | . . . 18. t : ℕ
. . | . . . 19. ¬isnull(a(j;t))
. . | . . . 20. j = i
```

```
. . | . . . 21. kind(<j,t>) = locl(a)
. . | . . . 22. ¬isnull(a(j;t))
. . | . . . 23. y : Id
. . | . . . 24. inr(y) = locl(a)
. . | . . . ⊢  (V(j;locl(act(inr(y)))) ⊆r T) ∈ Type
. . | . . .   by Unfolds [‘locl‘;‘actof‘] 0 THEN Reduce 0
. . | . . .      THEN
. . | . . .      Fold ‘locl‘ 0
. . |
. . .\
. . . 1. i : Id
. . . 2. a : Id
. . . 3. T : Type
. . . 4. ds : x:Id fp-> Type
. . . 5. P : State(ds)→T→Prop
. . . 6. w : World
. . . 7. p : FairFifo
. . . 8. FairFifo
. . . 9. ∀l:IdLnk, tg:Id.
. . . |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . |                    <ds,<[locl(a)],λx.T>,,<[a],λx.P>,,,,,•>
. . . |                 else  fi.da(rcv(l; tg))
. . . 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . 11. ∀a@0:Id, t:ℕ.
. . . |   ∃t':ℕ.
. . . |   t≤t'
. . . |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . |     ∨ P@0 != <[a],λx.P>(a@0) ==> ∀v:<[locl(a)]
. . . |                                      ,λx.T>(locl(a@0))?Top.
. . . |       ¬P@0((λx.s(i;t').x),v)
. . . 12. ∀t:ℕ.
. . . |   ¬isnull(a(i;t))
. . . |   ⇒
. . . |   (islocal(kind(a(i;t)))
. . . |    ⇒
. . . |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . |    ⇒
. . . |    P((λx.s(i;t).x),val(a(i;t))))
. . . |   & (∀x:Id.
. . . |      deq-member(product-deq(Knd;Id;KindDeq;IdDeq);<kind(...)
. . . |                                                    ,x>;1of())
. . . |      ⇒
. . . |      s(i;t+1).x
. . . |      =
. . . |      2of()(<kind(a(i;t)),x>,λx.s(i;t).x,val(a(i;t))))
. . . |   & (∀l:IdLnk.
. . . |      deq-member(product-deq(Knd;IdLnk;KindDeq;...);<kind(...)
. . . |                                                     ,l>;1of())
. . . |      ⇒
. . . |      withlnk(l;m(i;t))
. . . |      =
. . . |      if source(l) = i→
. . . |         concat(map(λtgf.map(λx.
. . . |         <1of(tgf),x>;2of(tgf)
```

```
. . . |                      ((λx.s(i;t).x)
. . . |                      ,val(a(i;t))));2of()(<kind(a(i;t)),l>)))
. . . |     else nil fi)
. . . |   & (∀x:Id.
. . . |     ¬(deq-member(IdDeq;x;1of())
. . . |       ⇒
. . . |       deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . . |     ⇒
. . . |     s(i;t).x = s(i;t+1).x)
. . . |   & (∀l:IdLnk, tg:Id.
. . . |     ¬(deq-member(product-deq(IdLnk;Id;IdLnkDeq;...);...;1of(
. . . |                                                        ))
. . . |       ⇒
. . . |       deq-member(KindDeq;kind(a(i;t));2of()(<l,tg>)))
. . . |     ⇒
. . . |     w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . 13. ∀x:Id. deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . . 14. ∀a@0:Action(i).
. . . |   ¬isnull(a@0)
. . . |   ⇒
. . . |   (valtype(i;a@0) ⊆r <[locl(a)],λx.T>(kind(a@0))?Top)
. . . 15. ∀x:Id.
. . . |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→ 2of(ds)(x)
. . . |                    else Top fi
. . . 16. IdDeq ∈ EqDecider(Id)
. . . 17. (∀x:Id. vartype(i;x) ⊆r ds(x)?Top)
. . . |   & (∀e:E.
. . . |     loc(e) = i ⇒ kind(e) = locl(a) ⇒ (valtype(e) ⊆r T))
. . . ⊢  ∀e:E.
. . . |  loc(e) = i
. . . |  ⇒
. . . |  (kind(e) = locl(a) ⇒ P((λz.(z when e)),val(e)))
. . . |  & (∃e':E.
. . . |     (e <loc e') ∨ e = e'
. . . |     & kind(e') = locl(a) ∨ (∀v:T. ¬P((λz.(z after e')),v)))
. . . | by Analyze -1 THEN Thin -1
. . . |
. . . 1. i : Id
. . . 2. a : Id
. . . 3. T : Type
. . . 4. ds : x:Id fp-> Type
. . . 5. P : State(ds)→T→Prop
. . . 6. w : World
. . . 7. p : FairFifo
. . . 8. FairFifo
. . . 9. ∀l:IdLnk, tg:Id.
. . . |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . |                    <ds,<[locl(a)],λx.T>,,<[a],λx.P>,,,,,·>
. . . |                 else  fi.da(rcv(l; tg))
. . . 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . 11. ∀a@0:Id, t:ℕ.
. . . |   ∃t':ℕ.
. . . |   t≤t'
. . . |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
```

```
. . . |     ∨ P@0 != <[a],λx.P>(a@0) ==> ∀v:<[locl(a)]
. . . |                                    ,λx.T>(locl(a@0))?Top.
. . . |       ¬P@0((λx.s(i;t').x),v)
. . . 12. ∀t:ℕ.
. . . |   ¬isnull(a(i;t))
. . . |   ⇒
. . . |   (islocal(kind(a(i;t)))
. . . |    ⇒
. . . |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . |    ⇒
. . . |    P((λx.s(i;t).x),val(a(i;t))))
. . . |   & (∀x:Id.
. . . |      deq-member(product-deq(Knd;Id;KindDeq;IdDeq);<kind(...)
. . . |                                                   ,x>;1of())
. . . |      ⇒
. . . |      s(i;t+1).x
. . . |      =
. . . |      2of()(<kind(a(i;t)),x>,λx.s(i;t).x,val(a(i;t))))
. . . |   & (∀l:IdLnk.
. . . |      deq-member(product-deq(Knd;IdLnk;KindDeq;...);<kind(...)
. . . |                                                    ,l>;1of())
. . . |      ⇒
. . . |      withlnk(l;m(i;t))
. . . |      =
. . . |      if source(l) = i→
. . . |         concat(map(λtgf.map(λx.
. . . |         <1of(tgf),x>;2of(tgf)
. . . |                      ((λx.s(i;t).x)
. . . |                      ,val(a(i;t))));2of()(<kind(a(i;t)),l>)))
. . . |      else nil fi)
. . . |   & (∀x:Id.
. . . |      ¬(deq-member(IdDeq;x;1of())
. . . |        ⇒
. . . |        deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . . |      ⇒
. . . |      s(i;t).x = s(i;t+1).x)
. . . |   & (∀l:IdLnk, tg:Id.
. . . |      ¬(deq-member(product-deq(IdLnk;Id;IdLnkDeq;...);...;1of(
. . . |                                                        ))
. . . |        ⇒
. . . |        deq-member(KindDeq;kind(a(i;t));2of()(<l,tg>)))
. . . |      ⇒
. . . |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . 13. ∀x:Id. deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . . 14. ∀a@0:Action(i).
. . . |   ¬isnull(a@0)
. . . |   ⇒
. . . |   (valtype(i;a@0) ⊆r <[locl(a)],λx.T>(kind(a@0))?Top)
. . . 15. ∀x:Id.
. . . |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→ 2of(ds)(x)
. . . |                  else Top fi
. . . 16. IdDeq ∈ EqDecider(Id)
. . . 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . ⊢  ∀e:E.
. . . |  loc(e) = i
```

```
. . . |  ⇒
. . . |  (kind(e) = locl(a) ⇒ P((λz.(z when e)),val(e)))
. . . |  & (∃e':E.
. . . |     (e <loc e') ∨ e = e'
. . . |     & kind(e') = locl(a) ∨ (∀v:T. ¬P((λz.(z after e')),v)))
. . . | by RepeatFor 2 (Analyze 0 THENA (Auto THEN D_ES_Subtype))
. . . |    THEN
. . . |    Analyze -2
. . . |    THEN
. . . |    Analyze -3
. . . |    THEN
. . . |    RenameVar `j' -4
. . . |    THEN
. . . |    RenameVar `t' -3
. . . |    THEN
. . . |    All Reduce
. . . |    THEN
. . . |    Decide isnull(a(j;t))
. . . |    THEN
. . . |    Try (Assert False THEN Unhide THEN Complete Auto)
. . . |    THEN
. . . |    Thin -3

. . . |
. . . 1. i : Id
. . . 2. a : Id
. . . 3. T : Type
. . . 4. ds : x:Id fp-> Type
. . . 5. P : State(ds)→T→Prop
. . . 6. w : World
. . . 7. p : FairFifo
. . . 8. FairFifo
. . . 9. ∀l:IdLnk, tg:Id.
. . . |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . |                    <ds,<[locl(a)],λx.T>,,<[a],λx.P>,,,,,•>
. . . |                 else  fi.da(rcv(l; tg))
. . . 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . 11. ∀a@0:Id, t:ℕ.
. . . |   ∃t':ℕ.
. . . |   t≤t'
. . . |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . |     ∨ P@0 != <[a],λx.P>(a@0) ==> ∀v:<[locl(a)]
. . . |                                     ,λx.T>(locl(a@0))?Top.
. . . |       ¬P@0((λx.s(i;t').x),v)
. . . 12. ∀t:ℕ.
. . . |   ¬isnull(a(i;t))
. . . |   ⇒
. . . |   (islocal(kind(a(i;t)))
. . . |    ⇒
. . . |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . |    ⇒
. . . |    P((λx.s(i;t).x),val(a(i;t))))
. . . |   & (∀x:Id.
. . . |      deq-member(product-deq(Knd;Id;KindDeq;IdDeq);<kind(...)
. . . |                                                  ,x>;1of())
```

```
. . . |      ⇒
. . . |      s(i;t+1).x
. . . |      =
. . . |      2of()(<kind(a(i;t)),x>,λx.s(i;t).x,val(a(i;t))))
. . . |   & (∀l:IdLnk.
. . . |      deq-member(product-deq(Knd;IdLnk;KindDeq;...);<kind(...)
. . . |                                                    ,l>;1of())
. . . |      ⇒
. . . |      withlnk(l;m(i;t))
. . . |      =
. . . |      if source(l) = i→
. . . |         concat(map(λtgf.map(λx.
. . . |         <1of(tgf),x>;2of(tgf)
. . . |                      ((λx.s(i;t).x)
. . . |                      ,val(a(i;t))));2of()(<kind(a(i;t)),l>)))
. . . |      else nil fi)
. . . |   & (∀x:Id.
. . . |      ¬(deq-member(IdDeq;x;1of())
. . . |        ⇒
. . . |        deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . . |      ⇒
. . . |      s(i;t).x = s(i;t+1).x)
. . . |   & (∀l:IdLnk, tg:Id.
. . . |      ¬(deq-member(product-deq(IdLnk;Id;IdLnkDeq;...);...;1of(
. . . |                                                        ))
. . . |        ⇒
. . . |        deq-member(KindDeq;kind(a(i;t));2of()(<l,tg>)))
. . . |      ⇒
. . . |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . 13. ∀x:Id. deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . . 14. ∀a@0:Action(i).
. . . |   ¬isnull(a@0)
. . . |   ⇒
. . . |   (valtype(i;a@0) ⊆r <[locl(a)],λx.T>(kind(a@0))?Top)
. . . 15. ∀x:Id.
. . . |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→ 2of(ds)(x)
. . . |                  else Top fi
. . . 16. IdDeq ∈ EqDecider(Id)
. . . 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . 18. j : Id
. . . 19. t : ℕ
. . . 20. j = i
. . . 21. ¬isnull(a(j;t))
. . . ⊢  (kind(<j,t>) = locl(a) ⇒ P((λz.(z when <j,t>)),val(<j,t>)))
. . . |  & (∃e':E.
. . . |     (<j,t> <loc e') ∨ <j,t> = e'
. . . |     & kind(e') = locl(a) ∨ (∀v:T. ¬P((λz.(z after e')),v)))
. . . | by AssertBY (¬isnull(a(i;t))) (WeakSubstFor i 0)
. . . |
. . . 1. i : Id
. . . 2. a : Id
. . . 3. T : Type
. . . 4. ds : x:Id fp-> Type
. . . 5. P : State(ds)→T→Prop
. . . 6. w : World
```

```
. . . 7. p : FairFifo
. . . 8. FairFifo
. . . 9. ∀l:IdLnk, tg:Id.
. . . |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . |                    <ds,<[locl(a)],λx.T>,,<[a],λx.P>,,,,,•>
. . . |                 else  fi.da(rcv(l; tg))
. . . 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . 11. ∀a@0:Id, t:ℕ.
. . . |   ∃t':ℕ.
. . . |   t≤t'
. . . |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . |     ∨ P@0 != <[a],λx.P>(a@0) ==> ∀v:<[locl(a)]
. . . |                                     ,λx.T>(locl(a@0))?Top.
. . . |       ¬P@0((λx.s(i;t').x),v)
. . . 12. ∀t:ℕ.
. . . |   ¬isnull(a(i;t))
. . . |   ⇒
. . . |   (islocal(kind(a(i;t)))
. . . |    ⇒
. . . |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . |    ⇒
. . . |    P((λx.s(i;t).x),val(a(i;t))))
. . . |   & (∀x:Id.
. . . |      deq-member(product-deq(Knd;Id;KindDeq;IdDeq);<kind(...)
. . . |                                                    ,x>;1of())
. . . |      ⇒
. . . |      s(i;t+1).x
. . . |      =
. . . |      2of()(<kind(a(i;t)),x>,λx.s(i;t).x,val(a(i;t))))
. . . |   & (∀l:IdLnk.
. . . |      deq-member(product-deq(Knd;IdLnk;KindDeq;...);<kind(...)
. . . |                                                     ,l>;1of())
. . . |      ⇒
. . . |      withlnk(l;m(i;t))
. . . |      =
. . . |      if source(l) = i→
. . . |         concat(map(λtgf.map(λx.
. . . |         <1of(tgf),x>;2of(tgf)
. . . |                     ((λx.s(i;t).x)
. . . |                     ,val(a(i;t))));2of()(<kind(a(i;t)),l>)))
. . . |      else nil fi)
. . . |   & (∀x:Id.
. . . |      ¬(deq-member(IdDeq;x;1of())
. . . |        ⇒
. . . |        deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . . |      ⇒
. . . |      s(i;t).x = s(i;t+1).x)
. . . |   & (∀l:IdLnk, tg:Id.
. . . |      ¬(deq-member(product-deq(IdLnk;Id;IdLnkDeq;...);...;1of(
. . . |                                                        ))
. . . |        ⇒
. . . |        deq-member(KindDeq;kind(a(i;t));2of()(<l,tg>)))
. . . |      ⇒
. . . |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
```

```
. . . 13. ∀x:Id. deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . . 14. ∀a@0:Action(i).
. . . |   ¬isnull(a@0)
. . . |   ⇒
. . . |   (valtype(i;a@0) ⊆r <[locl(a)],λx.T>(kind(a@0))?Top)
. . . 15. ∀x:Id.
. . . |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→ 2of(ds)(x)
. . . |                  else Top fi
. . . 16. IdDeq ∈ EqDecider(Id)
. . . 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . 18. j : Id
. . . 19. t : ℕ
. . . 20. j = i
. . . 21. ¬isnull(a(j;t))
. . . 22. ¬isnull(a(i;t))
. . . ⊢  (kind(<j,t>) = locl(a) ⇒ P((λz.(z when <j,t>)),val(<j,t>)))
. . . |  & (∃e':E.
. . . |     (<j,t> <loc e') ∨ <j,t> = e'
. . . |     & kind(e') = locl(a) ∨ (∀v:T. ¬P((λz.(z after e')),v)))
. . . | by Assert ((λx.s(i;t).x) ∈ State(ds))
. . . |
. . . |\
. . . | .....assertion .....
. . . | 1. i : Id
. . . | 2. a : Id
. . . | 3. T : Type
. . . | 4. ds : x:Id fp-> Type
. . . | 5. P : State(ds)→T→Prop
. . . | 6. w : World
. . . | 7. FairFifo
. . . | 8. FairFifo
. . . | 9. ∀l:IdLnk, tg:Id.
. . . |    (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . |                      <ds,<[locl(a)],λx.T>,,<[a],λx.P>,,,,,•>
. . . |                   else  fi.da(rcv(l; tg))
. . . | 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . | 11. ∀a@0:Id, t:ℕ.
. . . |     ∃t':ℕ.
. . . |     t≤t'
. . . |     & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . |       ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . |       ∨ P@0 != <[a],λx.P>(a@0) ==> ∀v:<[locl(a)]
. . . |                                        ,λx.T>(locl(a@0))?Top.
. . . |         ¬P@0((λx.s(i;t').x),v)
. . . | 12. ∀t:ℕ.
. . . |     ¬isnull(a(i;t))
. . . |     ⇒
. . . |     (islocal(kind(a(i;t)))
. . . |      ⇒
. . . |      (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . |      ⇒
. . . |      P((λx.s(i;t).x),val(a(i;t))))
. . . |     & (∀x:Id.
. . . |        deq-member(product-deq(Knd;Id;KindDeq;IdDeq);<kind(...)
. . . |                                                    ,x>;1of())
```

```
. . . |        ⇒
. . . |        s(i;t+1).x

. . . |        =
. . . |        2of()(<kind(a(i;t)),x>,λx.s(i;t).x,val(a(i;t))))
. . . |     & (∀l:IdLnk.
. . . |        deq-member(product-deq(Knd;IdLnk;KindDeq;...);<...
. . . |                                                    ,l>;1of(
. . . |                                                        ))
. . . |        ⇒
. . . |        withlnk(l;m(i;t))
. . . |        =
. . . |        if source(l) = i→
. . . |           concat(map(λtgf.map(λx.
. . . |           <1of(tgf),x>;2of(tgf)
. . . |                       ((λx.s(i;t).x)
. . . |                       ,val(a(i;t))));2of()
. . . |                                    (<kind(a(i;t)),l>)))
. . . |        else nil fi)
. . . |     & (∀x:Id.
. . . |        ¬(deq-member(IdDeq;x;1of())
. . . |          ⇒
. . . |          deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . . |        ⇒
. . . |        s(i;t).x = s(i;t+1).x)
. . . |     & (∀l:IdLnk, tg:Id.
. . . |        ¬(deq-member(product-deq(IdLnk;Id;...;IdDeq);...;1of())
. . . |          ⇒
. . . |          deq-member(KindDeq;kind(a(i;t));2of()(<l,tg>)))
. . . |        ⇒
. . . |        w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . | 13. ∀x:Id. deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . . | 14. ∀a@0:Action(i).
. . . |     ¬isnull(a@0)
. . . |     ⇒
. . . |     (valtype(i;a@0) ⊆r <[locl(a)],λx.T>(kind(a@0))?Top)
. . . | 15. ∀x:Id.
. . . |     vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→ 2of(ds)(x)
. . . |                      else Top fi
. . . | 16. IdDeq ∈ EqDecider(Id)
. . . | 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . | 18. j : Id
. . . | 19. t : ℕ
. . . | 20. j = i
. . . | 21. ¬isnull(a(j;t))
. . . | 22. ¬isnull(a(i;t))
. . . | ⊢  (λx.s(i;t).x) ∈ State(ds)
. . . |   by Unfold ‘ma-state‘ 0 THEN DoSubsume
. . . |      THEN
. . . |      Try BackThruSomeHyp
. . . |      THEN
. . . |      Try D_ES_Subtype
. . . |
. . . .\
. . . . 1. i : Id
. . . . 2. a : Id
```

```
. . . . 3. T : Type
. . . . 4. ds : x:Id fp-> Type
. . . . 5. P : State(ds)→T→Prop
. . . . 6. w : World
. . . . 7. p : FairFifo
. . . . 8. FairFifo
. . . . 9. ∀l:IdLnk, tg:Id.
. . . . |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . |                    <ds,<[locl(a)],λx.T>,,<[a],λx.P>,,,,,•>
. . . . |                 else  fi.da(rcv(l; tg))
. . . . 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . 11. ∀a@0:Id, t:ℕ.
. . . . |   ∃t':ℕ.
. . . . |   t≤t'
. . . . |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . |     ∨ P@0 != <[a],λx.P>(a@0) ==> ∀v:<[locl(a)]
. . . . |                                      ,λx.T>(locl(a@0))?Top.
. . . . |       ¬P@0((λx.s(i;t').x),v)
. . . . 12. ∀t:ℕ.
. . . . |   ¬isnull(a(i;t))
. . . . |   ⇒
. . . . |   (islocal(kind(a(i;t)))
. . . . |    ⇒
. . . . |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . |    ⇒
. . . . |    P((λx.s(i;t).x),val(a(i;t))))
. . . . |   & (∀x:Id.
. . . . |      deq-member(product-deq(Knd;Id;KindDeq;IdDeq);<kind(...)
. . . . |                                                    ,x>;1of())
. . . . |      ⇒
. . . . |      s(i;t+1).x
. . . . |      =
. . . . |      2of()(<kind(a(i;t)),x>,λx.s(i;t).x,val(a(i;t))))
. . . . |   & (∀l:IdLnk.
. . . . |      deq-member(product-deq(Knd;IdLnk;KindDeq;...);<...
. . . . |                                                     ,l>;1of(
. . . . |                                                         ))
. . . . |      ⇒
. . . . |      withlnk(l;m(i;t))
. . . . |      =
. . . . |      if source(l) = i→
. . . . |         concat(map(λtgf.map(λx.
. . . . |         <1of(tgf),x>;2of(tgf)
. . . . |                     ((λx.s(i;t).x)
. . . . |                     ,val(a(i;t))));2of()
. . . . |                                    (<kind(a(i;t)),l>)))
. . . . |      else nil fi)
. . . . |   & (∀x:Id.
. . . . |      ¬(deq-member(IdDeq;x;1of())
. . . . |        ⇒
. . . . |        deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . . . |      ⇒
. . . . |      s(i;t).x = s(i;t+1).x)
. . . . |   & (∀l:IdLnk, tg:Id.
```

```
. . . . |      ¬(deq-member(product-deq(IdLnk;Id;...;IdDeq);...;1of())
. . . . |        ⇒
. . . . |        deq-member(KindDeq;kind(a(i;t));2of()(<l,tg>)))
. . . . |      ⇒
. . . . |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . 13. ∀x:Id. deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . . . 14. ∀a@0:Action(i).
. . . . |   ¬isnull(a@0)
. . . . |   ⇒
. . . . |   (valtype(i;a@0) ⊆r <[locl(a)],λx.T>(kind(a@0))?Top)
. . . . 15. ∀x:Id.
. . . . |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→ 2of(ds)(x)
. . . . |                   else Top fi
. . . . 16. IdDeq ∈ EqDecider(Id)
. . . . 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . 18. j : Id
. . . . 19. t : ℕ
. . . . 20. j = i
. . . . 21. ¬isnull(a(j;t))
. . . . 22. ¬isnull(a(i;t))
. . . . 23. (λx.s(i;t).x) ∈ State(ds)
. . . . ⊢  (kind(<j,t>) = locl(a)
. . . . |   ⇒
. . . . |   P((λz.(z when <j,t>)),val(<j,t>)))
. . . . |  & (∃e':E.
. . . . |     (<j,t> <loc e') ∨ <j,t> = e'
. . . . |     & kind(e') = locl(a) ∨ (∀v:T. ¬P((λz.(z after e')),v)))
. . . . | by Analyze 0
. . . . |
. . . . |\
. . . . | 1. i : Id
. . . . | 2. a : Id
. . . . | 3. T : Type
. . . . | 4. ds : x:Id fp-> Type
. . . . | 5. P : State(ds)→T→Prop
. . . . | 6. w : World
. . . . | 7. p : FairFifo
. . . . | 8. FairFifo
. . . . | 9. ∀l:IdLnk, tg:Id.
. . . . | |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . | |                   <ds,<[locl(a)],λx.T>,,<[a],λx.P>,,,,,•>
. . . . | |                 else  fi.da(rcv(l; tg))
. . . . | 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . | 11. ∀a@0:Id, t:ℕ.
. . . . | |   ∃t':ℕ.
. . . . | |   t≤t'
. . . . | |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . | |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . | |     ∨ P@0 != <[a],λx.P>(a@0) ==> ∀v:<[locl(a)]
. . . . | |                                    ,λx.T>(locl(a@0))?Top.
. . . . | |       ¬P@0((λx.s(i;t').x),v)
. . . . | 12. ∀t:ℕ.
. . . . | |   ¬isnull(a(i;t))
. . . . | |   ⇒
. . . . | |   (islocal(kind(a(i;t)))
```

```
. . . . | |    ⇒
. . . . | |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . | |    ⇒
. . . . | |    P((λx.s(i;t).x),val(a(i;t))))
. . . . | |   & (∀x:Id.
. . . . | |      deq-member(product-deq(Knd;Id;KindDeq;IdDeq);<...
. . . . | |                                                  ,x>;1of(
. . . . | |                                                      ))
. . . . | |      ⇒
. . . . | |      s(i;t+1).x
. . . . | |      =
. . . . | |      2of()(<kind(a(i;t)),x>,λx.s(i;t).x,val(a(i;t))))
. . . . | |   & (∀l:IdLnk.
. . . . | |      deq-member(product-deq(Knd;IdLnk;...;...);<kind(...)
. . . . | |                                               ,l>;1of())
. . . . | |      ⇒
. . . . | |      withlnk(l;m(i;t))
. . . . | |      =
. . . . | |      if source(l) = i→
. . . . | |         concat(map(λtgf.map(λx.
. . . . | |         <1of(tgf),x>;2of(tgf)
. . . . | |                     ((λx.s(i;t).x)
. . . . | |                     ,val(a(i;t))));2of()
. . . . | |                                  (<kind(a(i;t)),l>)))
. . . . | |      else nil fi)
. . . . | |   & (∀x:Id.
. . . . | |      ¬(deq-member(IdDeq;x;1of())
. . . . | |        ⇒
. . . . | |        deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . . . | |      ⇒
. . . . | |      s(i;t).x = s(i;t+1).x)
. . . . | |   & (∀l:IdLnk, tg:Id.
. . . . | |      ¬(deq-member(product-deq(IdLnk;Id;...;IdDeq);...;1of(
. . . . | |                                                      ))
. . . . | |        ⇒
. . . . | |        deq-member(KindDeq;kind(a(i;t));2of()(<l,tg>)))
. . . . | |      ⇒
. . . . | |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . | 13. ∀x:Id. deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . . . | 14. ∀a@0:Action(i).
. . . . | |   ¬isnull(a@0)
. . . . | |   ⇒
. . . . | |   (valtype(i;a@0) ⊆r <[locl(a)],λx.T>(kind(a@0))?Top)
. . . . | 15. ∀x:Id.
. . . . | |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . . . | |                      2of(ds)(x)
. . . . | |                  else Top fi
. . . . | 16. IdDeq ∈ EqDecider(Id)
. . . . | 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . | 18. j : Id
. . . . | 19. t : ℕ
. . . . | 20. j = i
. . . . | 21. ¬isnull(a(j;t))
. . . . | 22. ¬isnull(a(i;t))
. . . . | 23. (λx.s(i;t).x) ∈ State(ds)
```

```
. . . . | ⊢  kind(<j,t>) = locl(a)
. . . . | |  ⇒
. . . . | |  P((λz.(z when <j,t>)),val(<j,t>))  by Analyze 0
. . . . | |
. . . . | |\
. . . . | | 1. i : Id
. . . . | | 2. a : Id
. . . . | | 3. T : Type
. . . . | | 4. ds : x:Id fp-> Type
. . . . | | 5. P : State(ds)→T→Prop
. . . . | | 6. w : World
. . . . | | 7. p : FairFifo
. . . . | | 8. FairFifo
. . . . | | 9. ∀l:IdLnk, tg:Id.
. . . . | | |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . | | |                    <ds
. . . . | | |                    ,<[locl(a)],λx.T>
. . . . | | |                    ,
. . . . | | |                    ,<[a],λx.P>
. . . . | | |                    ,
. . . . | | |                    ,
. . . . | | |                    ,
. . . . | | |                    ,
. . . . | | |                    ,.>
. . . . | | |                else  fi.da(rcv(l; tg))
. . . . | | 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . | | 11. ∀a@0:Id, t:ℕ.
. . . . | | |   ∃t':ℕ.
. . . . | | |   t≤t'
. . . . | | |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . | | |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . | | |     ∨ P@0 != <[a],λx.P>(a@0) ==> ∀v:<[locl(a)]
. . . . | | |                                    ,λx.
. . . . | | |                                     T>(locl(a@0))?Top.
. . . . | | |       ¬P@0((λx.s(i;t').x),v)
. . . . | | 12. ∀t:ℕ.
. . . . | | |   ¬isnull(a(i;t))
. . . . | | |   ⇒
. . . . | | |   (islocal(kind(a(i;t)))
. . . . | | |    ⇒
. . . . | | |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . | | |    ⇒
. . . . | | |    P((λx.s(i;t).x),val(a(i;t))))
. . . . | | |   & (∀x:Id.
. . . . | | |      deq-member(product-deq(Knd;Id;KindDeq;...);<...
. . . . | | |                                                ,x>;1of(
. . . . | | |                                                    ))
. . . . | | |      ⇒
. . . . | | |      s(i;t+1).x
. . . . | | |      =
. . . . | | |      2of()(<kind(a(i;t)),x>,λx.s(i;t).x,val(a(i;t))))
. . . . | | |   & (∀l:IdLnk.
. . . . | | |      deq-member(product-deq(Knd;IdLnk;...;...);<...
. . . . | | |                                              ,l>;1of(
. . . . | | |                                                  ))
```

```
. . . . | | |      ⇒
. . . . | | |      withlnk(l;m(i;t))
. . . . | | |      =
. . . . | | |      if source(l) = i→
. . . . | | |         concat(map(λtgf.map(λx.
. . . . | | |         <1of(tgf),x>;2of(tgf)
. . . . | | |                      ((λx.s(i;t).x)
. . . . | | |                      ,val(a(i;t))));2of()
. . . . | | |                                   (<kind(a(i;t)),l>)))
. . . . | | |      else nil fi)
. . . . | | |   & (∀x:Id.
. . . . | | |      ¬(deq-member(IdDeq;x;1of())
. . . . | | |        ⇒
. . . . | | |        deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . . . | | |      ⇒
. . . . | | |      s(i;t).x = s(i;t+1).x)
. . . . | | |   & (∀l:IdLnk, tg:Id.
. . . . | | |      ¬(deq-member(product-deq(IdLnk;Id;...;...);...;1of(
. . . . | | |                                                    ))
. . . . | | |        ⇒
. . . . | | |        deq-member(KindDeq;kind(a(i;t));2of()(<l,tg>)))
. . . . | | |      ⇒
. . . . | | |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . | | 13. ∀x:Id.
. . . . | | |   deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . . . | | 14. ∀a@0:Action(i).
. . . . | | |   ¬isnull(a@0)
. . . . | | |   ⇒
. . . . | | |   (valtype(i;a@0) ⊆r <[locl(a)],λx.T>(kind(a@0))?Top)
. . . . | | 15. ∀x:Id.
. . . . | | |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . . . | | |                      2of(ds)(x)
. . . . | | |                   else Top fi
. . . . | | 16. IdDeq ∈ EqDecider(Id)
. . . . | | 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . | | 18. j : Id
. . . . | | 19. t : ℕ
. . . . | | 20. j = i
. . . . | | 21. ¬isnull(a(j;t))
. . . . | | 22. ¬isnull(a(i;t))
. . . . | | 23. (λx.s(i;t).x) ∈ State(ds)
. . . . | | 24. kind(<j,t>) = locl(a)
. . . . | | ⊢  P((λz.(z when <j,t>)),val(<j,t>))
. . . . | | | by Unfolds [‘w-when‘;‘es-val‘] 0 THEN Reduce 0
. . . . | | |    THEN
. . . . | | |    Unfold ‘w-eval‘ 0
. . . . | | |    THEN
. . . . | | |    Unfold ‘w-act‘ 0
. . . . | | |    THEN
. . . . | | |    Reduce 0
. . . . | | |
. . . . | | 1. i : Id
. . . . | | 2. a : Id
. . . . | | 3. T : Type
. . . . | | 4. ds : x:Id fp-> Type
```

```
. . . . | | 5. P : State(ds)→T→Prop
. . . . | | 6. w : World
. . . . | | 7. FairFifo
. . . . | | 8. FairFifo
. . . . | | 9. ∀l:IdLnk, tg:Id.
. . . . | | |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . | | |                    <ds
. . . . | | |                    ,<[locl(a)],λx.T>
. . . . | | |                    ,
. . . . | | |                    ,<[a],λx.P>
. . . . | | |                    ,
. . . . | | |                    ,
. . . . | | |                    ,
. . . . | | |                    ,
. . . . | | |                    ,•>
. . . . | | |                else  fi.da(rcv(l; tg))
. . . . | | 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . | | 11. ∀a@0:Id, t:ℕ.
. . . . | | |   ∃t':ℕ.
. . . . | | |   t≤t'
. . . . | | |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . | | |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . | | |     ∨ P@0 != <[a],λx.P>(a@0) ==> ∀v:<[locl(a)]
. . . . | | |                                    ,λx.
. . . . | | |                                     T>(locl(a@0))?Top.
. . . . | | |       ¬P@0((λx.s(i;t').x),v)
. . . . | | 12. ∀t:ℕ.
. . . . | | |   ¬isnull(a(i;t))
. . . . | | |   ⇒
. . . . | | |   (islocal(kind(a(i;t)))
. . . . | | |    ⇒
. . . . | | |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . | | |    ⇒
. . . . | | |    P((λx.s(i;t).x),val(a(i;t))))
. . . . | | |   & (∀x:Id.
. . . . | | |      deq-member(product-deq(Knd;Id;KindDeq;...);<...
. . . . | | |                                                ,x>;1of(
. . . . | | |                                                    ))
. . . . | | |      ⇒
. . . . | | |      s(i;t+1).x
. . . . | | |      =
. . . . | | |      2of()(<kind(a(i;t)),x>,λx.s(i;t).x,val(a(i;t))))
. . . . | | |   & (∀l:IdLnk.
. . . . | | |      deq-member(product-deq(Knd;IdLnk;...;...);<...
. . . . | | |                                              ,l>;1of(
. . . . | | |                                                  ))
. . . . | | |      ⇒
. . . . | | |      withlnk(l;m(i;t))
. . . . | | |      =
. . . . | | |      if source(l) = i→
. . . . | | |         concat(map(λtgf.map(λx.
. . . . | | |         <1of(tgf),x>;2of(tgf)
. . . . | | |                      ((λx.s(i;t).x)
. . . . | | |                      ,val(a(i;t))));2of()
. . . . | | |                                    (<kind(a(i;t)),l>)))
```

```
. . . . | | |      else nil fi)
. . . . | | |   & (∀x:Id.
. . . . | | |      ¬(deq-member(IdDeq;x;1of())
. . . . | | |        ⇒
. . . . | | |        deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . . . | | |      ⇒
. . . . | | |      s(i;t).x = s(i;t+1).x)
. . . . | | |   & (∀l:IdLnk, tg:Id.
. . . . | | |      ¬(deq-member(product-deq(IdLnk;Id;...;...);...;1of(
. . . . | | |                                                    ))
. . . . | | |        ⇒
. . . . | | |        deq-member(KindDeq;kind(a(i;t));2of()(<l,tg>)))
. . . . | | |      ⇒
. . . . | | |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . | | 13. ∀x:Id.
. . . . | | |   deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . . . | | 14. ∀a@0:Action(i).

. . . . | | |   ¬isnull(a@0)
. . . . | | |   ⇒
. . . . | | |   (valtype(i;a@0) ⊆r <[locl(a)],λx.T>(kind(a@0))?Top)
. . . . | | 15. ∀x:Id.
. . . . | | |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . . . | | |                      2of(ds)(x)
. . . . | | |                   else Top fi
. . . . | | 16. IdDeq ∈ EqDecider(Id)
. . . . | | 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . | | 18. j : Id
. . . . | | 19. t : ℕ
. . . . | | 20. j = i
. . . . | | 21. ¬isnull(a(j;t))
. . . . | | 22. ¬isnull(a(i;t))
. . . . | | 23. (λx.s(i;t).x) ∈ State(ds)
. . . . | | 24. kind(<j,t>) = locl(a)
. . . . | | ⊢  P((λz.s(j;t).z),val(a(j;t)))
. . . . | | | by AllHyps
. . . . | | |    (λh.
. . . . | | |     InstHyp [t] h THENA Complete Auto THEN Analyze -1
. . . . | | |     THEN
. . . . | | |     Thin -1)
. . . . | | |    THEN
. . . . | | |    Analyze -1
. . . . | | |
. . . . | | |\
. . . . | | | .....antecedent .....
. . . . | | | 1. i : Id
. . . . | | | 2. a : Id
. . . . | | | 3. T : Type
. . . . | | | 4. ds : x:Id fp-> Type
. . . . | | | 5. P : State(ds)→T→Prop
. . . . | | | 6. w : World
. . . . | | | 7. FairFifo
. . . . | | | 8. FairFifo
. . . . | | | 9. ∀l:IdLnk, tg:Id.
. . . . | | | |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . | | | |                    <ds
```

```
. . . . | | | |                    ,<[locl(a)],λx.T>
. . . . | | | |                    ,
. . . . | | | |                    ,<[a],λx.P>
. . . . | | | |                    ,
. . . . | | | |                    ,
. . . . | | | |                    ,
. . . . | | | |                    ,
. . . . | | | |                    ,·>
. . . . | | | |                else  fi.da(rcv(l; tg))
. . . . | | | 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . | | | 11. ∀a@0:Id, t:ℕ.
. . . . | | | |   ∃t':ℕ.
. . . . | | | |   t≤t'
. . . . | | | |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . | | | |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . | | | |     ∨ P@0 != <[a]
. . . . | | | |              ,λx.P>(a@0) ==> ∀v:<[locl(a)]
. . . . | | | |                                 ,λx.T>(locl(a@0))?Top.
. . . . | | | |       ¬P@0((λx.s(i;t').x),v)
. . . . | | | 12. ∀t:ℕ.
. . . . | | | |   ¬isnull(a(i;t))
. . . . | | | |   ⇒
. . . . | | | |   (islocal(kind(a(i;t)))
. . . . | | | |    ⇒
. . . . | | | |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . | | | |    ⇒
. . . . | | | |    P((λx.s(i;t).x),val(a(i;t))))
. . . . | | | |   & (∀x:Id.
. . . . | | | |      deq-member(product-deq(Knd;Id;...;IdDeq);<...
. . . . | | | |                                                ,x>;1of(
. . . . | | | |                                                    ))
. . . . | | | |      ⇒
. . . . | | | |      s(i;t+1).x
. . . . | | | |      =
. . . . | | | |      2of()(<kind(a(i;t)),x>,λx.s(i;t).x,val(a(i;t))))
. . . . | | | |   & (∀l:IdLnk.
. . . . | | | |      deq-member(product-deq(Knd;...;...;...);<...
. . . . | | | |                                              ,l>;1of(
. . . . | | | |                                                  ))
. . . . | | | |      ⇒
. . . . | | | |      withlnk(l;m(i;t))
. . . . | | | |      =
. . . . | | | |      if source(l) = i→
. . . . | | | |         concat(map(λtgf.map(λx.
. . . . | | | |         <1of(tgf)
. . . . | | | |         ,x>;2of(tgf)
. . . . | | | |             ((λx.s(i;t).x)
. . . . | | | |             ,val(a(i;t))));2of()(<kind(a(i;t)),l>)))
. . . . | | | |      else nil fi)
. . . . | | | |   & (∀x:Id.
. . . . | | | |      ¬(deq-member(IdDeq;x;1of())
. . . . | | | |        ⇒
. . . . | | | |        deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . . . | | | |      ⇒
. . . . | | | |      s(i;t).x = s(i;t+1).x)
```

```
. . . . | | | |   & (∀l:IdLnk, tg:Id.
. . . . | | | |      ¬(deq-member(product-deq(...;Id;...;...);...;1of(
. . . . | | | |                                                    ))
. . . . | | | |        ⇒
. . . . | | | |        deq-member(KindDeq;kind(a(i;t));2of()(<l,tg>)))
. . . . | | | |      ⇒
. . . . | | | |      w-tagged(tg; onlnk(l;m(i;t))) = nil)

. . . . | | 13. ∀x:Id.
. . . . | | |   deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . . . | | 14. ∀a@0:Action(i).
. . . . | | |   ¬isnull(a@0)
. . . . | | |   ⇒
. . . . | | |   (valtype(i;a@0) ⊆r <[locl(a)],λx.T>(kind(a@0))?Top)
. . . . | | 15. ∀x:Id.
. . . . | | |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . . . | | |                      2of(ds)(x)
. . . . | | |                   else Top fi
. . . . | | 16. IdDeq ∈ EqDecider(Id)
. . . . | | 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . | | 18. j : Id
. . . . | | 19. t : ℕ
. . . . | | 20. j = i
. . . . | | 21. ¬isnull(a(j;t))
. . . . | | 22. ¬isnull(a(i;t))
. . . . | | 23. (λx.s(i;t).x) ∈ State(ds)
. . . . | | 24. kind(<j,t>) = locl(a)
. . . . | | ⊢  islocal(kind(a(i;t)))
. . . . | | | by Unfold ‘w-ekind‘ -1 THEN Unfold ‘w-act‘ -1
. . . . | | |    THEN
. . . . | | |    Reduce -1
. . . . | | |    THEN
. . . . | | |    StrongRevHypSubst -5 0
. . . . | | |    THEN
. . . . | | |    HypSubst -1 0
. . . . | | |
. . . . | | 1. i : Id
. . . . | | 2. a : Id
. . . . | | 3. T : Type
. . . . | | 4. ds : x:Id fp-> Type
. . . . | | 5. P : State(ds)→T→Prop
. . . . | | 6. w : World
. . . . | | 7. FairFifo
. . . . | | 8. FairFifo
. . . . | | 9. ∀l:IdLnk, tg:Id.
. . . . | | |   (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . | | |                     <ds
. . . . | | |                     ,<[locl(a)],λx.T>
. . . . | | |                     ,
. . . . | | |                     ,<[a],λx.P>
. . . . | | |                     ,
. . . . | | |                     ,
. . . . | | |                     ,
. . . . | | |                     ,
. . . . | | |                     ,·>
. . . . | | |                  else  fi.da(rcv(l; tg))
```

```
. . . . | | | 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . | | | 11. ∀a@0:Id, t:ℕ.
. . . . | | |     ∃t':ℕ.
. . . . | | |     t≤t'
. . . . | | |     & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . | | |       ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . | | |       ∨ P@0 != <[a]
. . . . | | |                ,λx.P>(a@0) ==> ∀v:<[locl(a)]
. . . . | | |                                ,λx.T>(locl(a@0))?Top.
. . . . | | |         ¬P@0((λx.s(i;t').x),v)
. . . . | | | 12. ∀t:ℕ.
. . . . | | |     ¬isnull(a(i;t))
. . . . | | |     ⇒
. . . . | | |     (islocal(kind(a(i;t)))
. . . . | | |      ⇒
. . . . | | |      (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . | | |      ⇒
. . . . | | |      P((λx.s(i;t).x),val(a(i;t))))
. . . . | | |     & (∀x:Id.
. . . . | | |        deq-member(product-deq(Knd;Id;...;IdDeq);<...
. . . . | | |                                                ,x>;1of(
. . . . | | |                                                    ))
. . . . | | |        ⇒
. . . . | | |        s(i;t+1).x
. . . . | | |        =
. . . . | | |        2of()(<kind(a(i;t)),x>,λx.s(i;t).x,val(a(i;t))))
. . . . | | |     & (∀l:IdLnk.
. . . . | | |        deq-member(product-deq(Knd;...;...;...);<...
. . . . | | |                                              ,l>;1of(
. . . . | | |                                                  ))
. . . . | | |        ⇒
. . . . | | |        withlnk(l;m(i;t))
. . . . | | |        =
. . . . | | |        if source(l) = i→
. . . . | | |           concat(map(λtgf.map(λx.
. . . . | | |           <1of(tgf)
. . . . | | |           ,x>;2of(tgf)
. . . . | | |               ((λx.s(i;t).x)
. . . . | | |               ,val(a(i;t))));2of()(<kind(a(i;t)),l>)))
. . . . | | |        else nil fi)
. . . . | | |     & (∀x:Id.
. . . . | | |        ¬(deq-member(IdDeq;x;1of())
. . . . | | |          ⇒
. . . . | | |          deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . . . | | |        ⇒
. . . . | | |        s(i;t).x = s(i;t+1).x)
. . . . | | |     & (∀l:IdLnk, tg:Id.
. . . . | | |        ¬(deq-member(product-deq(...;Id;...;...);...;1of(
. . . . | | |                                                  ))
. . . . | | |          ⇒
. . . . | | |          deq-member(KindDeq;kind(a(i;t));2of()(<l,tg>)))
. . . . | | |        ⇒
. . . . | | |        w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . | | | 13. ∀x:Id.
. . . . | | |     deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
```

```
. . . . | | | 14. ∀a@0:Action(i).
. . . . | | |     ¬isnull(a@0)
. . . . | | |     ⇒
. . . . | | |     (valtype(i;a@0) ⊆r <[locl(a)],λx.T>(kind(a@0))?Top)
. . . . | | | 15. ∀x:Id.
. . . . | | |     vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . . . | | |                       2of(ds)(x)
. . . . | | |                     else Top fi
. . . . | | | 16. IdDeq ∈ EqDecider(Id)
. . . . | | | 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . | | | 18. j : Id
. . . . | | | 19. t : ℕ
. . . . | | | 20. j = i
. . . . | | | 21. ¬isnull(a(j;t))
. . . . | | | 22. ¬isnull(a(i;t))
. . . . | | | 23. (λx.s(i;t).x) ∈ State(ds)
. . . . | | | 24. kind(a(j;t)) = locl(a)
. . . . | | | ⊢  islocal(locl(a))
. . . . | | |   by Unfolds [‘islocal‘;‘locl‘] 0 THEN Reduce 0
. . . . | | |      THEN
. . . . | | |      Trivial
. . . . | | |
. . . . | | .\
. . . . | | . 1. i : Id
. . . . | | . 2. a : Id
. . . . | | . 3. T : Type
. . . . | | . 4. ds : x:Id fp-> Type
. . . . | | . 5. P : State(ds)→T→Prop
. . . . | | . 6. w : World
. . . . | | . 7. FairFifo
. . . . | | . 8. FairFifo
. . . . | | . 9. ∀l:IdLnk, tg:Id.
. . . . | | . |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . | | . |                   <ds
. . . . | | . |                   ,<[locl(a)],λx.T>
. . . . | | . |                   ,
. . . . | | . |                   ,<[a],λx.P>
. . . . | | . |                   ,
. . . . | | . |                   ,
. . . . | | . |                   ,
. . . . | | . |                   ,
. . . . | | . |                   ,.>
. . . . | | . |                 else  fi.da(rcv(l; tg))
. . . . | | . 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . | | . 11. ∀a@0:Id, t:ℕ.
. . . . | | . |   ∃t':ℕ.
. . . . | | . |   t≤t'
. . . . | | . |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . | | . |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . | | . |     ∨ P@0 != <[a]
. . . . | | . |              ,λx.P>(a@0) ==> ∀v:<[locl(a)]
. . . . | | . |                                  ,λx.T>(locl(a@0))?Top.
. . . . | | . |       ¬P@0((λx.s(i;t').x),v)
. . . . | | . 12. ∀t:ℕ.
. . . . | | . |   ¬isnull(a(i;t))
```

```
. . . . | | . |   ⇒
. . . . | | . |   (islocal(kind(a(i;t)))
. . . . | | . |    ⇒
. . . . | | . |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . | | . |    ⇒
. . . . | | . |    P((λx.s(i;t).x),val(a(i;t))))
. . . . | | . |   & (∀x:Id.
. . . . | | . |      deq-member(product-deq(Knd;Id;...;IdDeq);<...
. . . . | | . |                                              ,x>;1of(
. . . . | | . |                                                  ))
. . . . | | . |      ⇒
. . . . | | . |      s(i;t+1).x
. . . . | | . |      =
. . . . | | . |      2of()(<kind(a(i;t)),x>,λx.s(i;t).x,val(a(i;t))))
. . . . | | . |   & (∀l:IdLnk.
. . . . | | . |      deq-member(product-deq(Knd;...;...;...);<...
. . . . | | . |                                            ,l>;1of(
. . . . | | . |                                               ))
. . . . | | . |      ⇒
. . . . | | . |      withlnk(l;m(i;t))
. . . . | | . |      =
. . . . | | . |      if source(l) = i→
. . . . | | . |         concat(map(λtgf.map(λx.
. . . . | | . |         <1of(tgf)
. . . . | | . |         ,x>;2of(tgf)
. . . . | | . |             ((λx.s(i;t).x)
. . . . | | . |             ,val(a(i;t))));2of()(<kind(a(i;t)),l>)))
. . . . | | . |      else nil fi)
. . . . | | . |   & (∀x:Id.
. . . . | | . |      ¬(deq-member(IdDeq;x;1of())
. . . . | | . |        ⇒
. . . . | | . |        deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . . . | | . |      ⇒
. . . . | | . |      s(i;t).x = s(i;t+1).x)
. . . . | | . |   & (∀l:IdLnk, tg:Id.
. . . . | | . |      ¬(deq-member(product-deq(...;Id;...;...);...;1of(
. . . . | | . |                                                  ))
. . . . | | . |        ⇒
. . . . | | . |        deq-member(KindDeq;kind(a(i;t));2of()(<l,tg>)))
. . . . | | . |      ⇒
. . . . | | . |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . | | . 13. ∀x:Id.
. . . . | | . |   deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . . . | | . 14. ∀a@0:Action(i).
. . . . | | . |   ¬isnull(a@0)
. . . . | | . |   ⇒
. . . . | | . |   (valtype(i;a@0) ⊆r <[locl(a)],λx.T>(kind(a@0))?Top)
. . . . | | . 15. ∀x:Id.
. . . . | | . |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . . . | | . |                        2of(ds)(x)
. . . . | | . |                   else Top fi
. . . . | | . 16. IdDeq ∈ EqDecider(Id)
. . . . | | . 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . | | . 18. j : Id
. . . . | | . 19. t : ℕ
```

```
. . . . | | . 20. j = i
. . . . | | . 21. ¬isnull(a(j;t))
. . . . | | . 22. ¬isnull(a(i;t))
. . . . | | . 23. (λx.s(i;t).x) ∈ State(ds)
. . . . | | . 24. kind(<j,t>) = locl(a)
. . . . | | . 25. (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . | | . |   ⇒
. . . . | | . |   P((λx.s(i;t).x),val(a(i;t)))
. . . . | | . ⊢  P((λz.s(j;t).z),val(a(j;t)))  by Analyze -1
. . . . | | . |
. . . . | | . |\
. . . . | | . | .....antecedent .....
. . . . | | . | 1. i : Id
. . . . | | . | 2. a : Id
. . . . | | . | 3. T : Type
. . . . | | . | 4. ds : x:Id fp-> Type
. . . . | | . | 5. P : State(ds)→T→Prop
. . . . | | . | 6. w : World
. . . . | | . | 7. FairFifo
. . . . | | . | 8. FairFifo
. . . . | | . | 9. ∀l:IdLnk, tg:Id.
. . . . | | . | |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . | | . | |                  <ds
. . . . | | . | |                  ,<[locl(a)],λx.T>
. . . . | | . | |                  ,
. . . . | | . | |                  ,<[a],λx.P>
. . . . | | . | |                  ,
. . . . | | . | |                  ,
. . . . | | . | |                  ,
. . . . | | . | |                  ,
. . . . | | . | |                  ,.>
. . . . | | . | |               else  fi.da(rcv(l; tg))
. . . . | | . | 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . | | . | 11. ∀a@0:Id, t:ℕ.
. . . . | | . | |   ∃t':ℕ.
. . . . | | . | |   t≤t'
. . . . | | . | |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . | | . | |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . | | . | |     ∨ P@0 != <[a]
. . . . | | . | |              ,λx.P>(a@0) ==> ∀v:<[locl(a)]
. . . . | | . | |                                ,λx.
. . . . | | . | |                                 T>(locl(a@0))?Top.
. . . . | | . | |       ¬P@0((λx.s(i;t').x),v)
. . . . | | . | 12. ∀t:ℕ.
. . . . | | . | |   ¬isnull(a(i;t))
. . . . | | . | |   ⇒
. . . . | | . | |   (islocal(kind(a(i;t)))
. . . . | | . | |    ⇒
. . . . | | . | |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . | | . | |    ⇒
. . . . | | . | |    P((λx.s(i;t).x),val(a(i;t))))
. . . . | | . | |   & (∀x:Id.
. . . . | | . | |      deq-member(product-deq(Knd;Id;...;...);<...
. . . . | | . | |                                          ,x>;1of(
. . . . | | . | |                                              ))
```

```
. . . . | | . | |      ⇒
. . . . | | . | |      s(i;t+1).x
. . . . | | . | |      =
. . . . | | . | |      2of()
. . . . | | . | |      (<kind(a(i;t)),x>
. . . . | | . | |      ,λx.s(i;t).x
. . . . | | . | |      ,val(a(i;t))))
. . . . | | . | |   & (∀l:IdLnk.
. . . . | | . | |      deq-member(...;<kind(a(i;t)),l>;1of())
. . . . | | . | |      ⇒
. . . . | | . | |      withlnk(l;m(i;t))
. . . . | | . | |      =
. . . . | | . | |      if source(l) = i→
. . . . | | . | |         concat(map(λtgf.map(λx.
. . . . | | . | |         <1of(tgf),x>;2of(tgf)
. . . . | | . | |                     ((λx.s(i;t).x)
. . . . | | . | |                     ,val(a(i;t))));2of()
. . . . | | . | |                                   (<kind(a(i;t))
. . . . | | . | |                                    ,l>)))
. . . . | | . | |      else nil fi)
. . . . | | . | |   & (∀x:Id.
. . . . | | . | |      ¬(deq-member(IdDeq;x;1of())
. . . . | | . | |        ⇒
. . . . | | . | |        deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . . . | | . | |      ⇒
. . . . | | . | |      s(i;t).x = s(i;t+1).x)
. . . . | | . | |   & (∀l:IdLnk, tg:Id.
. . . . | | . | |      ¬(deq-member(...;<l,tg>;1of())
. . . . | | . | |        ⇒
. . . . | | . | |        deq-member(KindDeq;kind(a(i;t));2of()
. . . . | | . | |                                     (<l,tg>)))
. . . . | | . | |      ⇒
. . . . | | . | |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . | | . | 13. ∀x:Id.
. . . . | | . | |   deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . . . | | . | 14. ∀a@0:Action(i).
. . . . | | . | |   ¬isnull(a@0)
. . . . | | . | |   ⇒
. . . . | | . | |   (valtype(i;a@0) ⊆r <[locl(a)]
. . . . | | . | |                     ,λx.T>(kind(a@0))?Top)
. . . . | | . | 15. ∀x:Id.
. . . . | | . | |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . . . | | . | |                      2of(ds)(x)
. . . . | | . | |                   else Top fi
. . . . | | . | 16. IdDeq ∈ EqDecider(Id)
. . . . | | . | 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . | | . | 18. j : Id
. . . . | | . | 19. t : ℕ
. . . . | | . | 20. j = i
. . . . | | . | 21. ¬isnull(a(j;t))
. . . . | | . | 22. ¬isnull(a(i;t))
. . . . | | . | 23. (λx.s(i;t).x) ∈ State(ds)
. . . . | | . | 24. kind(<j,t>) = locl(a)
. . . . | | . | ⊢  eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂
. . . . | | . | | by Unfold ‘w-ekind‘ -1 THEN Unfold ‘w-act‘ -1
```

```
. . . . | | . | |    THEN
. . . . | | . | |    Reduce -1
. . . . | | . | |
. . . . | | . | 1. i : Id
. . . . | | . | 2. a : Id
. . . . | | . | 3. T : Type
. . . . | | . | 4. ds : x:Id fp-> Type
. . . . | | . | 5. P : State(ds)→T→Prop
. . . . | | . | 6. w : World
. . . . | | . | 7. FairFifo
. . . . | | . | 8. FairFifo
. . . . | | . | 9. ∀l:IdLnk, tg:Id.
. . . . | | . | |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . | | . | |                    <ds
. . . . | | . | |                    ,<[locl(a)],λx.T>
. . . . | | . | |                    ,
. . . . | | . | |                    ,<[a],λx.P>
. . . . | | . | |                    ,
. . . . | | . | |                    ,
. . . . | | . | |                    ,
. . . . | | . | |                    ,
. . . . | | . | |                    ,·>
. . . . | | . | |                else  fi.da(rcv(l; tg))
. . . . | | . | 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . | | . | 11. ∀a@0:Id, t:ℕ.
. . . . | | . | |   ∃t':ℕ.
. . . . | | . | |   t≤t'
. . . . | | . | |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . | | . | |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . | | . | |     ∨ P@0 != <[a]
. . . . | | . | |              ,λx.P>(a@0) ==> ∀v:<[locl(a)]
. . . . | | . | |                                ,λx.
. . . . | | . | |                                 T>(locl(a@0))?Top.
. . . . | | . | |       ¬P@0((λx.s(i;t').x),v)
. . . . | | . | 12. ∀t:ℕ.
. . . . | | . | |   ¬isnull(a(i;t))
. . . . | | . | |   ⇒
. . . . | | . | |   (islocal(kind(a(i;t)))
. . . . | | . | |    ⇒
. . . . | | . | |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . | | . | |    ⇒
. . . . | | . | |    P((λx.s(i;t).x),val(a(i;t))))
. . . . | | . | |   & (∀x:Id.
. . . . | | . | |      deq-member(product-deq(Knd;Id;...;...);<...
. . . . | | . | |                                          ,x>;1of(
. . . . | | . | |                                              ))
. . . . | | . | |      ⇒
. . . . | | . | |      s(i;t+1).x
. . . . | | . | |      =
. . . . | | . | |      2of()
. . . . | | . | |      (<kind(a(i;t)),x>
. . . . | | . | |      ,λx.s(i;t).x
. . . . | | . | |      ,val(a(i;t))))
. . . . | | . | |   & (∀l:IdLnk.
. . . . | | . | |      deq-member(...;<kind(a(i;t)),l>;1of())
```

```
. . . . | | . | |      ⇒
. . . . | | . | |      withlnk(l;m(i;t))
. . . . | | . | |      =
. . . . | | . | |      if source(l) = i→
. . . . | | . | |         concat(map(λtgf.map(λx.
. . . . | | . | |         <1of(tgf),x>;2of(tgf)
. . . . | | . | |                      ((λx.s(i;t).x)
. . . . | | . | |                      ,val(a(i;t))));2of()
. . . . | | . | |                                    (<kind(a(i;t))
. . . . | | . | |                                     ,l>)))
. . . . | | . | |      else nil fi)
. . . . | | . | |   & (∀x:Id.
. . . . | | . | |      ¬(deq-member(IdDeq;x;1of())
. . . . | | . | |        ⇒
. . . . | | . | |        deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . . . | | . | |      ⇒
. . . . | | . | |      s(i;t).x = s(i;t+1).x)
. . . . | | . | |   & (∀l:IdLnk, tg:Id.
. . . . | | . | |      ¬(deq-member(...;<l,tg>;1of())
. . . . | | . | |        ⇒
. . . . | | . | |        deq-member(KindDeq;kind(a(i;t));2of()
. . . . | | . | |                                      (<l,tg>)))

. . . . | | . | |      ⇒
. . . . | | . | |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . | | . | 13. ∀x:Id.
. . . . | | . | |   deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . . . | | . | 14. ∀a@0:Action(i).
. . . . | | . | |   ¬isnull(a@0)
. . . . | | . | |   ⇒
. . . . | | . | |   (valtype(i;a@0) ⊆r <[locl(a)]
. . . . | | . | |                      ,λx.T>(kind(a@0))?Top)
. . . . | | . | 15. ∀x:Id.
. . . . | | . | |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . . . | | . | |                      2of(ds)(x)
. . . . | | . | |                   else Top fi
. . . . | | . | 16. IdDeq ∈ EqDecider(Id)
. . . . | | . | 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . | | . | 18. j : Id
. . . . | | . | 19. t : ℕ
. . . . | | . | 20. j = i
. . . . | | . | 21. ¬isnull(a(j;t))
. . . . | | . | 22. ¬isnull(a(i;t))
. . . . | | . | 23. (λx.s(i;t).x) ∈ State(ds)
. . . . | | . | 24. kind(a(j;t)) = locl(a)
. . . . | | . | ⊢  eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂
. . . . | | . | | by Subst (act(kind(a(i;t))) = a) 0
. . . . | | . | |
. . . . | | . | |\
. . . . | | . | | .....equality .....
. . . . | | . | | 1. i : Id
. . . . | | . | | 2. a : Id
. . . . | | . | | 3. T : Type
. . . . | | . | | 4. ds : x:Id fp-> Type
. . . . | | . | | 5. P : State(ds)→T→Prop
. . . . | | . | | 6. w : World
```

```
. . . . | | . | | 7. FairFifo
. . . . | | . | | 8. FairFifo
. . . . | | . | | 9. ∀l:IdLnk, tg:Id.
. . . . | | . | | |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . | | . | | |                   <ds
. . . . | | . | | |                   ,<[locl(a)],λx.T>
. . . . | | . | | |                   ,
. . . . | | . | | |                   ,<[a],λx.P>
. . . . | | . | | |                   ,
. . . . | | . | | |                   ,
. . . . | | . | | |                   ,
. . . . | | . | | |                   ,
. . . . | | . | | |                   ,.>
. . . . | | . | | |                 else  fi.da(rcv(l; tg))
. . . . | | . | | 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . | | . | | 11. ∀a@0:Id, t:ℕ.
. . . . | | . | | |   ∃t':ℕ.
. . . . | | . | | |   t≤t'
. . . . | | . | | |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . | | . | | |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . | | . | | |     ∨ P@0 != <[a]
. . . . | | . | | |              ,λx.
. . . . | | . | | |               P>(a@0) ==> ∀v:<[locl(a)]
. . . . | | . | | |                                ,λx.
. . . . | | . | | |                                 T>(locl(a@0))?Top.
. . . . | | . | | |       ¬P@0((λx.s(i;t').x),v)
. . . . | | . | | 12. ∀t:ℕ.
. . . . | | . | | |   ¬isnull(a(i;t))
. . . . | | . | | |   ⇒
. . . . | | . | | |   (islocal(kind(a(i;t)))
. . . . | | . | | |    ⇒
. . . . | | . | | |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . | | . | | |    ⇒
. . . . | | . | | |    P((λx.s(i;t).x),val(a(i;t))))
. . . . | | . | | |   & (∀x:Id.
. . . . | | . | | |      deq-member(...;<kind(a(i;t)),x>;1of())
. . . . | | . | | |      ⇒
. . . . | | . | | |      s(i;t+1).x
. . . . | | . | | |      =
. . . . | | . | | |      2of()
. . . . | | . | | |      (<kind(a(i;t)),x>
. . . . | | . | | |      ,λx.s(i;t).x
. . . . | | . | | |      ,val(a(i;t))))
. . . . | | . | | |   & (∀l:IdLnk.
. . . . | | . | | |      deq-member(...;<kind(a(i;t)),l>;1of())
. . . . | | . | | |      ⇒
. . . . | | . | | |      withlnk(l;m(i;t))
. . . . | | . | | |      =
. . . . | | . | | |      if source(l) = i→
. . . . | | . | | |         concat(map(λtgf.map(λx.
. . . . | | . | | |         <1of(tgf),x>;2of(tgf)
. . . . | | . | | |                      ((λx.s(i;t).x)
. . . . | | . | | |                      ,val(a(i;t))));2of()
. . . . | | . | | |                                    (<kind(a(i;t))
. . . . | | . | | |                                     ,l>)))
```

```
. . . . | | . | | |      else nil fi)
. . . . | | . | | |   & (∀x:Id.
. . . . | | . | | |      ¬(deq-member(IdDeq;x;1of())
. . . . | | . | | |        ⇒
. . . . | | . | | |        deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . . . | | . | | |      ⇒
. . . . | | . | | |      s(i;t).x = s(i;t+1).x)
. . . . | | . | | |   & (∀l:IdLnk, tg:Id.
. . . . | | . | | |      ¬(deq-member(...;<l,tg>;1of())
. . . . | | . | | |        ⇒
. . . . | | . | | |        deq-member(KindDeq;kind(a(i;t));2of()
. . . . | | . | | |                                        (<l,tg>)))
. . . . | | . | | |      ⇒
. . . . | | . | | |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . | | . | | 13. ∀x:Id.
. . . . | | . | | |   deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . . . | | . | | 14. ∀a@0:Action(i).
. . . . | | . | | |   ¬isnull(a@0)
. . . . | | . | | |   ⇒
. . . . | | . | | |   (valtype(i;a@0) ⊆r <[locl(a)]
. . . . | | . | | |                      ,λx.T>(kind(a@0))?Top)
. . . . | | . | | 15. ∀x:Id.
. . . . | | . | | |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . . . | | . | | |                      2of(ds)(x)
. . . . | | . | | |                   else Top fi
. . . . | | . | | 16. IdDeq ∈ EqDecider(Id)
. . . . | | . | | 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . | | . | | 18. j : Id
. . . . | | . | | 19. t : ℕ
. . . . | | . | | 20. j = i
. . . . | | . | | 21. ¬isnull(a(j;t))
. . . . | | . | | 22. ¬isnull(a(i;t))
. . . . | | . | | 23. (λx.s(i;t).x) ∈ State(ds)
. . . . | | . | | 24. kind(a(j;t)) = locl(a)
. . . . | | . | | ⊢  act(kind(a(i;t))) = a
. . . . | | . | |  by Subst (kind(a(j;t)) = kind(a(i;t))) -1
. . . . | | . | |
. . . . | | . | | \
. . . . | | . | |  .....equality .....
. . . . | | . | |  1. i : Id
. . . . | | . | |  2. a : Id
. . . . | | . | |  3. T : Type
. . . . | | . | |  4. ds : x:Id fp-> Type
. . . . | | . | |  5. P : State(ds)→T→Prop
. . . . | | . | |  6. w : World
. . . . | | . | |  7. FairFifo
. . . . | | . | |  8. FairFifo
. . . . | | . | |  9. ∀l:IdLnk, tg:Id.
. . . . | | . | |     (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . | | . | |                      <ds
. . . . | | . | |                      ,<[locl(a)],λx.T>
. . . . | | . | |                      ,
. . . . | | . | |                      ,<[a],λx.P>
. . . . | | . | |                      ,
. . . . | | . | |                      ,
```

```
. . . . | | . | | |                      ,
. . . . | | . | | |                      ,
. . . . | | . | | |                      ,·>
. . . . | | . | | |                   else  fi.da(rcv(l; tg))
. . . . | | . | | | 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . | | . | | | 11. ∀a@0:Id, t:ℕ.
. . . . | | . | | |     ∃t':ℕ.
. . . . | | . | | |     t≤t'
. . . . | | . | | |     & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . | | . | | |       ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . | | . | | |       ∨ P@0 != <[a]
. . . . | | . | | |                ,λx.
. . . . | | . | | |                 P>(a@0) ==> ∀v:<[locl(a)]
. . . . | | . | | |                                ,λx.
. . . . | | . | | |                                 T>(locl(a@0))?Top.
. . . . | | . | | |         ¬P@0((λx.s(i;t').x),v)
. . . . | | . | | | 12. ∀t:ℕ.
. . . . | | . | | |     ¬isnull(a(i;t))
. . . . | | . | | |     ⇒
. . . . | | . | | |     (islocal(kind(a(i;t)))
. . . . | | . | | |      ⇒
. . . . | | . | | |      (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . | | . | | |      ⇒
. . . . | | . | | |      P((λx.s(i;t).x),val(a(i;t))))
. . . . | | . | | |     & (∀x:Id.
. . . . | | . | | |        deq-member(...;<kind(a(i;t)),x>;1of())
. . . . | | . | | |        ⇒
. . . . | | . | | |        s(i;t+1).x
. . . . | | . | | |        =
. . . . | | . | | |        2of()
. . . . | | . | | |        (<kind(a(i;t)),x>
. . . . | | . | | |        ,λx.s(i;t).x
. . . . | | . | | |        ,val(a(i;t))))
. . . . | | . | | |     & (∀l:IdLnk.
. . . . | | . | | |        deq-member(...;<kind(a(i;t)),l>;1of())
. . . . | | . | | |        ⇒
. . . . | | . | | |        withlnk(l;m(i;t))
. . . . | | . | | |        =
. . . . | | . | | |        if source(l) = i→
. . . . | | . | | |           concat(map(λtgf.map(λx.
. . . . | | . | | |           <1of(tgf)
. . . . | | . | | |           ,x>;2of(tgf)
. . . . | | . | | |               ((λx.s(i;t).x)
. . . . | | . | | |               ,val(a(i;t))));2of()
. . . . | | . | | |                              (<kind(a(i;t)),l>)))
. . . . | | . | | |        else nil fi)
. . . . | | . | | |     & (∀x:Id.
. . . . | | . | | |        ¬(deq-member(IdDeq;x;1of())
. . . . | | . | | |          ⇒
. . . . | | . | | |          deq-member(KindDeq;kind(a(i;t));2of()
. . . . | | . | | |                                          (x)))
. . . . | | . | | |        ⇒
. . . . | | . | | |        s(i;t).x = s(i;t+1).x)
. . . . | | . | | |     & (∀l:IdLnk, tg:Id.
. . . . | | . | | |        ¬...
```

```
. . . . | | . | | |        ⇒
. . . . | | . | | |        w-tagged(tg; onlnk(l;m(i;t))) = nil)

. . . . | | . | | | 13. ∀x:Id.
. . . . | | . | | |     deq-member(IdDeq;x;1of())
. . . . | | . | | |     ⇒
. . . . | | . | | |     s(i;0).x = 2of()(x)
. . . . | | . | | | 14. ∀a@0:Action(i).
. . . . | | . | | |     ¬isnull(a@0)
. . . . | | . | | |     ⇒
. . . . | | . | | |     (valtype(i;a@0) ⊆r <[locl(a)]
. . . . | | . | | |                        ,λx.T>(kind(a@0))?Top)
. . . . | | . | | | 15. ∀x:Id.
. . . . | | . | | |     vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(
. . . . | | . | | |                                          ds))→
. . . . | | . | | |                        2of(ds)(x)
. . . . | | . | | |                      else Top fi
. . . . | | . | | | 16. IdDeq ∈ EqDecider(Id)
. . . . | | . | | | 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . | | . | | | 18. j : Id
. . . . | | . | | | 19. t : ℕ
. . . . | | . | | | 20. j = i
. . . . | | . | | | 21. ¬isnull(a(j;t))
. . . . | | . | | | 22. ¬isnull(a(i;t))
. . . . | | . | | | 23. (λx.s(i;t).x) ∈ State(ds)
. . . . | | . | | | 24. kind(a(j;t)) = locl(a)
. . . . | | . | | | ⊢  kind(a(j;t)) = kind(a(i;t))
. . . . | | . | | |   by Analyze THEN Analyze
. . . . | | . | | |
. . . . | | . | | .\
. . . . | | . | | . 1. i : Id
. . . . | | . | | . 2. a : Id
. . . . | | . | | . 3. T : Type
. . . . | | . | | . 4. ds : x:Id fp-> Type
. . . . | | . | | . 5. P : State(ds)→T→Prop
. . . . | | . | | . 6. w : World
. . . . | | . | | . 7. FairFifo
. . . . | | . | | . 8. FairFifo
. . . . | | . | | . 9. ∀l:IdLnk, tg:Id.
. . . . | | . | | . |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . | | . | | . |                    <ds
. . . . | | . | | . |                    ,<[locl(a)],λx.T>
. . . . | | . | | . |                    ,
. . . . | | . | | . |                    ,<[a],λx.P>
. . . . | | . | | . |                    ,
. . . . | | . | | . |                    ,
. . . . | | . | | . |                    ,
. . . . | | . | | . |                    ,
. . . . | | . | | . |                    ,.>
. . . . | | . | | . |                 else  fi.da(rcv(l; tg))
. . . . | | . | | . 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . | | . | | . 11. ∀a@0:Id, t:ℕ.
. . . . | | . | | . |   ∃t':ℕ.
. . . . | | . | | . |   t≤t'
. . . . | | . | | . |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . | | . | | . |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
```

```
. . . . | | . | | . |     ∨ P@0 != <[a]
. . . . | | . | | . |              ,λx.
. . . . | | . | | . |               P>(a@0) ==> ∀v:<[locl(a)]
. . . . | | . | | . |                                ,λx.
. . . . | | . | | . |                                 T>(locl(a@0))?Top.
. . . . | | . | | . |       ¬P@0((λx.s(i;t').x),v)
. . . . | | . | | . 12. ∀t:ℕ.
. . . . | | . | | . |   ¬isnull(a(i;t))
. . . . | | . | | . |   ⇒
. . . . | | . | | . |   (islocal(kind(a(i;t)))
. . . . | | . | | . |    ⇒
. . . . | | . | | . |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . | | . | | . |    ⇒
. . . . | | . | | . |    P((λx.s(i;t).x),val(a(i;t))))
. . . . | | . | | . |   & (∀x:Id.
. . . . | | . | | . |      deq-member(...;<kind(a(i;t)),x>;1of())
. . . . | | . | | . |      ⇒
. . . . | | . | | . |      s(i;t+1).x
. . . . | | . | | . |      =
. . . . | | . | | . |      2of()
. . . . | | . | | . |      (<kind(a(i;t)),x>
. . . . | | . | | . |      ,λx.s(i;t).x
. . . . | | . | | . |      ,val(a(i;t))))
. . . . | | . | | . |   & (∀l:IdLnk.
. . . . | | . | | . |      deq-member(...;<kind(a(i;t)),l>;1of())
. . . . | | . | | . |      ⇒
. . . . | | . | | . |      withlnk(l;m(i;t))
. . . . | | . | | . |      =
. . . . | | . | | . |      if source(l) = i→
. . . . | | . | | . |         concat(map(λtgf.map(λx.
. . . . | | . | | . |         <1of(tgf)
. . . . | | . | | . |         ,x>;2of(tgf)
. . . . | | . | | . |             ((λx.s(i;t).x)
. . . . | | . | | . |             ,val(a(i;t))));2of()
. . . . | | . | | . |                              (<kind(a(i;t)),l>)))
. . . . | | . | | . |      else nil fi)
. . . . | | . | | . |   & (∀x:Id.
. . . . | | . | | . |      ¬(deq-member(IdDeq;x;1of())
. . . . | | . | | . |        ⇒
. . . . | | . | | . |        deq-member(KindDeq;kind(a(i;t));2of()
. . . . | | . | | . |                                        (x)))
. . . . | | . | | . |      ⇒
. . . . | | . | | . |      s(i;t).x = s(i;t+1).x)
. . . . | | . | | . |   & (∀l:IdLnk, tg:Id.
. . . . | | . | | . |      ¬...
. . . . | | . | | . |      ⇒
. . . . | | . | | . |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . | | . | | . 13. ∀x:Id.
. . . . | | . | | . |   deq-member(IdDeq;x;1of())
. . . . | | . | | . |   ⇒
. . . . | | . | | . |   s(i;0).x = 2of()(x)
. . . . | | . | | . 14. ∀a@0:Action(i).
. . . . | | . | | . |   ¬isnull(a@0)
. . . . | | . | | . |   ⇒
. . . . | | . | | . |   (valtype(i;a@0) ⊆r <[locl(a)]
```

```
. . . . | | . | | . |                      ,λx.T>(kind(a@0))?Top)
. . . . | | . | | . 15. ∀x:Id.
. . . . | | . | | . |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(
. . . . | | . | | . |                                        ds))→
. . . . | | . | | . |                    2of(ds)(x)
. . . . | | . | | . |                  else Top fi
. . . . | | . | | . 16. IdDeq ∈ EqDecider(Id)
. . . . | | . | | . 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . | | . | | . 18. j : Id
. . . . | | . | | . 19. t : ℕ
. . . . | | . | | . 20. j = i
. . . . | | . | | . 21. ¬isnull(a(j;t))
. . . . | | . | | . 22. ¬isnull(a(i;t))
. . . . | | . | | . 23. (λx.s(i;t).x) ∈ State(ds)
. . . . | | . | | . 24. kind(a(i;t)) = locl(a)
. . . . | | . | | . ⊢  act(kind(a(i;t))) = a
. . . . | | . | | . | by MoveToConcl -1
. . . . | | . | | . |    THEN
. . . . | | . | | . |    GenConcl (kind(a(i;t)) = k)
. . . . | | . | | . |
. . . . | | . | | . 1. i : Id
. . . . | | . | | . 2. a : Id
. . . . | | . | | . 3. T : Type
. . . . | | . | | . 4. ds : x:Id fp-> Type
. . . . | | . | | . 5. P : State(ds)→T→Prop
. . . . | | . | | . 6. w : World
. . . . | | . | | . 7. FairFifo
. . . . | | . | | . 8. FairFifo
. . . . | | . | | . 9. ∀l:IdLnk, tg:Id.
. . . . | | . | | . |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . | | . | | . |                    <ds
. . . . | | . | | . |                    ,<[locl(a)],λx.T>
. . . . | | . | | . |                    ,
. . . . | | . | | . |                    ,<[a],λx.P>
. . . . | | . | | . |                    ,
. . . . | | . | | . |                    ,
. . . . | | . | | . |                    ,
. . . . | | . | | . |                    ,
. . . . | | . | | . |                    ,·>
. . . . | | . | | . |                 else  fi.da(rcv(l; tg))
. . . . | | . | | . 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . | | . | | . 11. ∀a@0:Id, t:ℕ.
. . . . | | . | | . |   ∃t':ℕ.
. . . . | | . | | . |   t≤t'
. . . . | | . | | . |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . | | . | | . |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . | | . | | . |     ∨ P@0 != <[a]
. . . . | | . | | . |              ,λx.
. . . . | | . | | . |               P>(a@0) ==> ∀v:<[locl(a)]
. . . . | | . | | . |                                ,λx.
. . . . | | . | | . |                                 T>(locl(a@0))?Top.
. . . . | | . | | . |       ¬P@0((λx.s(i;t').x),v)
. . . . | | . | | . 12. ∀t:ℕ.
. . . . | | . | | . |   ¬isnull(a(i;t))
. . . . | | . | | . |   ⇒
```

```
. . . . | | . | | . |   (islocal(kind(a(i;t)))
. . . . | | . | | . |    ⇒
. . . . | | . | | . |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . | | . | | . |    ⇒
. . . . | | . | | . |    P((λx.s(i;t).x),val(a(i;t))))
. . . . | | . | | . |   & (∀x:Id.
. . . . | | . | | . |      deq-member(...;<kind(a(i;t)),x>;1of())
. . . . | | . | | . |      ⇒
. . . . | | . | | . |      s(i;t+1).x
. . . . | | . | | . |      =
. . . . | | . | | . |      2of()
. . . . | | . | | . |      (<kind(a(i;t)),x>
. . . . | | . | | . |      ,λx.s(i;t).x
. . . . | | . | | . |      ,val(a(i;t))))
. . . . | | . | | . |   & (∀l:IdLnk.
. . . . | | . | | . |      deq-member(...;<kind(a(i;t)),l>;1of())
. . . . | | . | | . |      ⇒
. . . . | | . | | . |      withlnk(l;m(i;t))
. . . . | | . | | . |      =
. . . . | | . | | . |      if source(l) = i→
. . . . | | . | | . |         concat(map(λtgf.map(λx.
. . . . | | . | | . |         <1of(tgf)
. . . . | | . | | . |         ,x>;2of(tgf)
. . . . | | . | | . |             ((λx.s(i;t).x)
. . . . | | . | | . |             ,val(a(i;t))));2of()
. . . . | | . | | . |                              (<kind(a(i;t)),l>)))
. . . . | | . | | . |      else nil fi)
. . . . | | . | | . |   & (∀x:Id.
. . . . | | . | | . |      ¬(deq-member(IdDeq;x;1of())
. . . . | | . | | . |        ⇒
. . . . | | . | | . |        deq-member(KindDeq;kind(a(i;t));2of()
. . . . | | . | | . |                                          (x)))
. . . . | | . | | . |      ⇒
. . . . | | . | | . |      s(i;t).x = s(i;t+1).x)
. . . . | | . | | . |   & (∀l:IdLnk, tg:Id.
. . . . | | . | | . |      ¬...
. . . . | | . | | . |      ⇒

. . . . | | . | | . |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . | | . | | . 13. ∀x:Id.
. . . . | | . | | . |   deq-member(IdDeq;x;1of())
. . . . | | . | | . |   ⇒
. . . . | | . | | . |   s(i;0).x = 2of()(x)
. . . . | | . | | . 14. ∀a@0:Action(i).
. . . . | | . | | . |   ¬isnull(a@0)
. . . . | | . | | . |   ⇒
. . . . | | . | | . |   (valtype(i;a@0) ⊆r <[locl(a)]
. . . . | | . | | . |                       ,λx.T>(kind(a@0))?Top)
. . . . | | . | | . 15. ∀x:Id.
. . . . | | . | | . |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(
. . . . | | . | | . |                                          ds))→
. . . . | | . | | . |                      2of(ds)(x)
. . . . | | . | | . |                   else Top fi
. . . . | | . | | . 16. IdDeq ∈ EqDecider(Id)
. . . . | | . | | . 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . | | . | | . 18. j : Id
```

```
. . . . | | . | | . 19. t : ℕ
. . . . | | . | | . 20. j = i
. . . . | | . | | . 21. ¬isnull(a(j;t))
. . . . | | . | | . 22. ¬isnull(a(i;t))
. . . . | | . | | . 23. (λx.s(i;t).x) ∈ State(ds)
. . . . | | . | | . 24. k : Knd
. . . . | | . | | . 25. kind(a(i;t)) = k
. . . . | | . | | . ⊢  k = locl(a) ⇒ act(k) = a  by Analyze -2
. . . . | | . | | . |
. . . . | | . | | . |\
. . . . | | . | | . | 1. i : Id
. . . . | | . | | . | 2. a : Id
. . . . | | . | | . | 3. T : Type
. . . . | | . | | . | 4. ds : x:Id fp-> Type
. . . . | | . | | . | 5. P : State(ds)→T→Prop
. . . . | | . | | . | 6. w : World
. . . . | | . | | . | 7. FairFifo
. . . . | | . | | . | 8. FairFifo
. . . . | | . | | . | 9. ∀l:IdLnk, tg:Id.
. . . . | | . | | . | |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . | | . | | . | |                    <ds
. . . . | | . | | . | |                    ,<[locl(a)],λx.T>
. . . . | | . | | . | |                    ,
. . . . | | . | | . | |                    ,<[a],λx.P>
. . . . | | . | | . | |                    ,
. . . . | | . | | . | |                    ,
. . . . | | . | | . | |                    ,
. . . . | | . | | . | |                    ,
. . . . | | . | | . | |                    ,·>
. . . . | | . | | . | |                 else  fi.da(rcv(l; tg))
. . . . | | . | | . | 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . | | . | | . | 11. ∀a@0:Id, t:ℕ.
. . . . | | . | | . | |   ∃t':ℕ.
. . . . | | . | | . | |   t≤t'
. . . . | | . | | . | |   & ¬isnull(a(i;t'))
. . . . | | . | | . | |     & kind(a(i;t')) = locl(a@0)
. . . . | | . | | . | |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . | | . | | . | |     ∨ P@0 != <[a]
. . . . | | . | | . | |              ,λx.
. . . . | | . | | . | |               P>(a@0) ==> ∀v:<[locl(a)]
. . . . | | . | | . | |                                ,λx.
. . . . | | . | | . | |                                 T>(...)?Top.
. . . . | | . | | . | |       ¬P@0((λx.s(i;t').x),v)
. . . . | | . | | . | 12. ∀t:ℕ.
. . . . | | . | | . | |   ¬isnull(a(i;t))
. . . . | | . | | . | |   ⇒
. . . . | | . | | . | |   (islocal(kind(a(i;t)))
. . . . | | . | | . | |    ⇒
. . . . | | . | | . | |    (eqof(IdDeq)(a,act(kind(a(i;t))))
. . . . | | . | | . | |     ∨₂ false₂)
. . . . | | . | | . | |    ⇒
. . . . | | . | | . | |    P((λx.s(i;t).x),val(a(i;t))))
. . . . | | . | | . | |   & (∀x:Id.
. . . . | | . | | . | |      deq-member(...;<kind(a(i;t)),x>;1of())
. . . . | | . | | . | |      ⇒
```

```
. . . . | | . | | . | |      s(i;t+1).x
. . . . | | . | | . | |      =
. . . . | | . | | . | |      2of()
. . . . | | . | | . | |      (<kind(a(i;t)),x>
. . . . | | . | | . | |      ,λx.s(i;t).x
. . . . | | . | | . | |      ,val(a(i;t))))
. . . . | | . | | . | |   & (∀l:IdLnk.
. . . . | | . | | . | |      deq-member(...;<kind(a(i;t)),l>;1of())
. . . . | | . | | . | |      ⇒
. . . . | | . | | . | |      withlnk(l;m(i;t))
. . . . | | . | | . | |      =
. . . . | | . | | . | |      if source(l) = i→
. . . . | | . | | . | |         concat(map(λtgf.map(λx.
. . . . | | . | | . | |         <1of(tgf)
. . . . | | . | | . | |         ,x>;2of(tgf)
. . . . | | . | | . | |             ((λx.s(i;t).x)
. . . . | | . | | . | |             ,val(a(i;t))));...))
. . . . | | . | | . | |      else nil fi)
. . . . | | . | | . | |   & (∀x:Id.
. . . . | | . | | . | |      ¬(deq-member(IdDeq;x;1of())
. . . . | | . | | . | |        ⇒
. . . . | | . | | . | |        deq-member(KindDeq;kind(a(i;t));2of()
. . . . | | . | | . | |                                        (x)))
. . . . | | . | | . | |      ⇒
. . . . | | . | | . | |      s(i;t).x = s(i;t+1).x)
. . . . | | . | | . | |   & (∀l:IdLnk, tg:Id.
. . . . | | . | | . | |      ¬(deq-member(...;<l,tg>;1of())
. . . . | | . | | . | |        ⇒
. . . . | | . | | . | |        deq-member(KindDeq;kind(a(i;t));...))
. . . . | | . | | . | |      ⇒
. . . . | | . | | . | |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . | | . | | . | 13. ∀x:Id.
. . . . | | . | | . | |   deq-member(IdDeq;x;1of())
. . . . | | . | | . | |   ⇒
. . . . | | . | | . | |   s(i;0).x = 2of()(x)
. . . . | | . | | . | 14. ∀a@0:Action(i).
. . . . | | . | | . | |   ¬isnull(a@0)
. . . . | | . | | . | |   ⇒
. . . . | | . | | . | |   (valtype(i;a@0) ⊆r <[locl(a)]
. . . . | | . | | . | |                      ,λx.T>(kind(a@0))?Top)
. . . . | | . | | . | 15. ∀x:Id.
. . . . | | . | | . | |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(
. . . . | | . | | . | |                                        ds))→
. . . . | | . | | . | |                      2of(ds)(x)
. . . . | | . | | . | |                   else Top fi
. . . . | | . | | . | 16. IdDeq ∈ EqDecider(Id)
. . . . | | . | | . | 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . | | . | | . | 18. j : Id
. . . . | | . | | . | 19. t : ℕ
. . . . | | . | | . | 20. j = i
. . . . | | . | | . | 21. ¬isnull(a(j;t))
. . . . | | . | | . | 22. ¬isnull(a(i;t))
. . . . | | . | | . | 23. (λx.s(i;t).x) ∈ State(ds)
. . . . | | . | | . | 24. x : IdLnk×Id
. . . . | | . | | . | 25. kind(a(i;t)) = inl(x)
```

```
. . . . | | . | | . | ⊢  inl(x) = locl(a) ⇒ act(inl(x)) = a
. . . . | | . | | . | | by Analyze -2 THEN Fold ‘rcv‘ 0
. . . . | | . | | . | |
. . . . | | . | | . | 1. i : Id
. . . . | | . | | . | 2. a : Id
. . . . | | . | | . | 3. T : Type
. . . . | | . | | . | 4. ds : x:Id fp-> Type
. . . . | | . | | . | 5. P : State(ds)→T→Prop
. . . . | | . | | . | 6. w : World
. . . . | | . | | . | 7. FairFifo
. . . . | | . | | . | 8. FairFifo
. . . . | | . | | . | 9. ∀l:IdLnk, tg:Id.
. . . . | | . | | . | |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . | | . | | . | |                    <ds
. . . . | | . | | . | |                    ,<[locl(a)],λx.T>
. . . . | | . | | . | |                    ,
. . . . | | . | | . | |                    ,<[a],λx.P>
. . . . | | . | | . | |                    ,
. . . . | | . | | . | |                    ,
. . . . | | . | | . | |                    ,
. . . . | | . | | . | |                    ,
. . . . | | . | | . | |                    ,·>
. . . . | | . | | . | |                else  fi.da(rcv(l; tg))
. . . . | | . | | . | 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . | | . | | . | 11. ∀a@0:Id, t:ℕ.
. . . . | | . | | . | |   ∃t’:ℕ.
. . . . | | . | | . | |   t≤t’
. . . . | | . | | . | |   & ¬isnull(a(i;t’))
. . . . | | . | | . | |     & kind(a(i;t’)) = locl(a@0)
. . . . | | . | | . | |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . | | . | | . | |     ∨ P@0 != <[a]
. . . . | | . | | . | |              ,λx.
. . . . | | . | | . | |               P>(a@0) ==> ∀v:<[locl(a)]
. . . . | | . | | . | |                                ,λx.
. . . . | | . | | . | |                                 T>(...)?Top.
. . . . | | . | | . | |       ¬P@0((λx.s(i;t’).x),v)
. . . . | | . | | . | 12. ∀t:ℕ.
. . . . | | . | | . | |   ¬isnull(a(i;t))
. . . . | | . | | . | |   ⇒
. . . . | | . | | . | |   (islocal(kind(a(i;t)))
. . . . | | . | | . | |    ⇒
. . . . | | . | | . | |    (eqof(IdDeq)(a,act(kind(a(i;t))))
. . . . | | . | | . | |     ∨₂ false₂)
. . . . | | . | | . | |    ⇒
. . . . | | . | | . | |    P((λx.s(i;t).x),val(a(i;t))))
. . . . | | . | | . | |   & (∀x:Id.
. . . . | | . | | . | |      deq-member(...;<kind(a(i;t)),x>;1of())
. . . . | | . | | . | |      ⇒
. . . . | | . | | . | |      s(i;t+1).x
. . . . | | . | | . | |      =
. . . . | | . | | . | |      2of()
. . . . | | . | | . | |      (<kind(a(i;t)),x>
. . . . | | . | | . | |      ,λx.s(i;t).x
. . . . | | . | | . | |      ,val(a(i;t))))
. . . . | | . | | . | |   & (∀l:IdLnk.
```

```
. . . . | | . | | . | |      deq-member(...;<kind(a(i;t)),l>;1of())
. . . . | | . | | . | |      ⇒
. . . . | | . | | . | |      withlnk(l;m(i;t))
. . . . | | . | | . | |      =
. . . . | | . | | . | |      if source(l) = i→
. . . . | | . | | . | |         concat(map(λtgf.map(λx.
. . . . | | . | | . | |         <1of(tgf)
. . . . | | . | | . | |         ,x>;2of(tgf)
. . . . | | . | | . | |             ((λx.s(i;t).x)
. . . . | | . | | . | |             ,val(a(i;t))));...))
. . . . | | . | | . | |      else nil fi)
. . . . | | . | | . | |   & (∀x:Id.
. . . . | | . | | . | |      ¬(deq-member(IdDeq;x;1of())
. . . . | | . | | . | |        ⇒
. . . . | | . | | . | |        deq-member(KindDeq;kind(a(i;t));2of()
. . . . | | . | | . | |                                        (x)))
. . . . | | . | | . | |      ⇒

. . . . | | . | | . | |      s(i;t).x = s(i;t+1).x)
. . . . | | . | | . | |   & (∀l:IdLnk, tg:Id.
. . . . | | . | | . | |      ¬(deq-member(...;<l,tg>;1of())
. . . . | | . | | . | |        ⇒
. . . . | | . | | . | |        deq-member(KindDeq;kind(a(i;t));...))
. . . . | | . | | . | |      ⇒
. . . . | | . | | . | |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . | | . | | . | 13. ∀x:Id.
. . . . | | . | | . | |   deq-member(IdDeq;x;1of())
. . . . | | . | | . | |   ⇒
. . . . | | . | | . | |   s(i;0).x = 2of()(x)
. . . . | | . | | . | 14. ∀a@0:Action(i).
. . . . | | . | | . | |   ¬isnull(a@0)
. . . . | | . | | . | |   ⇒
. . . . | | . | | . | |   (valtype(i;a@0) ⊆r <[locl(a)]
. . . . | | . | | . | |                      ,λx.T>(kind(a@0))?Top)
. . . . | | . | | . | 15. ∀x:Id.
. . . . | | . | | . | |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(
. . . . | | . | | . | |                                        ds))→
. . . . | | . | | . | |                     2of(ds)(x)
. . . . | | . | | . | |                  else Top fi
. . . . | | . | | . | 16. IdDeq ∈ EqDecider(Id)
. . . . | | . | | . | 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . | | . | | . | 18. j : Id
. . . . | | . | | . | 19. t : ℕ
. . . . | | . | | . | 20. j = i
. . . . | | . | | . | 21. ¬isnull(a(j;t))
. . . . | | . | | . | 22. ¬isnull(a(i;t))
. . . . | | . | | . | 23. (λx.s(i;t).x) ∈ State(ds)
. . . . | | . | | . | 24. x1 : IdLnk
. . . . | | . | | . | 25. x2 : Id
. . . . | | . | | . | 26. kind(a(i;t)) = inl(<x1,x2>)
. . . . | | . | | . | ⊢  rcv(x1; x2) = locl(a) ⇒ act(rcv(x1; x2)) = a
. . . . | | . | | . | | by Auto
. . . . | | . | | . | |
. . . . | | . | | . | 1. i : Id
. . . . | | . | | . | 2. a : Id
. . . . | | . | | . | 3. T : Type
```

```
. . . . | | . | | . | 4. ds : x:Id fp-> Type
. . . . | | . | | . | 5. P : State(ds)→T→Prop
. . . . | | . | | . | 6. w : World
. . . . | | . | | . | 7. FairFifo
. . . . | | . | | . | 8. FairFifo
. . . . | | . | | . | 9. ∀l:IdLnk, tg:Id.
. . . . | | . | | . |    (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . | | . | | . |                       <ds
. . . . | | . | | . |                       ,<[locl(a)],λx.T>
. . . . | | . | | . |                       ,
. . . . | | . | | . |                       ,<[a],λx.P>
. . . . | | . | | . |                       ,
. . . . | | . | | . |                       ,
. . . . | | . | | . |                       ,
. . . . | | . | | . |                       ,
. . . . | | . | | . |                       ,·>
. . . . | | . | | . |                    else  fi.da(rcv(l; tg))
. . . . | | . | | . | 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . | | . | | . | 11. ∀a@0:Id, t:ℕ.
. . . . | | . | | . |     ∃t':ℕ.
. . . . | | . | | . |     t≤t'
. . . . | | . | | . |     & ¬isnull(a(i;t'))
. . . . | | . | | . |       & kind(a(i;t')) = locl(a@0)
. . . . | | . | | . |       ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . | | . | | . |       ∨ P@0 != <[a]
. . . . | | . | | . |                ,λx.
. . . . | | . | | . |                 P>(a@0) ==> ∀v:<[locl(a)]
. . . . | | . | | . |                                ,λx.
. . . . | | . | | . |                                 T>(...)?Top.
. . . . | | . | | . |          ¬P@0((λx.s(i;t').x),v)
. . . . | | . | | . | 12. ∀t:ℕ.
. . . . | | . | | . |     ¬isnull(a(i;t))
. . . . | | . | | . |     ⇒
. . . . | | . | | . |     (islocal(kind(a(i;t)))
. . . . | | . | | . |      ⇒
. . . . | | . | | . |      (eqof(IdDeq)(a,act(kind(a(i;t))))
. . . . | | . | | . |       ∨₂ false₂)
. . . . | | . | | . |      ⇒
. . . . | | . | | . |      P((λx.s(i;t).x),val(a(i;t))))
. . . . | | . | | . |     & (∀x:Id.
. . . . | | . | | . |        deq-member(...;<kind(a(i;t)),x>;1of())
. . . . | | . | | . |        ⇒
. . . . | | . | | . |        s(i;t+1).x
. . . . | | . | | . |        =
. . . . | | . | | . |        2of()
. . . . | | . | | . |        (<kind(a(i;t)),x>
. . . . | | . | | . |        ,λx.s(i;t).x
. . . . | | . | | . |        ,val(a(i;t))))
. . . . | | . | | . |     & (∀l:IdLnk.
. . . . | | . | | . |        deq-member(...;<kind(a(i;t)),l>;1of())
. . . . | | . | | . |        ⇒
. . . . | | . | | . |        withlnk(l;m(i;t))
. . . . | | . | | . |        =
. . . . | | . | | . |        if source(l) = i→
. . . . | | . | | . |           concat(map(λtgf.map(λx.
```

```
. . . . | | . | | . |           <1of(tgf)
. . . . | | . | | . |           ,x>;2of(tgf)
. . . . | | . | | . |               ((λx.s(i;t).x)
. . . . | | . | | . |               ,val(a(i;t))));...))
. . . . | | . | | . |       else nil fi)
. . . . | | . | | . |    & (∀x:Id.
. . . . | | . | | . |       ¬(deq-member(IdDeq;x;1of())
. . . . | | . | | . |         ⇒
. . . . | | . | | . |         deq-member(KindDeq;kind(a(i;t));2of()
. . . . | | . | | . |                                        (x)))
. . . . | | . | | . |       ⇒
. . . . | | . | | . |       s(i;t).x = s(i;t+1).x)
. . . . | | . | | . |    & (∀l:IdLnk, tg:Id.
. . . . | | . | | . |       ¬(deq-member(...;<l,tg>;1of())
. . . . | | . | | . |         ⇒
. . . . | | . | | . |         deq-member(KindDeq;kind(a(i;t));...))
. . . . | | . | | . |       ⇒
. . . . | | . | | . |       w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . | | . | | . | 13. ∀x:Id.
. . . . | | . | | . |     deq-member(IdDeq;x;1of())
. . . . | | . | | . |     ⇒
. . . . | | . | | . |     s(i;0).x = 2of()(x)
. . . . | | . | | . | 14. ∀a@0:Action(i).
. . . . | | . | | . |     ¬isnull(a@0)
. . . . | | . | | . |     ⇒
. . . . | | . | | . |     (valtype(i;a@0) ⊆r <[locl(a)]
. . . . | | . | | . |                          ,λx.T>(kind(a@0))?Top)
. . . . | | . | | . | 15. ∀x:Id.
. . . . | | . | | . |     vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(
. . . . | | . | | . |                                          ds))→
. . . . | | . | | . |                        2of(ds)(x)
. . . . | | . | | . |                     else Top fi
. . . . | | . | | . | 16. IdDeq ∈ EqDecider(Id)
. . . . | | . | | . | 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . | | . | | . | 18. j : Id
. . . . | | . | | . | 19. t : ℕ
. . . . | | . | | . | 20. j = i
. . . . | | . | | . | 21. ¬isnull(a(j;t))
. . . . | | . | | . | 22. ¬isnull(a(i;t))
. . . . | | . | | . | 23. (λx.s(i;t).x) ∈ State(ds)
. . . . | | . | | . | 24. x1 : IdLnk
. . . . | | . | | . | 25. x2 : Id
. . . . | | . | | . | 26. kind(a(i;t)) = inl(<x1,x2>)
. . . . | | . | | . | 27. rcv(x1; x2) = locl(a)
. . . . | | . | | . | ⊢ act(rcv(x1; x2)) = a
. . . . | | . | | . |   by FwdThru
. . . . | | . | | . |      Thm* ∀a:Id, l:IdLnk, tg:Id.
. . . . | | . | | . |           rcv(l; tg) = locl(a) ⇒ False
. . . . | | . | | . |      {not_rcv_locl}
. . . . | | . | | . |      [-1]
. . . . | | . | | . |
. . . . | | . | | . .\
. . . . | | . | | . . 1. i : Id
. . . . | | . | | . . 2. a : Id
. . . . | | . | | . . 3. T : Type
```

```
. . . . | | . | | . . 4. ds : x:Id fp-> Type
. . . . | | . | | . . 5. P : State(ds)→T→Prop
. . . . | | . | | . . 6. w : World
. . . . | | . | | . . 7. FairFifo
. . . . | | . | | . . 8. FairFifo
. . . . | | . | | . . 9. ∀l:IdLnk, tg:Id.
. . . . | | . | | . . |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . | | . | | . . |                  <ds
. . . . | | . | | . . |                  ,<[locl(a)],λx.T>
. . . . | | . | | . . |                  ,
. . . . | | . | | . . |                  ,<[a],λx.P>
. . . . | | . | | . . |                  ,
. . . . | | . | | . . |                  ,
. . . . | | . | | . . |                  ,
. . . . | | . | | . . |                  ,
. . . . | | . | | . . |                  ,·>
. . . . | | . | | . . |               else  fi.da(rcv(l; tg))
. . . . | | . | | . . 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . | | . | | . . 11. ∀a@0:Id, t:ℕ.
. . . . | | . | | . . |   ∃t':ℕ.
. . . . | | . | | . . |   t≤t'
. . . . | | . | | . . |   & ¬isnull(a(i;t'))
. . . . | | . | | . . |     & kind(a(i;t')) = locl(a@0)
. . . . | | . | | . . |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . | | . | | . . |     ∨ P@0 != <[a]
. . . . | | . | | . . |              ,λx.
. . . . | | . | | . . |               P>(a@0) ==> ∀v:<[locl(a)]
. . . . | | . | | . . |                                ,λx.
. . . . | | . | | . . |                                 T>(...)?Top.
. . . . | | . | | . . |       ¬P@0((λx.s(i;t').x),v)
. . . . | | . | | . . 12. ∀t:ℕ.
. . . . | | . | | . . |   ¬isnull(a(i;t))
. . . . | | . | | . . |   ⇒
. . . . | | . | | . . |   (islocal(kind(a(i;t)))
. . . . | | . | | . . |    ⇒
. . . . | | . | | . . |    (eqof(IdDeq)(a,act(kind(a(i;t))))
. . . . | | . | | . . |     ∨₂ false₂)
. . . . | | . | | . . |    ⇒
. . . . | | . | | . . |    P((λx.s(i;t).x),val(a(i;t))))
. . . . | | . | | . . |   & (∀x:Id.
. . . . | | . | | . . |      deq-member(...;<kind(a(i;t)),x>;1of())
. . . . | | . | | . . |      ⇒
. . . . | | . | | . . |      s(i;t+1).x
. . . . | | . | | . . |      =
. . . . | | . | | . . |      2of()
. . . . | | . | | . . |      (<kind(a(i;t)),x>
. . . . | | . | | . . |      ,λx.s(i;t).x
. . . . | | . | | . . |      ,val(a(i;t))))
. . . . | | . | | . . |   & (∀l:IdLnk.
. . . . | | . | | . . |      deq-member(...;<kind(a(i;t)),l>;1of())
. . . . | | . | | . . |      ⇒
. . . . | | . | | . . |      withlnk(l;m(i;t))
. . . . | | . | | . . |      =
. . . . | | . | | . . |      if source(l) = i→
. . . . | | . | | . . |         concat(map(λtgf.map(λx.
```

```
. . . . | | . | | . . |         <1of(tgf)
. . . . | | . | | . . |         ,x>;2of(tgf)
. . . . | | . | | . . |             ((λx.s(i;t).x)
. . . . | | . | | . . |             ,val(a(i;t))));...))
. . . . | | . | | . . |      else nil fi)
. . . . | | . | | . . |   & (∀x:Id.
. . . . | | . | | . . |      ¬(deq-member(IdDeq;x;1of())
. . . . | | . | | . . |        ⇒
. . . . | | . | | . . |        deq-member(KindDeq;kind(a(i;t));2of()
. . . . | | . | | . . |                                        (x)))
. . . . | | . | | . . |      ⇒
. . . . | | . | | . . |      s(i;t).x = s(i;t+1).x)
. . . . | | . | | . . |   & (∀l:IdLnk, tg:Id.
. . . . | | . | | . . |      ¬(deq-member(...;<l,tg>;1of())
. . . . | | . | | . . |        ⇒
. . . . | | . | | . . |        deq-member(KindDeq;kind(a(i;t));...))
. . . . | | . | | . . |      ⇒
. . . . | | . | | . . |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . | | . | | . . 13. ∀x:Id.
. . . . | | . | | . . |   deq-member(IdDeq;x;1of())
. . . . | | . | | . . |   ⇒
. . . . | | . | | . . |   s(i;0).x = 2of()(x)
. . . . | | . | | . . 14. ∀a@0:Action(i).
. . . . | | . | | . . |   ¬isnull(a@0)
. . . . | | . | | . . |   ⇒
. . . . | | . | | . . |   (valtype(i;a@0) ⊆r <[locl(a)]
. . . . | | . | | . . |                       ,λx.T>(kind(a@0))?Top)
. . . . | | . | | . . 15. ∀x:Id.
. . . . | | . | | . . |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(
. . . . | | . | | . . |                                        ds))→
. . . . | | . | | . . |                      2of(ds)(x)
. . . . | | . | | . . |                  else Top fi
. . . . | | . | | . . 16. IdDeq ∈ EqDecider(Id)
. . . . | | . | | . . 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . | | . | | . . 18. j : Id
. . . . | | . | | . . 19. t : ℕ
. . . . | | . | | . . 20. j = i
. . . . | | . | | . . 21. ¬isnull(a(j;t))
. . . . | | . | | . . 22. ¬isnull(a(i;t))
. . . . | | . | | . . 23. (λx.s(i;t).x) ∈ State(ds)
. . . . | | . | | . . 24. y : Id
. . . . | | . | | . . 25. kind(a(i;t)) = inr(y)
. . . . | | . | | . . ⊢  inr(y) = locl(a) ⇒ act(inr(y)) = a
. . . . | | . | | . . | by Unfold ‘actof‘ 0 THEN Reduce 0
. . . . | | . | | . . |    THEN
. . . . | | . | | . . |    Fold ‘locl‘ 0
. . . . | | . | | . . |
. . . . | | . | | . . 1. i : Id
. . . . | | . | | . . 2. a : Id
. . . . | | . | | . . 3. T : Type
. . . . | | . | | . . 4. ds : x:Id fp-> Type
. . . . | | . | | . . 5. P : State(ds)→T→Prop
. . . . | | . | | . . 6. w : World
. . . . | | . | | . . 7. FairFifo
. . . . | | . | | . . 8. FairFifo
```

```
. . . . | | . | | . . 9. ∀l:IdLnk, tg:Id.
. . . . | | . | | . . |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . | | . | | . . |                    <ds
. . . . | | . | | . . |                    ,<[locl(a)],λx.T>
. . . . | | . | | . . |                    ,
. . . . | | . | | . . |                    ,<[a],λx.P>
. . . . | | . | | . . |                    ,
. . . . | | . | | . . |                    ,
. . . . | | . | | . . |                    ,
. . . . | | . | | . . |                    ,
. . . . | | . | | . . |                    ,·>
. . . . | | . | | . . |                 else  fi.da(rcv(l; tg))
. . . . | | . | | . . 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . | | . | | . . 11. ∀a@0:Id, t:ℕ.
. . . . | | . | | . . |   ∃t':ℕ.
. . . . | | . | | . . |   t≤t'
. . . . | | . | | . . |   & ¬isnull(a(i;t'))
. . . . | | . | | . . |     & kind(a(i;t')) = locl(a@0)
. . . . | | . | | . . |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . | | . | | . . |     ∨ P@0 != <[a]
. . . . | | . | | . . |              ,λx.
. . . . | | . | | . . |               P>(a@0) ==> ∀v:<[locl(a)]
. . . . | | . | | . . |                                ,λx.
. . . . | | . | | . . |                                 T>(...)?Top.
. . . . | | . | | . . |       ¬P@0((λx.s(i;t').x),v)
. . . . | | . | | . . 12. ∀t:ℕ.
. . . . | | . | | . . |   ¬isnull(a(i;t))
. . . . | | . | | . . |   ⇒
. . . . | | . | | . . |   (islocal(kind(a(i;t)))
. . . . | | . | | . . |    ⇒
. . . . | | . | | . . |    (eqof(IdDeq)(a,act(kind(a(i;t))))
. . . . | | . | | . . |     ∨₂ false₂)
. . . . | | . | | . . |    ⇒
. . . . | | . | | . . |    P((λx.s(i;t).x),val(a(i;t))))
. . . . | | . | | . . |   & (∀x:Id.
. . . . | | . | | . . |      deq-member(...;<kind(a(i;t)),x>;1of())
. . . . | | . | | . . |      ⇒
. . . . | | . | | . . |      s(i;t+1).x
. . . . | | . | | . . |      =
. . . . | | . | | . . |      2of()
. . . . | | . | | . . |      (<kind(a(i;t)),x>
. . . . | | . | | . . |      ,λx.s(i;t).x
. . . . | | . | | . . |      ,val(a(i;t))))
. . . . | | . | | . . |   & (∀l:IdLnk.
. . . . | | . | | . . |      deq-member(...;<kind(a(i;t)),l>;1of())
. . . . | | . | | . . |      ⇒
. . . . | | . | | . . |      withlnk(l;m(i;t))
. . . . | | . | | . . |      =
. . . . | | . | | . . |      if source(l) = i→
. . . . | | . | | . . |         concat(map(λtgf.map(λx.
. . . . | | . | | . . |         <1of(tgf)
. . . . | | . | | . . |         ,x>;2of(tgf)
. . . . | | . | | . . |             ((λx.s(i;t).x)
. . . . | | . | | . . |             ,val(a(i;t))));...))
. . . . | | . | | . . |      else nil fi)
```

```
. . . . | | . | | . . |   & (∀x:Id.
. . . . | | . | | . . |      ¬(deq-member(IdDeq;x;1of())
. . . . | | . | | . . |        ⇒
. . . . | | . | | . . |        deq-member(KindDeq;kind(a(i;t));2of()
. . . . | | . | | . . |                                          (x)))
. . . . | | . | | . . |      ⇒
. . . . | | . | | . . |      s(i;t).x = s(i;t+1).x)
. . . . | | . | | . . |   & (∀l:IdLnk, tg:Id.
. . . . | | . | | . . |      ¬(deq-member(...;<l,tg>;1of())
. . . . | | . | | . . |        ⇒
. . . . | | . | | . . |        deq-member(KindDeq;kind(a(i;t));...))
. . . . | | . | | . . |      ⇒
. . . . | | . | | . . |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . | | . | | . . 13. ∀x:Id.
. . . . | | . | | . . |   deq-member(IdDeq;x;1of())
. . . . | | . | | . . |   ⇒
. . . . | | . | | . . |   s(i;0).x = 2of()(x)
. . . . | | . | | . . 14. ∀a@0:Action(i).
. . . . | | . | | . . |   ¬isnull(a@0)
. . . . | | . | | . . |   ⇒
. . . . | | . | | . . |   (valtype(i;a@0) ⊆r <[locl(a)]
. . . . | | . | | . . |                       ,λx.T>(kind(a@0))?Top)
. . . . | | . | | . . 15. ∀x:Id.
. . . . | | . | | . . |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(
. . . . | | . | | . . |                                          ds))→
. . . . | | . | | . . |                      2of(ds)(x)
. . . . | | . | | . . |                   else Top fi
. . . . | | . | | . . 16. IdDeq ∈ EqDecider(Id)
. . . . | | . | | . . 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . | | . | | . . 18. j : Id
. . . . | | . | | . . 19. t : ℕ
. . . . | | . | | . . 20. j = i
. . . . | | . | | . . 21. ¬isnull(a(j;t))
. . . . | | . | | . . 22. ¬isnull(a(i;t))
. . . . | | . | | . . 23. (λx.s(i;t).x) ∈ State(ds)
. . . . | | . | | . . 24. y : Id
. . . . | | . | | . . 25. kind(a(i;t)) = inr(y)
. . . . | | . | | . . ⊢  locl(y) = locl(a) ⇒ y = a  by Auto
. . . . | | . | | . . |
. . . . | | . | | . . 1. i : Id
. . . . | | . | | . . 2. a : Id
. . . . | | . | | . . 3. T : Type
. . . . | | . | | . . 4. ds : x:Id fp-> Type
. . . . | | . | | . . 5. P : State(ds)→T→Prop
. . . . | | . | | . . 6. w : World
. . . . | | . | | . . 7. FairFifo
. . . . | | . | | . . 8. FairFifo
. . . . | | . | | . . 9. ∀l:IdLnk, tg:Id.
. . . . | | . | | .    (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . | | . | | .                    <ds
. . . . | | . | | .                    ,<[locl(a)],λx.T>
. . . . | | . | | .                    ,
. . . . | | . | | .                    ,<[a],λx.P>
. . . . | | . | | .                    ,
. . . . | | . | | .                    ,
```

```
. . . . | | . | | . .                    ,
. . . . | | . | | . .                    ,
. . . . | | . | | . .                    ,·>
. . . . | | . | | . .                  else  fi.da(rcv(l; tg))
. . . . | | . | | . . 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . | | . | | . . 11. ∀a@0:Id, t:ℕ.
. . . . | | . | | . .     ∃t':ℕ.
. . . . | | . | | . .     t≤t'
. . . . | | . | | . .     & ¬isnull(a(i;t'))
. . . . | | . | | . .       & kind(a(i;t')) = locl(a@0)
. . . . | | . | | . .       ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . | | . | | . .       ∨ P@0 != <[a]
. . . . | | . | | . .                ,λx.
. . . . | | . | | . .                 P>(a@0) ==> ∀v:<[locl(a)]
. . . . | | . | | . .                                ,λx.
. . . . | | . | | . .                                 T>(...)?Top.
. . . . | | . | | . .         ¬P@0((λx.s(i;t').x),v)
. . . . | | . | | . . 12. ∀t:ℕ.
. . . . | | . | | . .     ¬isnull(a(i;t))
. . . . | | . | | . .     ⇒
. . . . | | . | | . .     (islocal(kind(a(i;t)))
. . . . | | . | | . .      ⇒
. . . . | | . | | . .      (eqof(IdDeq)(a,act(kind(a(i;t))))
. . . . | | . | | . .       ∨₂ false₂)
. . . . | | . | | . .      ⇒
. . . . | | . | | . .      P((λx.s(i;t).x),val(a(i;t))))
. . . . | | . | | . .     & (∀x:Id.
. . . . | | . | | . .        deq-member(...;<kind(a(i;t)),x>;1of())
. . . . | | . | | . .        ⇒
. . . . | | . | | . .        s(i;t+1).x
. . . . | | . | | . .        =
. . . . | | . | | . .        2of()

. . . . | | . | | . .        (<kind(a(i;t)),x>
. . . . | | . | | . .        ,λx.s(i;t).x
. . . . | | . | | . .        ,val(a(i;t))))
. . . . | | . | | . .     & (∀l:IdLnk.
. . . . | | . | | . .        deq-member(...;<kind(a(i;t)),l>;1of())
. . . . | | . | | . .        ⇒
. . . . | | . | | . .        withlnk(l;m(i;t))
. . . . | | . | | . .        =
. . . . | | . | | . .        if source(l) = i→
. . . . | | . | | . .           concat(map(λtgf.map(λx.
. . . . | | . | | . .           <1of(tgf)
. . . . | | . | | . .           ,x>;2of(tgf)
. . . . | | . | | . .               ((λx.s(i;t).x)
. . . . | | . | | . .               ,val(a(i;t))));...))
. . . . | | . | | . .        else nil fi)
. . . . | | . | | . .     & (∀x:Id.
. . . . | | . | | . .        ¬(deq-member(IdDeq;x;1of())
. . . . | | . | | . .          ⇒
. . . . | | . | | . .          deq-member(KindDeq;kind(a(i;t));2of()
. . . . | | . | | . .                                          (x)))
. . . . | | . | | . .        ⇒
. . . . | | . | | . .        s(i;t).x = s(i;t+1).x)
. . . . | | . | | . .     & (∀l:IdLnk, tg:Id.
```

```
. . . . | | . | | . .        ¬(deq-member(...;<l,tg>;1of())
. . . . | | . | | . .          ⇒
. . . . | | . | | . .          deq-member(KindDeq;kind(a(i;t));...))
. . . . | | . | | . .        ⇒
. . . . | | . | | . .        w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . | | . | | . . 13. ∀x:Id.
. . . . | | . | | . .     deq-member(IdDeq;x;1of())
. . . . | | . | | . .     ⇒
. . . . | | . | | . .     s(i;0).x = 2of()(x)
. . . . | | . | | . . 14. ∀a@0:Action(i).
. . . . | | . | | . .     ¬isnull(a@0)
. . . . | | . | | . .     ⇒
. . . . | | . | | . .     (valtype(i;a@0) ⊆r <[locl(a)]
. . . . | | . | | . .                        ,λx.T>(kind(a@0))?Top)
. . . . | | . | | . . 15. ∀x:Id.
. . . . | | . | | . .     vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(
. . . . | | . | | . .                                          ds))→
. . . . | | . | | . .                          2of(ds)(x)
. . . . | | . | | . .                       else Top fi
. . . . | | . | | . . 16. IdDeq ∈ EqDecider(Id)
. . . . | | . | | . . 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . | | . | | . . 18. j : Id
. . . . | | . | | . . 19. t : ℕ
. . . . | | . | | . . 20. j = i
. . . . | | . | | . . 21. ¬isnull(a(j;t))
. . . . | | . | | . . 22. ¬isnull(a(i;t))
. . . . | | . | | . . 23. (λx.s(i;t).x) ∈ State(ds)
. . . . | | . | | . . 24. y : Id
. . . . | | . | | . . 25. kind(a(i;t)) = inr(y)
. . . . | | . | | . . 26. locl(y) = locl(a)
. . . . | | . | | . . ⊢  y = a
. . . . | | . | | . .   by FwdThru
. . . . | | . | | . .      Thm* ∀a,b:Id. locl(a) = locl(b) ⇒ a = b
. . . . | | . | | . .      {locl_one_one}
. . . . | | . | | . .      [-1]
. . . . | | . | |
. . . . | | . | .\
. . . . | | . | . 1. i : Id
. . . . | | . | . 2. a : Id
. . . . | | . | . 3. T : Type
. . . . | | . | . 4. ds : x:Id fp-> Type
. . . . | | . | . 5. P : State(ds)→T→Prop
. . . . | | . | . 6. w : World
. . . . | | . | . 7. FairFifo
. . . . | | . | . 8. FairFifo
. . . . | | . | . 9. ∀l:IdLnk, tg:Id.
. . . . | | . | .    (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . | | . | .                    <ds
. . . . | | . | .                    ,<[locl(a)],λx.T>
. . . . | | . | .                    ,
. . . . | | . | .                    ,<[a],λx.P>
. . . . | | . | .                    ,
. . . . | | . | .                    ,
. . . . | | . | .                    ,
. . . . | | . | .                    ,
```

```
. . . . | | . | .                        ,·>
. . . . | | . | .                    else  fi.da(rcv(l; tg))
. . . . | | . | . 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . | | . | . 11. ∀a@0:Id, t:ℕ.
. . . . | | . | .     ∃t':ℕ.
. . . . | | . | .     t≤t'
. . . . | | . | .     & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . | | . | .       ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . | | . | .       ∨ P@0 != <[a]
. . . . | | . | .                ,λx.
. . . . | | . | .                 P>(a@0) ==> ∀v:<[locl(a)]
. . . . | | . | .                                ,λx.
. . . . | | . | .                                 T>(locl(a@0))?Top.
. . . . | | . | .         ¬P@0((λx.s(i;t').x),v)
. . . . | | . | . 12. ∀t:ℕ.
. . . . | | . | .     ¬isnull(a(i;t))
. . . . | | . | .     ⇒
. . . . | | . | .     (islocal(kind(a(i;t)))
. . . . | | . | .      ⇒
. . . . | | . | .      (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . | | . | .      ⇒
. . . . | | . | .      P((λx.s(i;t).x),val(a(i;t))))

. . . . | | . | .     & (∀x:Id.
. . . . | | . | .        deq-member(...;<kind(a(i;t)),x>;1of())
. . . . | | . | .        ⇒
. . . . | | . | .        s(i;t+1).x
. . . . | | . | .        =
. . . . | | . | .        2of()
. . . . | | . | .        (<kind(a(i;t)),x>
. . . . | | . | .        ,λx.s(i;t).x
. . . . | | . | .        ,val(a(i;t))))
. . . . | | . | .     & (∀l:IdLnk.
. . . . | | . | .        deq-member(...;<kind(a(i;t)),l>;1of())
. . . . | | . | .        ⇒
. . . . | | . | .        withlnk(l;m(i;t))
. . . . | | . | .        =
. . . . | | . | .        if source(l) = i→
. . . . | | . | .           concat(map(λtgf.map(λx.
. . . . | | . | .           <1of(tgf),x>;2of(tgf)
. . . . | | . | .                        ((λx.s(i;t).x)
. . . . | | . | .                        ,val(a(i;t))));2of()
. . . . | | . | .                                      (<kind(a(i;t))
. . . . | | . | .                                       ,l>)))
. . . . | | . | .        else nil fi)
. . . . | | . | .     & (∀x:Id.
. . . . | | . | .        ¬(deq-member(IdDeq;x;1of())
. . . . | | . | .          ⇒
. . . . | | . | .          deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . . . | | . | .        ⇒
. . . . | | . | .        s(i;t).x = s(i;t+1).x)
. . . . | | . | .     & (∀l:IdLnk, tg:Id.
. . . . | | . | .        ¬(deq-member(...;<l,tg>;1of())
. . . . | | . | .          ⇒
. . . . | | . | .          deq-member(KindDeq;kind(a(i;t));2of()
. . . . | | . | .                                          (<l,tg>)))
```

```
. . . . | | . | .        ⇒
. . . . | | . | .        w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . | | . | . 13. ∀x:Id.
. . . . | | . | .     deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . . . | | . | . 14. ∀a@0:Action(i).
. . . . | | . | .     ¬isnull(a@0)
. . . . | | . | .     ⇒
. . . . | | . | .     (valtype(i;a@0) ⊆r <[locl(a)]
. . . . | | . | .                        ,λx.T>(kind(a@0))?Top)
. . . . | | . | . 15. ∀x:Id.
. . . . | | . | .     vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . . . | | . | .                        2of(ds)(x)
. . . . | | . | .                     else Top fi
. . . . | | . | . 16. IdDeq ∈ EqDecider(Id)
. . . . | | . | . 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . | | . | . 18. j : Id
. . . . | | . | . 19. t : ℕ
. . . . | | . | . 20. j = i
. . . . | | . | . 21. ¬isnull(a(j;t))
. . . . | | . | . 22. ¬isnull(a(i;t))
. . . . | | . | . 23. (λx.s(i;t).x) ∈ State(ds)
. . . . | | . | . 24. kind(a(j;t)) = locl(a)
. . . . | | . | . ⊢  eqof(IdDeq)(a,a) ∨₂ false₂
. . . . | | . | .   by RWO
. . . . | | . | .      Thm* ∀d:EqDecider(A), i:A.
. . . . | | . | .           (eqof(d)(i,i)) ∼ true₂
. . . . | | . | .      {eqof_eq_btrue}
. . . . | | . | .      0
. . . . | | . | .      THEN
. . . . | | . | .      Reduce 0
. . . . | | . |
. . . . | | . .\
. . . . | | . . 1. i : Id
. . . . | | . . 2. a : Id
. . . . | | . . 3. T : Type
. . . . | | . . 4. ds : x:Id fp-> Type
. . . . | | . . 5. P : State(ds)→T→Prop
. . . . | | . . 6. w : World
. . . . | | . . 7. FairFifo
. . . . | | . . 8. FairFifo
. . . . | | . . 9. ∀l:IdLnk, tg:Id.
. . . . | | . . |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . | | . . |                  <ds
. . . . | | . . |                  ,<[locl(a)],λx.T>
. . . . | | . . |                  ,
. . . . | | . . |                  ,<[a],λx.P>
. . . . | | . . |                  ,
. . . . | | . . |                  ,
. . . . | | . . |                  ,
. . . . | | . . |                  ,
. . . . | | . . |                  ,·>
. . . . | | . . |               else  fi.da(rcv(l; tg))
. . . . | | . . 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . | | . . 11. ∀a@0:Id, t:ℕ.
. . . . | | . . |   ∃t':ℕ.
```

```
. . . . | | . . |   t≤t'
. . . . | | . . |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . | | . . |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . | | . . |     ∨ P@0 != <[a]
. . . . | | . . |              ,λx.P>(a@0) ==> ∀v:<[locl(a)]
. . . . | | . . |                                ,λx.
. . . . | | . . |                                 T>(locl(a@0))?Top.
. . . . | | . . |       ¬P@0((λx.s(i;t').x),v)
. . . . | | . . 12. ∀t:ℕ.
. . . . | | . . |   ¬isnull(a(i;t))
. . . . | | . . |   ⇒
. . . . | | . . |   (islocal(kind(a(i;t)))
. . . . | | . . |    ⇒
. . . . | | . . |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . | | . . |    ⇒
. . . . | | . . |    P((λx.s(i;t).x),val(a(i;t))))
. . . . | | . . |   & (∀x:Id.
. . . . | | . . |      deq-member(product-deq(Knd;Id;...;...);<...
. . . . | | . . |                                          ,x>;1of(
. . . . | | . . |                                              ))
. . . . | | . . |      ⇒
. . . . | | . . |      s(i;t+1).x
. . . . | | . . |      =
. . . . | | . . |      2of()
. . . . | | . . |      (<kind(a(i;t)),x>
. . . . | | . . |      ,λx.s(i;t).x
. . . . | | . . |      ,val(a(i;t))))
. . . . | | . . |   & (∀l:IdLnk.
. . . . | | . . |      deq-member(...;<kind(a(i;t)),l>;1of())
. . . . | | . . |      ⇒
. . . . | | . . |      withlnk(l;m(i;t))
. . . . | | . . |      =
. . . . | | . . |      if source(l) = i→
. . . . | | . . |         concat(map(λtgf.map(λx.
. . . . | | . . |         <1of(tgf),x>;2of(tgf)
. . . . | | . . |                      ((λx.s(i;t).x)
. . . . | | . . |                      ,val(a(i;t))));2of()
. . . . | | . . |                                    (<kind(a(i;t))
. . . . | | . . |                                     ,l>)))
. . . . | | . . |      else nil fi)
. . . . | | . . |   & (∀x:Id.
. . . . | | . . |      ¬(deq-member(IdDeq;x;1of())
. . . . | | . . |        ⇒
. . . . | | . . |        deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . . . | | . . |      ⇒
. . . . | | . . |      s(i;t).x = s(i;t+1).x)
. . . . | | . . |   & (∀l:IdLnk, tg:Id.
. . . . | | . . |      ¬(deq-member(...;<l,tg>;1of())
. . . . | | . . |        ⇒
. . . . | | . . |        deq-member(KindDeq;kind(a(i;t));2of()
. . . . | | . . |                                       (<l,tg>)))
. . . . | | . . |      ⇒
. . . . | | . . |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . | | . . 13. ∀x:Id.
. . . . | | . . |   deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
```

```
. . . . | | . . 14. ∀a@0:Action(i).
. . . . | | . . |   ¬isnull(a@0)
. . . . | | . . |   ⇒
. . . . | | . . |   (valtype(i;a@0) ⊆r <[locl(a)]
. . . . | | . . |                      ,λx.T>(kind(a@0))?Top)
. . . . | | . . 15. ∀x:Id.
. . . . | | . . |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . . . | | . . |                     2of(ds)(x)
. . . . | | . . |                  else Top fi
. . . . | | . . 16. IdDeq ∈ EqDecider(Id)
. . . . | | . . 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . | | . . 18. j : Id
. . . . | | . . 19. t : ℕ
. . . . | | . . 20. j = i
. . . . | | . . 21. ¬isnull(a(j;t))
. . . . | | . . 22. ¬isnull(a(i;t))
. . . . | | . . 23. (λx.s(i;t).x) ∈ State(ds)
. . . . | | . . 24. kind(<j,t>) = locl(a)
. . . . | | . . 25. P((λx.s(i;t).x),val(a(i;t)))
. . . . | | . . ⊢  P((λz.s(j;t).z),val(a(j;t)))
. . . . | | . . | by NthHypEq -1 THEN Analyze
. . . . | | . . |
. . . . | | . . |\
. . . . | | . . | .....subterm .....
. . . . | | . . | 1. i : Id
. . . . | | . . | 2. a : Id
. . . . | | . . | 3. T : Type
. . . . | | . . | 4. ds : x:Id fp-> Type
. . . . | | . . | 5. P : State(ds)→T→Prop
. . . . | | . . | 6. w : World
. . . . | | . . | 7. FairFifo
. . . . | | . . | 8. FairFifo
. . . . | | . . | 9. ∀l:IdLnk, tg:Id.
. . . . | | . . | |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . | | . . | |                    <ds
. . . . | | . . | |                    ,<[locl(a)],λx.T>
. . . . | | . . | |                    ,
. . . . | | . . | |                    ,<[a],λx.P>
. . . . | | . . | |                    ,
. . . . | | . . | |                    ,
. . . . | | . . | |                    ,
. . . . | | . . | |                    ,
. . . . | | . . | |                    ,·>
. . . . | | . . | |                 else  fi.da(rcv(l; tg))
. . . . | | . . | 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . | | . . | 11. ∀a@0:Id, t:ℕ.
. . . . | | . . | |   ∃t':ℕ.
. . . . | | . . | |   t≤t'
. . . . | | . . | |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . | | . . | |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . | | . . | |     ∨ P@0 != <[a]
. . . . | | . . | |              ,λx.
. . . . | | . . | |               P>(a@0) ==> ∀v:<[locl(a)]
. . . . | | . . | |                              ,λx.
. . . . | | . . | |                               T>(locl(a@0))?Top.
```

```
. . . . | | . . | |       ¬P@0((λx.s(i;t').x),v)
. . . . | | . . | 12. ∀t:ℕ.
. . . . | | . . | |   ¬isnull(a(i;t))
. . . . | | . . | |   ⇒
. . . . | | . . | |   (islocal(kind(a(i;t)))
. . . . | | . . | |    ⇒
. . . . | | . . | |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . | | . . | |    ⇒
. . . . | | . . | |    P((λx.s(i;t).x),val(a(i;t))))
. . . . | | . . | |   & (∀x:Id.
. . . . | | . . | |      deq-member(...;<kind(a(i;t)),x>;1of())
. . . . | | . . | |      ⇒
. . . . | | . . | |      s(i;t+1).x
. . . . | | . . | |      =
. . . . | | . . | |      2of()
. . . . | | . . | |      (<kind(a(i;t)),x>
. . . . | | . . | |      ,λx.s(i;t).x
. . . . | | . . | |      ,val(a(i;t))))
. . . . | | . . | |   & (∀l:IdLnk.
. . . . | | . . | |      deq-member(...;<kind(a(i;t)),l>;1of())
. . . . | | . . | |      ⇒
. . . . | | . . | |      withlnk(l;m(i;t))
. . . . | | . . | |      =
. . . . | | . . | |      if source(l) = i→
. . . . | | . . | |         concat(map(λtgf.map(λx.
. . . . | | . . | |         <1of(tgf),x>;2of(tgf)
. . . . | | . . | |                     ((λx.s(i;t).x)
. . . . | | . . | |                     ,val(a(i;t))));2of()
. . . . | | . . | |                                   (<kind(a(i;t))
. . . . | | . . | |                                    ,l>)))
. . . . | | . . | |      else nil fi)
. . . . | | . . | |   & (∀x:Id.
. . . . | | . . | |      ¬(deq-member(IdDeq;x;1of())
. . . . | | . . | |        ⇒
. . . . | | . . | |        deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . . . | | . . | |      ⇒
. . . . | | . . | |      s(i;t).x = s(i;t+1).x)
. . . . | | . . | |   & (∀l:IdLnk, tg:Id.
. . . . | | . . | |      ¬(deq-member(...;<l,tg>;1of())
. . . . | | . . | |        ⇒
. . . . | | . . | |        deq-member(KindDeq;kind(a(i;t));2of()
. . . . | | . . | |                                      (<l,tg>)))
. . . . | | . . | |      ⇒
. . . . | | . . | |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . | | . . | 13. ∀x:Id.
. . . . | | . . | |   deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . . . | | . . | 14. ∀a@0:Action(i).
. . . . | | . . | |   ¬isnull(a@0)
. . . . | | . . | |   ⇒
. . . . | | . . | |   (valtype(i;a@0) ⊆r <[locl(a)]
. . . . | | . . | |                     ,λx.T>(kind(a@0))?Top)
. . . . | | . . | 15. ∀x:Id.
. . . . | | . . | |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . . . | | . . | |                     2of(ds)(x)
. . . . | | . . | |                  else Top fi
```

```
. . . . | | . . | 16. IdDeq ∈ EqDecider(Id)
. . . . | | . . | 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . | | . . | 18. j : Id
. . . . | | . . | 19. t : ℕ
. . . . | | . . | 20. j = i
. . . . | | . . | 21. ¬isnull(a(j;t))
. . . . | | . . | 22. ¬isnull(a(i;t))
. . . . | | . . | 23. (λx.s(i;t).x) ∈ State(ds)
. . . . | | . . | 24. kind(<j,t>) = locl(a)
. . . . | | . . | 25. P((λx.s(i;t).x),val(a(i;t)))
. . . . | | . . | ⊢  P(λz.s(j;t).z) = P(λx.s(i;t).x)
. . . . | | . . | | by Analyze THEN Unfold `ma-state` 0 THEN Analyze
. . . . | | . . | |
. . . . | | . . | .....subterm .....
. . . . | | . . | 1. i : Id
. . . . | | . . | 2. a : Id
. . . . | | . . | 3. T : Type
. . . . | | . . | 4. ds : x:Id fp-> Type
. . . . | | . . | 5. P : State(ds)→T→Prop
. . . . | | . . | 6. w : World
. . . . | | . . | 7. FairFifo
. . . . | | . . | 8. FairFifo
. . . . | | . . | 9. ∀l:IdLnk, tg:Id.
. . . . | | . . | |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . | | . . | |                  <ds
. . . . | | . . | |                  ,<[locl(a)],λx.T>
. . . . | | . . | |                  ,
. . . . | | . . | |                  ,<[a],λx.P>
. . . . | | . . | |                  ,
. . . . | | . . | |                  ,
. . . . | | . . | |                  ,
. . . . | | . . | |                  ,
. . . . | | . . | |                  ,·>
. . . . | | . . | |               else  fi.da(rcv(l; tg))
. . . . | | . . | 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . | | . . | 11. ∀a@0:Id, t:ℕ.
. . . . | | . . | |   ∃t':ℕ.
. . . . | | . . | |   t≤t'
. . . . | | . . | |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . | | . . | |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . | | . . | |     ∨ P@0 != <[a]
. . . . | | . . | |              ,λx.
. . . . | | . . | |               P>(a@0) ==> ∀v:<[locl(a)]
. . . . | | . . | |                              ,λx.
. . . . | | . . | |                               T>(locl(a@0))?Top.
. . . . | | . . | |       ¬P@0((λx.s(i;t').x),v)
. . . . | | . . | 12. ∀t:ℕ.

. . . . | | . . | |   ¬isnull(a(i;t))
. . . . | | . . | |   ⇒
. . . . | | . . | |   (islocal(kind(a(i;t)))
. . . . | | . . | |    ⇒
. . . . | | . . | |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . | | . . | |    ⇒
. . . . | | . . | |    P((λx.s(i;t).x),val(a(i;t))))
. . . . | | . . | |   & (∀x:Id.
```

```
. . . . | | . . | |      deq-member(...;<kind(a(i;t)),x>;1of())
. . . . | | . . | |      ⇒
. . . . | | . . | |      s(i;t+1).x
. . . . | | . . | |      =
. . . . | | . . | |      2of()
. . . . | | . . | |      (<kind(a(i;t)),x>
. . . . | | . . | |      ,λx.s(i;t).x
. . . . | | . . | |      ,val(a(i;t))))
. . . . | | . . | |   & (∀l:IdLnk.
. . . . | | . . | |      deq-member(...;<kind(a(i;t)),l>;1of())
. . . . | | . . | |      ⇒
. . . . | | . . | |      withlnk(l;m(i;t))
. . . . | | . . | |      =
. . . . | | . . | |      if source(l) = i→
. . . . | | . . | |         concat(map(λtgf.map(λx.
. . . . | | . . | |         <1of(tgf),x>;2of(tgf)
. . . . | | . . | |                     ((λx.s(i;t).x)
. . . . | | . . | |                     ,val(a(i;t))));2of()
. . . . | | . . | |                                   (<kind(a(i;t))
. . . . | | . . | |                                    ,l>)))
. . . . | | . . | |      else nil fi)
. . . . | | . . | |   & (∀x:Id.
. . . . | | . . | |      ¬(deq-member(IdDeq;x;1of())
. . . . | | . . | |        ⇒
. . . . | | . . | |        deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . . . | | . . | |      ⇒
. . . . | | . . | |      s(i;t).x = s(i;t+1).x)
. . . . | | . . | |   & (∀l:IdLnk, tg:Id.
. . . . | | . . | |      ¬(deq-member(...;<l,tg>;1of())
. . . . | | . . | |        ⇒
. . . . | | . . | |        deq-member(KindDeq;kind(a(i;t));2of()
. . . . | | . . | |                                      (<l,tg>)))
. . . . | | . . | |      ⇒
. . . . | | . . | |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . | | . . | 13. ∀x:Id.
. . . . | | . . | |   deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . . . | | . . | 14. ∀a@0:Action(i).
. . . . | | . . | |   ¬isnull(a@0)
. . . . | | . . | |   ⇒
. . . . | | . . | |   (valtype(i;a@0) ⊆r <[locl(a)]
. . . . | | . . | |                      ,λx.T>(kind(a@0))?Top)
. . . . | | . . | 15. ∀x:Id.
. . . . | | . . | |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . . . | | . . | |                      2of(ds)(x)
. . . . | | . . | |                   else Top fi
. . . . | | . . | 16. IdDeq ∈ EqDecider(Id)
. . . . | | . . | 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . | | . . | 18. j : Id
. . . . | | . . | 19. t : ℕ
. . . . | | . . | 20. j = i
. . . . | | . . | 21. ¬isnull(a(j;t))
. . . . | | . . | 22. ¬isnull(a(i;t))
. . . . | | . . | 23. (λx.s(i;t).x) ∈ State(ds)
. . . . | | . . | 24. kind(<j,t>) = locl(a)
. . . . | | . . | 25. P((λx.s(i;t).x),val(a(i;t)))
```

```
. . . . | | . . | 26. z : Id
. . . . | | . . | ⊢  s(j;t).z = s(i;t).z
. . . . | | . . | | by DoSubsumeEq THEN Try BackThruSomeHyp
. . . . | | . . | |
. . . . | | . . | .....assertion .....
. . . . | | . . | 1. i : Id
. . . . | | . . | 2. a : Id
. . . . | | . . | 3. T : Type
. . . . | | . . | 4. ds : x:Id fp-> Type
. . . . | | . . | 5. P : State(ds)→T→Prop
. . . . | | . . | 6. w : World
. . . . | | . . | 7. FairFifo
. . . . | | . . | 8. FairFifo
. . . . | | . . | 9. ∀l:IdLnk, tg:Id.
. . . . | | . . | |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . | | . . | |                    <ds
. . . . | | . . | |                    ,<[locl(a)],λx.T>
. . . . | | . . | |                    ,
. . . . | | . . | |                    ,<[a],λx.P>
. . . . | | . . | |                    ,
. . . . | | . . | |                    ,
. . . . | | . . | |                    ,
. . . . | | . . | |                    ,
. . . . | | . . | |                    ,.>
. . . . | | . . | |                else  fi.da(rcv(l; tg))
. . . . | | . . | 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . | | . . | 11. ∀a@0:Id, t:ℕ.
. . . . | | . . | |   ∃t':ℕ.
. . . . | | . . | |   t≤t'
. . . . | | . . | |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . | | . . | |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . | | . . | |     ∨ P@0 != <[a]
. . . . | | . . | |              ,λx.
. . . . | | . . | |               P>(a@0) ==> ∀v:<[locl(a)]
. . . . | | . . | |                                ,λx.
. . . . | | . . | |                                 T>(locl(a@0))?Top.
. . . . | | . . | |       ¬P@0((λx.s(i;t').x),v)
. . . . | | . . | 12. ∀t:ℕ.
. . . . | | . . | |   ¬isnull(a(i;t))
. . . . | | . . | |   ⇒
. . . . | | . . | |   (islocal(kind(a(i;t)))
. . . . | | . . | |    ⇒
. . . . | | . . | |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . | | . . | |    ⇒
. . . . | | . . | |    P((λx.s(i;t).x),val(a(i;t))))
. . . . | | . . | |   & (∀x:Id.
. . . . | | . . | |      deq-member(...;<kind(a(i;t)),x>;1of())
. . . . | | . . | |      ⇒
. . . . | | . . | |      s(i;t+1).x
. . . . | | . . | |      =
. . . . | | . . | |      2of()
. . . . | | . . | |      (<kind(a(i;t)),x>
. . . . | | . . | |      ,λx.s(i;t).x
. . . . | | . . | |      ,val(a(i;t))))
. . . . | | . . | |   & (∀l:IdLnk.
```

```
. . . . | | . . | |      deq-member(...;<kind(a(i;t)),l>;1of())
. . . . | | . . | |      ⇒
. . . . | | . . | |      withlnk(l;m(i;t))
. . . . | | . . | |      =
. . . . | | . . | |      if source(l) = i⟶
. . . . | | . . | |         concat(map(λtgf.map(λx.
. . . . | | . . | |         <1of(tgf),x>;2of(tgf)
. . . . | | . . | |                      ((λx.s(i;t).x)
. . . . | | . . | |                      ,val(a(i;t))));2of()
. . . . | | . . | |                                    (<kind(a(i;t))
. . . . | | . . | |                                     ,l>)))
. . . . | | . . | |      else nil fi)
. . . . | | . . | |   & (∀x:Id.
. . . . | | . . | |      ¬(deq-member(IdDeq;x;1of())
. . . . | | . . | |        ⇒
. . . . | | . . | |        deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . . . | | . . | |      ⇒
. . . . | | . . | |      s(i;t).x = s(i;t+1).x)
. . . . | | . . | |   & (∀l:IdLnk, tg:Id.
. . . . | | . . | |      ¬(deq-member(...;<l,tg>;1of())
. . . . | | . . | |        ⇒
. . . . | | . . | |        deq-member(KindDeq;kind(a(i;t));2of()
. . . . | | . . | |                                       (<l,tg>)))
. . . . | | . . | |      ⇒
. . . . | | . . | |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . | | . . | 13. ∀x:Id.
. . . . | | . . | |   deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . . . | | . . | 14. ∀a@0:Action(i).
. . . . | | . . | |   ¬isnull(a@0)
. . . . | | . . | |   ⇒
. . . . | | . . | |   (valtype(i;a@0) ⊆r <[locl(a)]
. . . . | | . . | |                      ,λx.T>(kind(a@0))?Top)
. . . . | | . . | 15. ∀x:Id.
. . . . | | . . | |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))⟶
. . . . | | . . | |                      2of(ds)(x)
. . . . | | . . | |                   else Top fi
. . . . | | . . | 16. IdDeq ∈ EqDecider(Id)
. . . . | | . . | 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . | | . . | 18. j : Id
. . . . | | . . | 19. t : ℕ
. . . . | | . . | 20. j = i
. . . . | | . . | 21. ¬isnull(a(j;t))
. . . . | | . . | 22. ¬isnull(a(i;t))
. . . . | | . . | 23. (λx.s(i;t).x) ∈ State(ds)
. . . . | | . . | 24. kind(<j,t>) = locl(a)
. . . . | | . . | 25. P((λx.s(i;t).x),val(a(i;t)))
. . . . | | . . | 26. z : Id
. . . . | | . . | 27. vartype(i;z) ⊆r ds(z)?Top
. . . . | | . . | ⊢  s(j;t).z = s(i;t).z
. . . . | | . . | | by AssertBY (z ∈ Id) D_ES_Subtype
. . . . | | . . | |    THEN
. . . . | | . . | |    Subst (j = i) 0
. . . . | | . . | |
. . . . | | . . | |\
. . . . | | . . | | .....equality .....
```

```
. . . . | | . . | | 1. i : Id
. . . . | | . . | | 2. a : Id
. . . . | | . . | | 3. T : Type
. . . . | | . . | | 4. ds : x:Id fp-> Type
. . . . | | . . | | 5. P : State(ds)→T→Prop
. . . . | | . . | | 6. w : World
. . . . | | . . | | 7. FairFifo
. . . . | | . . | | 8. FairFifo
. . . . | | . . | | 9. ∀l:IdLnk, tg:Id.
. . . . | | . . | |    (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . | | . . | |                       <ds
. . . . | | . . | |                       ,<[locl(a)],λx.T>
. . . . | | . . | |                       ,
. . . . | | . . | |                       ,<[a],λx.P>
. . . . | | . . | |                       ,
. . . . | | . . | |                       ,
. . . . | | . . | |                       ,
. . . . | | . . | |                       ,
. . . . | | . . | |                       ,·>
. . . . | | . . | |                    else  fi.da(rcv(l; tg))
. . . . | | . . | | 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . | | . . | | 11. ∀a@0:Id, t:ℕ.
. . . . | | . . | |     ∃t':ℕ.
. . . . | | . . | |     t≤t'
. . . . | | . . | |     & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . | | . . | |       ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . | | . . | |       ∨ P@0 != <[a]
. . . . | | . . | |                 ,λx.
. . . . | | . . | |                  P>(a@0) ==> ∀v:<[locl(a)]
. . . . | | . . | |                                 ,λx.
. . . . | | . . | |                                  T>(locl(a@0))?Top.
. . . . | | . . | |         ¬P@0((λx.s(i;t').x),v)
. . . . | | . . | | 12. ∀t:ℕ.
. . . . | | . . | |     ¬isnull(a(i;t))
. . . . | | . . | |     ⇒
. . . . | | . . | |     (islocal(kind(a(i;t)))
. . . . | | . . | |      ⇒
. . . . | | . . | |      (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . | | . . | |      ⇒
. . . . | | . . | |      P((λx.s(i;t).x),val(a(i;t))))
. . . . | | . . | |     & (∀x:Id.
. . . . | | . . | |        deq-member(...;<kind(a(i;t)),x>;1of())
. . . . | | . . | |        ⇒
. . . . | | . . | |        s(i;t+1).x
. . . . | | . . | |        =
. . . . | | . . | |        2of()
. . . . | | . . | |        (<kind(a(i;t)),x>
. . . . | | . . | |        ,λx.s(i;t).x
. . . . | | . . | |        ,val(a(i;t))))
. . . . | | . . | |     & (∀l:IdLnk.
. . . . | | . . | |        deq-member(...;<kind(a(i;t)),l>;1of())
. . . . | | . . | |        ⇒
. . . . | | . . | |        withlnk(l;m(i;t))
. . . . | | . . | |        =
. . . . | | . . | |        if source(l) = i→
```

```
. . . . | | . . | |           concat(map(λtgf.map(λx.
. . . . | | . . | |           <1of(tgf)
. . . . | | . . | |           ,x>;2of(tgf)
. . . . | | . . | |               ((λx.s(i;t).x)
. . . . | | . . | |               ,val(a(i;t))));2of()
. . . . | | . . | |                              (<kind(a(i;t)),l>)))
. . . . | | . . | |       else nil fi)
. . . . | | . . | |    & (∀x:Id.
. . . . | | . . | |       ¬(deq-member(IdDeq;x;1of())
. . . . | | . . | |         ⇒
. . . . | | . . | |         deq-member(KindDeq;kind(a(i;t));2of()
. . . . | | . . | |                                        (x)))
. . . . | | . . | |       ⇒
. . . . | | . . | |       s(i;t).x = s(i;t+1).x)
. . . . | | . . | |    & (∀l:IdLnk, tg:Id.
. . . . | | . . | |       ¬...
. . . . | | . . | |       ⇒
. . . . | | . . | |       w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . | | . . | | 13. ∀x:Id.
. . . . | | . . | |     deq-member(IdDeq;x;1of())
. . . . | | . . | |     ⇒
. . . . | | . . | |     s(i;0).x = 2of()(x)
. . . . | | . . | | 14. ∀a@0:Action(i).
. . . . | | . . | |     ¬isnull(a@0)
. . . . | | . . | |     ⇒
. . . . | | . . | |     (valtype(i;a@0) ⊆r <[locl(a)]
. . . . | | . . | |                         ,λx.T>(kind(a@0))?Top)
. . . . | | . . | | 15. ∀x:Id.
. . . . | | . . | |     vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(
. . . . | | . . | |                                          ds))→
. . . . | | . . | |                        2of(ds)(x)
. . . . | | . . | |                      else Top fi
. . . . | | . . | | 16. IdDeq ∈ EqDecider(Id)
. . . . | | . . | | 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . | | . . | | 18. j : Id
. . . . | | . . | | 19. t : ℕ
. . . . | | . . | | 20. j = i
. . . . | | . . | | 21. ¬isnull(a(j;t))
. . . . | | . . | | 22. ¬isnull(a(i;t))
. . . . | | . . | | 23. (λx.s(i;t).x) ∈ State(ds)
. . . . | | . . | | 24. kind(<j,t>) = locl(a)
. . . . | | . . | | 25. P((λx.s(i;t).x),val(a(i;t)))
. . . . | | . . | | 26. z : Id
. . . . | | . . | | 27. vartype(i;z) ⊆r ds(z)?Top
. . . . | | . . | | 28. z ∈ Id
. . . . | | . . | | ⊢  j = i  by Analyze
. . . . | | . . | |
. . . . | | . . | |\
. . . . | | . . | | 1. i : Id
. . . . | | . . | | 2. a : Id
. . . . | | . . | | 3. T : Type
. . . . | | . . | | 4. ds : x:Id fp-> Type
. . . . | | . . | | 5. P : State(ds)→T→Prop
. . . . | | . . | | 6. w : World
. . . . | | . . | | 7. FairFifo
```

```
. . . . | | . . | | 8. FairFifo
. . . . | | . . | | 9. ∀l:IdLnk, tg:Id.
. . . . | | . . | |    (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . | | . . | |                      <ds
. . . . | | . . | |                      ,<[locl(a)],λx.T>
. . . . | | . . | |                      ,
. . . . | | . . | |                      ,<[a],λx.P>
. . . . | | . . | |                      ,
. . . . | | . . | |                      ,
. . . . | | . . | |                      ,
. . . . | | . . | |                      ,
. . . . | | . . | |                      ,·>
. . . . | | . . | |                   else  fi.da(rcv(l; tg))
. . . . | | . . | | 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . | | . . | | 11. ∀a@0:Id, t:ℕ.
. . . . | | . . | |     ∃t':ℕ.
. . . . | | . . | |     t≤t'
. . . . | | . . | |     & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . | | . . | |       ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . | | . . | |       ∨ P@0 != <[a]
. . . . | | . . | |                ,λx.
. . . . | | . . | |                 P>(a@0) ==> ∀v:<[locl(a)]
. . . . | | . . | |                                ,λx.
. . . . | | . . | |                                 T>(locl(a@0))?Top.
. . . . | | . . | |         ¬P@0((λx.s(i;t').x),v)
. . . . | | . . | | 12. ∀t:ℕ.
. . . . | | . . | |     ¬isnull(a(i;t))
. . . . | | . . | |     ⇒
. . . . | | . . | |     (islocal(kind(a(i;t)))
. . . . | | . . | |      ⇒
. . . . | | . . | |      (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . | | . . | |      ⇒
. . . . | | . . | |      P((λx.s(i;t).x),val(a(i;t))))
. . . . | | . . | |     & (∀x:Id.
. . . . | | . . | |        deq-member(...;<kind(a(i;t)),x>;1of())
. . . . | | . . | |        ⇒
. . . . | | . . | |        s(i;t+1).x
. . . . | | . . | |        =
. . . . | | . . | |        2of()
. . . . | | . . | |        (<kind(a(i;t)),x>
. . . . | | . . | |        ,λx.s(i;t).x
. . . . | | . . | |        ,val(a(i;t))))
. . . . | | . . | |     & (∀l:IdLnk.
. . . . | | . . | |        deq-member(...;<kind(a(i;t)),l>;1of())
. . . . | | . . | |        ⇒
. . . . | | . . | |        withlnk(l;m(i;t))
. . . . | | . . | |        =
. . . . | | . . | |        if source(l) = i→
. . . . | | . . | |           concat(map(λtgf.map(λx.
. . . . | | . . | |           <1of(tgf)
. . . . | | . . | |           ,x>;2of(tgf)
. . . . | | . . | |               ((λx.s(i;t).x)
. . . . | | . . | |               ,val(a(i;t))));2of()
. . . . | | . . | |                                (<kind(a(i;t)),l>)))
. . . . | | . . | |        else nil fi)
```

```
. . . . | | . . | |     & (∀x:Id.
. . . . | | . . | |        ¬(deq-member(IdDeq;x;1of())
. . . . | | . . | |          ⇒
. . . . | | . . | |          deq-member(KindDeq;kind(a(i;t));2of()
. . . . | | . . | |                                          (x)))
. . . . | | . . | |        ⇒
. . . . | | . . | |        s(i;t).x = s(i;t+1).x)
. . . . | | . . | |     & (∀l:IdLnk, tg:Id.
. . . . | | . . | |        ¬...
. . . . | | . . | |        ⇒
. . . . | | . . | |        w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . | | . . | | 13. ∀x:Id.
. . . . | | . . | |     deq-member(IdDeq;x;1of())
. . . . | | . . | |     ⇒
. . . . | | . . | |     s(i;0).x = 2of()(x)
. . . . | | . . | | 14. ∀a@0:Action(i).
. . . . | | . . | |     ¬isnull(a@0)
. . . . | | . . | |     ⇒
. . . . | | . . | |     (valtype(i;a@0) ⊆r <[locl(a)]
. . . . | | . . | |                         ,λx.T>(kind(a@0))?Top)
. . . . | | . . | | 15. ∀x:Id.
. . . . | | . . | |     vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(
. . . . | | . . | |                                          ds))→
. . . . | | . . | |                           2of(ds)(x)
. . . . | | . . | |                       else Top fi
. . . . | | . . | | 16. IdDeq ∈ EqDecider(Id)
. . . . | | . . | | 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . | | . . | | 18. j : Id
. . . . | | . . | | 19. t : ℕ
. . . . | | . . | | 20. j = i
. . . . | | . . | | 21. ¬isnull(a(j;t))
. . . . | | . . | | 22. ¬isnull(a(i;t))
. . . . | | . . | | 23. (λx.s(i;t).x) ∈ State(ds)
. . . . | | . . | | 24. kind(<j,t>) = locl(a)
. . . . | | . . | | 25. P((λx.s(i;t).x),val(a(i;t)))
. . . . | | . . | | 26. z : Id
. . . . | | . . | | 27. vartype(i;z) ⊆r ds(z)?Top
. . . . | | . . | | 28. z ∈ Id
. . . . | | . . | | ⊢  s(i;t).z = s(i;t).z  by Auto
. . . . | | . . | |
. . . . | | . . | .\
. . . . | | . . | . .....wf .....
. . . . | | . . | . 1. i : Id
. . . . | | . . | . 2. a : Id
. . . . | | . . | . 3. T : Type
. . . . | | . . | . 4. ds : x:Id fp-> Type
. . . . | | . . | . 5. P : State(ds)→T→Prop
. . . . | | . . | . 6. w : World
. . . . | | . . | . 7. FairFifo
. . . . | | . . | . 8. FairFifo
. . . . | | . . | . 9. ∀l:IdLnk, tg:Id.
. . . . | | . . | . |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . | | . . | . |                    <ds
. . . . | | . . | . |                    ,<[locl(a)],λx.T>
. . . . | | . . | . |                    ,
```

```
. . . . | | . . | . |                    ,<[a],λx.P>
. . . . | | . . | . |                    ,
. . . . | | . . | . |                    ,
. . . . | | . . | . |                    ,
. . . . | | . . | . |                    ,
. . . . | | . . | . |                    ,.>
. . . . | | . . | . |                 else  fi.da(rcv(l; tg))

. . . . | | . . | . 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . | | . . | . 11. ∀a@0:Id, t:ℕ.
. . . . | | . . | . |   ∃t':ℕ.
. . . . | | . . | . |   t≤t'
. . . . | | . . | . |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . | | . . | . |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . | | . . | . |     ∨ P@0 != <[a]
. . . . | | . . | . |              ,λx.
. . . . | | . . | . |               P>(a@0) ==> ∀v:<[locl(a)]
. . . . | | . . | . |                                ,λx.
. . . . | | . . | . |                                 T>(locl(a@0))?Top.
. . . . | | . . | . |       ¬P@0((λx.s(i;t').x),v)
. . . . | | . . | . 12. ∀t:ℕ.
. . . . | | . . | . |   ¬isnull(a(i;t))
. . . . | | . . | . |   ⇒
. . . . | | . . | . |   (islocal(kind(a(i;t)))
. . . . | | . . | . |    ⇒
. . . . | | . . | . |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . | | . . | . |    ⇒
. . . . | | . . | . |    P((λx.s(i;t).x),val(a(i;t))))
. . . . | | . . | . |   & (∀x:Id.
. . . . | | . . | . |      deq-member(...;<kind(a(i;t)),x>;1of())
. . . . | | . . | . |      ⇒
. . . . | | . . | . |      s(i;t+1).x
. . . . | | . . | . |      =
. . . . | | . . | . |      2of()
. . . . | | . . | . |      (<kind(a(i;t)),x>
. . . . | | . . | . |      ,λx.s(i;t).x
. . . . | | . . | . |      ,val(a(i;t))))
. . . . | | . . | . |   & (∀l:IdLnk.
. . . . | | . . | . |      deq-member(...;<kind(a(i;t)),l>;1of())
. . . . | | . . | . |      ⇒
. . . . | | . . | . |      withlnk(l;m(i;t))
. . . . | | . . | . |      =
. . . . | | . . | . |      if source(l) = i→
. . . . | | . . | . |         concat(map(λtgf.map(λx.
. . . . | | . . | . |         <1of(tgf)
. . . . | | . . | . |         ,x>;2of(tgf)
. . . . | | . . | . |             ((λx.s(i;t).x)
. . . . | | . . | . |             ,val(a(i;t))));2of()
. . . . | | . . | . |                              (<kind(a(i;t)),l>)))
. . . . | | . . | . |      else nil fi)
. . . . | | . . | . |   & (∀x:Id.
. . . . | | . . | . |      ¬(deq-member(IdDeq;x;1of())
. . . . | | . . | . |        ⇒
. . . . | | . . | . |        deq-member(KindDeq;kind(a(i;t));2of()
. . . . | | . . | . |                                        (x)))
. . . . | | . . | . |      ⇒
```

```
. . . . | | . . | . |      s(i;t).x = s(i;t+1).x)
. . . . | | . . | . |   & (∀l:IdLnk, tg:Id.
. . . . | | . . | . |      ¬...
. . . . | | . . | . |      ⇒
. . . . | | . . | . |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . | | . . | . 13. ∀x:Id.
. . . . | | . . | . |   deq-member(IdDeq;x;1of())
. . . . | | . . | . |   ⇒
. . . . | | . . | . |   s(i;0).x = 2of()(x)
. . . . | | . . | . 14. ∀a@0:Action(i).
. . . . | | . . | . |   ¬isnull(a@0)
. . . . | | . . | . |   ⇒
. . . . | | . . | . |   (valtype(i;a@0) ⊆r <[locl(a)]
. . . . | | . . | . |                      ,λx.T>(kind(a@0))?Top)
. . . . | | . . | . 15. ∀x:Id.
. . . . | | . . | . |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(
. . . . | | . . | . |                                        ds))→
. . . . | | . . | . |                     2of(ds)(x)
. . . . | | . . | . |                  else Top fi
. . . . | | . . | . 16. IdDeq ∈ EqDecider(Id)
. . . . | | . . | . 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . | | . . | . 18. j : Id
. . . . | | . . | . 19. t : ℕ
. . . . | | . . | . 20. j = i
. . . . | | . . | . 21. ¬isnull(a(j;t))
. . . . | | . . | . 22. ¬isnull(a(i;t))
. . . . | | . . | . 23. (λx.s(i;t).x) ∈ State(ds)
. . . . | | . . | . 24. kind(<j,t>) = locl(a)
. . . . | | . . | . 25. P((λx.s(i;t).x),val(a(i;t)))
. . . . | | . . | . 26. z : Id
. . . . | | . . | . 27. vartype(i;z) ⊆r ds(z)?Top
. . . . | | . . | . 28. z ∈ Id
. . . . | | . . | . 29. z1 : {j:Id| j = i }
. . . . | | . . | . ⊢  (s(z1;t).z = s(i;t).z) ∈ Prop  by Analyze -1
. . . . | | . . | . |
. . . . | | . . | . .....subterm .....
. . . . | | . . | . 1. i : Id
. . . . | | . . | . 2. a : Id
. . . . | | . . | . 3. T : Type
. . . . | | . . | . 4. ds : x:Id fp-> Type
. . . . | | . . | . 5. P : State(ds)→T→Prop
. . . . | | . . | . 6. w : World
. . . . | | . . | . 7. FairFifo
. . . . | | . . | . 8. FairFifo
. . . . | | . . | . 9. ∀l:IdLnk, tg:Id.
. . . . | | . . | .    (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . | | . . | .                     <ds
. . . . | | . . | .                     ,<[locl(a)],λx.T>
. . . . | | . . | .                     ,
. . . . | | . . | .                     ,<[a],λx.P>
. . . . | | . . | .                     ,
. . . . | | . . | .                     ,

. . . . | | . . | .                     ,
. . . . | | . . | .                     ,
. . . . | | . . | .                     ,.>
```

```
. . . . | | . . | .                    else  fi.da(rcv(l; tg))
. . . . | | . . | . 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . | | . . | . 11. ∀a@0:Id, t:ℕ.
. . . . | | . . | .     ∃t':ℕ.
. . . . | | . . | .     t≤t'
. . . . | | . . | .     & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . | | . . | .       ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . | | . . | .       ∨ P@0 != <[a]
. . . . | | . . | .                ,λx.
. . . . | | . . | .                 P>(a@0) ==> ∀v:<[locl(a)]
. . . . | | . . | .                                ,λx.
. . . . | | . . | .                                 T>(locl(a@0))?Top.
. . . . | | . . | .         ¬P@0((λx.s(i;t').x),v)
. . . . | | . . | . 12. ∀t:ℕ.
. . . . | | . . | .     ¬isnull(a(i;t))
. . . . | | . . | .     ⇒
. . . . | | . . | .     (islocal(kind(a(i;t)))
. . . . | | . . | .      ⇒
. . . . | | . . | .      (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . | | . . | .      ⇒
. . . . | | . . | .      P((λx.s(i;t).x),val(a(i;t))))
. . . . | | . . | .     & (∀x:Id.
. . . . | | . . | .        deq-member(...;<kind(a(i;t)),x>;1of())
. . . . | | . . | .        ⇒
. . . . | | . . | .        s(i;t+1).x
. . . . | | . . | .        =
. . . . | | . . | .        2of()
. . . . | | . . | .        (<kind(a(i;t)),x>
. . . . | | . . | .        ,λx.s(i;t).x
. . . . | | . . | .        ,val(a(i;t))))
. . . . | | . . | .     & (∀l:IdLnk.
. . . . | | . . | .        deq-member(...;<kind(a(i;t)),l>;1of())
. . . . | | . . | .        ⇒
. . . . | | . . | .        withlnk(l;m(i;t))
. . . . | | . . | .        =
. . . . | | . . | .        if source(l) = i→
. . . . | | . . | .           concat(map(λtgf.map(λx.
. . . . | | . . | .           <1of(tgf)
. . . . | | . . | .           ,x>;2of(tgf)
. . . . | | . . | .               ((λx.s(i;t).x)
. . . . | | . . | .               ,val(a(i;t))));2of()
. . . . | | . . | .                              (<kind(a(i;t)),l>)))
. . . . | | . . | .        else nil fi)
. . . . | | . . | .     & (∀x:Id.
. . . . | | . . | .        ¬(deq-member(IdDeq;x;1of())
. . . . | | . . | .          ⇒
. . . . | | . . | .          deq-member(KindDeq;kind(a(i;t));2of()
. . . . | | . . | .                                          (x)))
. . . . | | . . | .        ⇒
. . . . | | . . | .        s(i;t).x = s(i;t+1).x)
. . . . | | . . | .     & (∀l:IdLnk, tg:Id.
. . . . | | . . | .        ¬...
. . . . | | . . | .        ⇒
. . . . | | . . | .        w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . | | . . | . 13. ∀x:Id.
```

```
. . . . | | . . | .     deq-member(IdDeq;x;1of())
. . . . | | . . | .     ⇒
. . . . | | . . | .     s(i;0).x = 2of()(x)
. . . . | | . . | . 14. ∀a@0:Action(i).
. . . . | | . . | .     ¬isnull(a@0)
. . . . | | . . | .     ⇒
. . . . | | . . | .     (valtype(i;a@0) ⊆r <[locl(a)]
. . . . | | . . | .                        ,λx.T>(kind(a@0))?Top)
. . . . | | . . | . 15. ∀x:Id.
. . . . | | . . | .     vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(
. . . . | | . . | .                                          ds))→
. . . . | | . . | .                          2of(ds)(x)
. . . . | | . . | .                        else Top fi
. . . . | | . . | . 16. IdDeq ∈ EqDecider(Id)
. . . . | | . . | . 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . | | . . | . 18. j : Id
. . . . | | . . | . 19. t : ℕ
. . . . | | . . | . 20. j = i
. . . . | | . . | . 21. ¬isnull(a(j;t))
. . . . | | . . | . 22. ¬isnull(a(i;t))
. . . . | | . . | . 23. (λx.s(i;t).x) ∈ State(ds)
. . . . | | . . | . 24. kind(<j,t>) = locl(a)
. . . . | | . . | . 25. P((λx.s(i;t).x),val(a(i;t)))
. . . . | | . . | . 26. z : Id
. . . . | | . . | . 27. vartype(i;z) ⊆r ds(z)?Top
. . . . | | . . | . 28. z ∈ Id
. . . . | | . . | . 29. z1 : Id
. . . . | | . . | . 30. z1 = i
. . . . | | . . | . ⊢  s(z1;t).z ∈ vartype(i;z)
. . . . | | . . | .   by DoSubsume THEN HypSubst -1 0
. . . . | | . . |
. . . . | | . . .\
. . . . | | . . . .....subterm .....
. . . . | | . . . 1. i : Id
. . . . | | . . . 2. a : Id
. . . . | | . . . 3. T : Type
. . . . | | . . . 4. ds : x:Id fp-> Type
. . . . | | . . . 5. P : State(ds)→T→Prop
. . . . | | . . . 6. w : World
. . . . | | . . . 7. FairFifo
. . . . | | . . . 8. FairFifo
. . . . | | . . . 9. ∀l:IdLnk, tg:Id.
. . . . | | . . . |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . | | . . . |                    <ds
. . . . | | . . . |                    ,<[locl(a)],λx.T>
. . . . | | . . . |                    ,
. . . . | | . . . |                    ,<[a],λx.P>
. . . . | | . . . |                    ,
. . . . | | . . . |                    ,
. . . . | | . . . |                    ,
. . . . | | . . . |                    ,
. . . . | | . . . |                    ,.>
. . . . | | . . . |                 else  fi.da(rcv(l; tg))
. . . . | | . . . 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . | | . . . 11. ∀a@0:Id, t:ℕ.
```

```
. . . . | | . . . |   ∃t':ℕ.
. . . . | | . . . |   t≤t'
. . . . | | . . . |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . | | . . . |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . | | . . . |     ∨ P@0 != <[a]
. . . . | | . . . |               ,λx.
. . . . | | . . . |                P>(a@0) ==> ∀v:<[locl(a)]
. . . . | | . . . |                                ,λx.
. . . . | | . . . |                                 T>(locl(a@0))?Top.
. . . . | | . . . |       ¬P@0((λx.s(i;t').x),v)
. . . . | | . . . 12. ∀t:ℕ.
. . . . | | . . . |   ¬isnull(a(i;t))
. . . . | | . . . |   ⇒
. . . . | | . . . |   (islocal(kind(a(i;t)))
. . . . | | . . . |    ⇒
. . . . | | . . . |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . | | . . . |    ⇒
. . . . | | . . . |    P((λx.s(i;t).x),val(a(i;t))))
. . . . | | . . . |   & (∀x:Id.
. . . . | | . . . |      deq-member(...;<kind(a(i;t)),x>;1of())
. . . . | | . . . |      ⇒
. . . . | | . . . |      s(i;t+1).x
. . . . | | . . . |      =
. . . . | | . . . |      2of()
. . . . | | . . . |      (<kind(a(i;t)),x>
. . . . | | . . . |      ,λx.s(i;t).x
. . . . | | . . . |      ,val(a(i;t))))
. . . . | | . . . |   & (∀l:IdLnk.
. . . . | | . . . |      deq-member(...;<kind(a(i;t)),l>;1of())
. . . . | | . . . |      ⇒
. . . . | | . . . |      withlnk(l;m(i;t))
. . . . | | . . . |      =
. . . . | | . . . |      if source(l) = i→
. . . . | | . . . |         concat(map(λtgf.map(λx.
. . . . | | . . . |         <1of(tgf),x>;2of(tgf)
. . . . | | . . . |                      ((λx.s(i;t).x)
. . . . | | . . . |                      ,val(a(i;t))));2of()
. . . . | | . . . |                                    (<kind(a(i;t))
. . . . | | . . . |                                     ,l>)))
. . . . | | . . . |      else nil fi)
. . . . | | . . . |   & (∀x:Id.
. . . . | | . . . |      ¬(deq-member(IdDeq;x;1of())
. . . . | | . . . |        ⇒
. . . . | | . . . |        deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . . . | | . . . |      ⇒
. . . . | | . . . |      s(i;t).x = s(i;t+1).x)
. . . . | | . . . |   & (∀l:IdLnk, tg:Id.
. . . . | | . . . |      ¬(deq-member(...;<l,tg>;1of())
. . . . | | . . . |        ⇒
. . . . | | . . . |        deq-member(KindDeq;kind(a(i;t));2of()
. . . . | | . . . |                                        (<l,tg>)))
. . . . | | . . . |      ⇒
. . . . | | . . . |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . | | . . . 13. ∀x:Id.
. . . . | | . . . |   deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
```

```
. . . . | | . . . 14. ∀a@0:Action(i).
. . . . | | . . . |   ¬isnull(a@0)
. . . . | | . . . |   ⇒
. . . . | | . . . |   (valtype(i;a@0) ⊆r <[locl(a)]
. . . . | | . . . |                      ,λx.T>(kind(a@0))?Top)
. . . . | | . . . 15. ∀x:Id.
. . . . | | . . . |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . . . | | . . . |                      2of(ds)(x)
. . . . | | . . . |                   else Top fi
. . . . | | . . . 16. IdDeq ∈ EqDecider(Id)
. . . . | | . . . 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . | | . . . 18. j : Id
. . . . | | . . . 19. t : ℕ
. . . . | | . . . 20. j = i
. . . . | | . . . 21. ¬isnull(a(j;t))
. . . . | | . . . 22. ¬isnull(a(i;t))
. . . . | | . . . 23. (λx.s(i;t).x) ∈ State(ds)
. . . . | | . . . 24. kind(<j,t>) = locl(a)
. . . . | | . . . 25. P((λx.s(i;t).x),val(a(i;t)))
. . . . | | . . . ⊢  val(a(j;t)) = val(a(i;t))  by DoSubsumeEq
. . . . | | . . . |
. . . . | | . . . |\
. . . . | | . . . | .....assertion .....
. . . . | | . . . | 1. i : Id
. . . . | | . . . | 2. a : Id
. . . . | | . . . | 3. T : Type
. . . . | | . . . | 4. ds : x:Id fp-> Type
. . . . | | . . . | 5. P : State(ds)→T→Prop
. . . . | | . . . | 6. w : World
. . . . | | . . . | 7. FairFifo
. . . . | | . . . | 8. FairFifo
. . . . | | . . . | 9. ∀l:IdLnk, tg:Id.
. . . . | | . . . | |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . | | . . . | |                  <ds
. . . . | | . . . | |                  ,<[locl(a)],λx.T>
. . . . | | . . . | |                  ,
. . . . | | . . . | |                  ,<[a],λx.P>
. . . . | | . . . | |                  ,
. . . . | | . . . | |                  ,
. . . . | | . . . | |                  ,
. . . . | | . . . | |                  ,
. . . . | | . . . | |                  ,·>
. . . . | | . . . | |               else  fi.da(rcv(l; tg))
. . . . | | . . . | 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . | | . . . | 11. ∀a@0:Id, t:ℕ.
. . . . | | . . . | |   ∃t':ℕ.
. . . . | | . . . | |   t≤t'
. . . . | | . . . | |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . | | . . . | |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . | | . . . | |     ∨ P@0 != <[a]
. . . . | | . . . | |              ,λx.
. . . . | | . . . | |               P>(a@0) ==> ∀v:<[locl(a)]
. . . . | | . . . | |                              ,λx.
. . . . | | . . . | |                               T>(locl(a@0))?Top.
. . . . | | . . . | |       ¬P@0((λx.s(i;t').x),v)
```

```
. . . . | | . . . | 12. ∀t:ℕ.
. . . . | | . . . | |   ¬isnull(a(i;t))
. . . . | | . . . | |   ⇒
. . . . | | . . . | |   (islocal(kind(a(i;t)))
. . . . | | . . . | |    ⇒
. . . . | | . . . | |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . | | . . . | |    ⇒
. . . . | | . . . | |    P((λx.s(i;t).x),val(a(i;t))))
. . . . | | . . . | |   & (∀x:Id.
. . . . | | . . . | |      deq-member(...;<kind(a(i;t)),x>;1of())
. . . . | | . . . | |      ⇒
. . . . | | . . . | |      s(i;t+1).x
. . . . | | . . . | |      =
. . . . | | . . . | |      2of()
. . . . | | . . . | |      (<kind(a(i;t)),x>
. . . . | | . . . | |      ,λx.s(i;t).x
. . . . | | . . . | |      ,val(a(i;t))))
. . . . | | . . . | |   & (∀l:IdLnk.
. . . . | | . . . | |      deq-member(...;<kind(a(i;t)),l>;1of())
. . . . | | . . . | |      ⇒
. . . . | | . . . | |      withlnk(l;m(i;t))
. . . . | | . . . | |      =
. . . . | | . . . | |      if source(l) = i→
. . . . | | . . . | |         concat(map(λtgf.map(λx.
. . . . | | . . . | |         <1of(tgf)
. . . . | | . . . | |         ,x>;2of(tgf)
. . . . | | . . . | |             ((λx.s(i;t).x)
. . . . | | . . . | |             ,val(a(i;t))));2of()
. . . . | | . . . | |                              (<kind(a(i;t)),l>)))
. . . . | | . . . | |      else nil fi)
. . . . | | . . . | |   & (∀x:Id.
. . . . | | . . . | |      ¬(deq-member(IdDeq;x;1of())
. . . . | | . . . | |        ⇒
. . . . | | . . . | |        deq-member(KindDeq;kind(a(i;t));2of()
. . . . | | . . . | |                                        (x)))
. . . . | | . . . | |      ⇒
. . . . | | . . . | |      s(i;t).x = s(i;t+1).x)
. . . . | | . . . | |   & (∀l:IdLnk, tg:Id.
. . . . | | . . . | |      ¬...
. . . . | | . . . | |      ⇒
. . . . | | . . . | |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . | | . . . | 13. ∀x:Id.
. . . . | | . . . | |   deq-member(IdDeq;x;1of())
. . . . | | . . . | |   ⇒
. . . . | | . . . | |   s(i;0).x = 2of()(x)
. . . . | | . . . | 14. ∀a@0:Action(i).
. . . . | | . . . | |   ¬isnull(a@0)
. . . . | | . . . | |   ⇒
. . . . | | . . . | |   (valtype(i;a@0) ⊆r <[locl(a)]
. . . . | | . . . | |                       ,λx.T>(kind(a@0))?Top)
. . . . | | . . . | 15. ∀x:Id.
. . . . | | . . . | |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(
. . . . | | . . . | |                                         ds))→
. . . . | | . . . | |                       2of(ds)(x)
. . . . | | . . . | |                   else Top fi
```

```
. . . . | | . . . | 16. IdDeq ∈ EqDecider(Id)
. . . . | | . . . | 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . | | . . . | 18. j : Id
. . . . | | . . . | 19. t : ℕ
. . . . | | . . . | 20. j = i
. . . . | | . . . | 21. ¬isnull(a(j;t))
. . . . | | . . . | 22. ¬isnull(a(i;t))
. . . . | | . . . | 23. (λx.s(i;t).x) ∈ State(ds)
. . . . | | . . . | 24. kind(<j,t>) = locl(a)
. . . . | | . . . | 25. P((λx.s(i;t).x),val(a(i;t)))
. . . . | | . . . | ⊢  valtype(i;a(i;t)) ⊆r T
. . . . | | . . . | | by AllHyps
. . . . | | . . . | |    (λh.InstHyp [a(i;t)] h THENA Complete Auto)
. . . . | | . . . | |
. . . . | | . . . | 1. i : Id
. . . . | | . . . | 2. a : Id
. . . . | | . . . | 3. T : Type
. . . . | | . . . | 4. ds : x:Id fp-> Type
. . . . | | . . . | 5. P : State(ds)→T→Prop
. . . . | | . . . | 6. w : World
. . . . | | . . . | 7. FairFifo
. . . . | | . . . | 8. FairFifo

. . . . | | . . . | 9. ∀l:IdLnk, tg:Id.
. . . . | | . . . | |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . | | . . . | |                    <ds
. . . . | | . . . | |                    ,<[locl(a)],λx.T>
. . . . | | . . . | |                    ,
. . . . | | . . . | |                    ,<[a],λx.P>
. . . . | | . . . | |                    ,
. . . . | | . . . | |                    ,
. . . . | | . . . | |                    ,
. . . . | | . . . | |                    ,
. . . . | | . . . | |                    ,·>
. . . . | | . . . | |                 else  fi.da(rcv(l; tg))
. . . . | | . . . | 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . | | . . . | 11. ∀a@0:Id, t:ℕ.
. . . . | | . . . | |   ∃t':ℕ.
. . . . | | . . . | |   t≤t'
. . . . | | . . . | |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . | | . . . | |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . | | . . . | |     ∨ P@0 != <[a]
. . . . | | . . . | |              ,λx.
. . . . | | . . . | |               P>(a@0) ==> ∀v:<[locl(a)]
. . . . | | . . . | |                                ,λx.
. . . . | | . . . | |                                 T>(locl(a@0))?Top.
. . . . | | . . . | |       ¬P@0((λx.s(i;t').x),v)
. . . . | | . . . | 12. ∀t:ℕ.
. . . . | | . . . | |   ¬isnull(a(i;t))
. . . . | | . . . | |   ⇒
. . . . | | . . . | |   (islocal(kind(a(i;t)))
. . . . | | . . . | |    ⇒
. . . . | | . . . | |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . | | . . . | |    ⇒
. . . . | | . . . | |    P((λx.s(i;t).x),val(a(i;t))))
. . . . | | . . . | |   & (∀x:Id.
```

```
. . . . | | . . . | |      deq-member(...;<kind(a(i;t)),x>;1of())
. . . . | | . . . | |      ⇒
. . . . | | . . . | |      s(i;t+1).x
. . . . | | . . . | |      =
. . . . | | . . . | |      2of()
. . . . | | . . . | |      (<kind(a(i;t)),x>
. . . . | | . . . | |      ,λx.s(i;t).x
. . . . | | . . . | |      ,val(a(i;t))))
. . . . | | . . . | |   & (∀l:IdLnk.
. . . . | | . . . | |      deq-member(...;<kind(a(i;t)),l>;1of())
. . . . | | . . . | |      ⇒
. . . . | | . . . | |      withlnk(l;m(i;t))
. . . . | | . . . | |      =
. . . . | | . . . | |      if source(l) = i→
. . . . | | . . . | |         concat(map(λtgf.map(λx.
. . . . | | . . . | |         <1of(tgf)
. . . . | | . . . | |         ,x>;2of(tgf)
. . . . | | . . . | |             ((λx.s(i;t).x)
. . . . | | . . . | |             ,val(a(i;t))));2of()
. . . . | | . . . | |                              (<kind(a(i;t)),l>)))
. . . . | | . . . | |      else nil fi)
. . . . | | . . . | |   & (∀x:Id.
. . . . | | . . . | |      ¬(deq-member(IdDeq;x;1of())
. . . . | | . . . | |        ⇒
. . . . | | . . . | |        deq-member(KindDeq;kind(a(i;t));2of()
. . . . | | . . . | |                                       (x)))
. . . . | | . . . | |      ⇒
. . . . | | . . . | |      s(i;t).x = s(i;t+1).x)
. . . . | | . . . | |   & (∀l:IdLnk, tg:Id.
. . . . | | . . . | |      ¬...
. . . . | | . . . | |      ⇒
. . . . | | . . . | |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . | | . . . | 13. ∀x:Id.
. . . . | | . . . | |   deq-member(IdDeq;x;1of())
. . . . | | . . . | |   ⇒
. . . . | | . . . | |   s(i;0).x = 2of()(x)
. . . . | | . . . | 14. ∀a@0:Action(i).
. . . . | | . . . | |   ¬isnull(a@0)
. . . . | | . . . | |   ⇒
. . . . | | . . . | |   (valtype(i;a@0) ⊆r <[locl(a)]
. . . . | | . . . | |                      ,λx.T>(kind(a@0))?Top)
. . . . | | . . . | 15. ∀x:Id.
. . . . | | . . . | |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(
. . . . | | . . . | |                                         ds))→
. . . . | | . . . | |                      2of(ds)(x)
. . . . | | . . . | |                   else Top fi
. . . . | | . . . | 16. IdDeq ∈ EqDecider(Id)
. . . . | | . . . | 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . | | . . . | 18. j : Id
. . . . | | . . . | 19. t : ℕ
. . . . | | . . . | 20. j = i
. . . . | | . . . | 21. ¬isnull(a(j;t))
. . . . | | . . . | 22. ¬isnull(a(i;t))
. . . . | | . . . | 23. (λx.s(i;t).x) ∈ State(ds)
. . . . | | . . . | 24. kind(<j,t>) = locl(a)
```

```
. . . . | | . . . | 25. P((λx.s(i;t).x),val(a(i;t)))
. . . . | | . . . | 26. valtype(i;a(i;t)) ⊆r <[locl(a)]
. . . . | | . . . | |                      ,λx.T>(kind(a(i;t)))?Top
. . . . | | . . . | ⊢  valtype(i;a(i;t)) ⊆r T
. . . . | | . . . | | by Assert (locl(a) = kind(a(i;t)))
. . . . | | . . . | |
. . . . | | . . . | |\
. . . . | | . . . | | .....assertion .....
. . . . | | . . . | | 1. i : Id
. . . . | | . . . | | 2. a : Id
. . . . | | . . . | | 3. T : Type
. . . . | | . . . | | 4. ds : x:Id fp-> Type
. . . . | | . . . | | 5. P : State(ds)→T→Prop
. . . . | | . . . | | 6. w : World
. . . . | | . . . | | 7. FairFifo
. . . . | | . . . | | 8. FairFifo
. . . . | | . . . | | 9. ∀l:IdLnk, tg:Id.
. . . . | | . . . | | |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . | | . . . | | |                  <ds
. . . . | | . . . | | |                  ,<[locl(a)],λx.T>
. . . . | | . . . | | |                  ,
. . . . | | . . . | | |                  ,<[a],λx.P>
. . . . | | . . . | | |                  ,
. . . . | | . . . | | |                  ,
. . . . | | . . . | | |                  ,
. . . . | | . . . | | |                  ,
. . . . | | . . . | | |                  ,·>
. . . . | | . . . | | |               else  fi.da(rcv(l; tg))
. . . . | | . . . | | 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . | | . . . | | 11. ∀a@0:Id, t:ℕ.
. . . . | | . . . | | |   ∃t':ℕ.
. . . . | | . . . | | |   t≤t'
. . . . | | . . . | | |   & ¬isnull(a(i;t'))
. . . . | | . . . | | |     & kind(a(i;t')) = locl(a@0)
. . . . | | . . . | | |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . | | . . . | | |     ∨ P@0 != <[a]
. . . . | | . . . | | |              ,λx.
. . . . | | . . . | | |               P>(a@0) ==> ∀v:<[locl(a)]
. . . . | | . . . | | |                                ,λx.
. . . . | | . . . | | |                                 T>(...)?Top.
. . . . | | . . . | | |       ¬P@0((λx.s(i;t').x),v)
. . . . | | . . . | | 12. ∀t:ℕ.
. . . . | | . . . | | |   ¬isnull(a(i;t))
. . . . | | . . . | | |   ⇒
. . . . | | . . . | | |   (islocal(kind(a(i;t)))
. . . . | | . . . | | |    ⇒
. . . . | | . . . | | |    (eqof(IdDeq)(a,act(kind(a(i;t))))
. . . . | | . . . | | |     ∨₂ false₂)
. . . . | | . . . | | |    ⇒
. . . . | | . . . | | |    P((λx.s(i;t).x),val(a(i;t))))
. . . . | | . . . | | |   & (∀x:Id.
. . . . | | . . . | | |      deq-member(...;<kind(a(i;t)),x>;1of())
. . . . | | . . . | | |      ⇒
. . . . | | . . . | | |      s(i;t+1).x
. . . . | | . . . | | |      =
```

```
. . . . | | . . . | | |      2of()
. . . . | | . . . | | |      (<kind(a(i;t)),x>
. . . . | | . . . | | |      ,λx.s(i;t).x
. . . . | | . . . | | |      ,val(a(i;t))))
. . . . | | . . . | | |   & (∀l:IdLnk.
. . . . | | . . . | | |      deq-member(...;<kind(a(i;t)),l>;1of())
. . . . | | . . . | | |      ⇒
. . . . | | . . . | | |      withlnk(l;m(i;t))
. . . . | | . . . | | |      =
. . . . | | . . . | | |      if source(l) = i→
. . . . | | . . . | | |         concat(map(λtgf.map(λx.
. . . . | | . . . | | |         <1of(tgf)
. . . . | | . . . | | |         ,x>;2of(tgf)
. . . . | | . . . | | |             ((λx.s(i;t).x)
. . . . | | . . . | | |             ,val(a(i;t))));...))
. . . . | | . . . | | |      else nil fi)
. . . . | | . . . | | |   & (∀x:Id.
. . . . | | . . . | | |      ¬(deq-member(IdDeq;x;1of())
. . . . | | . . . | | |        ⇒
. . . . | | . . . | | |        deq-member(KindDeq;kind(a(i;t));2of()
. . . . | | . . . | | |                                        (x)))
. . . . | | . . . | | |      ⇒
. . . . | | . . . | | |      s(i;t).x = s(i;t+1).x)
. . . . | | . . . | | |   & (∀l:IdLnk, tg:Id.
. . . . | | . . . | | |      ¬(deq-member(...;<l,tg>;1of())
. . . . | | . . . | | |        ⇒
. . . . | | . . . | | |        deq-member(KindDeq;kind(a(i;t));...))
. . . . | | . . . | | |      ⇒
. . . . | | . . . | | |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . | | . . . | | 13. ∀x:Id.
. . . . | | . . . | | |   deq-member(IdDeq;x;1of())
. . . . | | . . . | | |   ⇒
. . . . | | . . . | | |   s(i;0).x = 2of()(x)
. . . . | | . . . | | 14. ∀a@0:Action(i).
. . . . | | . . . | | |   ¬isnull(a@0)
. . . . | | . . . | | |   ⇒
. . . . | | . . . | | |   (valtype(i;a@0) ⊆r <[locl(a)]
. . . . | | . . . | | |                      ,λx.T>(kind(a@0))?Top)
. . . . | | . . . | | 15. ∀x:Id.
. . . . | | . . . | | |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(
. . . . | | . . . | | |                                        ds))→
. . . . | | . . . | | |                     2of(ds)(x)
. . . . | | . . . | | |                  else Top fi
. . . . | | . . . | | 16. IdDeq ∈ EqDecider(Id)
. . . . | | . . . | | 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . | | . . . | | 18. j : Id
. . . . | | . . . | | 19. t : ℕ
. . . . | | . . . | | 20. j = i
. . . . | | . . . | | 21. ¬isnull(a(j;t))
. . . . | | . . . | | 22. ¬isnull(a(i;t))
. . . . | | . . . | | 23. (λx.s(i;t).x) ∈ State(ds)
. . . . | | . . . | | 24. kind(<j,t>) = locl(a)
. . . . | | . . . | | 25. P((λx.s(i;t).x),val(a(i;t)))
. . . . | | . . . | | 26. valtype(i;a(i;t)) ⊆r <[locl(a)]
. . . . | | . . . | | |                      ,λx.
```

```
. . . . | | . . . | | |                          T>(kind(a(i;t)))?Top
. . . . | | . . . | | ⊢  locl(a) = kind(a(i;t))

. . . . | | . . . | | | by Unfold ‘w-ekind‘ -3 THEN Unfold ‘w-act‘ -3
. . . . | | . . . | | |    THEN
. . . . | | . . . | | |    Reduce -3
. . . . | | . . . | | |
. . . . | | . . . | | | 1. i : Id
. . . . | | . . . | | | 2. a : Id
. . . . | | . . . | | | 3. T : Type
. . . . | | . . . | | | 4. ds : x:Id fp-> Type
. . . . | | . . . | | | 5. P : State(ds)→T→Prop
. . . . | | . . . | | | 6. w : World
. . . . | | . . . | | | 7. FairFifo
. . . . | | . . . | | | 8. FairFifo
. . . . | | . . . | | | 9. ∀l:IdLnk, tg:Id.
. . . . | | . . . | | | |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . | | . . . | | | |                    <ds
. . . . | | . . . | | | |                    ,<[locl(a)],λx.T>
. . . . | | . . . | | | |                    ,
. . . . | | . . . | | | |                    ,<[a],λx.P>
. . . . | | . . . | | | |                    ,
. . . . | | . . . | | | |                    ,
. . . . | | . . . | | | |                    ,
. . . . | | . . . | | | |                    ,
. . . . | | . . . | | | |                    ,·>
. . . . | | . . . | | | |                else  fi.da(rcv(l; tg))
. . . . | | . . . | | | 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . | | . . . | | | 11. ∀a@0:Id, t:ℕ.
. . . . | | . . . | | | |   ∃t':ℕ.
. . . . | | . . . | | | |   t≤t'
. . . . | | . . . | | | |   & ¬isnull(a(i;t'))
. . . . | | . . . | | | |     & kind(a(i;t')) = locl(a@0)
. . . . | | . . . | | | |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . | | . . . | | | |     ∨ P@0 != <[a]
. . . . | | . . . | | | |              ,λx.
. . . . | | . . . | | | |               P>(a@0) ==> ∀v:<[locl(a)]
. . . . | | . . . | | | |                                ,λx.
. . . . | | . . . | | | |                                 T>(...)?Top.
. . . . | | . . . | | | |       ¬P@0((λx.s(i;t').x),v)
. . . . | | . . . | | | 12. ∀t:ℕ.
. . . . | | . . . | | | |   ¬isnull(a(i;t))
. . . . | | . . . | | | |   ⇒
. . . . | | . . . | | | |   (islocal(kind(a(i;t)))
. . . . | | . . . | | | |    ⇒
. . . . | | . . . | | | |    (eqof(IdDeq)(a,act(kind(a(i;t))))
. . . . | | . . . | | | |     ∨₂ false₂)
. . . . | | . . . | | | |    ⇒
. . . . | | . . . | | | |    P((λx.s(i;t).x),val(a(i;t))))
. . . . | | . . . | | | |   & (∀x:Id.
. . . . | | . . . | | | |      deq-member(...;<kind(a(i;t)),x>;1of())
. . . . | | . . . | | | |      ⇒
. . . . | | . . . | | | |      s(i;t+1).x
. . . . | | . . . | | | |      =
. . . . | | . . . | | | |      2of()
. . . . | | . . . | | | |      (<kind(a(i;t)),x>
```

```
. . . . | | . . . | | |      ,λx.s(i;t).x
. . . . | | . . . | | |      ,val(a(i;t))))
. . . . | | . . . | | |   & (∀l:IdLnk.
. . . . | | . . . | | |      deq-member(...;<kind(a(i;t)),l>;1of())
. . . . | | . . . | | |      ⇒
. . . . | | . . . | | |      withlnk(l;m(i;t))
. . . . | | . . . | | |      =
. . . . | | . . . | | |      if source(l) = i→
. . . . | | . . . | | |         concat(map(λtgf.map(λx.
. . . . | | . . . | | |         <1of(tgf)
. . . . | | . . . | | |         ,x>;2of(tgf)
. . . . | | . . . | | |             ((λx.s(i;t).x)
. . . . | | . . . | | |             ,val(a(i;t))));...))
. . . . | | . . . | | |      else nil fi)
. . . . | | . . . | | |   & (∀x:Id.
. . . . | | . . . | | |      ¬(deq-member(IdDeq;x;1of())
. . . . | | . . . | | |        ⇒
. . . . | | . . . | | |        deq-member(KindDeq;kind(a(i;t));2of()
. . . . | | . . . | | |                                        (x)))
. . . . | | . . . | | |      ⇒
. . . . | | . . . | | |      s(i;t).x = s(i;t+1).x)
. . . . | | . . . | | |   & (∀l:IdLnk, tg:Id.
. . . . | | . . . | | |      ¬(deq-member(...;<l,tg>;1of())
. . . . | | . . . | | |        ⇒
. . . . | | . . . | | |        deq-member(KindDeq;kind(a(i;t));...))
. . . . | | . . . | | |      ⇒
. . . . | | . . . | | |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . | | . . . | | 13. ∀x:Id.
. . . . | | . . . | | |   deq-member(IdDeq;x;1of())
. . . . | | . . . | | |   ⇒
. . . . | | . . . | | |   s(i;0).x = 2of()(x)
. . . . | | . . . | | 14. ∀a@0:Action(i).
. . . . | | . . . | | |   ¬isnull(a@0)
. . . . | | . . . | | |   ⇒
. . . . | | . . . | | |   (valtype(i;a@0) ⊆r <[locl(a)]
. . . . | | . . . | | |                      ,λx.T>(kind(a@0))?Top)
. . . . | | . . . | | 15. ∀x:Id.
. . . . | | . . . | | |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(
. . . . | | . . . | | |                                        ds))→
. . . . | | . . . | | |                     2of(ds)(x)
. . . . | | . . . | | |                  else Top fi
. . . . | | . . . | | 16. IdDeq ∈ EqDecider(Id)
. . . . | | . . . | | 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . | | . . . | | 18. j : Id
. . . . | | . . . | | 19. t : ℕ
. . . . | | . . . | | 20. j = i
. . . . | | . . . | | 21. ¬isnull(a(j;t))

. . . . | | . . . | | 22. ¬isnull(a(i;t))
. . . . | | . . . | | 23. (λx.s(i;t).x) ∈ State(ds)
. . . . | | . . . | | 24. kind(a(j;t)) = locl(a)
. . . . | | . . . | | 25. P((λx.s(i;t).x),val(a(i;t)))
. . . . | | . . . | | 26. valtype(i;a(i;t)) ⊆r <[locl(a)]
. . . . | | . . . | | |                      ,λx.
. . . . | | . . . | | |                       T>(kind(a(i;t)))?Top
. . . . | | . . . | | ⊢  locl(a) = kind(a(i;t))
```

```
. . . . | | . . . | | | by Assert (kind(a(j;t)) = kind(a(i;t)))
. . . . | | . . . | | |
. . . . | | . . . | | |\
. . . . | | . . . | | | .....assertion .....
. . . . | | . . . | | | 1. i : Id
. . . . | | . . . | | | 2. a : Id
. . . . | | . . . | | | 3. T : Type
. . . . | | . . . | | | 4. ds : x:Id fp-> Type
. . . . | | . . . | | | 5. P : State(ds)→T→Prop
. . . . | | . . . | | | 6. w : World
. . . . | | . . . | | | 7. FairFifo
. . . . | | . . . | | | 8. FairFifo
. . . . | | . . . | | | 9. ∀l:IdLnk, tg:Id.
. . . . | | . . . | | |    (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . | | . . . | | |                       <ds
. . . . | | . . . | | |                       ,<[locl(a)],λx.T>
. . . . | | . . . | | |                       ,
. . . . | | . . . | | |                       ,<[a],λx.P>
. . . . | | . . . | | |                       ,
. . . . | | . . . | | |                       ,
. . . . | | . . . | | |                       ,
. . . . | | . . . | | |                       ,
. . . . | | . . . | | |                       ,·>
. . . . | | . . . | | |                    else  fi.da(rcv(l; tg))
. . . . | | . . . | | | 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . | | . . . | | | 11. ∀a@0:Id, t:ℕ.
. . . . | | . . . | | |     ∃t':ℕ.
. . . . | | . . . | | |     t≤t'
. . . . | | . . . | | |     & ¬isnull(a(i;t'))
. . . . | | . . . | | |       & kind(a(i;t')) = locl(a@0)
. . . . | | . . . | | |       ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . | | . . . | | |       ∨ P@0 != <[a]
. . . . | | . . . | | |                ,λx.
. . . . | | . . . | | |                 P>(a@0) ==> ∀v:<[locl(a)]
. . . . | | . . . | | |                                ,λx.
. . . . | | . . . | | |                                 T>(...)?Top.
. . . . | | . . . | | |         ¬P@0((λx.s(i;t').x),v)
. . . . | | . . . | | | 12. ∀t:ℕ.
. . . . | | . . . | | |     ¬isnull(a(i;t))
. . . . | | . . . | | |     ⇒
. . . . | | . . . | | |     (islocal(kind(a(i;t)))
. . . . | | . . . | | |      ⇒
. . . . | | . . . | | |      (eqof(IdDeq)(a,act(kind(a(i;t))))
. . . . | | . . . | | |       ∨₂ false₂)
. . . . | | . . . | | |      ⇒
. . . . | | . . . | | |      P((λx.s(i;t).x),val(a(i;t))))
. . . . | | . . . | | |     & (∀x:Id.
. . . . | | . . . | | |        deq-member(...;<kind(a(i;t)),x>;1of())
. . . . | | . . . | | |        ⇒
. . . . | | . . . | | |        s(i;t+1).x
. . . . | | . . . | | |        =
. . . . | | . . . | | |        2of()
. . . . | | . . . | | |        (<kind(a(i;t)),x>
. . . . | | . . . | | |        ,λx.s(i;t).x
. . . . | | . . . | | |        ,val(a(i;t))))
```

```
. . . . | | . . . | | |     & (∀l:IdLnk.
. . . . | | . . . | | |        deq-member(...;<kind(a(i;t)),l>;1of())
. . . . | | . . . | | |        ⇒
. . . . | | . . . | | |        withlnk(l;m(i;t))
. . . . | | . . . | | |        =
. . . . | | . . . | | |        if source(l) = i⟶
. . . . | | . . . | | |           concat(map(λtgf.map(λx.
. . . . | | . . . | | |           <1of(tgf)
. . . . | | . . . | | |           ,x>;2of(tgf)
. . . . | | . . . | | |               ((λx.s(i;t).x)
. . . . | | . . . | | |               ,val(a(i;t))));...))
. . . . | | . . . | | |        else nil fi)
. . . . | | . . . | | |     & (∀x:Id.
. . . . | | . . . | | |        ¬(deq-member(IdDeq;x;1of())
. . . . | | . . . | | |          ⇒
. . . . | | . . . | | |          deq-member(KindDeq;kind(a(i;t));2of()
. . . . | | . . . | | |                                          (x)))
. . . . | | . . . | | |        ⇒
. . . . | | . . . | | |        s(i;t).x = s(i;t+1).x)
. . . . | | . . . | | |     & (∀l:IdLnk, tg:Id.
. . . . | | . . . | | |        ¬(deq-member(...;<l,tg>;1of())
. . . . | | . . . | | |          ⇒
. . . . | | . . . | | |          deq-member(KindDeq;kind(a(i;t));...))
. . . . | | . . . | | |        ⇒
. . . . | | . . . | | |        w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . | | . . . | | | 13. ∀x:Id.
. . . . | | . . . | | |     deq-member(IdDeq;x;1of())
. . . . | | . . . | | |     ⇒
. . . . | | . . . | | |     s(i;0).x = 2of()(x)
. . . . | | . . . | | | 14. ∀a@0:Action(i).
. . . . | | . . . | | |     ¬isnull(a@0)
. . . . | | . . . | | |     ⇒
. . . . | | . . . | | |     (valtype(i;a@0) ⊆r <[locl(a)]
. . . . | | . . . | | |                         ,λx.T>(kind(a@0))?Top)
. . . . | | . . . | | | 15. ∀x:Id.
. . . . | | . . . | | |     vartype(i;x) ⊆r if deq-member(...;x;1of(
. . . . | | . . . | | |                                          ds))⟶
. . . . | | . . . | | |                            2of(ds)(x)
. . . . | | . . . | | |                        else Top fi
. . . . | | . . . | | | 16. IdDeq ∈ EqDecider(Id)
. . . . | | . . . | | | 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . | | . . . | | | 18. j : Id
. . . . | | . . . | | | 19. t : ℕ
. . . . | | . . . | | | 20. j = i
. . . . | | . . . | | | 21. ¬isnull(a(j;t))
. . . . | | . . . | | | 22. ¬isnull(a(i;t))
. . . . | | . . . | | | 23. (λx.s(i;t).x) ∈ State(ds)
. . . . | | . . . | | | 24. kind(a(j;t)) = locl(a)
. . . . | | . . . | | | 25. P((λx.s(i;t).x),val(a(i;t)))
. . . . | | . . . | | | 26. valtype(i;a(i;t)) ⊆r <[locl(a)]
. . . . | | . . . | | |                            ,λx.
. . . . | | . . . | | |                             T>(kind(a(i;t)))?Top
. . . . | | . . . | | | ⊢  kind(a(j;t)) = kind(a(i;t))
. . . . | | . . . | | |   by Analyze THEN Analyze
. . . . | | . . . | | |
```

```
. . . . | | . . . | | .\
. . . . | | . . . | | . 1. i : Id
. . . . | | . . . | | . 2. a : Id
. . . . | | . . . | | . 3. T : Type
. . . . | | . . . | | . 4. ds : x:Id fp-> Type
. . . . | | . . . | | . 5. P : State(ds)→T→Prop
. . . . | | . . . | | . 6. w : World
. . . . | | . . . | | . 7. FairFifo
. . . . | | . . . | | . 8. FairFifo
. . . . | | . . . | | . 9. ∀l:IdLnk, tg:Id.
. . . . | | . . . | | .    (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . | | . . . | | .                      <ds
. . . . | | . . . | | .                      ,<[locl(a)],λx.T>
. . . . | | . . . | | .                      ,
. . . . | | . . . | | .                      ,<[a],λx.P>
. . . . | | . . . | | .                      ,
. . . . | | . . . | | .                      ,
. . . . | | . . . | | .                      ,
. . . . | | . . . | | .                      ,
. . . . | | . . . | | .                      ,.>
. . . . | | . . . | | .                    else  fi.da(rcv(l; tg))
. . . . | | . . . | | . 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . | | . . . | | . 11. ∀a@0:Id, t:ℕ.
. . . . | | . . . | | .     ∃t':ℕ.
. . . . | | . . . | | .     t≤t'
. . . . | | . . . | | .     & ¬isnull(a(i;t'))
. . . . | | . . . | | .       & kind(a(i;t')) = locl(a@0)
. . . . | | . . . | | .       ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . | | . . . | | .       ∨ P@0 != <[a]
. . . . | | . . . | | .                ,λx.
. . . . | | . . . | | .                 P>(a@0) ==> ∀v:<[locl(a)]
. . . . | | . . . | | .                                ,λx.
. . . . | | . . . | | .                                 T>(...)?Top.
. . . . | | . . . | | .         ¬P@0((λx.s(i;t').x),v)
. . . . | | . . . | | . 12. ∀t:ℕ.
. . . . | | . . . | | .     ¬isnull(a(i;t))
. . . . | | . . . | | .     ⇒
. . . . | | . . . | | .     (islocal(kind(a(i;t)))
. . . . | | . . . | | .      ⇒
. . . . | | . . . | | .      (eqof(IdDeq)(a,act(kind(a(i;t))))
. . . . | | . . . | | .       ∨₂ false₂)
. . . . | | . . . | | .      ⇒
. . . . | | . . . | | .      P((λx.s(i;t).x),val(a(i;t))))
. . . . | | . . . | | .     & (∀x:Id.
. . . . | | . . . | | .        deq-member(...;<kind(a(i;t)),x>;1of())
. . . . | | . . . | | .        ⇒
. . . . | | . . . | | .        s(i;t+1).x
. . . . | | . . . | | .        =
. . . . | | . . . | | .        2of()
. . . . | | . . . | | .        (<kind(a(i;t)),x>
. . . . | | . . . | | .        ,λx.s(i;t).x
. . . . | | . . . | | .        ,val(a(i;t))))
. . . . | | . . . | | .     & (∀l:IdLnk.
. . . . | | . . . | | .        deq-member(...;<kind(a(i;t)),l>;1of())
. . . . | | . . . | | .        ⇒
```

```
withlnk(l;m(i;t))
=
if source(l) = i→
   concat(map(λtgf.map(λx.
   <1of(tgf)
   ,x>;2of(tgf)
       ((λx.s(i;t).x)
       ,val(a(i;t))));...))
else nil fi)
& (∀x:Id.
   ¬(deq-member(IdDeq;x;1of())
     ⇒
     deq-member(KindDeq;kind(a(i;t));2of()
                                       (x)))
   ⇒
   s(i;t).x = s(i;t+1).x)
& (∀l:IdLnk, tg:Id.
   ¬(deq-member(...;<l,tg>;1of())
     ⇒
     deq-member(KindDeq;kind(a(i;t));...))
   ⇒
   w-tagged(tg; onlnk(l;m(i;t))) = nil)
13. ∀x:Id.
    deq-member(IdDeq;x;1of())
    ⇒
    s(i;0).x = 2of()(x)
14. ∀a@0:Action(i).
    ¬isnull(a@0)
    ⇒
    (valtype(i;a@0) ⊆r <[locl(a)]
                        ,λx.T>(kind(a@0))?Top)
15. ∀x:Id.
    vartype(i;x) ⊆r if deq-member(...;x;1of(
                                       ds))→
                        2of(ds)(x)
                    else Top fi
16. IdDeq ∈ EqDecider(Id)
17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
18. j : Id
19. t : ℕ
20. j = i
21. ¬isnull(a(j;t))
22. ¬isnull(a(i;t))
23. (λx.s(i;t).x) ∈ State(ds)
24. kind(a(j;t)) = locl(a)
25. P((λx.s(i;t).x),val(a(i;t)))
26. valtype(i;a(i;t)) ⊆r <[locl(a)]
                          ,λx.
                           T>(kind(a(i;t)))?Top
27. kind(a(j;t)) = kind(a(i;t))
⊢  locl(a) = kind(a(i;t))  by Auto

.\
1. i : Id
2. a : Id
```

```
. . . . | | . . . | . 3. T : Type
. . . . | | . . . | . 4. ds : x:Id fp-> Type
. . . . | | . . . | . 5. P : State(ds)→T→Prop
. . . . | | . . . | . 6. w : World
. . . . | | . . . | . 7. FairFifo
. . . . | | . . . | . 8. FairFifo
. . . . | | . . . | . 9. ∀l:IdLnk, tg:Id.
. . . . | | . . . | . |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . | | . . . | . |                  <ds
. . . . | | . . . | . |                  ,<[locl(a)],λx.T>
. . . . | | . . . | . |                  ,
. . . . | | . . . | . |                  ,<[a],λx.P>
. . . . | | . . . | . |                  ,
. . . . | | . . . | . |                  ,
. . . . | | . . . | . |                  ,
. . . . | | . . . | . |                  ,
. . . . | | . . . | . |                  ,·>
. . . . | | . . . | . |               else  fi.da(rcv(l; tg))
. . . . | | . . . | . 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . | | . . . | . 11. ∀a@0:Id, t:ℕ.
. . . . | | . . . | . |   ∃t':ℕ.
. . . . | | . . . | . |   t≤t'
. . . . | | . . . | . |   & ¬isnull(a(i;t'))
. . . . | | . . . | . |     & kind(a(i;t')) = locl(a@0)
. . . . | | . . . | . |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . | | . . . | . |     ∨ P@0 != <[a]
. . . . | | . . . | . |              ,λx.
. . . . | | . . . | . |               P>(a@0) ==> ∀v:<[locl(a)]
. . . . | | . . . | . |                                ,λx.
. . . . | | . . . | . |                                 T>(...)?Top.
. . . . | | . . . | . |       ¬P@0((λx.s(i;t').x),v)
. . . . | | . . . | . 12. ∀t:ℕ.
. . . . | | . . . | . |   ¬isnull(a(i;t))
. . . . | | . . . | . |   ⇒
. . . . | | . . . | . |   (islocal(kind(a(i;t)))
. . . . | | . . . | . |    ⇒
. . . . | | . . . | . |    (eqof(IdDeq)(a,act(kind(a(i;t))))
. . . . | | . . . | . |     ∨₂ false₂)
. . . . | | . . . | . |    ⇒
. . . . | | . . . | . |    P((λx.s(i;t).x),val(a(i;t))))
. . . . | | . . . | . |   & (∀x:Id.
. . . . | | . . . | . |      deq-member(...;<kind(a(i;t)),x>;1of())
. . . . | | . . . | . |      ⇒
. . . . | | . . . | . |      s(i;t+1).x
. . . . | | . . . | . |      =
. . . . | | . . . | . |      2of()
. . . . | | . . . | . |      (<kind(a(i;t)),x>
. . . . | | . . . | . |      ,λx.s(i;t).x
. . . . | | . . . | . |      ,val(a(i;t))))
. . . . | | . . . | . |   & (∀l:IdLnk.
. . . . | | . . . | . |      deq-member(...;<kind(a(i;t)),l>;1of())
. . . . | | . . . | . |      ⇒
. . . . | | . . . | . |      withlnk(l;m(i;t))
. . . . | | . . . | . |      =
. . . . | | . . . | . |      if source(l) = i→
```

```
. . . . | | . . . | . |         concat(map(λtgf.map(λx.
. . . . | | . . . | . |         <1of(tgf)
. . . . | | . . . | . |         ,x>;2of(tgf)
. . . . | | . . . | . |             ((λx.s(i;t).x)
. . . . | | . . . | . |             ,val(a(i;t))));...))
. . . . | | . . . | . |      else nil fi)
. . . . | | . . . | . |   & (∀x:Id.
. . . . | | . . . | . |      ¬(deq-member(IdDeq;x;1of())
. . . . | | . . . | . |        ⇒
. . . . | | . . . | . |        deq-member(KindDeq;kind(a(i;t));2of()
. . . . | | . . . | . |                                        (x)))
. . . . | | . . . | . |      ⇒
. . . . | | . . . | . |      s(i;t).x = s(i;t+1).x)
. . . . | | . . . | . |   & (∀l:IdLnk, tg:Id.
. . . . | | . . . | . |      ¬(deq-member(...;<l,tg>;1of())
. . . . | | . . . | . |        ⇒
. . . . | | . . . | . |        deq-member(KindDeq;kind(a(i;t));...))

. . . . | | . . . | . |      ⇒
. . . . | | . . . | . |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . | | . . . | . 13. ∀x:Id.
. . . . | | . . . | . |   deq-member(IdDeq;x;1of())
. . . . | | . . . | . |   ⇒
. . . . | | . . . | . |   s(i;0).x = 2of()(x)
. . . . | | . . . | . 14. ∀a@0:Action(i).
. . . . | | . . . | . |   ¬isnull(a@0)
. . . . | | . . . | . |   ⇒
. . . . | | . . . | . |   (valtype(i;a@0) ⊆r <[locl(a)]
. . . . | | . . . | . |                      ,λx.T>(kind(a@0))?Top)
. . . . | | . . . | . 15. ∀x:Id.
. . . . | | . . . | . |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(
. . . . | | . . . | . |                                        ds))→
. . . . | | . . . | . |                      2of(ds)(x)
. . . . | | . . . | . |                  else Top fi
. . . . | | . . . | . 16. IdDeq ∈ EqDecider(Id)
. . . . | | . . . | . 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . | | . . . | . 18. j : Id
. . . . | | . . . | . 19. t : ℕ
. . . . | | . . . | . 20. j = i
. . . . | | . . . | . 21. ¬isnull(a(j;t))
. . . . | | . . . | . 22. ¬isnull(a(i;t))
. . . . | | . . . | . 23. (λx.s(i;t).x) ∈ State(ds)
. . . . | | . . . | . 24. kind(<j,t>) = locl(a)
. . . . | | . . . | . 25. P((λx.s(i;t).x),val(a(i;t)))
. . . . | | . . . | . 26. valtype(i;a(i;t)) ⊆r <[locl(a)]
. . . . | | . . . | . |                         ,λx.
. . . . | | . . . | . |                          T>(kind(a(i;t)))?Top
. . . . | | . . . | . 27. locl(a) = kind(a(i;t))
. . . . | | . . . | . ⊢  valtype(i;a(i;t)) ⊆r T  by Assert True
. . . . | | . . . | . |
. . . . | | . . . | . |\
. . . . | | . . . | . | .....assertion .....
. . . . | | . . . | . | 1. i : Id
. . . . | | . . . | . | 2. a : Id
. . . . | | . . . | . | 3. T : Type
. . . . | | . . . | . | 4. ds : x:Id fp-> Type
```

```
. . . . | | . . . | . | 5. P : State(ds)→T→Prop
. . . . | | . . . | . | 6. w : World
. . . . | | . . . | . | 7. FairFifo
. . . . | | . . . | . | 8. FairFifo
. . . . | | . . . | . | 9. ∀l:IdLnk, tg:Id.
. . . . | | . . . | . |    (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . | | . . . | . |                       <ds
. . . . | | . . . | . |                       ,<[locl(a)],λx.T>
. . . . | | . . . | . |                       ,
. . . . | | . . . | . |                       ,<[a],λx.P>
. . . . | | . . . | . |                       ,
. . . . | | . . . | . |                       ,
. . . . | | . . . | . |                       ,
. . . . | | . . . | . |                       ,
. . . . | | . . . | . |                       ,·>
. . . . | | . . . | . |                    else  fi.da(rcv(l; tg))
. . . . | | . . . | . | 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . | | . . . | . | 11. ∀a@0:Id, t:ℕ.
. . . . | | . . . | . |     ∃t':ℕ.
. . . . | | . . . | . |     t≤t'
. . . . | | . . . | . |     & ¬isnull(a(i;t'))
. . . . | | . . . | . |       & kind(a(i;t')) = locl(a@0)
. . . . | | . . . | . |       ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . | | . . . | . |       ∨ P@0 != <[a]
. . . . | | . . . | . |                ,λx.
. . . . | | . . . | . |                 P>(a@0) ==> ∀v:<[locl(a)]
. . . . | | . . . | . |                                ,λx.
. . . . | | . . . | . |                                 T>(...)?Top.
. . . . | | . . . | . |         ¬P@0((λx.s(i;t').x),v)
. . . . | | . . . | . | 12. ∀t:ℕ.
. . . . | | . . . | . |     ¬isnull(a(i;t))
. . . . | | . . . | . |     ⇒
. . . . | | . . . | . |     (islocal(kind(a(i;t)))
. . . . | | . . . | . |      ⇒
. . . . | | . . . | . |      (eqof(IdDeq)(a,act(kind(a(i;t))))
. . . . | | . . . | . |       ∨₂ false₂)
. . . . | | . . . | . |      ⇒
. . . . | | . . . | . |      P((λx.s(i;t).x),val(a(i;t))))
. . . . | | . . . | . |     & (∀x:Id.
. . . . | | . . . | . |        deq-member(...;<kind(a(i;t)),x>;1of())
. . . . | | . . . | . |        ⇒
. . . . | | . . . | . |        s(i;t+1).x
. . . . | | . . . | . |        =
. . . . | | . . . | . |        2of()
. . . . | | . . . | . |        (<kind(a(i;t)),x>
. . . . | | . . . | . |        ,λx.s(i;t).x
. . . . | | . . . | . |        ,val(a(i;t))))
. . . . | | . . . | . |     & (∀l:IdLnk.
. . . . | | . . . | . |        deq-member(...;<kind(a(i;t)),l>;1of())
. . . . | | . . . | . |        ⇒
. . . . | | . . . | . |        withlnk(l;m(i;t))
. . . . | | . . . | . |        =
. . . . | | . . . | . |        if source(l) = i→
. . . . | | . . . | . |           concat(map(λtgf.map(λx.
. . . . | | . . . | . |           <1of(tgf)
```

```
. . . . | | . . . | . |           ,x>;2of(tgf)
. . . . | | . . . | . |               ((λx.s(i;t).x)
. . . . | | . . . | . |               ,val(a(i;t))));...))
. . . . | | . . . | . |       else nil fi)
. . . . | | . . . | . |     & (∀x:Id.
. . . . | | . . . | . |        ¬(deq-member(IdDeq;x;1of())
. . . . | | . . . | . |          ⇒
. . . . | | . . . | . |          deq-member(KindDeq;kind(a(i;t));2of()
. . . . | | . . . | . |                                        (x)))
. . . . | | . . . | . |        ⇒
. . . . | | . . . | . |        s(i;t).x = s(i;t+1).x)
. . . . | | . . . | . |     & (∀l:IdLnk, tg:Id.
. . . . | | . . . | . |        ¬(deq-member(...;<l,tg>;1of())
. . . . | | . . . | . |          ⇒
. . . . | | . . . | . |          deq-member(KindDeq;kind(a(i;t));...))
. . . . | | . . . | . |        ⇒
. . . . | | . . . | . |        w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . | | . . . | . | 13. ∀x:Id.
. . . . | | . . . | . |     deq-member(IdDeq;x;1of())
. . . . | | . . . | . |     ⇒
. . . . | | . . . | . |     s(i;0).x = 2of()(x)
. . . . | | . . . | . | 14. ∀a@0:Action(i).
. . . . | | . . . | . |     ¬isnull(a@0)
. . . . | | . . . | . |     ⇒
. . . . | | . . . | . |     (valtype(i;a@0) ⊆r <[locl(a)]
. . . . | | . . . | . |                         ,λx.T>(kind(a@0))?Top)
. . . . | | . . . | . | 15. ∀x:Id.
. . . . | | . . . | . |     vartype(i;x) ⊆r if deq-member(...;x;1of(
. . . . | | . . . | . |                                        ds))→
. . . . | | . . . | . |                       2of(ds)(x)
. . . . | | . . . | . |                    else Top fi
. . . . | | . . . | . | 16. IdDeq ∈ EqDecider(Id)
. . . . | | . . . | . | 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . | | . . . | . | 18. j : Id
. . . . | | . . . | . | 19. t : ℕ
. . . . | | . . . | . | 20. j = i
. . . . | | . . . | . | 21. ¬isnull(a(j;t))
. . . . | | . . . | . | 22. ¬isnull(a(i;t))
. . . . | | . . . | . | 23. (λx.s(i;t).x) ∈ State(ds)
. . . . | | . . . | . | 24. kind(<j,t>) = locl(a)
. . . . | | . . . | . | 25. P((λx.s(i;t).x),val(a(i;t)))
. . . . | | . . . | . | 26. valtype(i;a(i;t)) ⊆r <[locl(a)]
. . . . | | . . . | . |                           ,λx.
. . . . | | . . . | . |                            T>(kind(a(i;t)))?Top
. . . . | | . . . | . | 27. locl(a) = kind(a(i;t))
. . . . | | . . . | . | ⊢  True
. . . . | | . . . | . |   by Auto
. . . . | | . . . | . |      THEN
. . . . | | . . . | . |      Try
. . . . | | . . . | . |      (All (Unfold `dstype`) THEN All Reduce
. . . . | | . . . | . |       THEN
. . . . | | . . . | . |       Trivial)
. . . . | | . . . | . |
. . . . | | . . . | . .\
. . . . | | . . . | . . 1. i : Id
```

```
. . . . | | . . . | . . 2. a : Id
. . . . | | . . . | . . 3. T : Type
. . . . | | . . . | . . 4. ds : x:Id fp-> Type
. . . . | | . . . | . . 5. P : State(ds)→T→Prop
. . . . | | . . . | . . 6. w : World
. . . . | | . . . | . . 7. FairFifo
. . . . | | . . . | . . 8. FairFifo
. . . . | | . . . | . . 9. ∀l:IdLnk, tg:Id.
. . . . | | . . . | . . |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . | | . . . | . . |                  <ds
. . . . | | . . . | . . |                  ,<[locl(a)],λx.T>
. . . . | | . . . | . . |                  ,
. . . . | | . . . | . . |                  ,<[a],λx.P>
. . . . | | . . . | . . |                  ,
. . . . | | . . . | . . |                  ,
. . . . | | . . . | . . |                  ,
. . . . | | . . . | . . |                  ,
. . . . | | . . . | . . |                  ,·>
. . . . | | . . . | . . |               else  fi.da(rcv(l; tg))
. . . . | | . . . | . . 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . | | . . . | . . 11. ∀a@0:Id, t:ℕ.
. . . . | | . . . | . . |   ∃t':ℕ.
. . . . | | . . . | . . |   t≤t'
. . . . | | . . . | . . |   & ¬isnull(a(i;t'))
. . . . | | . . . | . . |     & kind(a(i;t')) = locl(a@0)
. . . . | | . . . | . . |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . | | . . . | . . |     ∨ P@0 != <[a]
. . . . | | . . . | . . |              ,λx.
. . . . | | . . . | . . |               P>(a@0) ==> ∀v:<[locl(a)]
. . . . | | . . . | . . |                                ,λx.
. . . . | | . . . | . . |                                 T>(...)?Top.
. . . . | | . . . | . . |       ¬P@0((λx.s(i;t').x),v)
. . . . | | . . . | . . 12. ∀t:ℕ.
. . . . | | . . . | . . |   ¬isnull(a(i;t))
. . . . | | . . . | . . |   ⇒
. . . . | | . . . | . . |   (islocal(kind(a(i;t)))
. . . . | | . . . | . . |    ⇒
. . . . | | . . . | . . |    (eqof(IdDeq)(a,act(kind(a(i;t))))
. . . . | | . . . | . . |     ∨₂ false₂)
. . . . | | . . . | . . |    ⇒
. . . . | | . . . | . . |    P((λx.s(i;t).x),val(a(i;t))))
. . . . | | . . . | . . |   & (∀x:Id.
. . . . | | . . . | . . |      deq-member(...;<kind(a(i;t)),x>;1of())
. . . . | | . . . | . . |      ⇒
. . . . | | . . . | . . |      s(i;t+1).x
. . . . | | . . . | . . |      =
. . . . | | . . . | . . |      2of()
. . . . | | . . . | . . |      (<kind(a(i;t)),x>
. . . . | | . . . | . . |      ,λx.s(i;t).x
. . . . | | . . . | . . |      ,val(a(i;t))))
. . . . | | . . . | . . |   & (∀l:IdLnk.
. . . . | | . . . | . . |      deq-member(...;<kind(a(i;t)),l>;1of())
. . . . | | . . . | . . |      ⇒
. . . . | | . . . | . . |      withlnk(l;m(i;t))
. . . . | | . . . | . . |      =
```

```
. . . . | | . . . | . . |      if source(l) = i→
. . . . | | . . . | . . |         concat(map(λtgf.map(λx.
. . . . | | . . . | . . |         <1of(tgf)
. . . . | | . . . | . . |         ,x>;2of(tgf)
. . . . | | . . . | . . |             ((λx.s(i;t).x)
. . . . | | . . . | . . |             ,val(a(i;t))));...))
. . . . | | . . . | . . |      else nil fi)
. . . . | | . . . | . . |   & (∀x:Id.
. . . . | | . . . | . . |      ¬(deq-member(IdDeq;x;1of())
. . . . | | . . . | . . |        ⇒
. . . . | | . . . | . . |        deq-member(KindDeq;kind(a(i;t));2of()
. . . . | | . . . | . . |                                        (x)))
. . . . | | . . . | . . |      ⇒
. . . . | | . . . | . . |      s(i;t).x = s(i;t+1).x)
. . . . | | . . . | . . |   & (∀l:IdLnk, tg:Id.
. . . . | | . . . | . . |      ¬(deq-member(...;<l,tg>;1of())
. . . . | | . . . | . . |        ⇒
. . . . | | . . . | . . |        deq-member(KindDeq;kind(a(i;t));...))
. . . . | | . . . | . . |      ⇒
. . . . | | . . . | . . |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . | | . . . | . . 13. ∀x:Id.
. . . . | | . . . | . . |   deq-member(IdDeq;x;1of())
. . . . | | . . . | . . |   ⇒
. . . . | | . . . | . . |   s(i;0).x = 2of()(x)
. . . . | | . . . | . . 14. ∀a@0:Action(i).
. . . . | | . . . | . . |   ¬isnull(a@0)
. . . . | | . . . | . . |   ⇒
. . . . | | . . . | . . |   (valtype(i;a@0) ⊆r <[locl(a)]
. . . . | | . . . | . . |                      ,λx.T>(kind(a@0))?Top)
. . . . | | . . . | . . 15. ∀x:Id.
. . . . | | . . . | . . |   vartype(i;x) ⊆r if deq-member(...;x;1of(
. . . . | | . . . | . . |                                      ds))→
. . . . | | . . . | . . |                     2of(ds)(x)
. . . . | | . . . | . . |                  else Top fi
. . . . | | . . . | . . 16. IdDeq ∈ EqDecider(Id)
. . . . | | . . . | . . 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . | | . . . | . . 18. j : Id
. . . . | | . . . | . . 19. t : ℕ
. . . . | | . . . | . . 20. j = i
. . . . | | . . . | . . 21. ¬isnull(a(j;t))
. . . . | | . . . | . . 22. ¬isnull(a(i;t))
. . . . | | . . . | . . 23. (λx.s(i;t).x) ∈ State(ds)
. . . . | | . . . | . . 24. kind(<j,t>) = locl(a)
. . . . | | . . . | . . 25. P((λx.s(i;t).x),val(a(i;t)))
. . . . | | . . . | . . 26. valtype(i;a(i;t)) ⊆r <[locl(a)]
. . . . | | . . . | . . |                        ,λx.
. . . . | | . . . | . . |                         T>(kind(a(i;t)))?Top
. . . . | | . . . | . . 27. locl(a) = kind(a(i;t))
. . . . | | . . . | . . 28. True
. . . . | | . . . | . . ⊢  valtype(i;a(i;t)) ⊆r T
. . . . | | . . . | . . | by Assert (kind(a(i;t)) ∈ Knd)
. . . . | | . . . | . . |
. . . . | | . . . | . . |\
. . . . | | . . . | . . | .....assertion .....
. . . . | | . . . | . . | 1. i : Id
```

```
. . . . | | . . . | . . | 2. a : Id
. . . . | | . . . | . . | 3. T : Type
. . . . | | . . . | . . | 4. ds : x:Id fp-> Type
. . . . | | . . . | . . | 5. P : State(ds)→T→Prop
. . . . | | . . . | . . | 6. w : World
. . . . | | . . . | . . | 7. FairFifo
. . . . | | . . . | . . | 8. FairFifo
. . . . | | . . . | . . | 9. ∀l:IdLnk, tg:Id.
. . . . | | . . . | . . |    (w.M(l,tg)) ⊆r if eqof(IdDeq)
. . . . | | . . . | . . |                       (source(l)
. . . . | | . . . | . . |                       ,i)→
. . . . | | . . . | . . |                       <ds
. . . . | | . . . | . . |                       ,<[locl(a)],λx.T>
. . . . | | . . . | . . |                       ,
. . . . | | . . . | . . |                       ,<[a],λx.P>
. . . . | | . . . | . . |                       ,
. . . . | | . . . | . . |                       ,
. . . . | | . . . | . . |                       ,
. . . . | | . . . | . . |                       ,
. . . . | | . . . | . . |                       ,.>
. . . . | | . . . | . . |                     else  fi.da(rcv(l; tg))
. . . . | | . . . | . . | 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . | | . . . | . . | 11. ∀a@0:Id, t:ℕ.
. . . . | | . . . | . . |     ∃t':ℕ.
. . . . | | . . . | . . |     t≤t'
. . . . | | . . . | . . |     & ¬isnull(a(i;t'))
. . . . | | . . . | . . |       & kind(a(i;t')) = locl(a@0)
. . . . | | . . . | . . |       ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . | | . . . | . . |       ∨ P@0 != <[a]
. . . . | | . . . | . . |                ,λx.
. . . . | | . . . | . . |                 P>(a@0) ==> ∀v:<[locl(a)]
. . . . | | . . . | . . |                                ,λx.
. . . . | | . . . | . . |                                 T>(...)?Top.
. . . . | | . . . | . . |         ¬P@0((λx.s(i;t').x),v)
. . . . | | . . . | . . | 12. ∀t:ℕ.
. . . . | | . . . | . . |     ¬isnull(a(i;t))
. . . . | | . . . | . . |     ⇒
. . . . | | . . . | . . |     (islocal(kind(a(i;t)))
. . . . | | . . . | . . |      ⇒
. . . . | | . . . | . . |      (eqof(IdDeq)(a,act(kind(a(i;t))))
. . . . | | . . . | . . |       ∨₂ false₂)
. . . . | | . . . | . . |      ⇒
. . . . | | . . . | . . |      P((λx.s(i;t).x),val(a(i;t))))
. . . . | | . . . | . . |     & (∀x:Id.
. . . . | | . . . | . . |        deq-member(...;<kind(a(i;t)),x>;1of(
. . . . | | . . . | . . |                                          ))
. . . . | | . . . | . . |        ⇒
. . . . | | . . . | . . |        s(i;t+1).x
. . . . | | . . . | . . |        =
. . . . | | . . . | . . |        2of()
. . . . | | . . . | . . |        (<kind(a(i;t)),x>
. . . . | | . . . | . . |        ,λx.s(i;t).x
. . . . | | . . . | . . |        ,val(a(i;t))))
. . . . | | . . . | . . |     & (∀l:IdLnk.
. . . . | | . . . | . . |        deq-member(...;<kind(a(i;t)),l>;1of(
```

```
. . . . | | . . . | . . |                                          ))
. . . . | | . . . | . . |        ⇒
. . . . | | . . . | . . |        withlnk(l;m(i;t))
. . . . | | . . . | . . |        =
. . . . | | . . . | . . |        if source(l) = i→
. . . . | | . . . | . . |           concat(map(λtgf.map(λx.
. . . . | | . . . | . . |           <1of(tgf)
. . . . | | . . . | . . |           ,x>;2of(tgf)
. . . . | | . . . | . . |               ((λx.s(i;t).x)
. . . . | | . . . | . . |               ,val(a(i;t))));2of()
. . . . | | . . . | . . |                                (<kind(a(i;t))
. . . . | | . . . | . . |                                 ,l>)))
. . . . | | . . . | . . |        else nil fi)
. . . . | | . . . | . . |     & (∀x:Id.
. . . . | | . . . | . . |        ¬(deq-member(IdDeq;x;1of())
. . . . | | . . . | . . |          ⇒
. . . . | | . . . | . . |          deq-member(KindDeq;kind(...);2of()
. . . . | | . . . | . . |                                    (x)))
. . . . | | . . . | . . |        ⇒
. . . . | | . . . | . . |        s(i;t).x = s(i;t+1).x)
. . . . | | . . . | . . |     & (∀l:IdLnk, tg:Id.
. . . . | | . . . | . . |        ¬(deq-member(...;<l,tg>;1of())
. . . . | | . . . | . . |          ⇒
. . . . | | . . . | . . |          deq-member(KindDeq;kind(...);...))
. . . . | | . . . | . . |        ⇒
. . . . | | . . . | . . |        w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . | | . . . | . . | 13. ∀x:Id.
. . . . | | . . . | . . |     deq-member(IdDeq;x;1of())
. . . . | | . . . | . . |     ⇒
. . . . | | . . . | . . |     s(i;0).x = 2of()(x)
. . . . | | . . . | . . | 14. ∀a@0:Action(i).
. . . . | | . . . | . . |     ¬isnull(a@0)
. . . . | | . . . | . . |     ⇒
. . . . | | . . . | . . |     (valtype(i;a@0) ⊆r <[locl(a)]
. . . . | | . . . | . . |                        ,λx.
. . . . | | . . . | . . |                         T>(kind(a@0))?Top)
. . . . | | . . . | . . | 15. ∀x:Id.
. . . . | | . . . | . . |     vartype(i;x) ⊆r if ...→
. . . . | | . . . | . . |                          2of(ds)(x)
. . . . | | . . . | . . |                      else Top fi
. . . . | | . . . | . . | 16. IdDeq ∈ EqDecider(Id)
. . . . | | . . . | . . | 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . | | . . . | . . | 18. j : Id
. . . . | | . . . | . . | 19. t : ℕ
. . . . | | . . . | . . | 20. j = i
. . . . | | . . . | . . | 21. ¬isnull(a(j;t))
. . . . | | . . . | . . | 22. ¬isnull(a(i;t))
. . . . | | . . . | . . | 23. (λx.s(i;t).x) ∈ State(ds)
. . . . | | . . . | . . | 24. kind(<j,t>) = locl(a)
. . . . | | . . . | . . | 25. P((λx.s(i;t).x),val(a(i;t)))
. . . . | | . . . | . . | 26. valtype(i;a(i;t)) ⊆r <[locl(a)]
. . . . | | . . . | . . |                           ,λx.
. . . . | | . . . | . . |                            T>(kind(...))?Top
. . . . | | . . . | . . | 27. locl(a) = kind(a(i;t))
. . . . | | . . . | . . | 28. True
```

```
. . . . | | . . . | . . | ⊢  kind(a(i;t)) ∈ Knd  by Auto
. . . . | | . . . | . . |
. . . . | | . . . | . . .\
. . . . | | . . . | . . . 1. i : Id
. . . . | | . . . | . . . 2. a : Id
. . . . | | . . . | . . . 3. T : Type
. . . . | | . . . | . . . 4. ds : x:Id fp-> Type
. . . . | | . . . | . . . 5. P : State(ds)→T→Prop
. . . . | | . . . | . . . 6. w : World
. . . . | | . . . | . . . 7. FairFifo
. . . . | | . . . | . . . 8. FairFifo
. . . . | | . . . | . . . 9. ∀l:IdLnk, tg:Id.
. . . . | | . . . | . . . |  (w.M(l,tg)) ⊆r if eqof(IdDeq)
. . . . | | . . . | . . . |                    (source(l)
. . . . | | . . . | . . . |                    ,i)→
. . . . | | . . . | . . . |                    <ds
. . . . | | . . . | . . . |                    ,<[locl(a)],λx.T>
. . . . | | . . . | . . . |                    ,
. . . . | | . . . | . . . |                    ,<[a],λx.P>
. . . . | | . . . | . . . |                    ,
. . . . | | . . . | . . . |                    ,
. . . . | | . . . | . . . |                    ,
. . . . | | . . . | . . . |                    ,
. . . . | | . . . | . . . |                    ,.>
. . . . | | . . . | . . . |                 else  fi.da(rcv(l; tg))
. . . . | | . . . | . . . 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . | | . . . | . . . 11. ∀a@0:Id, t:ℕ.
. . . . | | . . . | . . . |   ∃t':ℕ.
. . . . | | . . . | . . . |   t≤t'
. . . . | | . . . | . . . |   & ¬isnull(a(i;t'))
. . . . | | . . . | . . . |     & kind(a(i;t')) = locl(a@0)
. . . . | | . . . | . . . |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . | | . . . | . . . |     ∨ P@0 != <[a]
. . . . | | . . . | . . . |                ,λx.
. . . . | | . . . | . . . |                 P>(a@0) ==> ∀v:<[locl(a)]
. . . . | | . . . | . . . |                                ,λx.
. . . . | | . . . | . . . |                                 T>(...)?Top.
. . . . | | . . . | . . . |       ¬P@0((λx.s(i;t').x),v)
. . . . | | . . . | . . . 12. ∀t:ℕ.
. . . . | | . . . | . . . |   ¬isnull(a(i;t))
. . . . | | . . . | . . . |   ⇒
. . . . | | . . . | . . . |   (islocal(kind(a(i;t)))
. . . . | | . . . | . . . |    ⇒
. . . . | | . . . | . . . |    (eqof(IdDeq)(a,act(kind(a(i;t))))
. . . . | | . . . | . . . |     ∨₂ false₂)
. . . . | | . . . | . . . |    ⇒
. . . . | | . . . | . . . |    P((λx.s(i;t).x),val(a(i;t))))
. . . . | | . . . | . . . |   & (∀x:Id.
. . . . | | . . . | . . . |      deq-member(...;<kind(a(i;t)),x>;1of(
. . . . | | . . . | . . . |                                      ))
. . . . | | . . . | . . . |      ⇒
. . . . | | . . . | . . . |      s(i;t+1).x
. . . . | | . . . | . . . |      =
. . . . | | . . . | . . . |      2of()
. . . . | | . . . | . . . |      (<kind(a(i;t)),x>
```

```
. . . . | | . . . | . . . |      ,λx.s(i;t).x
. . . . | | . . . | . . . |      ,val(a(i;t))))
. . . . | | . . . | . . . |   & (∀l:IdLnk.
. . . . | | . . . | . . . |      deq-member(...;<kind(a(i;t)),l>;1of(
. . . . | | . . . | . . . |                                      ))
. . . . | | . . . | . . . |      ⇒
. . . . | | . . . | . . . |      withlnk(l;m(i;t))
. . . . | | . . . | . . . |      =
. . . . | | . . . | . . . |      if source(l) = i→
. . . . | | . . . | . . . |         concat(map(λtgf.map(λx.
. . . . | | . . . | . . . |         <1of(tgf)
. . . . | | . . . | . . . |         ,x>;2of(tgf)
. . . . | | . . . | . . . |             ((λx.s(i;t).x)
. . . . | | . . . | . . . |             ,val(a(i;t))));2of()
. . . . | | . . . | . . . |                              (<kind(a(i;t))
. . . . | | . . . | . . . |                               ,l>)))
. . . . | | . . . | . . . |      else nil fi)
. . . . | | . . . | . . . |   & (∀x:Id.
. . . . | | . . . | . . . |      ¬(deq-member(IdDeq;x;1of())
. . . . | | . . . | . . . |        ⇒
. . . . | | . . . | . . . |        deq-member(KindDeq;kind(...);2of()
. . . . | | . . . | . . . |                                      (x)))
. . . . | | . . . | . . . |      ⇒
. . . . | | . . . | . . . |      s(i;t).x = s(i;t+1).x)
. . . . | | . . . | . . . |   & (∀l:IdLnk, tg:Id.
. . . . | | . . . | . . . |      ¬(deq-member(...;<l,tg>;1of())
. . . . | | . . . | . . . |        ⇒
. . . . | | . . . | . . . |        deq-member(KindDeq;kind(...);...))
. . . . | | . . . | . . . |      ⇒
. . . . | | . . . | . . . |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . | | . . . | . . 13. ∀x:Id.
. . . . | | . . . | . . . |   deq-member(IdDeq;x;1of())
. . . . | | . . . | . . . |   ⇒
. . . . | | . . . | . . . |   s(i;0).x = 2of()(x)
. . . . | | . . . | . . 14. ∀a@0:Action(i).
. . . . | | . . . | . . . |   ¬isnull(a@0)
. . . . | | . . . | . . . |   ⇒
. . . . | | . . . | . . . |   (valtype(i;a@0) ⊆r <[locl(a)]
. . . . | | . . . | . . . |                     ,λx.
. . . . | | . . . | . . . |                      T>(kind(a@0))?Top)
. . . . | | . . . | . . 15. ∀x:Id.
. . . . | | . . . | . . . |   vartype(i;x) ⊆r if ...→
. . . . | | . . . | . . . |                      2of(ds)(x)
. . . . | | . . . | . . . |                   else Top fi
. . . . | | . . . | . . 16. IdDeq ∈ EqDecider(Id)
. . . . | | . . . | . . 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . | | . . . | . . 18. j : Id
. . . . | | . . . | . . 19. t : ℕ
. . . . | | . . . | . . 20. j = i
. . . . | | . . . | . . 21. ¬isnull(a(j;t))
. . . . | | . . . | . . 22. ¬isnull(a(i;t))
. . . . | | . . . | . . 23. (λx.s(i;t).x) ∈ State(ds)
. . . . | | . . . | . . 24. kind(<j,t>) = locl(a)
. . . . | | . . . | . . 25. P((λx.s(i;t).x),val(a(i;t)))
. . . . | | . . . | . . 26. valtype(i;a(i;t)) ⊆r <[locl(a)]
```

```
. . . . | | . . . | . . . |                        ,λx.
. . . . | | . . . | . . . |                         T>(kind(...))?Top
. . . . | | . . . | . . . 27. locl(a) = kind(a(i;t))
. . . . | | . . . | . . . 28. True
. . . . | | . . . | . . . 29. kind(a(i;t)) ∈ Knd
. . . . | | . . . | . . . ⊢  valtype(i;a(i;t)) ⊆r T
. . . . | | . . . | . . . | by Assert (locl(a) = kind(a(i;t)))
. . . . | | . . . | . . . |
. . . . | | . . . | . . . |\
. . . . | | . . . | . . . | .....assertion .....
. . . . | | . . . | . . . | 1. i : Id
. . . . | | . . . | . . . | 2. a : Id
. . . . | | . . . | . . . | 3. T : Type
. . . . | | . . . | . . . | 4. ds : x:Id fp-> Type
. . . . | | . . . | . . . | 5. P : State(ds)→T→Prop
. . . . | | . . . | . . . | 6. w : World
. . . . | | . . . | . . . | 7. FairFifo
. . . . | | . . . | . . . | 8. FairFifo
. . . . | | . . . | . . . | 9. ∀l:IdLnk, tg:Id.
. . . . | | . . . | . . . |    (w.M(l,tg)) ⊆r if eqof(IdDeq)
. . . . | | . . . | . . . |                       (source(l)
. . . . | | . . . | . . . |                       ,i)→
. . . . | | . . . | . . . |                       <ds
. . . . | | . . . | . . . |                       ,<[locl(a)],λx.T>
. . . . | | . . . | . . . |                       ,
. . . . | | . . . | . . . |                       ,<[a],λx.P>
. . . . | | . . . | . . . |                       ,
. . . . | | . . . | . . . |                       ,
. . . . | | . . . | . . . |                       ,
. . . . | | . . . | . . . |                       ,
. . . . | | . . . | . . . |                       ,·>
. . . . | | . . . | . . . |                    else  fi.da(rcv(l; tg))
. . . . | | . . . | . . . | 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . | | . . . | . . . | 11. ∀a@0:Id, t:ℕ.
. . . . | | . . . | . . . |     ∃t':ℕ.
. . . . | | . . . | . . . |     t≤t'
. . . . | | . . . | . . . |     & ¬isnull(a(i;t'))
. . . . | | . . . | . . . |       & kind(a(i;t')) = locl(a@0)
. . . . | | . . . | . . . |       ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . | | . . . | . . . |       ∨ P@0 != <[a]
. . . . | | . . . | . . . |                ,λx.
. . . . | | . . . | . . . |                 P>(a@0) ==> ∀v:....
. . . . | | . . . | . . . |          ¬P@0((λx.s(i;t').x),v)
. . . . | | . . . | . . . | 12. ∀t:ℕ.
. . . . | | . . . | . . . |     ¬isnull(a(i;t))
. . . . | | . . . | . . . |     ⇒
. . . . | | . . . | . . . |     (islocal(kind(a(i;t)))
. . . . | | . . . | . . . |      ⇒
. . . . | | . . . | . . . |      (eqof(IdDeq)(a,act(kind(a(i;t))))
. . . . | | . . . | . . . |       ∨₂ false₂)
. . . . | | . . . | . . . |      ⇒
. . . . | | . . . | . . . |      P((λx.s(i;t).x),val(a(i;t))))
. . . . | | . . . | . . . |     & (∀x:Id.
. . . . | | . . . | . . . |        deq-member(...;...;1of())
. . . . | | . . . | . . . |        ⇒
```

```
. . . . | | . . . | . . . |        s(i;t+1).x
. . . . | | . . . | . . . |        =
. . . . | | . . . | . . . |        2of()
. . . . | | . . . | . . . |        (<kind(a(i;t)),x>
. . . . | | . . . | . . . |        ,λx.s(i;t).x
. . . . | | . . . | . . . |        ,val(a(i;t))))
. . . . | | . . . | . . . |     & (∀l:IdLnk.
. . . . | | . . . | . . . |        deq-member(...;...;1of())
. . . . | | . . . | . . . |        ⇒
. . . . | | . . . | . . . |        withlnk(l;m(i;t))
. . . . | | . . . | . . . |        =
. . . . | | . . . | . . . |        if source(l) = i→
. . . . | | . . . | . . . |           concat(map(λtgf.map(λx.
. . . . | | . . . | . . . |           <1of(tgf)
. . . . | | . . . | . . . |           ,x>;2of(tgf)
. . . . | | . . . | . . . |               ((λx.s(i;t).x)
. . . . | | . . . | . . . |               ,val(a(i;t))));2of()
. . . . | | . . . | . . . |                                (<kind(...)
. . . . | | . . . | . . . |                                 ,l>)))
. . . . | | . . . | . . . |        else nil fi)
. . . . | | . . . | . . . |     & (∀x:Id.
. . . . | | . . . | . . . |        ¬...
. . . . | | . . . | . . . |        ⇒
. . . . | | . . . | . . . |        s(i;t).x = s(i;t+1).x)
. . . . | | . . . | . . . |     & (∀l:IdLnk, tg:Id.
. . . . | | . . . | . . . |        ¬...
. . . . | | . . . | . . . |        ⇒
. . . . | | . . . | . . . |        w-tagged(tg; onlnk(l;m(i;t)))
. . . . | | . . . | . . . |        =
. . . . | | . . . | . . . |        nil)
. . . . | | . . . | . . . | 13. ∀x:Id.
. . . . | | . . . | . . . |     deq-member(IdDeq;x;1of())
. . . . | | . . . | . . . |     ⇒
. . . . | | . . . | . . . |     s(i;0).x = 2of()(x)
. . . . | | . . . | . . . | 14. ∀a@0:Action(i).
. . . . | | . . . | . . . |     ¬isnull(a@0)
. . . . | | . . . | . . . |     ⇒
. . . . | | . . . | . . . |     (valtype(i;a@0) ⊆r <[locl(a)]
. . . . | | . . . | . . . |                         ,λx.
. . . . | | . . . | . . . |                          T>(kind(a@0))?Top)
. . . . | | . . . | . . . | 15. ∀x:Id.
. . . . | | . . . | . . . |     vartype(i;x) ⊆r if ...→
. . . . | | . . . | . . . |                         2of(ds)(x)
. . . . | | . . . | . . . |                      else Top fi
. . . . | | . . . | . . . | 16. IdDeq ∈ EqDecider(Id)
. . . . | | . . . | . . . | 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . | | . . . | . . . | 18. j : Id
. . . . | | . . . | . . . | 19. t : ℕ
. . . . | | . . . | . . . | 20. j = i
. . . . | | . . . | . . . | 21. ¬isnull(a(j;t))
. . . . | | . . . | . . . | 22. ¬isnull(a(i;t))
. . . . | | . . . | . . . | 23. (λx.s(i;t).x) ∈ State(ds)
. . . . | | . . . | . . . | 24. kind(<j,t>) = locl(a)
. . . . | | . . . | . . . | 25. P((λx.s(i;t).x),val(a(i;t)))
. . . . | | . . . | . . . | 26. valtype(i;a(i;t)) ⊆r <[locl(a)]
```

```
. . . . | | . . . | . . . |                          ,λx.
. . . . | | . . . | . . . |                           T>(...)?Top
. . . . | | . . . | . . . | 27. locl(a) = kind(a(i;t))
. . . . | | . . . | . . . | 28. True
. . . . | | . . . | . . . | 29. kind(a(i;t)) ∈ Knd
. . . . | | . . . | . . . | ⊢  locl(a) = kind(a(i;t))  by Auto
. . . . | | . . . | . . . |
. . . . | | . . . | . . .\
. . . . | | . . . | . . . . 1. i : Id
. . . . | | . . . | . . . . 2. a : Id
. . . . | | . . . | . . . . 3. T : Type
. . . . | | . . . | . . . . 4. ds : x:Id fp-> Type
. . . . | | . . . | . . . . 5. P : State(ds)→T→Prop
. . . . | | . . . | . . . . 6. w : World
. . . . | | . . . | . . . . 7. FairFifo
. . . . | | . . . | . . . . 8. FairFifo
. . . . | | . . . | . . . . 9. ∀l:IdLnk, tg:Id.
. . . . | | . . . | . . . . |  (w.M(l,tg)) ⊆r if eqof(IdDeq)
. . . . | | . . . | . . . . |                    (source(l)
. . . . | | . . . | . . . . |                    ,i)→
. . . . | | . . . | . . . . |                    <ds
. . . . | | . . . | . . . . |                    ,<[locl(a)],λx.T>
. . . . | | . . . | . . . . |                    ,
. . . . | | . . . | . . . . |                    ,<[a],λx.P>
. . . . | | . . . | . . . . |                    ,
. . . . | | . . . | . . . . |                    ,
. . . . | | . . . | . . . . |                    ,
. . . . | | . . . | . . . . |                    ,
. . . . | | . . . | . . . . |                    ,·>
. . . . | | . . . | . . . . |                 else  fi.da(rcv(l; tg))
. . . . | | . . . | . . . . 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . | | . . . | . . . . 11. ∀a@0:Id, t:ℕ.
. . . . | | . . . | . . . . |   ∃t':ℕ.
. . . . | | . . . | . . . . |   t≤t'
. . . . | | . . . | . . . . |   & ¬isnull(a(i;t'))
. . . . | | . . . | . . . . |     & kind(a(i;t')) = locl(a@0)
. . . . | | . . . | . . . . |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . | | . . . | . . . . |     ∨ P@0 != <[a]
. . . . | | . . . | . . . . |              ,λx.
. . . . | | . . . | . . . . |               P>(a@0) ==> ∀v:....
. . . . | | . . . | . . . . |       ¬P@0((λx.s(i;t').x),v)
. . . . | | . . . | . . . . 12. ∀t:ℕ.
. . . . | | . . . | . . . . |   ¬isnull(a(i;t))
. . . . | | . . . | . . . . |   ⇒
. . . . | | . . . | . . . . |   (islocal(kind(a(i;t)))
. . . . | | . . . | . . . . |    ⇒
. . . . | | . . . | . . . . |    (eqof(IdDeq)(a,act(kind(a(i;t))))
. . . . | | . . . | . . . . |     ∨₂ false₂)
. . . . | | . . . | . . . . |    ⇒
. . . . | | . . . | . . . . |    P((λx.s(i;t).x),val(a(i;t))))
. . . . | | . . . | . . . . |   & (∀x:Id.
. . . . | | . . . | . . . . |      deq-member(...;...;1of())
. . . . | | . . . | . . . . |      ⇒
. . . . | | . . . | . . . . |      s(i;t+1).x
. . . . | | . . . | . . . . |      =
```

```
. . . . | | . . . | . . . . |      2of()
. . . . | | . . . | . . . . |      (<kind(a(i;t)),x>
. . . . | | . . . | . . . . |      ,λx.s(i;t).x
. . . . | | . . . | . . . . |      ,val(a(i;t))))
. . . . | | . . . | . . . . |   & (∀l:IdLnk.
. . . . | | . . . | . . . . |      deq-member(...;...;1of())
. . . . | | . . . | . . . . |      ⇒
. . . . | | . . . | . . . . |      withlnk(l;m(i;t))
. . . . | | . . . | . . . . |      =
. . . . | | . . . | . . . . |      if source(l) = i→
. . . . | | . . . | . . . . |         concat(map(λtgf.map(λx.
. . . . | | . . . | . . . . |         <1of(tgf)
. . . . | | . . . | . . . . |         ,x>;2of(tgf)
. . . . | | . . . | . . . . |             ((λx.s(i;t).x)
. . . . | | . . . | . . . . |             ,val(a(i;t))));2of()
. . . . | | . . . | . . . . |                              (<kind(...)
. . . . | | . . . | . . . . |                               ,l>)))
. . . . | | . . . | . . . . |      else nil fi)
. . . . | | . . . | . . . . |   & (∀x:Id.
. . . . | | . . . | . . . . |      ¬...
. . . . | | . . . | . . . . |      ⇒
. . . . | | . . . | . . . . |      s(i;t).x = s(i;t+1).x)
. . . . | | . . . | . . . . |   & (∀l:IdLnk, tg:Id.
. . . . | | . . . | . . . . |      ¬...
. . . . | | . . . | . . . . |      ⇒
. . . . | | . . . | . . . . |      w-tagged(tg; onlnk(l;m(i;t)))
. . . . | | . . . | . . . . |      =
. . . . | | . . . | . . . . |      nil)
. . . . | | . . . | . . . . 13. ∀x:Id.
. . . . | | . . . | . . . . |   deq-member(IdDeq;x;1of())
. . . . | | . . . | . . . . |   ⇒
. . . . | | . . . | . . . . |   s(i;0).x = 2of()(x)
. . . . | | . . . | . . . . 14. ∀a@0:Action(i).
. . . . | | . . . | . . . . |   ¬isnull(a@0)
. . . . | | . . . | . . . . |   ⇒
. . . . | | . . . | . . . . |   (valtype(i;a@0) ⊆r <[locl(a)]
. . . . | | . . . | . . . . |                      ,λx.
. . . . | | . . . | . . . . |                       T>(kind(a@0))?Top)
. . . . | | . . . | . . . . 15. ∀x:Id.
. . . . | | . . . | . . . . |   vartype(i;x) ⊆r if ...→
. . . . | | . . . | . . . . |                      2of(ds)(x)
. . . . | | . . . | . . . . |                   else Top fi
. . . . | | . . . | . . . . 16. IdDeq ∈ EqDecider(Id)
. . . . | | . . . | . . . . 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . | | . . . | . . . . 18. j : Id
. . . . | | . . . | . . . . 19. t : ℕ
. . . . | | . . . | . . . . 20. j = i
. . . . | | . . . | . . . . 21. ¬isnull(a(j;t))
. . . . | | . . . | . . . . 22. ¬isnull(a(i;t))
. . . . | | . . . | . . . . 23. (λx.s(i;t).x) ∈ State(ds)
. . . . | | . . . | . . . . 24. kind(<j,t>) = locl(a)
. . . . | | . . . | . . . . 25. P((λx.s(i;t).x),val(a(i;t)))
. . . . | | . . . | . . . . 26. valtype(i;a(i;t)) ⊆r <[locl(a)]
. . . . | | . . . | . . . . |                        ,λx.
. . . . | | . . . | . . . . |                         T>(...)?Top
```

```
. . . . | | . . . | . . . . 27. locl(a) = kind(a(i;t))
. . . . | | . . . | . . . . 28. True

. . . . | | . . . | . . . . 29. kind(a(i;t)) ∈ Knd
. . . . | | . . . | . . . . 30. locl(a) = kind(a(i;t))
. . . . | | . . . | . . . . ⊢  valtype(i;a(i;t)) ⊆r T
. . . . | | . . . | . . . . | by RevHypSubst -1 -5
. . . . | | . . . | . . . . |
. . . . | | . . . | . . . . |\
. . . . | | . . . | . . . . | 1. i : Id
. . . . | | . . . | . . . . | 2. a : Id
. . . . | | . . . | . . . . | 3. T : Type
. . . . | | . . . | . . . . | 4. ds : x:Id fp-> Type
. . . . | | . . . | . . . . | 5. P : State(ds)→T→Prop
. . . . | | . . . | . . . . | 6. w : World
. . . . | | . . . | . . . . | 7. FairFifo
. . . . | | . . . | . . . . | 8. FairFifo
. . . . | | . . . | . . . . | 9. ∀l:IdLnk, tg:Id.
. . . . | | . . . | . . . . |    (w.M(l,tg)) ⊆r if eqof(IdDeq)
. . . . | | . . . | . . . . |                       (source(l)
. . . . | | . . . | . . . . |                       ,i)→
. . . . | | . . . | . . . . |                       <ds
. . . . | | . . . | . . . . |                       ,<[locl(a)],λx.T>
. . . . | | . . . | . . . . |                       ,
. . . . | | . . . | . . . . |                       ,<[a],λx.P>
. . . . | | . . . | . . . . |                       ,
. . . . | | . . . | . . . . |                       ,
. . . . | | . . . | . . . . |                       ,
. . . . | | . . . | . . . . |                       ,
. . . . | | . . . | . . . . |                       ,•>
. . . . | | . . . | . . . . |                     else  fi.da(rcv
. . . . | | . . . | . . . . |    (l; tg))
. . . . | | . . . | . . . . | 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . | | . . . | . . . . | 11. ∀a@0:Id, t:ℕ.
. . . . | | . . . | . . . . |     ∃t':ℕ.
. . . . | | . . . | . . . . |     t≤t'
. . . . | | . . . | . . . . |     & ¬isnull(a(i;t'))
. . . . | | . . . | . . . . |       & kind(a(i;t')) = locl(a@0)
. . . . | | . . . | . . . . |       ∨ ¬locl(a@0) ∈ dom(<[locl(a)]
. . . . | | . . . | . . . . |                           ,λx.T>)
. . . . | | . . . | . . . . |       ∨ P@0 != <[a]
. . . . | | . . . | . . . . |                ,λx.
. . . . | | . . . | . . . . |                 P>(a@0) ==> ∀v:....
. . . . | | . . . | . . . . |         ¬P@0((λx.s(i;t').x),v)
. . . . | | . . . | . . . . | 12. ∀t:ℕ.
. . . . | | . . . | . . . . |     ¬isnull(a(i;t))
. . . . | | . . . | . . . . |     ⇒
. . . . | | . . . | . . . . |     (islocal(kind(a(i;t)))
. . . . | | . . . | . . . . |      ⇒
. . . . | | . . . | . . . . |      (eqof(IdDeq)(a,act(kind(a(i;t))))
. . . . | | . . . | . . . . |       ∨₂ false₂)
. . . . | | . . . | . . . . |      ⇒
. . . . | | . . . | . . . . |      P((λx.s(i;t).x),val(a(i;t))))
. . . . | | . . . | . . . . |     & (∀x:Id.
. . . . | | . . . | . . . . |        deq-member(...;...;1of())
. . . . | | . . . | . . . . |        ⇒
```

```
. . . . | | . . . | . . . . |        s(i;t+1).x
. . . . | | . . . | . . . . |        =
. . . . | | . . . | . . . . |        2of()
. . . . | | . . . | . . . . |        (<kind(a(i;t)),x>
. . . . | | . . . | . . . . |        ,λx.s(i;t).x
. . . . | | . . . | . . . . |        ,val(a(i;t))))
. . . . | | . . . | . . . . |     & (∀l:IdLnk.
. . . . | | . . . | . . . . |        deq-member(...;...;1of())
. . . . | | . . . | . . . . |        ⇒
. . . . | | . . . | . . . . |        withlnk(l;m(i;t))
. . . . | | . . . | . . . . |        =
. . . . | | . . . | . . . . |        if source(l) = i→
. . . . | | . . . | . . . . |           concat(map(λtgf.map(λx.
. . . . | | . . . | . . . . |           <1of(tgf)
. . . . | | . . . | . . . . |           ,x>;2of(tgf)
. . . . | | . . . | . . . . |               ((λx.s(i;t).x)
. . . . | | . . . | . . . . |               ,val(a(i;t))));2of()
. . . . | | . . . | . . . . |                                (<kind(...)
. . . . | | . . . | . . . . |                                 ,l>)))
. . . . | | . . . | . . . . |        else nil fi)
. . . . | | . . . | . . . . |     & (∀x:Id.
. . . . | | . . . | . . . . |        ¬(deq-member(IdDeq;x;1of())
. . . . | | . . . | . . . . |          ⇒
. . . . | | . . . | . . . . |          deq-member(KindDeq;...;2of()
. . . . | | . . . | . . . . |                                (x)))
. . . . | | . . . | . . . . |        ⇒
. . . . | | . . . | . . . . |        s(i;t).x = s(i;t+1).x)
. . . . | | . . . | . . . . |     & (∀l:IdLnk, tg:Id.
. . . . | | . . . | . . . . |        ¬(deq-member(...;<l,tg>;1of())
. . . . | | . . . | . . . . |          ⇒
. . . . | | . . . | . . . . |          deq-member(KindDeq;...;...))
. . . . | | . . . | . . . . |        ⇒
. . . . | | . . . | . . . . |        w-tagged(tg; onlnk(l;m(i;t)))
. . . . | | . . . | . . . . |        =
. . . . | | . . . | . . . . |        nil)
. . . . | | . . . | . . . . | 13. ∀x:Id.
. . . . | | . . . | . . . . |     deq-member(IdDeq;x;1of())
. . . . | | . . . | . . . . |     ⇒
. . . . | | . . . | . . . . |     s(i;0).x = 2of()(x)
. . . . | | . . . | . . . . | 14. ∀a@0:Action(i).
. . . . | | . . . | . . . . |     ¬isnull(a@0)
. . . . | | . . . | . . . . |     ⇒
. . . . | | . . . | . . . . |     (valtype(i;a@0) ⊆r <[locl(a)]
. . . . | | . . . | . . . . |                         ,λx.
. . . . | | . . . | . . . . |                          T>(...)?Top)
. . . . | | . . . | . . . . | 15. ∀x:Id.
. . . . | | . . . | . . . . |     vartype(i;x) ⊆r if ...→
. . . . | | . . . | . . . . |                            2of(ds)(x)
. . . . | | . . . | . . . . |                        else Top fi
. . . . | | . . . | . . . . | 16. IdDeq ∈ EqDecider(Id)
. . . . | | . . . | . . . . | 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . | | . . . | . . . . | 18. j : Id
. . . . | | . . . | . . . . | 19. t : ℕ
. . . . | | . . . | . . . . | 20. j = i
. . . . | | . . . | . . . . | 21. ¬isnull(a(j;t))
```

```
. . . . | | . . . | . . . . | 22. ¬isnull(a(i;t))
. . . . | | . . . | . . . . | 23. (λx.s(i;t).x) ∈ State(ds)
. . . . | | . . . | . . . . | 24. kind(<j,t>) = locl(a)
. . . . | | . . . | . . . . | 25. P((λx.s(i;t).x),val(a(i;t)))
. . . . | | . . . | . . . . | 26. valtype(i;a(i;t)) ⊆r <[locl(a)]
. . . . | | . . . | . . . . |                          ,λx.
. . . . | | . . . | . . . . |                           T>(...)?Top
. . . . | | . . . | . . . . | 27. locl(a) = kind(a(i;t))
. . . . | | . . . | . . . . | 28. True
. . . . | | . . . | . . . . | 29. kind(a(i;t)) ∈ Knd
. . . . | | . . . | . . . . | 30. locl(a) = kind(a(i;t))
. . . . | | . . . | . . . . | 31. z : Knd
. . . . | | . . . | . . . . | ⊢  <[locl(a)],λx.T>(z)?Top ∈ Type
. . . . | | . . . | . . . . |   by Repeat
. . . . | | . . . | . . . . |      (Unfolds
. . . . | | . . . | . . . . |       [‘fpf-cap‘
. . . . | | . . . | . . . . |       ;‘fpf-ap‘
. . . . | | . . . | . . . . |       ;‘fpf-single‘
. . . . | | . . . | . . . . |       ;‘fpf-dom‘]
. . . . | | . . . | . . . . |       0
. . . . | | . . . | . . . . |       THEN
. . . . | | . . . | . . . . |       Reduce 0)
. . . . | | . . . | . . . . |
. . . . | | . . . | . . . .\
. . . . | | . . . | . . . . 1. i : Id
. . . . | | . . . | . . . . 2. a : Id
. . . . | | . . . | . . . . 3. T : Type
. . . . | | . . . | . . . . 4. ds : x:Id fp-> Type
. . . . | | . . . | . . . . 5. P : State(ds)→T→Prop
. . . . | | . . . | . . . . 6. w : World
. . . . | | . . . | . . . . 7. FairFifo
. . . . | | . . . | . . . . 8. FairFifo
. . . . | | . . . | . . . . 9. ∀l:IdLnk, tg:Id.
. . . . | | . . . | . . . .    (w.M(l,tg)) ⊆r if eqof(IdDeq)
. . . . | | . . . | . . . .                      (source(l)
. . . . | | . . . | . . . .                      ,i)→
. . . . | | . . . | . . . .                      <ds
. . . . | | . . . | . . . .                      ,<[locl(a)],λx.T>
. . . . | | . . . | . . . .                      ,
. . . . | | . . . | . . . .                      ,<[a],λx.P>
. . . . | | . . . | . . . .                      ,
. . . . | | . . . | . . . .                      ,
. . . . | | . . . | . . . .                      ,
. . . . | | . . . | . . . .                      ,
. . . . | | . . . | . . . .                      ,.>
. . . . | | . . . | . . . .                    else  fi.da(rcv
. . . . | | . . . | . . . .    (l; tg))
. . . . | | . . . | . . . . 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . | | . . . | . . . . 11. ∀a@0:Id, t:ℕ.
. . . . | | . . . | . . . .     ∃t’:ℕ.
. . . . | | . . . | . . . .     t≤t’
. . . . | | . . . | . . . .     & ¬isnull(a(i;t’))
. . . . | | . . . | . . . .       & kind(a(i;t’)) = locl(a@0)
. . . . | | . . . | . . . .       ∨ ¬locl(a@0) ∈ dom(<[locl(a)]
. . . . | | . . . | . . . .                          ,λx.T>)
```

```
. . . . | | . . . | . . . . .       ∨ P@0 != <[a]
. . . . | | . . . | . . . . .                ,λx.
. . . . | | . . . | . . . . .                 P>(a@0) ==> ∀v:....
. . . . | | . . . | . . . . .          ¬P@0((λx.s(i;t').x),v)
. . . . | | . . . | . . . . . 12. ∀t:ℕ.
. . . . | | . . . | . . . . .     ¬isnull(a(i;t))
. . . . | | . . . | . . . . .     ⇒
. . . . | | . . . | . . . . .     (islocal(kind(a(i;t)))
. . . . | | . . . | . . . . .      ⇒
. . . . | | . . . | . . . . .      (eqof(IdDeq)(a,act(kind(a(i;t))))
. . . . | | . . . | . . . . .       ∨₂ false₂)
. . . . | | . . . | . . . . .      ⇒
. . . . | | . . . | . . . . .      P((λx.s(i;t).x),val(a(i;t))))
. . . . | | . . . | . . . . .     & (∀x:Id.
. . . . | | . . . | . . . . .        deq-member(...;...;1of())
. . . . | | . . . | . . . . .        ⇒
. . . . | | . . . | . . . . .        s(i;t+1).x
. . . . | | . . . | . . . . .        =
. . . . | | . . . | . . . . .        2of()
. . . . | | . . . | . . . . .        (<kind(a(i;t)),x>
. . . . | | . . . | . . . . .        ,λx.s(i;t).x
. . . . | | . . . | . . . . .        ,val(a(i;t))))
. . . . | | . . . | . . . . .     & (∀l:IdLnk.
. . . . | | . . . | . . . . .        deq-member(...;...;1of())
. . . . | | . . . | . . . . .        ⇒
. . . . | | . . . | . . . . .        withlnk(l;m(i;t))
. . . . | | . . . | . . . . .        =
. . . . | | . . . | . . . . .        if source(l) = i→
. . . . | | . . . | . . . . .           concat(map(λtgf.map(λx.
. . . . | | . . . | . . . . .           <1of(tgf)
. . . . | | . . . | . . . . .           ,x>;2of(tgf)
. . . . | | . . . | . . . . .               ((λx.s(i;t).x)
. . . . | | . . . | . . . . .               ,val(a(i;t))));2of()
. . . . | | . . . | . . . . .                                (<kind(...)
. . . . | | . . . | . . . . .                                 ,l>)))
. . . . | | . . . | . . . . .        else nil fi)
. . . . | | . . . | . . . . .     & (∀x:Id.

. . . . | | . . . | . . . . .        ¬(deq-member(IdDeq;x;1of())
. . . . | | . . . | . . . . .          ⇒
. . . . | | . . . | . . . . .          deq-member(KindDeq;...;2of()
. . . . | | . . . | . . . . .                                (x)))
. . . . | | . . . | . . . . .        ⇒
. . . . | | . . . | . . . . .        s(i;t).x = s(i;t+1).x)
. . . . | | . . . | . . . . .     & (∀l:IdLnk, tg:Id.
. . . . | | . . . | . . . . .        ¬(deq-member(...;<l,tg>;1of())
. . . . | | . . . | . . . . .          ⇒
. . . . | | . . . | . . . . .          deq-member(KindDeq;...;...))
. . . . | | . . . | . . . . .        ⇒
. . . . | | . . . | . . . . .        w-tagged(tg; onlnk(l;m(i;t)))
. . . . | | . . . | . . . . .        =
. . . . | | . . . | . . . . .        nil)
. . . . | | . . . | . . . . . 13. ∀x:Id.
. . . . | | . . . | . . . . .     deq-member(IdDeq;x;1of())
. . . . | | . . . | . . . . .     ⇒
. . . . | | . . . | . . . . .     s(i;0).x = 2of()(x)
```

```
. . . . | | . . . | . . . . . 14. ∀a@0:Action(i).
. . . . | | . . . | . . . . .     ¬isnull(a@0)
. . . . | | . . . | . . . . .     ⇒
. . . . | | . . . | . . . . .     (valtype(i;a@0) ⊆r <[locl(a)]
. . . . | | . . . | . . . . .                        ,λx.
. . . . | | . . . | . . . . .                         T>(...)?Top)
. . . . | | . . . | . . . . . 15. ∀x:Id.
. . . . | | . . . | . . . . .     vartype(i;x) ⊆r if ...→
. . . . | | . . . | . . . . .                          2of(ds)(x)
. . . . | | . . . | . . . . .                       else Top fi
. . . . | | . . . | . . . . . 16. IdDeq ∈ EqDecider(Id)
. . . . | | . . . | . . . . . 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . | | . . . | . . . . . 18. j : Id
. . . . | | . . . | . . . . . 19. t : ℕ
. . . . | | . . . | . . . . . 20. j = i
. . . . | | . . . | . . . . . 21. ¬isnull(a(j;t))
. . . . | | . . . | . . . . . 22. ¬isnull(a(i;t))
. . . . | | . . . | . . . . . 23. (λx.s(i;t).x) ∈ State(ds)
. . . . | | . . . | . . . . . 24. kind(<j,t>) = locl(a)
. . . . | | . . . | . . . . . 25. P((λx.s(i;t).x),val(a(i;t)))
. . . . | | . . . | . . . . . 26. valtype(i;a(i;t)) ⊆r <[locl(a)]
. . . . | | . . . | . . . . .                           ,λx.
. . . . | | . . . | . . . . .                            T>(...)?Top
. . . . | | . . . | . . . . . 27. locl(a) = kind(a(i;t))
. . . . | | . . . | . . . . . 28. True
. . . . | | . . . | . . . . . 29. kind(a(i;t)) ∈ Knd
. . . . | | . . . | . . . . . 30. locl(a) = kind(a(i;t))
. . . . | | . . . | . . . . . ⊢  valtype(i;a(i;t)) ⊆r T
. . . . | | . . . | . . . . .   by (Repeat
. . . . | | . . . | . . . . .       (Unfolds
. . . . | | . . . | . . . . .        [‘fpf-single‘
. . . . | | . . . | . . . . .        ;‘fpf-cap‘
. . . . | | . . . | . . . . .        ;‘fpf-ap‘
. . . . | | . . . | . . . . .        ;‘fpf-dom‘]
. . . . | | . . . | . . . . .        -5
. . . . | | . . . | . . . . .        THEN
. . . . | | . . . | . . . . .        Reduce -5)
. . . . | | . . . | . . . . .       THEN
. . . . | | . . . | . . . . .       RWO
. . . . | | . . . | . . . . .       Thm* ∀d:EqDecider(A), i:A.
. . . . | | . . . | . . . . .            (eqof(d)(i,i)) ∼ true₂
. . . . | | . . . | . . . . .       {eqof_eq_btrue}
. . . . | | . . . | . . . . .       -5)
. . . . | | . . . | . . . . .      THEN
. . . . | | . . . | . . . . .      (Reduce -5)
. . . . | | . . . |
. . . . | | . . .\
. . . . | | . . . . .....assertion .....
. . . . | | . . . . 1. i : Id
. . . . | | . . . . 2. a : Id
. . . . | | . . . . 3. T : Type
. . . . | | . . . . 4. ds : x:Id fp-> Type
. . . . | | . . . . 5. P : State(ds)→T→Prop
. . . . | | . . . . 6. w : World
. . . . | | . . . . 7. FairFifo
```

```
. . . . | | . . . . 8. FairFifo
. . . . | | . . . . 9. ∀l:IdLnk, tg:Id.
. . . . | | . . . . |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . | | . . . . |                    <ds
. . . . | | . . . . |                    ,<[locl(a)],λx.T>
. . . . | | . . . . |                    ,
. . . . | | . . . . |                    ,<[a],λx.P>
. . . . | | . . . . |                    ,
. . . . | | . . . . |                    ,
. . . . | | . . . . |                    ,
. . . . | | . . . . |                    ,
. . . . | | . . . . |                    ,·>
. . . . | | . . . . |                  else  fi.da(rcv(l; tg))
. . . . | | . . . . 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . | | . . . . 11. ∀a@0:Id, t:ℕ.
. . . . | | . . . . |   ∃t':ℕ.
. . . . | | . . . . |   t≤t'
. . . . | | . . . . |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . | | . . . . |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . | | . . . . |     ∨ P@0 != <[a]
. . . . | | . . . . |              ,λx.
. . . . | | . . . . |               P>(a@0) ==> ∀v:<[locl(a)]
. . . . | | . . . . |                                ,λx.
. . . . | | . . . . |                                 T>(locl(a@0))?Top.
. . . . | | . . . . |       ¬P@0((λx.s(i;t').x),v)
. . . . | | . . . . 12. ∀t:ℕ.
. . . . | | . . . . |   ¬isnull(a(i;t))
. . . . | | . . . . |   ⇒
. . . . | | . . . . |   (islocal(kind(a(i;t)))
. . . . | | . . . . |    ⇒
. . . . | | . . . . |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . | | . . . . |    ⇒
. . . . | | . . . . |    P((λx.s(i;t).x),val(a(i;t))))
. . . . | | . . . . |   & (∀x:Id.
. . . . | | . . . . |      deq-member(...;<kind(a(i;t)),x>;1of())
. . . . | | . . . . |      ⇒
. . . . | | . . . . |      s(i;t+1).x
. . . . | | . . . . |      =
. . . . | | . . . . |      2of()
. . . . | | . . . . |      (<kind(a(i;t)),x>
. . . . | | . . . . |      ,λx.s(i;t).x
. . . . | | . . . . |      ,val(a(i;t))))
. . . . | | . . . . |   & (∀l:IdLnk.
. . . . | | . . . . |      deq-member(...;<kind(a(i;t)),l>;1of())
. . . . | | . . . . |      ⇒
. . . . | | . . . . |      withlnk(l;m(i;t))
. . . . | | . . . . |      =
. . . . | | . . . . |      if source(l) = i→
. . . . | | . . . . |         concat(map(λtgf.map(λx.
. . . . | | . . . . |         <1of(tgf)
. . . . | | . . . . |         ,x>;2of(tgf)
. . . . | | . . . . |             ((λx.s(i;t).x)
. . . . | | . . . . |             ,val(a(i;t))));2of()
. . . . | | . . . . |                              (<kind(a(i;t)),l>)))
. . . . | | . . . . |      else nil fi)
```

```
. . . . | | . . . . |   & (∀x:Id.
. . . . | | . . . . |      ¬(deq-member(IdDeq;x;1of())
. . . . | | . . . . |        ⇒
. . . . | | . . . . |        deq-member(KindDeq;kind(a(i;t));2of()
. . . . | | . . . . |                                          (x)))
. . . . | | . . . . |      ⇒
. . . . | | . . . . |      s(i;t).x = s(i;t+1).x)
. . . . | | . . . . |   & (∀l:IdLnk, tg:Id.
. . . . | | . . . . |      ¬...
. . . . | | . . . . |      ⇒
. . . . | | . . . . |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . | | . . . . 13. ∀x:Id.
. . . . | | . . . . |   deq-member(IdDeq;x;1of())
. . . . | | . . . . |   ⇒
. . . . | | . . . . |   s(i;0).x = 2of()(x)
. . . . | | . . . . 14. ∀a@0:Action(i).
. . . . | | . . . . |   ¬isnull(a@0)
. . . . | | . . . . |   ⇒
. . . . | | . . . . |   (valtype(i;a@0) ⊆r <[locl(a)]
. . . . | | . . . . |                        ,λx.T>(kind(a@0))?Top)
. . . . | | . . . . 15. ∀x:Id.
. . . . | | . . . . |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(
. . . . | | . . . . |                                          ds))→
. . . . | | . . . . |                      2of(ds)(x)
. . . . | | . . . . |                   else Top fi
. . . . | | . . . . 16. IdDeq ∈ EqDecider(Id)
. . . . | | . . . . 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . | | . . . . 18. j : Id
. . . . | | . . . . 19. t : ℕ
. . . . | | . . . . 20. j = i
. . . . | | . . . . 21. ¬isnull(a(j;t))
. . . . | | . . . . 22. ¬isnull(a(i;t))
. . . . | | . . . . 23. (λx.s(i;t).x) ∈ State(ds)
. . . . | | . . . . 24. kind(<j,t>) = locl(a)
. . . . | | . . . . 25. P((λx.s(i;t).x),val(a(i;t)))
. . . . | | . . . . 26. valtype(i;a(i;t)) ⊆r T
. . . . | | . . . . ⊢  val(a(j;t)) = val(a(i;t))
. . . . | | . . . . | by Assert (a(j;t) = a(i;t))
. . . . | | . . . . |
. . . . | | . . . . |\
. . . . | | . . . . | .....assertion .....
. . . . | | . . . . | 1. i : Id
. . . . | | . . . . | 2. a : Id
. . . . | | . . . . | 3. T : Type
. . . . | | . . . . | 4. ds : x:Id fp-> Type
. . . . | | . . . . | 5. P : State(ds)→T→Prop
. . . . | | . . . . | 6. w : World
. . . . | | . . . . | 7. FairFifo
. . . . | | . . . . | 8. FairFifo
. . . . | | . . . . | 9. ∀l:IdLnk, tg:Id.
. . . . | | . . . . | |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . | | . . . . | |                    <ds
. . . . | | . . . . | |                    ,<[locl(a)],λx.T>
. . . . | | . . . . | |                    ,
. . . . | | . . . . | |                    ,<[a],λx.P>
```

```
. . . . | | . . . . | |                    ,
. . . . | | . . . . | |                    ,
. . . . | | . . . . | |                    ,
. . . . | | . . . . | |                    ,
. . . . | | . . . . | |                    ,·>
. . . . | | . . . . | |                 else  fi.da(rcv(l; tg))
. . . . | | . . . . | 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . | | . . . . | 11. ∀a@0:Id, t:ℕ.
. . . . | | . . . . | |   ∃t':ℕ.
. . . . | | . . . . | |   t≤t'
. . . . | | . . . . | |   & ¬isnull(a(i;t'))
. . . . | | . . . . | |     & kind(a(i;t')) = locl(a@0)
. . . . | | . . . . | |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . | | . . . . | |     ∨ P@0 != <[a]
. . . . | | . . . . | |              ,λx.
. . . . | | . . . . | |               P>(a@0) ==> ∀v:<[locl(a)]
. . . . | | . . . . | |                                ,λx.

. . . . | | . . . . | |                                 T>(...)?Top.
. . . . | | . . . . | |       ¬P@0((λx.s(i;t').x),v)
. . . . | | . . . . | 12. ∀t:ℕ.
. . . . | | . . . . | |   ¬isnull(a(i;t))
. . . . | | . . . . | |   ⇒
. . . . | | . . . . | |   (islocal(kind(a(i;t)))
. . . . | | . . . . | |    ⇒
. . . . | | . . . . | |    (eqof(IdDeq)(a,act(kind(a(i;t))))
. . . . | | . . . . | |     ∨₂ false₂)
. . . . | | . . . . | |    ⇒
. . . . | | . . . . | |    P((λx.s(i;t).x),val(a(i;t))))
. . . . | | . . . . | |   & (∀x:Id.
. . . . | | . . . . | |      deq-member(...;<kind(a(i;t)),x>;1of())
. . . . | | . . . . | |      ⇒
. . . . | | . . . . | |      s(i;t+1).x
. . . . | | . . . . | |      =
. . . . | | . . . . | |      2of()
. . . . | | . . . . | |      (<kind(a(i;t)),x>
. . . . | | . . . . | |      ,λx.s(i;t).x
. . . . | | . . . . | |      ,val(a(i;t))))
. . . . | | . . . . | |   & (∀l:IdLnk.
. . . . | | . . . . | |      deq-member(...;<kind(a(i;t)),l>;1of())
. . . . | | . . . . | |      ⇒
. . . . | | . . . . | |      withlnk(l;m(i;t))
. . . . | | . . . . | |      =
. . . . | | . . . . | |      if source(l) = i→
. . . . | | . . . . | |         concat(map(λtgf.map(λx.
. . . . | | . . . . | |         <1of(tgf)
. . . . | | . . . . | |         ,x>;2of(tgf)
. . . . | | . . . . | |             ((λx.s(i;t).x)
. . . . | | . . . . | |             ,val(a(i;t))));...))
. . . . | | . . . . | |      else nil fi)
. . . . | | . . . . | |   & (∀x:Id.
. . . . | | . . . . | |      ¬(deq-member(IdDeq;x;1of())
. . . . | | . . . . | |        ⇒
. . . . | | . . . . | |        deq-member(KindDeq;kind(a(i;t));2of()
. . . . | | . . . . | |                                        (x)))
. . . . | | . . . . | |      ⇒
```

```
. . . . | | . . . . | |      s(i;t).x = s(i;t+1).x)
. . . . | | . . . . | |   & (∀l:IdLnk, tg:Id.
. . . . | | . . . . | |      ¬(deq-member(...;<l,tg>;1of())
. . . . | | . . . . | |        ⇒
. . . . | | . . . . | |        deq-member(KindDeq;kind(a(i;t));...))
. . . . | | . . . . | |      ⇒
. . . . | | . . . . | |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . | | . . . . | 13. ∀x:Id.
. . . . | | . . . . | |   deq-member(IdDeq;x;1of())
. . . . | | . . . . | |   ⇒
. . . . | | . . . . | |   s(i;0).x = 2of()(x)
. . . . | | . . . . | 14. ∀a@0:Action(i).
. . . . | | . . . . | |   ¬isnull(a@0)
. . . . | | . . . . | |   ⇒
. . . . | | . . . . | |   (valtype(i;a@0) ⊆r <[locl(a)]
. . . . | | . . . . | |                       ,λx.T>(kind(a@0))?Top)
. . . . | | . . . . | 15. ∀x:Id.
. . . . | | . . . . | |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(
. . . . | | . . . . | |                                          ds))→
. . . . | | . . . . | |                      2of(ds)(x)
. . . . | | . . . . | |                    else Top fi
. . . . | | . . . . | 16. IdDeq ∈ EqDecider(Id)
. . . . | | . . . . | 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . | | . . . . | 18. j : Id
. . . . | | . . . . | 19. t : ℕ
. . . . | | . . . . | 20. j = i
. . . . | | . . . . | 21. ¬isnull(a(j;t))
. . . . | | . . . . | 22. ¬isnull(a(i;t))
. . . . | | . . . . | 23. (λx.s(i;t).x) ∈ State(ds)
. . . . | | . . . . | 24. kind(<j,t>) = locl(a)
. . . . | | . . . . | 25. P((λx.s(i;t).x),val(a(i;t)))
. . . . | | . . . . | 26. valtype(i;a(i;t)) ⊆r T
. . . . | | . . . . | ⊢  a(j;t) = a(i;t)  by Analyze
. . . . | | . . . . | |
. . . . | | . . . . | 1. i : Id
. . . . | | . . . . | 2. a : Id
. . . . | | . . . . | 3. T : Type
. . . . | | . . . . | 4. ds : x:Id fp-> Type
. . . . | | . . . . | 5. P : State(ds)→T→Prop
. . . . | | . . . . | 6. w : World
. . . . | | . . . . | 7. FairFifo
. . . . | | . . . . | 8. FairFifo
. . . . | | . . . . | 9. ∀l:IdLnk, tg:Id.
. . . . | | . . . . | |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . | | . . . . | |                    <ds
. . . . | | . . . . | |                    ,<[locl(a)],λx.T>
. . . . | | . . . . | |                    ,
. . . . | | . . . . | |                    ,<[a],λx.P>
. . . . | | . . . . | |                    ,
. . . . | | . . . . | |                    ,
. . . . | | . . . . | |                    ,
. . . . | | . . . . | |                    ,
. . . . | | . . . . | |                    ,.>
. . . . | | . . . . | |                 else  fi.da(rcv(l; tg))
. . . . | | . . . . | 10. (eqof(IdDeq)(i,i)) ∼ true₂
```

```
. . . . | | . . . . | 11. ∀a@0:Id, t:ℕ.
. . . . | | . . . . | |   ∃t':ℕ.
. . . . | | . . . . | |   t≤t'
. . . . | | . . . . | |   & ¬isnull(a(i;t'))
. . . . | | . . . . | |     & kind(a(i;t')) = locl(a@0)
. . . . | | . . . . | |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . | | . . . . | |     ∨ P@0 != <[a]

. . . . | | . . . . | |              ,λx.
. . . . | | . . . . | |               P>(a@0) ==> ∀v:<[locl(a)]
. . . . | | . . . . | |                                ,λx.
. . . . | | . . . . | |                                 T>(...)?Top.
. . . . | | . . . . | |       ¬P@0((λx.s(i;t').x),v)
. . . . | | . . . . | 12. ∀t:ℕ.
. . . . | | . . . . | |   ¬isnull(a(i;t))
. . . . | | . . . . | |   ⇒
. . . . | | . . . . | |   (islocal(kind(a(i;t)))
. . . . | | . . . . | |    ⇒
. . . . | | . . . . | |    (eqof(IdDeq)(a,act(kind(a(i;t))))
. . . . | | . . . . | |     ∨₂ false₂)
. . . . | | . . . . | |    ⇒
. . . . | | . . . . | |    P((λx.s(i;t).x),val(a(i;t))))
. . . . | | . . . . | |   & (∀x:Id.
. . . . | | . . . . | |      deq-member(...;<kind(a(i;t)),x>;1of())
. . . . | | . . . . | |      ⇒
. . . . | | . . . . | |      s(i;t+1).x
. . . . | | . . . . | |      =
. . . . | | . . . . | |      2of()
. . . . | | . . . . | |      (<kind(a(i;t)),x>
. . . . | | . . . . | |      ,λx.s(i;t).x
. . . . | | . . . . | |      ,val(a(i;t))))
. . . . | | . . . . | |   & (∀l:IdLnk.
. . . . | | . . . . | |      deq-member(...;<kind(a(i;t)),l>;1of())
. . . . | | . . . . | |      ⇒
. . . . | | . . . . | |      withlnk(l;m(i;t))
. . . . | | . . . . | |      =
. . . . | | . . . . | |      if source(l) = i→
. . . . | | . . . . | |         concat(map(λtgf.map(λx.
. . . . | | . . . . | |         <1of(tgf)
. . . . | | . . . . | |         ,x>;2of(tgf)
. . . . | | . . . . | |             ((λx.s(i;t).x)
. . . . | | . . . . | |             ,val(a(i;t))));...))
. . . . | | . . . . | |      else nil fi)
. . . . | | . . . . | |   & (∀x:Id.
. . . . | | . . . . | |      ¬(deq-member(IdDeq;x;1of())
. . . . | | . . . . | |        ⇒
. . . . | | . . . . | |        deq-member(KindDeq;kind(a(i;t));2of()
. . . . | | . . . . | |                                        (x)))
. . . . | | . . . . | |      ⇒
. . . . | | . . . . | |      s(i;t).x = s(i;t+1).x)
. . . . | | . . . . | |   & (∀l:IdLnk, tg:Id.
. . . . | | . . . . | |      ¬(deq-member(...;<l,tg>;1of())
. . . . | | . . . . | |        ⇒
. . . . | | . . . . | |        deq-member(KindDeq;kind(a(i;t));...))
. . . . | | . . . . | |      ⇒
. . . . | | . . . . | |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
```

```
. . . . | | . . . . | 13. ∀x:Id.
. . . . | | . . . . | |   deq-member(IdDeq;x;1of())
. . . . | | . . . . | |   ⇒
. . . . | | . . . . | |   s(i;0).x = 2of()(x)
. . . . | | . . . . | 14. ∀a@0:Action(i).
. . . . | | . . . . | |   ¬isnull(a@0)
. . . . | | . . . . | |   ⇒
. . . . | | . . . . | |   (valtype(i;a@0) ⊆r <[locl(a)]
. . . . | | . . . . | |                       ,λx.T>(kind(a@0))?Top)
. . . . | | . . . . | 15. ∀x:Id.
. . . . | | . . . . | |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(
. . . . | | . . . . | |                                          ds))→
. . . . | | . . . . | |                       2of(ds)(x)
. . . . | | . . . . | |                     else Top fi
. . . . | | . . . . | 16. IdDeq ∈ EqDecider(Id)
. . . . | | . . . . | 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . | | . . . . | 18. j : Id
. . . . | | . . . . | 19. t : ℕ
. . . . | | . . . . | 20. j = i
. . . . | | . . . . | 21. ¬isnull(a(j;t))
. . . . | | . . . . | 22. ¬isnull(a(i;t))
. . . . | | . . . . | 23. (λx.s(i;t).x) ∈ State(ds)
. . . . | | . . . . | 24. kind(<j,t>) = locl(a)
. . . . | | . . . . | 25. P((λx.s(i;t).x),val(a(i;t)))
. . . . | | . . . . | 26. valtype(i;a(i;t)) ⊆r T
. . . . | | . . . . | ⊢  a(j;t) = a(i;t)  by StrongHypSubst -7 0
. . . . | | . . . . | |
. . . . | | . . . . | |\
. . . . | | . . . . | | 1. i : Id
. . . . | | . . . . | | 2. a : Id
. . . . | | . . . . | | 3. T : Type
. . . . | | . . . . | | 4. ds : x:Id fp-> Type
. . . . | | . . . . | | 5. P : State(ds)→T→Prop
. . . . | | . . . . | | 6. w : World
. . . . | | . . . . | | 7. FairFifo
. . . . | | . . . . | | 8. FairFifo
. . . . | | . . . . | | 9. ∀l:IdLnk, tg:Id.
. . . . | | . . . . | |    (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . | | . . . . | |                       <ds
. . . . | | . . . . | |                       ,<[locl(a)],λx.T>
. . . . | | . . . . | |                       ,
. . . . | | . . . . | |                       ,<[a],λx.P>
. . . . | | . . . . | |                       ,
. . . . | | . . . . | |                       ,
. . . . | | . . . . | |                       ,
. . . . | | . . . . | |                       ,
. . . . | | . . . . | |                       ,·>
. . . . | | . . . . | |                     else  fi.da(rcv(l; tg))
. . . . | | . . . . | | 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . | | . . . . | | 11. ∀a@0:Id, t:ℕ.
. . . . | | . . . . | |     ∃t':ℕ.
. . . . | | . . . . | |     t≤t'
. . . . | | . . . . | |     & ¬isnull(a(i;t'))
. . . . | | . . . . | |       & kind(a(i;t')) = locl(a@0)
. . . . | | . . . . | |       ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
```

```
. . . . | | . . . . | |       ∨ P@0 != <[a]
. . . . | | . . . . | |                ,λx.
. . . . | | . . . . | |                 P>(a@0) ==> ∀v:<[locl(a)]
. . . . | | . . . . | |                                ,λx.
. . . . | | . . . . | |                                 T>(...)?Top.
. . . . | | . . . . | |         ¬P@0((λx.s(i;t').x),v)
. . . . | | . . . . | | 12. ∀t:ℕ.
. . . . | | . . . . | |     ¬isnull(a(i;t))
. . . . | | . . . . | |     ⇒
. . . . | | . . . . | |     (islocal(kind(a(i;t)))
. . . . | | . . . . | |      ⇒
. . . . | | . . . . | |      (eqof(IdDeq)(a,act(kind(a(i;t))))
. . . . | | . . . . | |       ∨₂ false₂)
. . . . | | . . . . | |      ⇒
. . . . | | . . . . | |      P((λx.s(i;t).x),val(a(i;t))))
. . . . | | . . . . | |     & (∀x:Id.
. . . . | | . . . . | |        deq-member(...;<kind(a(i;t)),x>;1of())
. . . . | | . . . . | |        ⇒
. . . . | | . . . . | |        s(i;t+1).x
. . . . | | . . . . | |        =
. . . . | | . . . . | |        2of()
. . . . | | . . . . | |        (<kind(a(i;t)),x>
. . . . | | . . . . | |        ,λx.s(i;t).x
. . . . | | . . . . | |        ,val(a(i;t))))
. . . . | | . . . . | |     & (∀l:IdLnk.
. . . . | | . . . . | |        deq-member(...;<kind(a(i;t)),l>;1of())
. . . . | | . . . . | |        ⇒
. . . . | | . . . . | |        withlnk(l;m(i;t))
. . . . | | . . . . | |        =
. . . . | | . . . . | |        if source(l) = i→
. . . . | | . . . . | |           concat(map(λtgf.map(λx.
. . . . | | . . . . | |           <1of(tgf)
. . . . | | . . . . | |           ,x>;2of(tgf)
. . . . | | . . . . | |               ((λx.s(i;t).x)
. . . . | | . . . . | |               ,val(a(i;t))));...))
. . . . | | . . . . | |        else nil fi)
. . . . | | . . . . | |     & (∀x:Id.
. . . . | | . . . . | |        ¬(deq-member(IdDeq;x;1of())
. . . . | | . . . . | |          ⇒
. . . . | | . . . . | |          deq-member(KindDeq;kind(a(i;t));2of()
. . . . | | . . . . | |                                          (x)))
. . . . | | . . . . | |        ⇒
. . . . | | . . . . | |        s(i;t).x = s(i;t+1).x)
. . . . | | . . . . | |     & (∀l:IdLnk, tg:Id.
. . . . | | . . . . | |        ¬(deq-member(...;<l,tg>;1of())
. . . . | | . . . . | |          ⇒
. . . . | | . . . . | |          deq-member(KindDeq;kind(a(i;t));...))
. . . . | | . . . . | |        ⇒
. . . . | | . . . . | |        w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . | | . . . . | | 13. ∀x:Id.
. . . . | | . . . . | |     deq-member(IdDeq;x;1of())
. . . . | | . . . . | |     ⇒
. . . . | | . . . . | |     s(i;0).x = 2of()(x)
. . . . | | . . . . | | 14. ∀a@0:Action(i).
. . . . | | . . . . | |     ¬isnull(a@0)
```

```
. . . . | | . . . . | |     ⇒
. . . . | | . . . . | |     (valtype(i;a@0) ⊆r <[locl(a)]
. . . . | | . . . . | |                        ,λx.T>(kind(a@0))?Top)
. . . . | | . . . . | | 15. ∀x:Id.
. . . . | | . . . . | |     vartype(i;x) ⊆r if deq-member(...;x;1of(
. . . . | | . . . . | |                                          ds))→
. . . . | | . . . . | |                        2of(ds)(x)
. . . . | | . . . . | |                    else Top fi
. . . . | | . . . . | | 16. IdDeq ∈ EqDecider(Id)
. . . . | | . . . . | | 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . | | . . . . | | 18. j : Id
. . . . | | . . . . | | 19. t : ℕ
. . . . | | . . . . | | 20. j = i
. . . . | | . . . . | | 21. ¬isnull(a(j;t))
. . . . | | . . . . | | 22. ¬isnull(a(i;t))
. . . . | | . . . . | | 23. (λx.s(i;t).x) ∈ State(ds)
. . . . | | . . . . | | 24. kind(<j,t>) = locl(a)
. . . . | | . . . . | | 25. P((λx.s(i;t).x),val(a(i;t)))
. . . . | | . . . . | | 26. valtype(i;a(i;t)) ⊆r T
. . . . | | . . . . | | ⊢  a(i;t) = a(i;t)  by Auto
. . . . | | . . . . | |
. . . . | | . . . . | .\
. . . . | | . . . . | . 1. i : Id
. . . . | | . . . . | . 2. a : Id
. . . . | | . . . . | . 3. T : Type
. . . . | | . . . . | . 4. ds : x:Id fp-> Type
. . . . | | . . . . | . 5. P : State(ds)→T→Prop
. . . . | | . . . . | . 6. w : World
. . . . | | . . . . | . 7. FairFifo
. . . . | | . . . . | . 8. FairFifo
. . . . | | . . . . | . 9. ∀l:IdLnk, tg:Id.
. . . . | | . . . . | .    (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . | | . . . . | .                      <ds
. . . . | | . . . . | .                      ,<[locl(a)],λx.T>
. . . . | | . . . . | .                      ,
. . . . | | . . . . | .                      ,<[a],λx.P>
. . . . | | . . . . | .                      ,
. . . . | | . . . . | .                      ,
. . . . | | . . . . | .                      ,
. . . . | | . . . . | .                      ,
. . . . | | . . . . | .                      ,·>
. . . . | | . . . . | .                  else  fi.da(rcv(l; tg))
. . . . | | . . . . | . 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . | | . . . . | . 11. ∀a@0:Id, t:ℕ.
. . . . | | . . . . | .     ∃t':ℕ.
. . . . | | . . . . | .     t≤t'
. . . . | | . . . . | .     & ¬isnull(a(i;t'))
. . . . | | . . . . | .       & kind(a(i;t')) = locl(a@0)
. . . . | | . . . . | .       ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . | | . . . . | .       ∨ P@0 != <[a]
. . . . | | . . . . | .                ,λx.
. . . . | | . . . . | .                 P>(a@0) ==> ∀v:<[locl(a)]
. . . . | | . . . . | .                                ,λx.
. . . . | | . . . . | .                                 T>(...)?Top.
. . . . | | . . . . | .         ¬P@0((λx.s(i;t').x),v)
```

```
. . . . | | . . . . | . 12. ∀t:ℕ.
. . . . | | . . . . | .     ¬isnull(a(i;t))
. . . . | | . . . . | .     ⇒
. . . . | | . . . . | .     (islocal(kind(a(i;t)))
. . . . | | . . . . | .      ⇒
. . . . | | . . . . | .      (eqof(IdDeq)(a,act(kind(a(i;t))))
. . . . | | . . . . | .       ∨₂ false₂)
. . . . | | . . . . | .      ⇒
. . . . | | . . . . | .      P((λx.s(i;t).x),val(a(i;t))))
. . . . | | . . . . | .     & (∀x:Id.
. . . . | | . . . . | .        deq-member(...;<kind(a(i;t)),x>;1of())
. . . . | | . . . . | .        ⇒
. . . . | | . . . . | .        s(i;t+1).x
. . . . | | . . . . | .        =
. . . . | | . . . . | .        2of()
. . . . | | . . . . | .        (<kind(a(i;t)),x>
. . . . | | . . . . | .        ,λx.s(i;t).x
. . . . | | . . . . | .        ,val(a(i;t))))
. . . . | | . . . . | .     & (∀l:IdLnk.
. . . . | | . . . . | .        deq-member(...;<kind(a(i;t)),l>;1of())
. . . . | | . . . . | .        ⇒
. . . . | | . . . . | .        withlnk(l;m(i;t))
. . . . | | . . . . | .        =
. . . . | | . . . . | .        if source(l) = i→
. . . . | | . . . . | .           concat(map(λtgf.map(λx.
. . . . | | . . . . | .           <1of(tgf)
. . . . | | . . . . | .           ,x>;2of(tgf)
. . . . | | . . . . | .               ((λx.s(i;t).x)
. . . . | | . . . . | .               ,val(a(i;t))));...))
. . . . | | . . . . | .        else nil fi)
. . . . | | . . . . | .     & (∀x:Id.
. . . . | | . . . . | .        ¬(deq-member(IdDeq;x;1of())
. . . . | | . . . . | .          ⇒
. . . . | | . . . . | .          deq-member(KindDeq;kind(a(i;t));2of()
. . . . | | . . . . | .                                          (x)))
. . . . | | . . . . | .        ⇒
. . . . | | . . . . | .        s(i;t).x = s(i;t+1).x)
. . . . | | . . . . | .     & (∀l:IdLnk, tg:Id.
. . . . | | . . . . | .        ¬(deq-member(...;<l,tg>;1of())
. . . . | | . . . . | .          ⇒
. . . . | | . . . . | .          deq-member(KindDeq;kind(a(i;t));...))
. . . . | | . . . . | .        ⇒
. . . . | | . . . . | .        w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . | | . . . . | . 13. ∀x:Id.
. . . . | | . . . . | .     deq-member(IdDeq;x;1of())
. . . . | | . . . . | .     ⇒
. . . . | | . . . . | .     s(i;0).x = 2of()(x)
. . . . | | . . . . | . 14. ∀a@0:Action(i).
. . . . | | . . . . | .     ¬isnull(a@0)
. . . . | | . . . . | .     ⇒
. . . . | | . . . . | .     (valtype(i;a@0) ⊆r <[locl(a)]
. . . . | | . . . . | .                        ,λx.T>(kind(a@0))?Top)
. . . . | | . . . . | . 15. ∀x:Id.
. . . . | | . . . . | .     vartype(i;x) ⊆r if deq-member(...;x;1of(
. . . . | | . . . . | .                                          ds))→
```

```
. . . . | | . . . . | .                          2of(ds)(x)
. . . . | | . . . . | .                        else Top fi
. . . . | | . . . . | . 16. IdDeq ∈ EqDecider(Id)
. . . . | | . . . . | . 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . | | . . . . | . 18. j : Id
. . . . | | . . . . | . 19. t : ℕ
. . . . | | . . . . | . 20. j = i
. . . . | | . . . . | . 21. ¬isnull(a(j;t))
. . . . | | . . . . | . 22. ¬isnull(a(i;t))
. . . . | | . . . . | . 23. (λx.s(i;t).x) ∈ State(ds)
. . . . | | . . . . | . 24. kind(<j,t>) = locl(a)
. . . . | | . . . . | . 25. P((λx.s(i;t).x),val(a(i;t)))
. . . . | | . . . . | . 26. valtype(i;a(i;t)) ⊆r T
. . . . | | . . . . | . 27. z : Id
. . . . | | . . . . | . 28. z = i
. . . . | | . . . . | . ⊢  (a(z;t) = a(i;t)) ∈ Prop
. . . . | | . . . . | .   by Auto THEN DoSubsume THEN HypSubst -1 0
. . . . | | . . . . |
. . . . | | . . . . .\
. . . . | | . . . . . 1. i : Id
. . . . | | . . . . . 2. a : Id
. . . . | | . . . . . 3. T : Type
. . . . | | . . . . . 4. ds : x:Id fp-> Type
. . . . | | . . . . . 5. P : State(ds)→T→Prop
. . . . | | . . . . . 6. w : World
. . . . | | . . . . . 7. FairFifo
. . . . | | . . . . . 8. FairFifo
. . . . | | . . . . . 9. ∀l:IdLnk, tg:Id.
. . . . | | . . . . . |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . | | . . . . . |                    <ds
. . . . | | . . . . . |                    ,<[locl(a)],λx.T>
. . . . | | . . . . . |                    ,
. . . . | | . . . . . |                    ,<[a],λx.P>
. . . . | | . . . . . |                    ,
. . . . | | . . . . . |                    ,
. . . . | | . . . . . |                    ,
. . . . | | . . . . . |                    ,
. . . . | | . . . . . |                    ,·>
. . . . | | . . . . . |                  else  fi.da(rcv(l; tg))
. . . . | | . . . . . 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . | | . . . . . 11. ∀a@0:Id, t:ℕ.
. . . . | | . . . . . |   ∃t':ℕ.
. . . . | | . . . . . |   t≤t'
. . . . | | . . . . . |   & ¬isnull(a(i;t'))
. . . . | | . . . . . |     & kind(a(i;t')) = locl(a@0)
. . . . | | . . . . . |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . | | . . . . . |     ∨ P@0 != <[a]
. . . . | | . . . . . |               ,λx.
. . . . | | . . . . . |                P>(a@0) ==> ∀v:<[locl(a)]
. . . . | | . . . . . |                                ,λx.
. . . . | | . . . . . |                                 T>(...)?Top.
. . . . | | . . . . . |       ¬P@0((λx.s(i;t').x),v)
. . . . | | . . . . . 12. ∀t:ℕ.
. . . . | | . . . . . |   ¬isnull(a(i;t))
. . . . | | . . . . . |   ⇒
```

```
. . . . | | . . . . . |   (islocal(kind(a(i;t)))
. . . . | | . . . . . |    ⇒
. . . . | | . . . . . |    (eqof(IdDeq)(a,act(kind(a(i;t))))
. . . . | | . . . . . |     ∨₂ false₂)
. . . . | | . . . . . |    ⇒
. . . . | | . . . . . |    P((λx.s(i;t).x),val(a(i;t))))
. . . . | | . . . . . |   & (∀x:Id.
. . . . | | . . . . . |      deq-member(...;<kind(a(i;t)),x>;1of())
. . . . | | . . . . . |      ⇒
. . . . | | . . . . . |      s(i;t+1).x
. . . . | | . . . . . |      =
. . . . | | . . . . . |      2of()
. . . . | | . . . . . |      (<kind(a(i;t)),x>
. . . . | | . . . . . |      ,λx.s(i;t).x
. . . . | | . . . . . |      ,val(a(i;t))))
. . . . | | . . . . . |   & (∀l:IdLnk.
. . . . | | . . . . . |      deq-member(...;<kind(a(i;t)),l>;1of())
. . . . | | . . . . . |      ⇒
. . . . | | . . . . . |      withlnk(l;m(i;t))
. . . . | | . . . . . |      =
. . . . | | . . . . . |      if source(l) = i→
. . . . | | . . . . . |         concat(map(λtgf.map(λx.
. . . . | | . . . . . |         <1of(tgf)
. . . . | | . . . . . |         ,x>;2of(tgf)
. . . . | | . . . . . |             ((λx.s(i;t).x)
. . . . | | . . . . . |             ,val(a(i;t))));...))
. . . . | | . . . . . |      else nil fi)
. . . . | | . . . . . |   & (∀x:Id.
. . . . | | . . . . . |      ¬(deq-member(IdDeq;x;1of())
. . . . | | . . . . . |        ⇒
. . . . | | . . . . . |        deq-member(KindDeq;kind(a(i;t));2of()
. . . . | | . . . . . |                                          (x)))
. . . . | | . . . . . |      ⇒
. . . . | | . . . . . |      s(i;t).x = s(i;t+1).x)
. . . . | | . . . . . |   & (∀l:IdLnk, tg:Id.
. . . . | | . . . . . |      ¬(deq-member(...;<l,tg>;1of())
. . . . | | . . . . . |        ⇒
. . . . | | . . . . . |        deq-member(KindDeq;kind(a(i;t));...))
. . . . | | . . . . . |      ⇒
. . . . | | . . . . . |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . | | . . . . . 13. ∀x:Id.
. . . . | | . . . . . |   deq-member(IdDeq;x;1of())
. . . . | | . . . . . |   ⇒
. . . . | | . . . . . |   s(i;0).x = 2of()(x)
. . . . | | . . . . . 14. ∀a@0:Action(i).
. . . . | | . . . . . |   ¬isnull(a@0)
. . . . | | . . . . . |   ⇒
. . . . | | . . . . . |   (valtype(i;a@0) ⊆r <[locl(a)]
. . . . | | . . . . . |                        ,λx.T>(kind(a@0))?Top)
. . . . | | . . . . . 15. ∀x:Id.
. . . . | | . . . . . |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(
. . . . | | . . . . . |                                          ds))→
. . . . | | . . . . . |                       2of(ds)(x)
. . . . | | . . . . . |                   else Top fi
. . . . | | . . . . . 16. IdDeq ∈ EqDecider(Id)
```

```
. . . . | | . . . . . 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . | | . . . . . 18. j : Id
. . . . | | . . . . . 19. t : ℕ
. . . . | | . . . . . 20. j = i
. . . . | | . . . . . 21. ¬isnull(a(j;t))
. . . . | | . . . . . 22. ¬isnull(a(i;t))
. . . . | | . . . . . 23. (λx.s(i;t).x) ∈ State(ds)
. . . . | | . . . . . 24. kind(<j,t>) = locl(a)
. . . . | | . . . . . 25. P((λx.s(i;t).x),val(a(i;t)))
. . . . | | . . . . . 26. valtype(i;a(i;t)) ⊆r T
. . . . | | . . . . . 27. a(j;t) = a(i;t)
. . . . | | . . . . . ⊢  val(a(j;t)) = val(a(i;t))
. . . . | | . . . . . | by StrongHypSubst -1 0
. . . . | | . . . . . |
. . . . | | . . . . . |\
. . . . | | . . . . . | 1. i : Id
. . . . | | . . . . . | 2. a : Id
. . . . | | . . . . . | 3. T : Type
. . . . | | . . . . . | 4. ds : x:Id fp-> Type
. . . . | | . . . . . | 5. P : State(ds)→T→Prop
. . . . | | . . . . . | 6. w : World
. . . . | | . . . . . | 7. FairFifo

. . . . | | . . . . . | 8. FairFifo
. . . . | | . . . . . | 9. ∀l:IdLnk, tg:Id.
. . . . | | . . . . . |    (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . | | . . . . . |                       <ds
. . . . | | . . . . . |                       ,<[locl(a)],λx.T>
. . . . | | . . . . . |                       ,
. . . . | | . . . . . |                       ,<[a],λx.P>
. . . . | | . . . . . |                       ,
. . . . | | . . . . . |                       ,
. . . . | | . . . . . |                       ,
. . . . | | . . . . . |                       ,
. . . . | | . . . . . |                       ,.>
. . . . | | . . . . . |                     else  fi.da(rcv(l; tg))
. . . . | | . . . . . | 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . | | . . . . . | 11. ∀a@0:Id, t:ℕ.
. . . . | | . . . . . |     ∃t':ℕ.
. . . . | | . . . . . |     t≤t'
. . . . | | . . . . . |     & ¬isnull(a(i;t'))
. . . . | | . . . . . |       & kind(a(i;t')) = locl(a@0)
. . . . | | . . . . . |       ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . | | . . . . . |       ∨ P@0 != <[a]
. . . . | | . . . . . |                ,λx.
. . . . | | . . . . . |                 P>(a@0) ==> ∀v:<[locl(a)]
. . . . | | . . . . . |                                ,λx.
. . . . | | . . . . . |                                 T>(...)?Top.
. . . . | | . . . . . |         ¬P@0((λx.s(i;t').x),v)
. . . . | | . . . . . | 12. ∀t:ℕ.
. . . . | | . . . . . |     ¬isnull(a(i;t))
. . . . | | . . . . . |     ⇒
. . . . | | . . . . . |     (islocal(kind(a(i;t)))
. . . . | | . . . . . |      ⇒
. . . . | | . . . . . |      (eqof(IdDeq)(a,act(kind(a(i;t))))
. . . . | | . . . . . |       ∨₂ false₂)
```

```
. . . . | | . . . . . |      ⇒
. . . . | | . . . . . |      P((λx.s(i;t).x),val(a(i;t))))
. . . . | | . . . . . |     & (∀x:Id.
. . . . | | . . . . . |        deq-member(...;<kind(a(i;t)),x>;1of())
. . . . | | . . . . . |        ⇒
. . . . | | . . . . . |        s(i;t+1).x
. . . . | | . . . . . |        =
. . . . | | . . . . . |        2of()
. . . . | | . . . . . |        (<kind(a(i;t)),x>
. . . . | | . . . . . |        ,λx.s(i;t).x
. . . . | | . . . . . |        ,val(a(i;t))))
. . . . | | . . . . . |     & (∀l:IdLnk.
. . . . | | . . . . . |        deq-member(...;<kind(a(i;t)),l>;1of())
. . . . | | . . . . . |        ⇒
. . . . | | . . . . . |        withlnk(l;m(i;t))
. . . . | | . . . . . |        =
. . . . | | . . . . . |        if source(l) = i→
. . . . | | . . . . . |           concat(map(λtgf.map(λx.
. . . . | | . . . . . |           <1of(tgf)
. . . . | | . . . . . |           ,x>;2of(tgf)
. . . . | | . . . . . |               ((λx.s(i;t).x)
. . . . | | . . . . . |               ,val(a(i;t))));...))
. . . . | | . . . . . |        else nil fi)
. . . . | | . . . . . |     & (∀x:Id.
. . . . | | . . . . . |        ¬(deq-member(IdDeq;x;1of())
. . . . | | . . . . . |          ⇒
. . . . | | . . . . . |          deq-member(KindDeq;kind(a(i;t));2of()
. . . . | | . . . . . |                                          (x)))
. . . . | | . . . . . |        ⇒
. . . . | | . . . . . |        s(i;t).x = s(i;t+1).x)
. . . . | | . . . . . |     & (∀l:IdLnk, tg:Id.
. . . . | | . . . . . |        ¬(deq-member(...;<l,tg>;1of())
. . . . | | . . . . . |          ⇒
. . . . | | . . . . . |          deq-member(KindDeq;kind(a(i;t));...))
. . . . | | . . . . . |        ⇒
. . . . | | . . . . . |        w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . | | . . . . . | 13. ∀x:Id.
. . . . | | . . . . . |     deq-member(IdDeq;x;1of())
. . . . | | . . . . . |     ⇒
. . . . | | . . . . . |     s(i;0).x = 2of()(x)
. . . . | | . . . . . | 14. ∀a@0:Action(i).
. . . . | | . . . . . |     ¬isnull(a@0)
. . . . | | . . . . . |     ⇒
. . . . | | . . . . . |     (valtype(i;a@0) ⊆r <[locl(a)]
. . . . | | . . . . . |                         ,λx.T>(kind(a@0))?Top)
. . . . | | . . . . . | 15. ∀x:Id.
. . . . | | . . . . . |     vartype(i;x) ⊆r if deq-member(...;x;1of(
. . . . | | . . . . . |                                          ds))→
. . . . | | . . . . . |                        2of(ds)(x)
. . . . | | . . . . . |                     else Top fi
. . . . | | . . . . . | 16. IdDeq ∈ EqDecider(Id)
. . . . | | . . . . . | 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . | | . . . . . | 18. j : Id
. . . . | | . . . . . | 19. t : ℕ
. . . . | | . . . . . | 20. j = i
```

```
. . . . | | . . . . . | 21. ¬isnull(a(j;t))
. . . . | | . . . . . | 22. ¬isnull(a(i;t))
. . . . | | . . . . . | 23. (λx.s(i;t).x) ∈ State(ds)
. . . . | | . . . . . | 24. kind(<j,t>) = locl(a)
. . . . | | . . . . . | 25. P((λx.s(i;t).x),val(a(i;t)))
. . . . | | . . . . . | 26. valtype(i;a(i;t)) ⊆r T
. . . . | | . . . . . | 27. a(j;t) = a(i;t)
. . . . | | . . . . . | ⊢  val(a(i;t)) = val(a(i;t))  by Auto
. . . . | | . . . . . |
. . . . | | . . . . . .\
. . . . | | . . . . . . 1. i : Id
. . . . | | . . . . . . 2. a : Id
. . . . | | . . . . . . 3. T : Type
. . . . | | . . . . . . 4. ds : x:Id fp-> Type
. . . . | | . . . . . . 5. P : State(ds)→T→Prop
. . . . | | . . . . . . 6. w : World
. . . . | | . . . . . . 7. FairFifo
. . . . | | . . . . . . 8. FairFifo
. . . . | | . . . . . . 9. ∀l:IdLnk, tg:Id.
. . . . | | . . . . . . |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . | | . . . . . . |                  <ds
. . . . | | . . . . . . |                  ,<[locl(a)],λx.T>
. . . . | | . . . . . . |                  ,
. . . . | | . . . . . . |                  ,<[a],λx.P>
. . . . | | . . . . . . |                  ,
. . . . | | . . . . . . |                  ,
. . . . | | . . . . . . |                  ,
. . . . | | . . . . . . |                  ,
. . . . | | . . . . . . |                  ,·>
. . . . | | . . . . . . |               else  fi.da(rcv(l; tg))
. . . . | | . . . . . . 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . | | . . . . . . 11. ∀a@0:Id, t:ℕ.
. . . . | | . . . . . . |   ∃t':ℕ.
. . . . | | . . . . . . |   t≤t'
. . . . | | . . . . . . |   & ¬isnull(a(i;t'))
. . . . | | . . . . . . |     & kind(a(i;t')) = locl(a@0)
. . . . | | . . . . . . |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . | | . . . . . . |     ∨ P@0 != <[a]
. . . . | | . . . . . . |              ,λx.
. . . . | | . . . . . . |               P>(a@0) ==> ∀v:<[locl(a)]
. . . . | | . . . . . . |                                ,λx.
. . . . | | . . . . . . |                                 T>(...)?Top.
. . . . | | . . . . . . |       ¬P@0((λx.s(i;t').x),v)
. . . . | | . . . . . . 12. ∀t:ℕ.
. . . . | | . . . . . . |   ¬isnull(a(i;t))
. . . . | | . . . . . . |   ⇒
. . . . | | . . . . . . |   (islocal(kind(a(i;t)))
. . . . | | . . . . . . |    ⇒
. . . . | | . . . . . . |    (eqof(IdDeq)(a,act(kind(a(i;t))))
. . . . | | . . . . . . |     ∨₂ false₂)
. . . . | | . . . . . . |    ⇒
. . . . | | . . . . . . |    P((λx.s(i;t).x),val(a(i;t))))
. . . . | | . . . . . . |   & (∀x:Id.
. . . . | | . . . . . . |      deq-member(...;<kind(a(i;t)),x>;1of())
. . . . | | . . . . . . |      ⇒
```

```
. . . . | | . . . . . |      s(i;t+1).x
. . . . | | . . . . . |      =
. . . . | | . . . . . |      2of()
. . . . | | . . . . . |      (<kind(a(i;t)),x>
. . . . | | . . . . . |      ,λx.s(i;t).x
. . . . | | . . . . . |      ,val(a(i;t))))
. . . . | | . . . . . |   & (∀l:IdLnk.
. . . . | | . . . . . |      deq-member(...;<kind(a(i;t)),l>;1of())
. . . . | | . . . . . |      ⇒
. . . . | | . . . . . |      withlnk(l;m(i;t))
. . . . | | . . . . . |      =
. . . . | | . . . . . |      if source(l) = i→
. . . . | | . . . . . |         concat(map(λtgf.map(λx.
. . . . | | . . . . . |         <1of(tgf)
. . . . | | . . . . . |         ,x>;2of(tgf)
. . . . | | . . . . . |             ((λx.s(i;t).x)
. . . . | | . . . . . |             ,val(a(i;t))));...))
. . . . | | . . . . . |      else nil fi)
. . . . | | . . . . . |   & (∀x:Id.
. . . . | | . . . . . |      ¬(deq-member(IdDeq;x;1of())
. . . . | | . . . . . |        ⇒
. . . . | | . . . . . |        deq-member(KindDeq;kind(a(i;t));2of()
. . . . | | . . . . . |                                        (x)))
. . . . | | . . . . . |      ⇒
. . . . | | . . . . . |      s(i;t).x = s(i;t+1).x)
. . . . | | . . . . . |   & (∀l:IdLnk, tg:Id.
. . . . | | . . . . . |      ¬(deq-member(...;<l,tg>;1of())
. . . . | | . . . . . |        ⇒
. . . . | | . . . . . |        deq-member(KindDeq;kind(a(i;t));...))
. . . . | | . . . . . |      ⇒
. . . . | | . . . . . |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . | | . . . . . 13. ∀x:Id.
. . . . | | . . . . . |   deq-member(IdDeq;x;1of())
. . . . | | . . . . . |   ⇒
. . . . | | . . . . . |   s(i;0).x = 2of()(x)
. . . . | | . . . . . 14. ∀a@0:Action(i).
. . . . | | . . . . . |   ¬isnull(a@0)
. . . . | | . . . . . |   ⇒
. . . . | | . . . . . |   (valtype(i;a@0) ⊆r <[locl(a)]
. . . . | | . . . . . |                      ,λx.T>(kind(a@0))?Top)
. . . . | | . . . . . 15. ∀x:Id.
. . . . | | . . . . . |   vartype(i;x) ⊆r if deq-member(...;x;1of(
. . . . | | . . . . . |                                       ds))→
. . . . | | . . . . . |                      2of(ds)(x)
. . . . | | . . . . . |                   else Top fi
. . . . | | . . . . . 16. IdDeq ∈ EqDecider(Id)
. . . . | | . . . . . 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . | | . . . . . 18. j : Id
. . . . | | . . . . . 19. t : ℕ
. . . . | | . . . . . 20. j = i
. . . . | | . . . . . 21. ¬isnull(a(j;t))
. . . . | | . . . . . 22. ¬isnull(a(i;t))
. . . . | | . . . . . 23. (λx.s(i;t).x) ∈ State(ds)
. . . . | | . . . . . 24. kind(<j,t>) = locl(a)
. . . . | | . . . . . 25. P((λx.s(i;t).x),val(a(i;t)))
```

```
. . . . | | . . . . . 26. valtype(i;a(i;t)) ⊆r T
. . . . | | . . . . . 27. a(j;t) = a(i;t)

. . . . | | . . . . . 28. z : {aaa:Action(i)| ¬isnull(aaa) }
. . . . | | . . . . . 29. z = a(i;t)
. . . . | | . . . . . ⊢  (val(z) = val(a(i;t))) ∈ Prop  by Auto
. . . . | | . . . . . |
. . . . | | . . . . . .....subterm .....
. . . . | | . . . . . 1. i : Id
. . . . | | . . . . . 2. a : Id
. . . . | | . . . . . 3. T : Type
. . . . | | . . . . . 4. ds : x:Id fp-> Type
. . . . | | . . . . . 5. P : State(ds)→T→Prop
. . . . | | . . . . . 6. w : World
. . . . | | . . . . . 7. FairFifo
. . . . | | . . . . . 8. FairFifo
. . . . | | . . . . . 9. ∀l:IdLnk, tg:Id.
. . . . | | . . . . . |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . | | . . . . . |                    <ds
. . . . | | . . . . . |                    ,<[locl(a)],λx.T>
. . . . | | . . . . . |                    ,
. . . . | | . . . . . |                    ,<[a],λx.P>
. . . . | | . . . . . |                    ,
. . . . | | . . . . . |                    ,
. . . . | | . . . . . |                    ,
. . . . | | . . . . . |                    ,
. . . . | | . . . . . |                    ,·>
. . . . | | . . . . . |                 else  fi.da(rcv(l; tg))
. . . . | | . . . . . 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . | | . . . . . 11. ∀a@0:Id, t:ℕ.
. . . . | | . . . . . |   ∃t':ℕ.
. . . . | | . . . . . |   t≤t'
. . . . | | . . . . . |   & ¬isnull(a(i;t'))
. . . . | | . . . . . |     & kind(a(i;t')) = locl(a@0)
. . . . | | . . . . . |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . | | . . . . . |     ∨ P@0 != <[a]
. . . . | | . . . . . |              ,λx.
. . . . | | . . . . . |               P>(a@0) ==> ∀v:<[locl(a)]
. . . . | | . . . . . |                                ,λx.
. . . . | | . . . . . |                                 T>(...)?Top.
. . . . | | . . . . . |       ¬P@0((λx.s(i;t').x),v)
. . . . | | . . . . . 12. ∀t:ℕ.
. . . . | | . . . . . |   ¬isnull(a(i;t))
. . . . | | . . . . . |   ⇒
. . . . | | . . . . . |   (islocal(kind(a(i;t)))
. . . . | | . . . . . |    ⇒
. . . . | | . . . . . |    (eqof(IdDeq)(a,act(kind(a(i;t))))
. . . . | | . . . . . |     ∨₂ false₂)
. . . . | | . . . . . |    ⇒
. . . . | | . . . . . |    P((λx.s(i;t).x),val(a(i;t))))
. . . . | | . . . . . |   & (∀x:Id.
. . . . | | . . . . . |      deq-member(...;<kind(a(i;t)),x>;1of())
. . . . | | . . . . . |      ⇒
. . . . | | . . . . . |      s(i;t+1).x
. . . . | | . . . . . |      =
. . . . | | . . . . . |      2of()
```

```
. . . . | | . . . . . |      (<kind(a(i;t)),x>
. . . . | | . . . . . |      ,λx.s(i;t).x
. . . . | | . . . . . |      ,val(a(i;t))))
. . . . | | . . . . . |   & (∀l:IdLnk.
. . . . | | . . . . . |      deq-member(...;<kind(a(i;t)),l>;1of())
. . . . | | . . . . . |      ⇒
. . . . | | . . . . . |      withlnk(l;m(i;t))
. . . . | | . . . . . |      =
. . . . | | . . . . . |      if source(l) = i→
. . . . | | . . . . . |         concat(map(λtgf.map(λx.
. . . . | | . . . . . |         <1of(tgf)
. . . . | | . . . . . |         ,x>;2of(tgf)
. . . . | | . . . . . |             ((λx.s(i;t).x)
. . . . | | . . . . . |             ,val(a(i;t))));...))
. . . . | | . . . . . |      else nil fi)
. . . . | | . . . . . |   & (∀x:Id.
. . . . | | . . . . . |      ¬(deq-member(IdDeq;x;1of())
. . . . | | . . . . . |        ⇒
. . . . | | . . . . . |        deq-member(KindDeq;kind(a(i;t));2of()
. . . . | | . . . . . |                                        (x)))
. . . . | | . . . . . |      ⇒
. . . . | | . . . . . |      s(i;t).x = s(i;t+1).x)
. . . . | | . . . . . |   & (∀l:IdLnk, tg:Id.
. . . . | | . . . . . |      ¬(deq-member(...;<l,tg>;1of())
. . . . | | . . . . . |        ⇒
. . . . | | . . . . . |        deq-member(KindDeq;kind(a(i;t));...))
. . . . | | . . . . . |      ⇒
. . . . | | . . . . . |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . | | . . . . . 13. ∀x:Id.
. . . . | | . . . . . |   deq-member(IdDeq;x;1of())
. . . . | | . . . . . |   ⇒
. . . . | | . . . . . |   s(i;0).x = 2of()(x)
. . . . | | . . . . . 14. ∀a@0:Action(i).
. . . . | | . . . . . |   ¬isnull(a@0)
. . . . | | . . . . . |   ⇒
. . . . | | . . . . . |   (valtype(i;a@0) ⊆r <[locl(a)]
. . . . | | . . . . . |                      ,λx.T>(kind(a@0))?Top)
. . . . | | . . . . . 15. ∀x:Id.
. . . . | | . . . . . |   vartype(i;x) ⊆r if deq-member(...;x;1of(
. . . . | | . . . . . |                                        ds))→
. . . . | | . . . . . |                     2of(ds)(x)
. . . . | | . . . . . |                  else Top fi
. . . . | | . . . . . 16. IdDeq ∈ EqDecider(Id)
. . . . | | . . . . . 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . | | . . . . . 18. j : Id
. . . . | | . . . . . 19. t : ℕ
. . . . | | . . . . . 20. j = i

. . . . | | . . . . . 21. ¬isnull(a(j;t))
. . . . | | . . . . . 22. ¬isnull(a(i;t))
. . . . | | . . . . . 23. (λx.s(i;t).x) ∈ State(ds)
. . . . | | . . . . . 24. kind(<j,t>) = locl(a)
. . . . | | . . . . . 25. P((λx.s(i;t).x),val(a(i;t)))
. . . . | | . . . . . 26. valtype(i;a(i;t)) ⊆r T
. . . . | | . . . . . 27. a(j;t) = a(i;t)
. . . . | | . . . . . 28. z : {aaa:Action(i)| ¬isnull(aaa) }
```

```
. . . . | | . . . . . 29. z = a(i;t)
. . . . | | . . . . . ⊢  val(z) ∈ valtype(i;a(i;t))
. . . . | | . . . . . | by Analyze -2 THEN DoSubsume
. . . . | | . . . . . |
. . . . | | . . . . . .....subtype_rel .....
. . . . | | . . . . . 1. i : Id
. . . . | | . . . . . 2. a : Id
. . . . | | . . . . . 3. T : Type
. . . . | | . . . . . 4. ds : x:Id fp-> Type
. . . . | | . . . . . 5. P : State(ds)→T→Prop
. . . . | | . . . . . 6. w : World
. . . . | | . . . . . 7. FairFifo
. . . . | | . . . . . 8. FairFifo
. . . . | | . . . . . 9. ∀l:IdLnk, tg:Id.
. . . . | | . . . . . |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . | | . . . . . |                  <ds
. . . . | | . . . . . |                  ,<[locl(a)],λx.T>
. . . . | | . . . . . |                  ,
. . . . | | . . . . . |                  ,<[a],λx.P>
. . . . | | . . . . . |                  ,
. . . . | | . . . . . |                  ,
. . . . | | . . . . . |                  ,
. . . . | | . . . . . |                  ,
. . . . | | . . . . . |                  ,.>
. . . . | | . . . . . |               else  fi.da(rcv(l; tg))
. . . . | | . . . . . 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . | | . . . . . 11. ∀a@0:Id, t:ℕ.
. . . . | | . . . . . |   ∃t':ℕ.
. . . . | | . . . . . |   t≤t'
. . . . | | . . . . . |   & ¬isnull(a(i;t'))
. . . . | | . . . . . |     & kind(a(i;t')) = locl(a@0)
. . . . | | . . . . . |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . | | . . . . . |     ∨ P@0 != <[a]
. . . . | | . . . . . |              ,λx.
. . . . | | . . . . . |               P>(a@0) ==> ∀v:<[locl(a)]
. . . . | | . . . . . |                                ,λx.
. . . . | | . . . . . |                                 T>(...)?Top.
. . . . | | . . . . . |       ¬P@0((λx.s(i;t').x),v)
. . . . | | . . . . . 12. ∀t:ℕ.
. . . . | | . . . . . |   ¬isnull(a(i;t))
. . . . | | . . . . . |   ⇒
. . . . | | . . . . . |   (islocal(kind(a(i;t)))
. . . . | | . . . . . |    ⇒
. . . . | | . . . . . |    (eqof(IdDeq)(a,act(kind(a(i;t))))
. . . . | | . . . . . |     ∨₂ false₂)
. . . . | | . . . . . |    ⇒
. . . . | | . . . . . |    P((λx.s(i;t).x),val(a(i;t))))
. . . . | | . . . . . |   & (∀x:Id.
. . . . | | . . . . . |      deq-member(...;<kind(a(i;t)),x>;1of())
. . . . | | . . . . . |      ⇒
. . . . | | . . . . . |      s(i;t+1).x
. . . . | | . . . . . |      =
. . . . | | . . . . . |      2of()
. . . . | | . . . . . |      (<kind(a(i;t)),x>
. . . . | | . . . . . |      ,λx.s(i;t).x
```

```
. . . . | | . . . . . |      ,val(a(i;t))))
. . . . | | . . . . . |   & (∀l:IdLnk.
. . . . | | . . . . . |      deq-member(...;<kind(a(i;t)),l>;1of())
. . . . | | . . . . . |      ⇒
. . . . | | . . . . . |      withlnk(l;m(i;t))
. . . . | | . . . . . |      =
. . . . | | . . . . . |      if source(l) = i→
. . . . | | . . . . . |         concat(map(λtgf.map(λx.
. . . . | | . . . . . |         <1of(tgf)
. . . . | | . . . . . |         ,x>;2of(tgf)
. . . . | | . . . . . |             ((λx.s(i;t).x)
. . . . | | . . . . . |             ,val(a(i;t))));...))
. . . . | | . . . . . |      else nil fi)
. . . . | | . . . . . |   & (∀x:Id.
. . . . | | . . . . . |      ¬(deq-member(IdDeq;x;1of())
. . . . | | . . . . . |        ⇒
. . . . | | . . . . . |        deq-member(KindDeq;kind(a(i;t));2of()
. . . . | | . . . . . |                                      (x)))
. . . . | | . . . . . |      ⇒
. . . . | | . . . . . |      s(i;t).x = s(i;t+1).x)
. . . . | | . . . . . |   & (∀l:IdLnk, tg:Id.
. . . . | | . . . . . |      ¬(deq-member(...;<l,tg>;1of())
. . . . | | . . . . . |        ⇒
. . . . | | . . . . . |        deq-member(KindDeq;kind(a(i;t));...))
. . . . | | . . . . . |      ⇒
. . . . | | . . . . . |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . | | . . . . . 13. ∀x:Id.
. . . . | | . . . . . |   deq-member(IdDeq;x;1of())
. . . . | | . . . . . |   ⇒
. . . . | | . . . . . |   s(i;0).x = 2of()(x)
. . . . | | . . . . . 14. ∀a@0:Action(i).
. . . . | | . . . . . |   ¬isnull(a@0)
. . . . | | . . . . . |   ⇒
. . . . | | . . . . . |   (valtype(i;a@0) ⊆r <[locl(a)]
. . . . | | . . . . . |                      ,λx.T>(kind(a@0))?Top)
. . . . | | . . . . . 15. ∀x:Id.
. . . . | | . . . . . |   vartype(i;x) ⊆r if deq-member(...;x;1of(
                                                          ds))→
. . . . | | . . . . . |                      2of(ds)(x)
. . . . | | . . . . . |                   else Top fi
. . . . | | . . . . . 16. IdDeq ∈ EqDecider(Id)
. . . . | | . . . . . 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . | | . . . . . 18. j : Id
. . . . | | . . . . . 19. t : ℕ
. . . . | | . . . . . 20. j = i
. . . . | | . . . . . 21. ¬isnull(a(j;t))
. . . . | | . . . . . 22. ¬isnull(a(i;t))
. . . . | | . . . . . 23. (λx.s(i;t).x) ∈ State(ds)
. . . . | | . . . . . 24. kind(<j,t>) = locl(a)
. . . . | | . . . . . 25. P((λx.s(i;t).x),val(a(i;t)))
. . . . | | . . . . . 26. valtype(i;a(i;t)) ⊆r T
. . . . | | . . . . . 27. a(j;t) = a(i;t)
. . . . | | . . . . . 28. z : Action(i)
. . . . | | . . . . . 29. ¬isnull(z)
. . . . | | . . . . . 30. z = a(i;t)
```

```
. . . . | | . . . . . ⊢  valtype(i;z) ⊆r valtype(i;a(i;t))
. . . . | | . . . . . | by HypSubst -1 0
. . . . | | . . . . . |
. . . . | | . . . . . 1. i : Id
. . . . | | . . . . . 2. a : Id
. . . . | | . . . . . 3. T : Type
. . . . | | . . . . . 4. ds : x:Id fp-> Type
. . . . | | . . . . . 5. P : State(ds)→T→Prop
. . . . | | . . . . . 6. w : World
. . . . | | . . . . . 7. FairFifo
. . . . | | . . . . . 8. FairFifo
. . . . | | . . . . . 9. ∀l:IdLnk, tg:Id.
. . . . | | . . . . . |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . | | . . . . . |                  <ds
. . . . | | . . . . . |                  ,<[locl(a)],λx.T>
. . . . | | . . . . . |                  ,
. . . . | | . . . . . |                  ,<[a],λx.P>
. . . . | | . . . . . |                  ,
. . . . | | . . . . . |                  ,
. . . . | | . . . . . |                  ,
. . . . | | . . . . . |                  ,
. . . . | | . . . . . |                  ,·>
. . . . | | . . . . . |               else  fi.da(rcv(l; tg))
. . . . | | . . . . . 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . | | . . . . . 11. ∀a@0:Id, t:ℕ.
. . . . | | . . . . . |   ∃t':ℕ.
. . . . | | . . . . . |   t≤t'
. . . . | | . . . . . |   & ¬isnull(a(i;t'))
. . . . | | . . . . . |     & kind(a(i;t')) = locl(a@0)
. . . . | | . . . . . |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . | | . . . . . |     ∨ P@0 != <[a]
. . . . | | . . . . . |              ,λx.
. . . . | | . . . . . |               P>(a@0) ==> ∀v:<[locl(a)]
. . . . | | . . . . . |                                ,λx.
. . . . | | . . . . . |                                 T>(...)?Top.
. . . . | | . . . . . |       ¬P@0((λx.s(i;t').x),v)
. . . . | | . . . . . 12. ∀t:ℕ.
. . . . | | . . . . . |   ¬isnull(a(i;t))
. . . . | | . . . . . |   ⇒
. . . . | | . . . . . |   (islocal(kind(a(i;t)))
. . . . | | . . . . . |    ⇒
. . . . | | . . . . . |    (eqof(IdDeq)(a,act(kind(a(i;t))))
. . . . | | . . . . . |     ∨₂ false₂)
. . . . | | . . . . . |    ⇒
. . . . | | . . . . . |    P((λx.s(i;t).x),val(a(i;t))))
. . . . | | . . . . . |   & (∀x:Id.
. . . . | | . . . . . |      deq-member(...;<kind(a(i;t)),x>;1of())
. . . . | | . . . . . |      ⇒
. . . . | | . . . . . |      s(i;t+1).x
. . . . | | . . . . . |      =
. . . . | | . . . . . |      2of()
. . . . | | . . . . . |      (<kind(a(i;t)),x>
. . . . | | . . . . . |      ,λx.s(i;t).x
. . . . | | . . . . . |      ,val(a(i;t))))
. . . . | | . . . . . |   & (∀l:IdLnk.
```

```
. . . . | | . . . . . |      deq-member(...;<kind(a(i;t)),l>;1of())
. . . . | | . . . . . |      ⇒
. . . . | | . . . . . |      withlnk(l;m(i;t))
. . . . | | . . . . . |      =
. . . . | | . . . . . |      if source(l) = i→
. . . . | | . . . . . |         concat(map(λtgf.map(λx.
. . . . | | . . . . . |         <1of(tgf)
. . . . | | . . . . . |         ,x>;2of(tgf)
. . . . | | . . . . . |             ((λx.s(i;t).x)
. . . . | | . . . . . |             ,val(a(i;t))));...))
. . . . | | . . . . . |      else nil fi)
. . . . | | . . . . . |   & (∀x:Id.
. . . . | | . . . . . |      ¬(deq-member(IdDeq;x;1of())
. . . . | | . . . . . |        ⇒
. . . . | | . . . . . |        deq-member(KindDeq;kind(a(i;t));2of()
. . . . | | . . . . . |                                        (x)))
. . . . | | . . . . . |      ⇒
. . . . | | . . . . . |      s(i;t).x = s(i;t+1).x)
. . . . | | . . . . . |   & (∀l:IdLnk, tg:Id.
. . . . | | . . . . . |      ¬(deq-member(...;<l,tg>;1of())
. . . . | | . . . . . |        ⇒
. . . . | | . . . . . |        deq-member(KindDeq;kind(a(i;t));...))
. . . . | | . . . . . |      ⇒
. . . . | | . . . . . |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . | | . . . . . 13. ∀x:Id.
. . . . | | . . . . . |   deq-member(IdDeq;x;1of())
. . . . | | . . . . . |   ⇒

. . . . | | . . . . . |   s(i;0).x = 2of()(x)
. . . . | | . . . . . 14. ∀a@0:Action(i).
. . . . | | . . . . . |   ¬isnull(a@0)
. . . . | | . . . . . |   ⇒
. . . . | | . . . . . |   (valtype(i;a@0) ⊆r <[locl(a)]
. . . . | | . . . . . |                      ,λx.T>(kind(a@0))?Top)
. . . . | | . . . . . 15. ∀x:Id.
. . . . | | . . . . . |   vartype(i;x) ⊆r if deq-member(...;x;1of(
. . . . | | . . . . . |                                       ds))→
. . . . | | . . . . . |                     2of(ds)(x)
. . . . | | . . . . . |                  else Top fi
. . . . | | . . . . . 16. IdDeq ∈ EqDecider(Id)
. . . . | | . . . . . 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . | | . . . . . 18. j : Id
. . . . | | . . . . . 19. t : ℕ
. . . . | | . . . . . 20. j = i
. . . . | | . . . . . 21. ¬isnull(a(j;t))
. . . . | | . . . . . 22. ¬isnull(a(i;t))
. . . . | | . . . . . 23. (λx.s(i;t).x) ∈ State(ds)
. . . . | | . . . . . 24. kind(<j,t>) = locl(a)
. . . . | | . . . . . 25. P((λx.s(i;t).x),val(a(i;t)))
. . . . | | . . . . . 26. valtype(i;a(i;t)) ⊆r T
. . . . | | . . . . . 27. a(j;t) = a(i;t)
. . . . | | . . . . . 28. z : Action(i)
. . . . | | . . . . . 29. ¬isnull(z)
. . . . | | . . . . . 30. z = a(i;t)
. . . . | | . . . . . 31. z1 : {aaa:Action(i)| ¬isnull(aaa) }
. . . . | | . . . . . ⊢  ¬isnull(z1)  by Analyze 0
```

```
. . . . | | . . . . . |
. . . . | | . . . . . 1. i : Id
. . . . | | . . . . . 2. a : Id
. . . . | | . . . . . 3. T : Type
. . . . | | . . . . . 4. ds : x:Id fp-> Type
. . . . | | . . . . . 5. P : State(ds)→T→Prop
. . . . | | . . . . . 6. w : World
. . . . | | . . . . . 7. FairFifo
. . . . | | . . . . . 8. FairFifo
. . . . | | . . . . . 9. ∀l:IdLnk, tg:Id.
. . . . | | . . . . .    (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . | | . . . . .                      <ds
. . . . | | . . . . .                      ,<[locl(a)],λx.T>
. . . . | | . . . . .                      ,
. . . . | | . . . . .                      ,<[a],λx.P>
. . . . | | . . . . .                      ,
. . . . | | . . . . .                      ,
. . . . | | . . . . .                      ,
. . . . | | . . . . .                      ,
. . . . | | . . . . .                      ,.>
. . . . | | . . . . .                    else  fi.da(rcv(l; tg))
. . . . | | . . . . . 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . | | . . . . . 11. ∀a@0:Id, t:ℕ.
. . . . | | . . . . .     ∃t':ℕ.
. . . . | | . . . . .     t≤t'
. . . . | | . . . . .     & ¬isnull(a(i;t'))
. . . . | | . . . . .       & kind(a(i;t')) = locl(a@0)
. . . . | | . . . . .       ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . | | . . . . .       ∨ P@0 != <[a]
. . . . | | . . . . .                ,λx.
. . . . | | . . . . .                 P>(a@0) ==> ∀v:<[locl(a)]
. . . . | | . . . . .                                ,λx.
. . . . | | . . . . .                                 T>(...)?Top.
. . . . | | . . . . .          ¬P@0((λx.s(i;t').x),v)
. . . . | | . . . . . 12. ∀t:ℕ.
. . . . | | . . . . .     ¬isnull(a(i;t))
. . . . | | . . . . .     ⇒
. . . . | | . . . . .     (islocal(kind(a(i;t)))
. . . . | | . . . . .      ⇒
. . . . | | . . . . .      (eqof(IdDeq)(a,act(kind(a(i;t))))
. . . . | | . . . . .       ∨₂ false₂)
. . . . | | . . . . .      ⇒
. . . . | | . . . . .      P((λx.s(i;t).x),val(a(i;t))))
. . . . | | . . . . .     & (∀x:Id.
. . . . | | . . . . .        deq-member(...;<kind(a(i;t)),x>;1of())
. . . . | | . . . . .        ⇒
. . . . | | . . . . .        s(i;t+1).x
. . . . | | . . . . .        =
. . . . | | . . . . .        2of()
. . . . | | . . . . .        (<kind(a(i;t)),x>
. . . . | | . . . . .        ,λx.s(i;t).x
. . . . | | . . . . .        ,val(a(i;t))))
. . . . | | . . . . .     & (∀l:IdLnk.
. . . . | | . . . . .        deq-member(...;<kind(a(i;t)),l>;1of())
. . . . | | . . . . .        ⇒
```

```
. . . . | | . . . . . .        withlnk(l;m(i;t))
. . . . | | . . . . . .        =
. . . . | | . . . . . .        if source(l) = i⟶
. . . . | | . . . . . .           concat(map(λtgf.map(λx.
. . . . | | . . . . . .           <1of(tgf)
. . . . | | . . . . . .           ,x>;2of(tgf)
. . . . | | . . . . . .               ((λx.s(i;t).x)
. . . . | | . . . . . .               ,val(a(i;t))));...))
. . . . | | . . . . . .        else nil fi)
. . . . | | . . . . . .     & (∀x:Id.
. . . . | | . . . . . .        ¬(deq-member(IdDeq;x;1of())
. . . . | | . . . . . .          ⇒
. . . . | | . . . . . .          deq-member(KindDeq;kind(a(i;t));2of()
. . . . | | . . . . . .                                          (x)))
. . . . | | . . . . . .        ⇒
. . . . | | . . . . . .        s(i;t).x = s(i;t+1).x)
. . . . | | . . . . . .     & (∀l:IdLnk, tg:Id.

. . . . | | . . . . . .        ¬(deq-member(...;<l,tg>;1of())
. . . . | | . . . . . .          ⇒
. . . . | | . . . . . .          deq-member(KindDeq;kind(a(i;t));...))
. . . . | | . . . . . .        ⇒
. . . . | | . . . . . .        w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . | | . . . . . . 13. ∀x:Id.
. . . . | | . . . . . .     deq-member(IdDeq;x;1of())
. . . . | | . . . . . .     ⇒
. . . . | | . . . . . .     s(i;0).x = 2of()(x)
. . . . | | . . . . . . 14. ∀a@0:Action(i).
. . . . | | . . . . . .     ¬isnull(a@0)
. . . . | | . . . . . .     ⇒
. . . . | | . . . . . .     (valtype(i;a@0) ⊆r <[locl(a)]
. . . . | | . . . . . .                        ,λx.T>(kind(a@0))?Top)
. . . . | | . . . . . . 15. ∀x:Id.
. . . . | | . . . . . .     vartype(i;x) ⊆r if deq-member(...;x;1of(
. . . . | | . . . . . .                                          ds))⟶
. . . . | | . . . . . .                        2of(ds)(x)
. . . . | | . . . . . .                    else Top fi
. . . . | | . . . . . . 16. IdDeq ∈ EqDecider(Id)
. . . . | | . . . . . . 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . | | . . . . . . 18. j : Id
. . . . | | . . . . . . 19. t : ℕ
. . . . | | . . . . . . 20. j = i
. . . . | | . . . . . . 21. ¬isnull(a(j;t))
. . . . | | . . . . . . 22. ¬isnull(a(i;t))
. . . . | | . . . . . . 23. (λx.s(i;t).x) ∈ State(ds)
. . . . | | . . . . . . 24. kind(<j,t>) = locl(a)
. . . . | | . . . . . . 25. P((λx.s(i;t).x),val(a(i;t)))
. . . . | | . . . . . . 26. valtype(i;a(i;t)) ⊆r T
. . . . | | . . . . . . 27. a(j;t) = a(i;t)
. . . . | | . . . . . . 28. z : Action(i)
. . . . | | . . . . . . 29. ¬isnull(z)
. . . . | | . . . . . . 30. z = a(i;t)
. . . . | | . . . . . . 31. z1 : {aaa:Action(i)| ¬isnull(aaa) }
. . . . | | . . . . . . 32. isnull(z1)
. . . . | | . . . . . . ⊢  False  by Analyze -2
. . . . | |
```

```
. . . . | .\
. . . . | . .....subterm .....
. . . . | . 1. i : Id
. . . . | . 2. a : Id
. . . . | . 3. T : Type
. . . . | . 4. ds : x:Id fp-> Type
. . . . | . 5. P : State(ds)→T→Prop
. . . . | . 6. w : World
. . . . | . 7. FairFifo
. . . . | . 8. FairFifo
. . . . | . 9. ∀l:IdLnk, tg:Id.
. . . . | .    (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . | .                      <ds
. . . . | .                      ,<[locl(a)],λx.T>
. . . . | .                      ,
. . . . | .                      ,<[a],λx.P>
. . . . | .                      ,
. . . . | .                      ,
. . . . | .                      ,
. . . . | .                      ,
. . . . | .                      ,•>
. . . . | .                   else  fi.da(rcv(l; tg))
. . . . | . 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . | . 11. ∀a@0:Id, t:ℕ.
. . . . | .     ∃t':ℕ.
. . . . | .     t≤t'
. . . . | .     & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . | .       ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . | .       ∨ P@0 != <[a],λx.P>(a@0) ==> ∀v:<[locl(a)]
. . . . | .                                    ,λx.
. . . . | .                                     T>(locl(a@0))?Top.
. . . . | .         ¬P@0((λx.s(i;t').x),v)
. . . . | . 12. ∀t:ℕ.
. . . . | .     ¬isnull(a(i;t))
. . . . | .     ⇒
. . . . | .     (islocal(kind(a(i;t)))
. . . . | .      ⇒
. . . . | .      (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . | .      ⇒
. . . . | .      P((λx.s(i;t).x),val(a(i;t))))
. . . . | .     & (∀x:Id.
. . . . | .        deq-member(product-deq(Knd;Id;KindDeq;...);<...
. . . . | .                                                  ,x>;1of(
. . . . | .                                                      ))
. . . . | .        ⇒
. . . . | .        s(i;t+1).x
. . . . | .        =
. . . . | .        2of()(<kind(a(i;t)),x>,λx.s(i;t).x,val(a(i;t))))
. . . . | .     & (∀l:IdLnk.
. . . . | .        deq-member(product-deq(Knd;IdLnk;...;...);<...
. . . . | .                                                ,l>;1of(
. . . . | .                                                    ))
. . . . | .        ⇒
. . . . | .        withlnk(l;m(i;t))
. . . . | .        =
```

```
. . . . | .        if source(l) = i→
. . . . | .           concat(map(λtgf.map(λx.
. . . . | .           <1of(tgf),x>;2of(tgf)
. . . . | .                        ((λx.s(i;t).x)
. . . . | .                        ,val(a(i;t))));2of()
. . . . | .                                      (<kind(a(i;t)),l>)))
. . . . | .        else nil fi)
. . . . | .     & (∀x:Id.
. . . . | .        ¬(deq-member(IdDeq;x;1of())
. . . . | .          ⇒
. . . . | .          deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . . . | .        ⇒
. . . . | .        s(i;t).x = s(i;t+1).x)
. . . . | .     & (∀l:IdLnk, tg:Id.
. . . . | .        ¬(deq-member(product-deq(IdLnk;Id;...;...);...;1of(
. . . . | .                                                      ))
. . . . | .          ⇒
. . . . | .          deq-member(KindDeq;kind(a(i;t));2of()(<l,tg>)))
. . . . | .        ⇒
. . . . | .        w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . | . 13. ∀x:Id.
. . . . | .     deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . . . | . 14. ∀a@0:Action(i).
. . . . | .     ¬isnull(a@0)
. . . . | .     ⇒
. . . . | .     (valtype(i;a@0) ⊆r <[locl(a)],λx.T>(kind(a@0))?Top)
. . . . | . 15. ∀x:Id.
. . . . | .     vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . . . | .                       2of(ds)(x)
. . . . | .                    else Top fi
. . . . | . 16. IdDeq ∈ EqDecider(Id)
. . . . | . 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . | . 18. j : Id
. . . . | . 19. t : ℕ
. . . . | . 20. j = i
. . . . | . 21. ¬isnull(a(j;t))
. . . . | . 22. ¬isnull(a(i;t))
. . . . | . 23. (λx.s(i;t).x) ∈ State(ds)
. . . . | . ⊢  <j,t> ∈ E
. . . . | .   by Unfold `w-E` 0 THEN Analyze THEN Reduce 0
. . . . |
. . . . .\
. . . . . 1. i : Id
. . . . . 2. a : Id
. . . . . 3. T : Type
. . . . . 4. ds : x:Id fp-> Type
. . . . . 5. P : State(ds)→T→Prop
. . . . . 6. w : World
. . . . . 7. p : FairFifo
. . . . . 8. FairFifo
. . . . . 9. ∀l:IdLnk, tg:Id.
. . . . . |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . |                    <ds,<[locl(a)],λx.T>,,<[a],λx.P>,,,,,•>
. . . . . |                 else  fi.da(rcv(l; tg))
. . . . . 10. (eqof(IdDeq)(i,i)) ∼ true₂
```

```
. . . . . 11. ∀a@0:Id, t:ℕ.
. . . . . |   ∃t':ℕ.
. . . . . |   t≤t'
. . . . . |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . . |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . . |     ∨ P@0 != <[a],λx.P>(a@0) ==> ∀v:<[locl(a)]
. . . . . |                                      ,λx.T>(locl(a@0))?Top.
. . . . . |       ¬P@0((λx.s(i;t').x),v)
. . . . . 12. ∀t:ℕ.
. . . . . |   ¬isnull(a(i;t))
. . . . . |   ⇒
. . . . . |   (islocal(kind(a(i;t)))
. . . . . |    ⇒
. . . . . |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . . |    ⇒
. . . . . |    P((λx.s(i;t).x),val(a(i;t))))
. . . . . |   & (∀x:Id.
. . . . . |      deq-member(product-deq(Knd;Id;KindDeq;IdDeq);<...
. . . . . |                                                  ,x>;1of(
. . . . . |                                                      ))
. . . . . |      ⇒
. . . . . |      s(i;t+1).x
. . . . . |      =
. . . . . |      2of()(<kind(a(i;t)),x>,λx.s(i;t).x,val(a(i;t))))
. . . . . |   & (∀l:IdLnk.
. . . . . |      deq-member(product-deq(Knd;IdLnk;...;...);<kind(...)
. . . . . |                                              ,l>;1of())
. . . . . |      ⇒
. . . . . |      withlnk(l;m(i;t))
. . . . . |      =
. . . . . |      if source(l) = i→
. . . . . |         concat(map(λtgf.map(λx.
. . . . . |         <1of(tgf),x>;2of(tgf)
. . . . . |                      ((λx.s(i;t).x)
. . . . . |                      ,val(a(i;t))));2of()
. . . . . |                                      (<kind(a(i;t)),l>)))
. . . . . |      else nil fi)
. . . . . |   & (∀x:Id.
. . . . . |      ¬(deq-member(IdDeq;x;1of())
. . . . . |        ⇒
. . . . . |        deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . . . . |      ⇒
. . . . . |      s(i;t).x = s(i;t+1).x)
. . . . . |   & (∀l:IdLnk, tg:Id.
. . . . . |      ¬(deq-member(product-deq(IdLnk;Id;...;IdDeq);...;1of(
. . . . . |                                                      ))
. . . . . |        ⇒
. . . . . |        deq-member(KindDeq;kind(a(i;t));2of()(<l,tg>)))
. . . . . |      ⇒
. . . . . |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . 13. ∀x:Id. deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . . . . 14. ∀a@0:Action(i).
. . . . . |   ¬isnull(a@0)
. . . . . |   ⇒
. . . . . |   (valtype(i;a@0) ⊆r <[locl(a)],λx.T>(kind(a@0))?Top)
```

```
. . . . . 15. ∀x:Id.
. . . . . |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . . . . |                      2of(ds)(x)
. . . . . |                   else Top fi
. . . . . 16. IdDeq ∈ EqDecider(Id)
. . . . . 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . . 18. j : Id
. . . . . 19. t : ℕ
. . . . . 20. j = i
. . . . . 21. ¬isnull(a(j;t))
. . . . . 22. ¬isnull(a(i;t))
. . . . . 23. (λx.s(i;t).x) ∈ State(ds)
. . . . . ⊢  ∃e':E.
. . . . . |  (<j,t> <loc e') ∨ <j,t> = e'
. . . . . |  & kind(e') = locl(a) ∨ (∀v:T. ¬P((λz.(z after e')),v))
. . . . . | by AllHyps
. . . . . |    (λh.
. . . . . |     InstHyp [a;t+1] h
. . . . . |     THENA
. . . . . |     (Auto THEN All (Unfold `dstype`) THEN All Reduce
. . . . . |      THEN
. . . . . |      Trivial))
. . . . . |    THEN
. . . . . |    ExRepD
. . . . . |    THEN
. . . . . |    SplitOrHyps
. . . . . |
. . . . . |\
. . . . . | 1. i : Id
. . . . . | 2. a : Id
. . . . . | 3. T : Type
. . . . . | 4. ds : x:Id fp-> Type
. . . . . | 5. P : State(ds)→T→Prop
. . . . . | 6. w : World
. . . . . | 7. p : FairFifo
. . . . . | 8. FairFifo
. . . . . | 9. ∀l:IdLnk, tg:Id.
. . . . . | |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | |                    <ds
. . . . . | |                    ,<[locl(a)],λx.T>
. . . . . | |                    ,
. . . . . | |                    ,<[a],λx.P>
. . . . . | |                    ,
. . . . . | |                    ,
. . . . . | |                    ,
. . . . . | |                    ,
. . . . . | |                    ,.>
. . . . . | |                 else  fi.da(rcv(l; tg))
. . . . . | 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . . | 11. ∀a@0:Id, t:ℕ.
. . . . . | |   ∃t':ℕ.
. . . . . | |   t≤t'
. . . . . | |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . . | |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . . | |     ∨ P@0 != <[a],λx.P>(a@0) ==> ∀v:<[locl(a)]
```

```
. . . . . | |                                          ,λx.
. . . . . | |                                           T>(locl(a@0))?Top.
. . . . . | |       ¬P@0((λx.s(i;t').x),v)
. . . . . | 12. ∀t:ℕ.
. . . . . | |   ¬isnull(a(i;t))
. . . . . | |   ⇒
. . . . . | |   (islocal(kind(a(i;t)))
. . . . . | |    ⇒
. . . . . | |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . . | |    ⇒
. . . . . | |    P((λx.s(i;t).x),val(a(i;t))))
. . . . . | |   & (∀x:Id.
. . . . . | |      deq-member(product-deq(Knd;Id;KindDeq;...);<...
. . . . . | |                                                  ,x>;1of(
. . . . . | |                                                      ))
. . . . . | |      ⇒
. . . . . | |      s(i;t+1).x
. . . . . | |      =
. . . . . | |      2of()(<kind(a(i;t)),x>,λx.s(i;t).x,val(a(i;t))))
. . . . . | |   & (∀l:IdLnk.
. . . . . | |      deq-member(product-deq(Knd;IdLnk;...;...);<...
. . . . . | |                                                ,l>;1of(
. . . . . | |                                                    ))
. . . . . | |      ⇒
. . . . . | |      withlnk(l;m(i;t))
. . . . . | |      =
. . . . . | |      if source(l) = i→
. . . . . | |         concat(map(λtgf.map(λx.
. . . . . | |         <1of(tgf),x>;2of(tgf)
. . . . . | |                     ((λx.s(i;t).x)
. . . . . | |                     ,val(a(i;t))));2of()
. . . . . | |                                    (<kind(a(i;t)),l>)))
. . . . . | |      else nil fi)
. . . . . | |   & (∀x:Id.
. . . . . | |      ¬(deq-member(IdDeq;x;1of())
. . . . . | |        ⇒
. . . . . | |        deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . . . . | |      ⇒
. . . . . | |      s(i;t).x = s(i;t+1).x)
. . . . . | |   & (∀l:IdLnk, tg:Id.
. . . . . | |      ¬(deq-member(product-deq(IdLnk;Id;...;...);...;1of(
. . . . . | |                                                    ))
. . . . . | |        ⇒
. . . . . | |        deq-member(KindDeq;kind(a(i;t));2of()(<l,tg>)))
. . . . . | |      ⇒
. . . . . | |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . | 13. ∀x:Id.
. . . . . | |   deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . . . . | 14. ∀a@0:Action(i).
. . . . . | |   ¬isnull(a@0)
. . . . . | |   ⇒
. . . . . | |   (valtype(i;a@0) ⊆r <[locl(a)],λx.T>(kind(a@0))?Top)
. . . . . | 15. ∀x:Id.
. . . . . | |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . . . . | |                     2of(ds)(x)
```

```
. . . . . | |                    else Top fi
. . . . . | 16. IdDeq ∈ EqDecider(Id)
. . . . . | 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . . | 18. j : Id
. . . . . | 19. t : ℕ
. . . . . | 20. j = i
. . . . . | 21. ¬isnull(a(j;t))
. . . . . | 22. ¬isnull(a(i;t))
. . . . . | 23. (λx.s(i;t).x) ∈ State(ds)
. . . . . | 24. t' : ℕ
. . . . . | 25. t+1≤t'
. . . . . | 26. ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a)
. . . . . | ⊢  ∃e':E.
. . . . . | |  (<j,t> <loc e') ∨ <j,t> = e'
. . . . . | |  & kind(e') = locl(a) ∨ (∀v:T. ¬P((λz.(z after e')),v))
. . . . . | | by Analyze -1 THEN InstConcl [<i,t'>]
. . . . . | |
. . . . . | |\
. . . . . | | .....wf .....
. . . . . | | 1. i : Id
. . . . . | | 2. a : Id
. . . . . | | 3. T : Type
. . . . . | | 4. ds : x:Id fp-> Type
. . . . . | | 5. P : State(ds)→T→Prop
. . . . . | | 6. w : World
. . . . . | | 7. FairFifo
. . . . . | | 8. FairFifo
. . . . . | | 9. ∀l:IdLnk, tg:Id.
. . . . . | |    (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | |                      <ds
. . . . . | |                      ,<[locl(a)],λx.T>
. . . . . | |                      ,
. . . . . | |                      ,<[a],λx.P>
. . . . . | |                      ,
. . . . . | |                      ,
. . . . . | |                      ,
. . . . . | |                      ,
. . . . . | |                      ,.>
. . . . . | |                    else  fi.da(rcv(l; tg))
. . . . . | | 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . . | | 11. ∀a@0:Id, t:ℕ.
. . . . . | |     ∃t':ℕ.
. . . . . | |     t≤t'
. . . . . | |     & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . . | |       ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . . | |       ∨ P@0 != <[a]
. . . . . | |                ,λx.P>(a@0) ==> ∀v:<[locl(a)]
. . . . . | |                                  ,λx.T>(locl(a@0))?Top.
. . . . . | |         ¬P@0((λx.s(i;t').x),v)
. . . . . | | 12. ∀t:ℕ.
. . . . . | |     ¬isnull(a(i;t))
. . . . . | |     ⇒
. . . . . | |     (islocal(kind(a(i;t)))
. . . . . | |      ⇒
. . . . . | |      (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
```

```
. . . . . | |      ⇒
. . . . . | |      P((λx.s(i;t).x),val(a(i;t))))
. . . . . | |     & (∀x:Id.
. . . . . | |        deq-member(product-deq(Knd;Id;...;IdDeq);<...
. . . . . | |                                                ,x>;1of(
. . . . . | |                                                    ))
. . . . . | |        ⇒
. . . . . | |        s(i;t+1).x
. . . . . | |        =
. . . . . | |        2of()(<kind(a(i;t)),x>,λx.s(i;t).x,val(a(i;t))))
. . . . . | |     & (∀l:IdLnk.
. . . . . | |        deq-member(product-deq(Knd;...;...;...);<...
. . . . . | |                                              ,l>;1of(
. . . . . | |                                                  ))
. . . . . | |        ⇒
. . . . . | |        withlnk(l;m(i;t))
. . . . . | |        =
. . . . . | |        if source(l) = i→
. . . . . | |           concat(map(λtgf.map(λx.
. . . . . | |           <1of(tgf)
. . . . . | |           ,x>;2of(tgf)
. . . . . | |               ((λx.s(i;t).x)
. . . . . | |               ,val(a(i;t))));2of()(<kind(a(i;t)),l>)))
. . . . . | |        else nil fi)
. . . . . | |     & (∀x:Id.
. . . . . | |        ¬(deq-member(IdDeq;x;1of())
. . . . . | |          ⇒
. . . . . | |          deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . . . . | |        ⇒
. . . . . | |        s(i;t).x = s(i;t+1).x)
. . . . . | |     & (∀l:IdLnk, tg:Id.
. . . . . | |        ¬(deq-member(product-deq(...;Id;...;...);...;1of(
. . . . . | |                                                    ))
. . . . . | |          ⇒
. . . . . | |          deq-member(KindDeq;kind(a(i;t));2of()(<l,tg>)))
. . . . . | |        ⇒
. . . . . | |        w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . | | 13. ∀x:Id.
. . . . . | |     deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . . . . | | 14. ∀a@0:Action(i).
. . . . . | |     ¬isnull(a@0)
. . . . . | |     ⇒
. . . . . | |     (valtype(i;a@0) ⊆r <[locl(a)],λx.T>(kind(a@0))?Top)
. . . . . | | 15. ∀x:Id.
. . . . . | |     vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . . . . | |                        2of(ds)(x)
. . . . . | |                     else Top fi
. . . . . | | 16. IdDeq ∈ EqDecider(Id)
. . . . . | | 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . . | | 18. j : Id
. . . . . | | 19. t : ℕ
. . . . . | | 20. j = i
. . . . . | | 21. ¬isnull(a(j;t))
. . . . . | | 22. ¬isnull(a(i;t))
. . . . . | | 23. (λx.s(i;t).x) ∈ State(ds)
```

```
. . . . . | | 24. t' : ℕ
. . . . . | | 25. t+1≤t'
. . . . . | | 26. ¬isnull(a(i;t'))
. . . . . | | 27. kind(a(i;t')) = locl(a)
. . . . . | | ⊢  <i,t'> ∈ E
. . . . . | |   by Unfold `w-E` 0 THEN Analyze THEN Try D_ES_Subtype
. . . . . | |      THEN
. . . . . | |      Reduce 0
. . . . . | |      THEN
. . . . . | |      Trivial
. . . . . | |
. . . . . | |\
. . . . . | | 1. i : Id
. . . . . | | 2. a : Id
. . . . . | | 3. T : Type
. . . . . | | 4. ds : x:Id fp-> Type
. . . . . | | 5. P : State(ds)→T→Prop
. . . . . | | 6. w : World
. . . . . | | 7. p : FairFifo
. . . . . | | 8. FairFifo
. . . . . | | 9. ∀l:IdLnk, tg:Id.
. . . . . | | |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | | |                  <ds
. . . . . | | |                  ,<[locl(a)],λx.T>
. . . . . | | |                  ,
. . . . . | | |                  ,<[a],λx.P>
. . . . . | | |                  ,
. . . . . | | |                  ,
. . . . . | | |                  ,
. . . . . | | |                  ,
. . . . . | | |                  ,.>
. . . . . | | |               else  fi.da(rcv(l; tg))
. . . . . | | 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . . | | 11. ∀a@0:Id, t:ℕ.
. . . . . | | |   ∃t':ℕ.
. . . . . | | |   t≤t'
. . . . . | | |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . . | | |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . . | | |     ∨ P@0 != <[a]
. . . . . | | |              ,λx.P>(a@0) ==> ∀v:<[locl(a)]
. . . . . | | |                                ,λx.T>(locl(a@0))?Top.
. . . . . | | |       ¬P@0((λx.s(i;t').x),v)
. . . . . | | 12. ∀t:ℕ.
. . . . . | | |   ¬isnull(a(i;t))
. . . . . | | |   ⇒
. . . . . | | |   (islocal(kind(a(i;t)))
. . . . . | | |    ⇒
. . . . . | | |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . . | | |    ⇒
. . . . . | | |    P((λx.s(i;t).x),val(a(i;t))))
. . . . . | | |   & (∀x:Id.
. . . . . | | |      deq-member(product-deq(Knd;Id;...;IdDeq);<...
. . . . . | | |                                              ,x>;1of(
. . . . . | | |                                                  ))
. . . . . | | |      ⇒
```

```
. . . . . | | |      s(i;t+1).x
. . . . . | | |      =
. . . . . | | |      2of()(<kind(a(i;t)),x>,λx.s(i;t).x,val(a(i;t))))
. . . . . | | |   & (∀l:IdLnk.
. . . . . | | |      deq-member(product-deq(Knd;...;...;...);<...
. . . . . | | |                                              ,l>;1of(
. . . . . | | |                                                  ))
. . . . . | | |      ⇒
. . . . . | | |      withlnk(l;m(i;t))
. . . . . | | |      =
. . . . . | | |      if source(l) = i→
. . . . . | | |         concat(map(λtgf.map(λx.
. . . . . | | |         <1of(tgf)
. . . . . | | |         ,x>;2of(tgf)
. . . . . | | |             ((λx.s(i;t).x)
. . . . . | | |             ,val(a(i;t))));2of()(<kind(a(i;t)),l>)))
. . . . . | | |      else nil fi)
. . . . . | | |   & (∀x:Id.
. . . . . | | |      ¬(deq-member(IdDeq;x;1of())
. . . . . | | |        ⇒
. . . . . | | |        deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . . . . | | |      ⇒

. . . . . | | |      s(i;t).x = s(i;t+1).x)
. . . . . | | |   & (∀l:IdLnk, tg:Id.
. . . . . | | |      ¬(deq-member(product-deq(...;Id;...;...);...;1of(
. . . . . | | |                                                  ))
. . . . . | | |        ⇒
. . . . . | | |        deq-member(KindDeq;kind(a(i;t));2of()(<l,tg>)))
. . . . . | | |      ⇒
. . . . . | | |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . | | 13. ∀x:Id.
. . . . . | | |   deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . . . . | | 14. ∀a@0:Action(i).
. . . . . | | |   ¬isnull(a@0)
. . . . . | | |   ⇒
. . . . . | | |   (valtype(i;a@0) ⊆r <[locl(a)],λx.T>(kind(a@0))?Top)
. . . . . | | 15. ∀x:Id.
. . . . . | | |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . . . . | | |                      2of(ds)(x)
. . . . . | | |                  else Top fi
. . . . . | | 16. IdDeq ∈ EqDecider(Id)
. . . . . | | 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . . | | 18. j : Id
. . . . . | | 19. t : ℕ
. . . . . | | 20. j = i
. . . . . | | 21. ¬isnull(a(j;t))
. . . . . | | 22. ¬isnull(a(i;t))
. . . . . | | 23. (λx.s(i;t).x) ∈ State(ds)
. . . . . | | 24. t' : ℕ
. . . . . | | 25. t+1≤t'
. . . . . | | 26. ¬isnull(a(i;t'))
. . . . . | | 27. kind(a(i;t')) = locl(a)
. . . . . | | ⊢  (<j,t> <loc <i,t'>) ∨ <j,t> = <i,t'>
. . . . . | | |  & kind(<i,t'>) = locl(a)
. . . . . | | |    ∨ (∀v:T. ¬P((λz.(z after <i,t'>)),v))
```

```
. . . . . | | | by Analyze 0
. . . . . | | |
. . . . . | | |\
. . . . . | | | 1. i : Id
. . . . . | | | 2. a : Id
. . . . . | | | 3. T : Type
. . . . . | | | 4. ds : x:Id fp-> Type
. . . . . | | | 5. P : State(ds)→T→Prop
. . . . . | | | 6. w : World
. . . . . | | | 7. p : FairFifo
. . . . . | | | 8. FairFifo
. . . . . | | | 9. ∀l:IdLnk, tg:Id.
. . . . . | | | |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | | | |                    <ds
. . . . . | | | |                    ,<[locl(a)],λx.T>
. . . . . | | | |                    ,
. . . . . | | | |                    ,<[a],λx.P>
. . . . . | | | |                    ,
. . . . . | | | |                    ,
. . . . . | | | |                    ,
. . . . . | | | |                    ,
. . . . . | | | |                    ,·>
. . . . . | | | |                 else  fi.da(rcv(l; tg))
. . . . . | | | 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . . | | | 11. ∀a@0:Id, t:ℕ.
. . . . . | | | |   ∃t':ℕ.
. . . . . | | | |   t≤t'
. . . . . | | | |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . . | | | |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . . | | | |     ∨ P@0 != <[a]
. . . . . | | | |              ,λx.P>(a@0) ==> ∀v:<[locl(a)]
. . . . . | | | |                                  ,λx.
. . . . . | | | |                                   T>(locl(a@0))?Top.
. . . . . | | | |       ¬P@0((λx.s(i;t').x),v)
. . . . . | | | 12. ∀t:ℕ.
. . . . . | | | |   ¬isnull(a(i;t))
. . . . . | | | |   ⇒
. . . . . | | | |   (islocal(kind(a(i;t)))
. . . . . | | | |    ⇒
. . . . . | | | |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . . | | | |    ⇒
. . . . . | | | |    P((λx.s(i;t).x),val(a(i;t))))
. . . . . | | | |   & (∀x:Id.
. . . . . | | | |      deq-member(product-deq(Knd;Id;...;...);<...
. . . . . | | | |                                              ,x>;1of(
. . . . . | | | |                                                  ))
. . . . . | | | |      ⇒
. . . . . | | | |      s(i;t+1).x
. . . . . | | | |      =
. . . . . | | | |      2of()
. . . . . | | | |      (<kind(a(i;t)),x>
. . . . . | | | |      ,λx.s(i;t).x
. . . . . | | | |      ,val(a(i;t))))
. . . . . | | | |   & (∀l:IdLnk.
. . . . . | | | |      deq-member(...;<kind(a(i;t)),l>;1of())
```

```
. . . . . | | | |      ⇒
. . . . . | | | |      withlnk(l;m(i;t))
. . . . . | | | |      =
. . . . . | | | |      if source(l) = i→
. . . . . | | | |         concat(map(λtgf.map(λx.
. . . . . | | | |         <1of(tgf),x>;2of(tgf)
. . . . . | | | |                      ((λx.s(i;t).x)
. . . . . | | | |                      ,val(a(i;t))));2of()
. . . . . | | | |                                   (<kind(a(i;t))
. . . . . | | | |                                    ,l>)))
. . . . . | | | |      else nil fi)
. . . . . | | | |   & (∀x:Id.
. . . . . | | | |      ¬(deq-member(IdDeq;x;1of())
. . . . . | | | |        ⇒
. . . . . | | | |        deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . . . . | | | |      ⇒
. . . . . | | | |      s(i;t).x = s(i;t+1).x)
. . . . . | | | |   & (∀l:IdLnk, tg:Id.
. . . . . | | | |      ¬(deq-member(...;<l,tg>;1of())
. . . . . | | | |        ⇒
. . . . . | | | |        deq-member(KindDeq;kind(a(i;t));2of()
. . . . . | | | |                                      (<l,tg>)))
. . . . . | | | |      ⇒
. . . . . | | | |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . | | | 13. ∀x:Id.
. . . . . | | | |   deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . . . . | | | 14. ∀a@0:Action(i).
. . . . . | | | |   ¬isnull(a@0)
. . . . . | | | |   ⇒
. . . . . | | | |   (valtype(i;a@0) ⊆r <[locl(a)]
. . . . . | | | |                      ,λx.T>(kind(a@0))?Top)
. . . . . | | | 15. ∀x:Id.
. . . . . | | | |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . . . . | | | |                      2of(ds)(x)
. . . . . | | | |                   else Top fi
. . . . . | | | 16. IdDeq ∈ EqDecider(Id)
. . . . . | | | 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . . | | | 18. j : Id
. . . . . | | | 19. t : ℕ
. . . . . | | | 20. j = i
. . . . . | | | 21. ¬isnull(a(j;t))
. . . . . | | | 22. ¬isnull(a(i;t))
. . . . . | | | 23. (λx.s(i;t).x) ∈ State(ds)
. . . . . | | | 24. t' : ℕ
. . . . . | | | 25. t+1≤t'
. . . . . | | | 26. ¬isnull(a(i;t'))
. . . . . | | | 27. kind(a(i;t')) = locl(a)
. . . . . | | | ⊢  (<j,t> <loc <i,t'>) ∨ <j,t> = <i,t'>
. . . . . | | | | by Repeat
. . . . . | | | |    (Unfolds
. . . . . | | | |     [‘es-Loc‘
. . . . . | | | |     ;‘es-causl‘
. . . . . | | | |     ;‘es-locl‘
. . . . . | | | |     ;‘es-loc‘
. . . . . | | | |     ;‘w-E‘
```

```
. . . . . | | | |     ;‘w-locl‘]
. . . . . | | | |     0
. . . . . | | | |     THEN
. . . . . | | | |     Reduce 0)
. . . . . | | | |    THEN
. . . . . | | | |    Decide (t<t’)
. . . . . | | | |    THEN
. . . . . | | | |    OrLeft
. . . . . | | | |    THEN
. . . . . | | | |    Try (Analyze THEN Reduce 0)
. . . . . | | | |
. . . . . | | | 1. i : Id
. . . . . | | | 2. a : Id
. . . . . | | | 3. T : Type
. . . . . | | | 4. ds : x:Id fp-> Type
. . . . . | | | 5. P : State(ds)→T→Prop
. . . . . | | | 6. w : World
. . . . . | | | 7. FairFifo
. . . . . | | | 8. FairFifo
. . . . . | | | 9. ∀l:IdLnk, tg:Id.
. . . . . | | | |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | | | |                  <ds
. . . . . | | | |                  ,<[locl(a)],λx.T>
. . . . . | | | |                  ,
. . . . . | | | |                  ,<[a],λx.P>
. . . . . | | | |                  ,
. . . . . | | | |                  ,
. . . . . | | | |                  ,
. . . . . | | | |                  ,
. . . . . | | | |                  ,•>
. . . . . | | | |               else  fi.da(rcv(l; tg))
. . . . . | | | 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . . | | | 11. ∀a@0:Id, t:ℕ.
. . . . . | | | |   ∃t’:ℕ.
. . . . . | | | |   t≤t’
. . . . . | | | |   & ¬isnull(a(i;t’)) & kind(a(i;t’)) = locl(a@0)
. . . . . | | | |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . . | | | |     ∨ P@0 != <[a]
. . . . . | | | |              ,λx.P>(a@0) ==> ∀v:<[locl(a)]
. . . . . | | | |                                ,λx.
. . . . . | | | |                                 T>(locl(a@0))?Top.
. . . . . | | | |       ¬P@0((λx.s(i;t’).x),v)
. . . . . | | | 12. ∀t:ℕ.
. . . . . | | | |   ¬isnull(a(i;t))
. . . . . | | | |   ⇒
. . . . . | | | |   (islocal(kind(a(i;t)))
. . . . . | | | |    ⇒
. . . . . | | | |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . . | | | |    ⇒
. . . . . | | | |    P((λx.s(i;t).x),val(a(i;t))))
. . . . . | | | |   & (∀x:Id.
. . . . . | | | |      deq-member(product-deq(Knd;Id;...;...);<...
. . . . . | | | |                                          ,x>;1of(
. . . . . | | | |                                              ))
. . . . . | | | |      ⇒
```

```
. . . . . | | | |      s(i;t+1).x
. . . . . | | | |      =

. . . . . | | | |      2of()
. . . . . | | | |      (<kind(a(i;t)),x>
. . . . . | | | |      ,λx.s(i;t).x
. . . . . | | | |      ,val(a(i;t))))
. . . . . | | | |   & (∀l:IdLnk.
. . . . . | | | |      deq-member(...;<kind(a(i;t)),l>;1of())
. . . . . | | | |      ⇒
. . . . . | | | |      withlnk(l;m(i;t))
. . . . . | | | |      =
. . . . . | | | |      if source(l) = i→
. . . . . | | | |         concat(map(λtgf.map(λx.
. . . . . | | | |         <1of(tgf),x>;2of(tgf)
. . . . . | | | |                     ((λx.s(i;t).x)
. . . . . | | | |                     ,val(a(i;t))));2of()
. . . . . | | | |                                   (<kind(a(i;t))
. . . . . | | | |                                    ,l>)))
. . . . . | | | |      else nil fi)
. . . . . | | | |   & (∀x:Id.
. . . . . | | | |      ¬(deq-member(IdDeq;x;1of())
. . . . . | | | |        ⇒
. . . . . | | | |        deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . . . . | | | |      ⇒
. . . . . | | | |      s(i;t).x = s(i;t+1).x)
. . . . . | | | |   & (∀l:IdLnk, tg:Id.
. . . . . | | | |      ¬(deq-member(...;<l,tg>;1of())
. . . . . | | | |        ⇒
. . . . . | | | |        deq-member(KindDeq;kind(a(i;t));2of()
. . . . . | | | |                                      (<l,tg>)))
. . . . . | | | |      ⇒
. . . . . | | | |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . | | 13. ∀x:Id.
. . . . . | | |   deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . . . . | | 14. ∀a@0:Action(i).
. . . . . | | |   ¬isnull(a@0)
. . . . . | | |   ⇒
. . . . . | | |   (valtype(i;a@0) ⊆r <[locl(a)]
. . . . . | | |                     ,λx.T>(kind(a@0))?Top)
. . . . . | | 15. ∀x:Id.
. . . . . | | |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . . . . | | |                      2of(ds)(x)
. . . . . | | |                   else Top fi
. . . . . | | 16. IdDeq ∈ EqDecider(Id)
. . . . . | | 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . . | | 18. j : Id
. . . . . | | 19. t : ℕ
. . . . . | | 20. j = i
. . . . . | | 21. ¬isnull(a(j;t))
. . . . . | | 22. ¬isnull(a(i;t))
. . . . . | | 23. (λx.s(i;t).x) ∈ State(ds)
. . . . . | | 24. t' : ℕ
. . . . . | | 25. t+1≤t'
. . . . . | | 26. ¬isnull(a(i;t'))
. . . . . | | 27. kind(a(i;t')) = locl(a)
```

```
. . . . . | | | 28. t<t'
. . . . . | | | ⊢  <j,t> <c <i,t'>
. . . . . | | | | by ((Unfold `w-causl` 0 THEN Unfold `rel_plus` 0
. . . . . | | | |      THEN
. . . . . | | | |      Reduce 0
. . . . . | | | |      THEN
. . . . . | | | |      InstConcl [1])
. . . . . | | | |     THEN
. . . . . | | | |     (Repeat (RecUnfold `rel_exp` 0 THEN Reduce 0))
. . . . . | | | |     THEN
. . . . . | | | |     (InstConcl [<i,t'>]))
. . . . . | | | |    THEN
. . . . . | | | |    Try (Unfold `w-E` 0 THEN Analyze THEN Reduce 0)
. . . . . | | | |
. . . . . | | | 1. i : Id
. . . . . | | | 2. a : Id
. . . . . | | | 3. T : Type
. . . . . | | | 4. ds : x:Id fp-> Type
. . . . . | | | 5. P : State(ds)→T→Prop
. . . . . | | | 6. w : World
. . . . . | | | 7. FairFifo
. . . . . | | | 8. FairFifo
. . . . . | | | 9. ∀l:IdLnk, tg:Id.
. . . . . | | | |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | | | |                   <ds
. . . . . | | | |                   ,<[locl(a)],λx.T>
. . . . . | | | |                   ,
. . . . . | | | |                   ,<[a],λx.P>
. . . . . | | | |                   ,
. . . . . | | | |                   ,
. . . . . | | | |                   ,
. . . . . | | | |                   ,
. . . . . | | | |                   ,·>
. . . . . | | | |                else  fi.da(rcv(l; tg))
. . . . . | | | 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . . | | | 11. ∀a@0:Id, t:ℕ.
. . . . . | | | |   ∃t':ℕ.
. . . . . | | | |   t≤t'
. . . . . | | | |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . . | | | |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . . | | | |     ∨ P@0 != <[a]
. . . . . | | | |              ,λx.P>(a@0) ==> ∀v:<[locl(a)]
. . . . . | | | |                                ,λx.
. . . . . | | | |                                 T>(locl(a@0))?Top.
. . . . . | | | |       ¬P@0((λx.s(i;t').x),v)
. . . . . | | | 12. ∀t:ℕ.
. . . . . | | | |   ¬isnull(a(i;t))

. . . . . | | | |   ⇒
. . . . . | | | |   (islocal(kind(a(i;t)))
. . . . . | | | |    ⇒
. . . . . | | | |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . . | | | |    ⇒
. . . . . | | | |    P((λx.s(i;t).x),val(a(i;t))))
. . . . . | | | |   & (∀x:Id.
. . . . . | | | |      deq-member(product-deq(Knd;Id;...;...);<...
```

```
. . . . . | | | |                                                ,x>;1of(
. . . . . | | | |                                                   ))
. . . . . | | | |      ⇒
. . . . . | | | |      s(i;t+1).x
. . . . . | | | |      =
. . . . . | | | |      2of()
. . . . . | | | |      (<kind(a(i;t)),x>
. . . . . | | | |      ,λx.s(i;t).x
. . . . . | | | |      ,val(a(i;t))))
. . . . . | | | |   & (∀l:IdLnk.
. . . . . | | | |      deq-member(...;<kind(a(i;t)),l>;1of())
. . . . . | | | |      ⇒
. . . . . | | | |      withlnk(l;m(i;t))
. . . . . | | | |      =
. . . . . | | | |      if source(l) = i→
. . . . . | | | |         concat(map(λtgf.map(λx.
. . . . . | | | |         <1of(tgf),x>;2of(tgf)
. . . . . | | | |                     ((λx.s(i;t).x)
. . . . . | | | |                     ,val(a(i;t))));2of()
. . . . . | | | |                                   (<kind(a(i;t))
. . . . . | | | |                                    ,l>)))
. . . . . | | | |      else nil fi)
. . . . . | | | |   & (∀x:Id.
. . . . . | | | |      ¬(deq-member(IdDeq;x;1of())
. . . . . | | | |        ⇒
. . . . . | | | |        deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . . . . | | | |      ⇒
. . . . . | | | |      s(i;t).x = s(i;t+1).x)
. . . . . | | | |   & (∀l:IdLnk, tg:Id.
. . . . . | | | |      ¬(deq-member(...;<l,tg>;1of())
. . . . . | | | |        ⇒
. . . . . | | | |        deq-member(KindDeq;kind(a(i;t));2of()
. . . . . | | | |                                      (<l,tg>)))
. . . . . | | | |      ⇒
. . . . . | | | |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . | | | 13. ∀x:Id.
. . . . . | | | |   deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . . . . | | | 14. ∀a@0:Action(i).
. . . . . | | | |   ¬isnull(a@0)
. . . . . | | | |   ⇒
. . . . . | | | |   (valtype(i;a@0) ⊆r <[locl(a)]
. . . . . | | | |                     ,λx.T>(kind(a@0))?Top)
. . . . . | | | 15. ∀x:Id.
. . . . . | | | |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . . . . | | | |                     2of(ds)(x)
. . . . . | | | |                   else Top fi
. . . . . | | | 16. IdDeq ∈ EqDecider(Id)
. . . . . | | | 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . . | | | 18. j : Id
. . . . . | | | 19. t : ℕ
. . . . . | | | 20. j = i
. . . . . | | | 21. ¬isnull(a(j;t))
. . . . . | | | 22. ¬isnull(a(i;t))
. . . . . | | | 23. (λx.s(i;t).x) ∈ State(ds)
. . . . . | | | 24. t' : ℕ
```

```
. . . . . | | | 25. t+1≤t'
. . . . . | | | 26. ¬isnull(a(i;t'))
. . . . . | | | 27. kind(a(i;t')) = locl(a)
. . . . . | | | 28. t<t'
. . . . . | | | ⊢  <j,t> <loc <i,t'>
. . . . . | | | |  ∨ isrcv(kind(<i,t'>)) & <j,t> = sender(<i,t'>)
. . . . . | | | | by OrLeft
. . . . . | | | |
. . . . . | | | |\
. . . . . | | | | 1. i : Id
. . . . . | | | | 2. a : Id
. . . . . | | | | 3. T : Type
. . . . . | | | | 4. ds : x:Id fp-> Type
. . . . . | | | | 5. P : State(ds)→T→Prop
. . . . . | | | | 6. w : World
. . . . . | | | | 7. FairFifo
. . . . . | | | | 8. FairFifo
. . . . . | | | | 9. ∀l:IdLnk, tg:Id.
. . . . . | | | |    (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | | | |                       <ds
. . . . . | | | |                       ,<[locl(a)],λx.T>
. . . . . | | | |                       ,
. . . . . | | | |                       ,<[a],λx.P>
. . . . . | | | |                       ,
. . . . . | | | |                       ,
. . . . . | | | |                       ,
. . . . . | | | |                       ,
. . . . . | | | |                       ,·>
. . . . . | | | |                    else  fi.da(rcv(l; tg))
. . . . . | | | | 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . . | | | | 11. ∀a@0:Id, t:ℕ.
. . . . . | | | |     ∃t':ℕ.
. . . . . | | | |     t≤t'
. . . . . | | | |     & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . . | | | |       ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . . | | | |       ∨ P@0 != <[a]
. . . . . | | | |                ,λx.
. . . . . | | | |                 P>(a@0) ==> ∀v:<[locl(a)]
. . . . . | | | |                                ,λx.
. . . . . | | | |                                 T>(locl(a@0))?Top.
. . . . . | | | |         ¬P@0((λx.s(i;t').x),v)
. . . . . | | | | 12. ∀t:ℕ.
. . . . . | | | |     ¬isnull(a(i;t))
. . . . . | | | |     ⇒
. . . . . | | | |     (islocal(kind(a(i;t)))
. . . . . | | | |      ⇒
. . . . . | | | |      (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . . | | | |      ⇒
. . . . . | | | |      P((λx.s(i;t).x),val(a(i;t))))
. . . . . | | | |     & (∀x:Id.
. . . . . | | | |        deq-member(...;<kind(a(i;t)),x>;1of())
. . . . . | | | |        ⇒
. . . . . | | | |        s(i;t+1).x
. . . . . | | | |        =
. . . . . | | | |        2of()
```

```
. . . . . | | | |        (<kind(a(i;t)),x>
. . . . . | | | |        ,λx.s(i;t).x
. . . . . | | | |        ,val(a(i;t))))
. . . . . | | | |     & (∀l:IdLnk.
. . . . . | | | |        deq-member(...;<kind(a(i;t)),l>;1of())
. . . . . | | | |        ⇒
. . . . . | | | |        withlnk(l;m(i;t))
. . . . . | | | |        =
. . . . . | | | |        if source(l) = i→
. . . . . | | | |           concat(map(λtgf.map(λx.
. . . . . | | | |           <1of(tgf),x>;2of(tgf)
. . . . . | | | |                       ((λx.s(i;t).x)
. . . . . | | | |                       ,val(a(i;t))));2of()
. . . . . | | | |                                     (<kind(a(i;t))
. . . . . | | | |                                      ,l>)))
. . . . . | | | |        else nil fi)
. . . . . | | | |     & (∀x:Id.
. . . . . | | | |        ¬(deq-member(IdDeq;x;1of())
. . . . . | | | |          ⇒
. . . . . | | | |          deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . . . . | | | |        ⇒
. . . . . | | | |        s(i;t).x = s(i;t+1).x)
. . . . . | | | |     & (∀l:IdLnk, tg:Id.
. . . . . | | | |        ¬(deq-member(...;<l,tg>;1of())
. . . . . | | | |          ⇒
. . . . . | | | |          deq-member(KindDeq;kind(a(i;t));2of()
. . . . . | | | |                                          (<l,tg>)))
. . . . . | | | |        ⇒
. . . . . | | | |        w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . | | | | 13. ∀x:Id.
. . . . . | | | |     deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . . . . | | | | 14. ∀a@0:Action(i).
. . . . . | | | |     ¬isnull(a@0)
. . . . . | | | |     ⇒
. . . . . | | | |     (valtype(i;a@0) ⊆r <[locl(a)]
. . . . . | | | |                        ,λx.T>(kind(a@0))?Top)
. . . . . | | | | 15. ∀x:Id.
. . . . . | | | |     vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . . . . | | | |                        2of(ds)(x)
. . . . . | | | |                     else Top fi
. . . . . | | | | 16. IdDeq ∈ EqDecider(Id)
. . . . . | | | | 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . . | | | | 18. j : Id
. . . . . | | | | 19. t : ℕ
. . . . . | | | | 20. j = i
. . . . . | | | | 21. ¬isnull(a(j;t))
. . . . . | | | | 22. ¬isnull(a(i;t))
. . . . . | | | | 23. (λx.s(i;t).x) ∈ State(ds)
. . . . . | | | | 24. t' : ℕ
. . . . . | | | | 25. t+1≤t'
. . . . . | | | | 26. ¬isnull(a(i;t'))
. . . . . | | | | 27. kind(a(i;t')) = locl(a)
. . . . . | | | | 28. t<t'
. . . . . | | | | ⊢  <j,t> <loc <i,t'>
. . . . . | | | |   by Unfold `w-locl` 0 THEN Reduce 0
```

```
. . . . . | | | |
. . . . . | | | .\
. . . . . | | | . .....wf .....
. . . . . | | | . 1. i : Id
. . . . . | | | . 2. a : Id
. . . . . | | | . 3. T : Type
. . . . . | | | . 4. ds : x:Id fp-> Type
. . . . . | | | . 5. P : State(ds)→T→Prop
. . . . . | | | . 6. w : World
. . . . . | | | . 7. FairFifo
. . . . . | | | . 8. FairFifo
. . . . . | | | . 9. ∀l:IdLnk, tg:Id.
. . . . . | | | .    (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | | | .                      <ds
. . . . . | | | .                      ,<[locl(a)],λx.T>
. . . . . | | | .                      ,
. . . . . | | | .                      ,<[a],λx.P>
. . . . . | | | .                      ,
. . . . . | | | .                      ,
. . . . . | | | .                      ,
. . . . . | | | .                      ,
. . . . . | | | .                      ,·>
. . . . . | | | .                   else  fi.da(rcv(l; tg))
. . . . . | | | . 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . . | | | . 11. ∀a@0:Id, t:ℕ.
. . . . . | | | .     ∃t':ℕ.
. . . . . | | | .     t≤t'
. . . . . | | | .     & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . . | | | .       ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . . | | | .       ∨ P@0 != <[a]
. . . . . | | | .                ,λx.
. . . . . | | | .                 P>(a@0) ==> ∀v:<[locl(a)]
. . . . . | | | .                                ,λx.
. . . . . | | | .                                 T>(locl(a@0))?Top.
. . . . . | | | .         ¬P@0((λx.s(i;t').x),v)
. . . . . | | | . 12. ∀t:ℕ.
. . . . . | | | .     ¬isnull(a(i;t))
. . . . . | | | .     ⇒
. . . . . | | | .     (islocal(kind(a(i;t)))
. . . . . | | | .      ⇒
. . . . . | | | .      (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . . | | | .      ⇒
. . . . . | | | .      P((λx.s(i;t).x),val(a(i;t))))
. . . . . | | | .     & (∀x:Id.
. . . . . | | | .        deq-member(...;<kind(a(i;t)),x>;1of())
. . . . . | | | .        ⇒
. . . . . | | | .        s(i;t+1).x
. . . . . | | | .        =
. . . . . | | | .        2of()
. . . . . | | | .        (<kind(a(i;t)),x>
. . . . . | | | .        ,λx.s(i;t).x
. . . . . | | | .        ,val(a(i;t))))
. . . . . | | | .     & (∀l:IdLnk.
. . . . . | | | .        deq-member(...;<kind(a(i;t)),l>;1of())
. . . . . | | | .        ⇒
```

```
. . . . . | | | .        withlnk(l;m(i;t))
. . . . . | | | .        =
. . . . . | | | .        if source(l) = i→
. . . . . | | | .           concat(map(λtgf.map(λx.
. . . . . | | | .           <1of(tgf),x>;2of(tgf)
. . . . . | | | .                        ((λx.s(i;t).x)
. . . . . | | | .                        ,val(a(i;t))));2of()
. . . . . | | | .                                      (<kind(a(i;t))
. . . . . | | | .                                       ,l>)))
. . . . . | | | .        else nil fi)
. . . . . | | | .     & (∀x:Id.
. . . . . | | | .        ¬(deq-member(IdDeq;x;1of())
. . . . . | | | .          ⇒
. . . . . | | | .          deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . . . . | | | .        ⇒
. . . . . | | | .        s(i;t).x = s(i;t+1).x)
. . . . . | | | .     & (∀l:IdLnk, tg:Id.
. . . . . | | | .        ¬(deq-member(...;<l,tg>;1of())
. . . . . | | | .          ⇒
. . . . . | | | .          deq-member(KindDeq;kind(a(i;t));2of()
. . . . . | | | .                                          (<l,tg>)))
. . . . . | | | .        ⇒
. . . . . | | | .        w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . | | | . 13. ∀x:Id.
. . . . . | | | .     deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . . . . | | | . 14. ∀a@0:Action(i).
. . . . . | | | .     ¬isnull(a@0)
. . . . . | | | .     ⇒
. . . . . | | | .     (valtype(i;a@0) ⊆r <[locl(a)]
. . . . . | | | .                        ,λx.T>(kind(a@0))?Top)
. . . . . | | | . 15. ∀x:Id.
. . . . . | | | .     vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . . . . | | | .                        2of(ds)(x)
. . . . . | | | .                     else Top fi
. . . . . | | | . 16. IdDeq ∈ EqDecider(Id)
. . . . . | | | . 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . . | | | . 18. j : Id
. . . . . | | | . 19. t : ℕ
. . . . . | | | . 20. j = i
. . . . . | | | . 21. ¬isnull(a(j;t))
. . . . . | | | . 22. ¬isnull(a(i;t))
. . . . . | | | . 23. (λx.s(i;t).x) ∈ State(ds)
. . . . . | | | . 24. t' : ℕ
. . . . . | | | . 25. t+1≤t'
. . . . . | | | . 26. ¬isnull(a(i;t'))
. . . . . | | | . 27. kind(a(i;t')) = locl(a)
. . . . . | | | . 28. t<t'
. . . . . | | | . ⊢  (isrcv(kind(<i,t'>)) & <j,t> = sender(<i,t'>))
. . . . . | | | .    ∈ Prop
. . . . . | | | .   by Auto
. . . . . | | | .      THEN
. . . . . | | | .      Try
. . . . . | | | .      (Unfold `w-E` 0 THEN Analyze THEN Reduce 0)
. . . . . | | |
. . . . . | | .\
```

```
. . . . . | | . 1. i : Id
. . . . . | | . 2. a : Id
. . . . . | | . 3. T : Type
. . . . . | | . 4. ds : x:Id fp-> Type
. . . . . | | . 5. P : State(ds)→T→Prop
. . . . . | | . 6. w : World
. . . . . | | . 7. p : FairFifo
. . . . . | | . 8. FairFifo
. . . . . | | . 9. ∀l:IdLnk, tg:Id.
. . . . . | | . |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | | . |                   <ds
. . . . . | | . |                   ,<[locl(a)],λx.T>
. . . . . | | . |                   ,
. . . . . | | . |                   ,<[a],λx.P>
. . . . . | | . |                   ,
. . . . . | | . |                   ,
. . . . . | | . |                   ,

. . . . . | | . |                   ,
. . . . . | | . |                   ,·>
. . . . . | | . |                else  fi.da(rcv(l; tg))
. . . . . | | . 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . . | | . 11. ∀a@0:Id, t:ℕ.
. . . . . | | . |   ∃t':ℕ.
. . . . . | | . |   t≤t'
. . . . . | | . |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . . | | . |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . . | | . |     ∨ P@0 != <[a]
. . . . . | | . |              ,λx.P>(a@0) ==> ∀v:<[locl(a)]
. . . . . | | . |                                  ,λx.
. . . . . | | . |                                   T>(locl(a@0))?Top.
. . . . . | | . |       ¬P@0((λx.s(i;t').x),v)
. . . . . | | . 12. ∀t:ℕ.
. . . . . | | . |   ¬isnull(a(i;t))
. . . . . | | . |   ⇒
. . . . . | | . |   (islocal(kind(a(i;t)))
. . . . . | | . |    ⇒
. . . . . | | . |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . . | | . |    ⇒
. . . . . | | . |    P((λx.s(i;t).x),val(a(i;t))))
. . . . . | | . |   & (∀x:Id.
. . . . . | | . |      deq-member(product-deq(Knd;Id;...;...);<...
. . . . . | | . |                                              ,x>;1of(
. . . . . | | . |                                                  ))
. . . . . | | . |      ⇒
. . . . . | | . |      s(i;t+1).x
. . . . . | | . |      =
. . . . . | | . |      2of()
. . . . . | | . |      (<kind(a(i;t)),x>
. . . . . | | . |      ,λx.s(i;t).x
. . . . . | | . |      ,val(a(i;t))))
. . . . . | | . |   & (∀l:IdLnk.
. . . . . | | . |      deq-member(...;<kind(a(i;t)),l>;1of())
. . . . . | | . |      ⇒
. . . . . | | . |      withlnk(l;m(i;t))
. . . . . | | . |      =
```

```
. . . . . | | . |      if source(l) = i→
. . . . . | | . |         concat(map(λtgf.map(λx.
. . . . . | | . |         <1of(tgf),x>;2of(tgf)
. . . . . | | . |                      ((λx.s(i;t).x)
. . . . . | | . |                      ,val(a(i;t))));2of()
. . . . . | | . |                                    (<kind(a(i;t))
. . . . . | | . |                                     ,l>)))
. . . . . | | . |      else nil fi)
. . . . . | | . |   & (∀x:Id.
. . . . . | | . |      ¬(deq-member(IdDeq;x;1of())
. . . . . | | . |        ⇒
. . . . . | | . |        deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . . . . | | . |      ⇒
. . . . . | | . |      s(i;t).x = s(i;t+1).x)
. . . . . | | . |   & (∀l:IdLnk, tg:Id.
. . . . . | | . |      ¬(deq-member(...;<l,tg>;1of())
. . . . . | | . |        ⇒
. . . . . | | . |        deq-member(KindDeq;kind(a(i;t));2of()
. . . . . | | . |                                       (<l,tg>)))
. . . . . | | . |      ⇒
. . . . . | | . |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . | | . 13. ∀x:Id.
. . . . . | | . |   deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . . . . | | . 14. ∀a@0:Action(i).
. . . . . | | . |   ¬isnull(a@0)
. . . . . | | . |   ⇒
. . . . . | | . |   (valtype(i;a@0) ⊆r <[locl(a)]
. . . . . | | . |                      ,λx.T>(kind(a@0))?Top)
. . . . . | | . 15. ∀x:Id.
. . . . . | | . |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . . . . | | . |                      2of(ds)(x)
. . . . . | | . |                   else Top fi
. . . . . | | . 16. IdDeq ∈ EqDecider(Id)
. . . . . | | . 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . . | | . 18. j : Id
. . . . . | | . 19. t : ℕ
. . . . . | | . 20. j = i
. . . . . | | . 21. ¬isnull(a(j;t))
. . . . . | | . 22. ¬isnull(a(i;t))
. . . . . | | . 23. (λx.s(i;t).x) ∈ State(ds)
. . . . . | | . 24. t' : ℕ
. . . . . | | . 25. t+1≤t'
. . . . . | | . 26. ¬isnull(a(i;t'))
. . . . . | | . 27. kind(a(i;t')) = locl(a)
. . . . . | | . 28. (<j,t> <loc <i,t'>) ∨ <j,t> = <i,t'>
. . . . . | | . ⊢  kind(<i,t'>) = locl(a)
. . . . . | | . |  ∨ (∀v:T. ¬P((λz.(z after <i,t'>)),v))  by OrLeft
. . . . . | | . |
. . . . . | | . |\
. . . . . | | . | 1. i : Id
. . . . . | | . | 2. a : Id
. . . . . | | . | 3. T : Type
. . . . . | | . | 4. ds : x:Id fp-> Type
. . . . . | | . | 5. P : State(ds)→T→Prop
. . . . . | | . | 6. w : World
```

```
. . . . . | | . | 7. p : FairFifo
. . . . . | | . | 8. FairFifo
. . . . . | | . | 9. ∀l:IdLnk, tg:Id.
. . . . . | | . |    (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | | . |                      <ds
. . . . . | | . |                      ,<[locl(a)],λx.T>
. . . . . | | . |                      ,
. . . . . | | . |                      ,<[a],λx.P>
. . . . . | | . |                      ,
. . . . . | | . |                      ,
. . . . . | | . |                      ,
. . . . . | | . |                      ,
. . . . . | | . |                      ,·>
. . . . . | | . |                    else  fi.da(rcv(l; tg))
. . . . . | | . | 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . . | | . | 11. ∀a@0:Id, t:ℕ.
. . . . . | | . |     ∃t':ℕ.
. . . . . | | . |     t≤t'
. . . . . | | . |     & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . . | | . |       ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . . | | . |       ∨ P@0 != <[a]
. . . . . | | . |                ,λx.
. . . . . | | . |                 P>(a@0) ==> ∀v:<[locl(a)]
. . . . . | | . |                                ,λx.
. . . . . | | . |                                 T>(locl(a@0))?Top.
. . . . . | | . |         ¬P@0((λx.s(i;t').x),v)
. . . . . | | . | 12. ∀t:ℕ.
. . . . . | | . |     ¬isnull(a(i;t))
. . . . . | | . |     ⇒
. . . . . | | . |     (islocal(kind(a(i;t)))
. . . . . | | . |      ⇒
. . . . . | | . |      (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . . | | . |      ⇒
. . . . . | | . |      P((λx.s(i;t).x),val(a(i;t))))
. . . . . | | . |     & (∀x:Id.
. . . . . | | . |        deq-member(...;<kind(a(i;t)),x>;1of())
. . . . . | | . |        ⇒
. . . . . | | . |        s(i;t+1).x
. . . . . | | . |        =
. . . . . | | . |        2of()
. . . . . | | . |        (<kind(a(i;t)),x>
. . . . . | | . |        ,λx.s(i;t).x
. . . . . | | . |        ,val(a(i;t))))
. . . . . | | . |     & (∀l:IdLnk.
. . . . . | | . |        deq-member(...;<kind(a(i;t)),l>;1of())
. . . . . | | . |        ⇒
. . . . . | | . |        withlnk(l;m(i;t))
. . . . . | | . |        =
. . . . . | | . |        if source(l) = i→
. . . . . | | . |           concat(map(λtgf.map(λx.
. . . . . | | . |           <1of(tgf),x>;2of(tgf)
. . . . . | | . |                        ((λx.s(i;t).x)
. . . . . | | . |                        ,val(a(i;t))));2of()
. . . . . | | . |                                      (<kind(a(i;t))
. . . . . | | . |                                       ,l>)))
```

```
. . . . . | | . |       else nil fi)
. . . . . | | . |    & (∀x:Id.
. . . . . | | . |       ¬(deq-member(IdDeq;x;1of())
. . . . . | | . |         ⇒
. . . . . | | . |         deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . . . . | | . |       ⇒
. . . . . | | . |       s(i;t).x = s(i;t+1).x)
. . . . . | | . |    & (∀l:IdLnk, tg:Id.
. . . . . | | . |       ¬(deq-member(...;<l,tg>;1of())
. . . . . | | . |         ⇒
. . . . . | | . |         deq-member(KindDeq;kind(a(i;t));2of()
. . . . . | | . |                                        (<l,tg>)))
. . . . . | | . |       ⇒
. . . . . | | . |       w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . | | . | 13. ∀x:Id.
. . . . . | | . |     deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . . . . | | . | 14. ∀a@0:Action(i).
. . . . . | | . |     ¬isnull(a@0)
. . . . . | | . |     ⇒
. . . . . | | . |     (valtype(i;a@0) ⊆r <[locl(a)]
. . . . . | | . |                         ,λx.T>(kind(a@0))?Top)
. . . . . | | . | 15. ∀x:Id.
. . . . . | | . |     vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . . . . | | . |                         2of(ds)(x)
. . . . . | | . |                      else Top fi
. . . . . | | . | 16. IdDeq ∈ EqDecider(Id)
. . . . . | | . | 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . . | | . | 18. j : Id
. . . . . | | . | 19. t : ℕ
. . . . . | | . | 20. j = i
. . . . . | | . | 21. ¬isnull(a(j;t))
. . . . . | | . | 22. ¬isnull(a(i;t))
. . . . . | | . | 23. (λx.s(i;t).x) ∈ State(ds)
. . . . . | | . | 24. t' : ℕ
. . . . . | | . | 25. t+1≤t'
. . . . . | | . | 26. ¬isnull(a(i;t'))
. . . . . | | . | 27. kind(a(i;t')) = locl(a)
. . . . . | | . | 28. (<j,t> <loc <i,t'>) ∨ <j,t> = <i,t'>
. . . . . | | . | ⊢  kind(<i,t'>) = locl(a)
. . . . . | | . |   by Unfold `w-ekind` 0 THEN Unfold `w-act` 0
. . . . . | | . |      THEN
. . . . . | | . |      Reduce 0
. . . . . | | . |
. . . . . | | .\
. . . . . | | . . .....subterm .....
. . . . . | | . . 1. i : Id
. . . . . | | . . 2. a : Id
. . . . . | | . . 3. T : Type
. . . . . | | . . 4. ds : x:Id fp-> Type
. . . . . | | . . 5. P : State(ds)→T→Prop
. . . . . | | . . 6. w : World
. . . . . | | . . 7. p : FairFifo

. . . . . | | . . 8. FairFifo
. . . . . | | . . 9. ∀l:IdLnk, tg:Id.
. . . . . | | . .    (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
```

```
. . . . . | | . .                      <ds
. . . . . | | . .                      ,<[locl(a)],λx.T>
. . . . . | | . .                      ,
. . . . . | | . .                      ,<[a],λx.P>
. . . . . | | . .                      ,
. . . . . | | . .                      ,
. . . . . | | . .                      ,
. . . . . | | . .                      ,
. . . . . | | . .                      ,·>
. . . . . | | . .                   else  fi.da(rcv(l; tg))
. . . . . | | . . 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . . | | . . 11. ∀a@0:Id, t:ℕ.
. . . . . | | . .     ∃t':ℕ.
. . . . . | | . .     t≤t'
. . . . . | | . .     & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . . | | . .       ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . . | | . .       ∨ P@0 != <[a]
. . . . . | | . .                ,λx.
. . . . . | | . .                 P>(a@0) ==> ∀v:<[locl(a)]
. . . . . | | . .                                ,λx.
. . . . . | | . .                                 T>(locl(a@0))?Top.
. . . . . | | . .          ¬P@0((λx.s(i;t').x),v)
. . . . . | | . . 12. ∀t:ℕ.
. . . . . | | . .     ¬isnull(a(i;t))
. . . . . | | . .     ⇒
. . . . . | | . .     (islocal(kind(a(i;t)))
. . . . . | | . .      ⇒
. . . . . | | . .      (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . . | | . .      ⇒
. . . . . | | . .      P((λx.s(i;t).x),val(a(i;t))))
. . . . . | | . .     & (∀x:Id.
. . . . . | | . .        deq-member(...;<kind(a(i;t)),x>;1of())
. . . . . | | . .        ⇒
. . . . . | | . .        s(i;t+1).x
. . . . . | | . .        =
. . . . . | | . .        2of()
. . . . . | | . .        (<kind(a(i;t)),x>
. . . . . | | . .        ,λx.s(i;t).x
. . . . . | | . .        ,val(a(i;t))))
. . . . . | | . .     & (∀l:IdLnk.
. . . . . | | . .        deq-member(...;<kind(a(i;t)),l>;1of())
. . . . . | | . .        ⇒
. . . . . | | . .        withlnk(l;m(i;t))
. . . . . | | . .        =
. . . . . | | . .        if source(l) = i→
. . . . . | | . .           concat(map(λtgf.map(λx.
. . . . . | | . .           <1of(tgf),x>;2of(tgf)
. . . . . | | . .                        ((λx.s(i;t).x)
. . . . . | | . .                        ,val(a(i;t))));2of()
. . . . . | | . .                                      (<kind(a(i;t))
. . . . . | | . .                                       ,l>)))
. . . . . | | . .        else nil fi)
. . . . . | | . .     & (∀x:Id.
. . . . . | | . .        ¬(deq-member(IdDeq;x;1of())
. . . . . | | . .          ⇒
```

```
. . . . . | | . .          deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . . . . | | . .        ⇒
. . . . . | | . .        s(i;t).x = s(i;t+1).x)
. . . . . | | . .     & (∀l:IdLnk, tg:Id.
. . . . . | | . .        ¬(deq-member(...;<l,tg>;1of())
. . . . . | | . .          ⇒
. . . . . | | . .          deq-member(KindDeq;kind(a(i;t));2of()
. . . . . | | . .                                          (<l,tg>)))
. . . . . | | . .        ⇒
. . . . . | | . .        w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . | | . . 13. ∀x:Id.
. . . . . | | . .     deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . . . . | | . . 14. ∀a@0:Action(i).
. . . . . | | . .     ¬isnull(a@0)
. . . . . | | . .     ⇒
. . . . . | | . .     (valtype(i;a@0) ⊆r <[locl(a)]
. . . . . | | . .                        ,λx.T>(kind(a@0))?Top)
. . . . . | | . . 15. ∀x:Id.
. . . . . | | . .     vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . . . . | | . .                        2of(ds)(x)
. . . . . | | . .                     else Top fi
. . . . . | | . . 16. IdDeq ∈ EqDecider(Id)
. . . . . | | . . 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . . | | . . 18. j : Id
. . . . . | | . . 19. t : ℕ
. . . . . | | . . 20. j = i
. . . . . | | . . 21. ¬isnull(a(j;t))
. . . . . | | . . 22. ¬isnull(a(i;t))
. . . . . | | . . 23. (λx.s(i;t).x) ∈ State(ds)
. . . . . | | . . 24. t' : ℕ
. . . . . | | . . 25. t+1≤t'
. . . . . | | . . 26. ¬isnull(a(i;t'))
. . . . . | | . . 27. kind(a(i;t')) = locl(a)
. . . . . | | . . 28. (<j,t> <loc <i,t'>) ∨ <j,t> = <i,t'>
. . . . . | | . . 29. T
. . . . . | | . . ⊢  (λz.(z after <i,t'>)) ∈ State(ds)
. . . . . | | . .   by Unfolds [`ma-state`;`w-after`] 0 THEN Reduce 0
. . . . . | | . .      THEN
. . . . . | | . .      DoSubsume
. . . . . | | . .      THEN
. . . . . | | . .      Try BackThruSomeHyp
. . . . . | | . .      THEN

. . . . . | | . .      Try D_ES_Subtype
. . . . . | |
. . . . . | .\
. . . . . | . .....wf .....
. . . . . | . 1. i : Id
. . . . . | . 2. a : Id
. . . . . | . 3. T : Type
. . . . . | . 4. ds : x:Id fp-> Type
. . . . . | . 5. P : State(ds)→T→Prop
. . . . . | . 6. w : World
. . . . . | . 7. p : FairFifo
. . . . . | . 8. FairFifo
. . . . . | . 9. ∀l:IdLnk, tg:Id.
```

```
. . . . . | . |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | . |                    <ds
. . . . . | . |                    ,<[locl(a)],λx.T>
. . . . . | . |                    ,
. . . . . | . |                    ,<[a],λx.P>
. . . . . | . |                    ,
. . . . . | . |                    ,
. . . . . | . |                    ,
. . . . . | . |                    ,
. . . . . | . |                    ,·>
. . . . . | . |                 else  fi.da(rcv(l; tg))
. . . . . | . 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . . | . 11. ∀a@0:Id, t:ℕ.
. . . . . | . |   ∃t':ℕ.
. . . . . | . |   t≤t'
. . . . . | . |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . . | . |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . . | . |     ∨ P@0 != <[a]
. . . . . | . |              ,λx.P>(a@0) ==> ∀v:<[locl(a)]
. . . . . | . |                                ,λx.T>(locl(a@0))?Top.
. . . . . | . |       ¬P@0((λx.s(i;t').x),v)
. . . . . | . 12. ∀t:ℕ.
. . . . . | . |   ¬isnull(a(i;t))
. . . . . | . |   ⇒
. . . . . | . |   (islocal(kind(a(i;t)))
. . . . . | . |    ⇒
. . . . . | . |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . . | . |    ⇒
. . . . . | . |    P((λx.s(i;t).x),val(a(i;t))))
. . . . . | . |   & (∀x:Id.
. . . . . | . |      deq-member(product-deq(Knd;Id;...;IdDeq);<...
. . . . . | . |                                                ,x>;1of(
. . . . . | . |                                                    ))
. . . . . | . |      ⇒
. . . . . | . |      s(i;t+1).x
. . . . . | . |      =
. . . . . | . |      2of()(<kind(a(i;t)),x>,λx.s(i;t).x,val(a(i;t))))
. . . . . | . |   & (∀l:IdLnk.
. . . . . | . |      deq-member(product-deq(Knd;...;...;...);<...
. . . . . | . |                                              ,l>;1of(
. . . . . | . |                                                  ))
. . . . . | . |      ⇒
. . . . . | . |      withlnk(l;m(i;t))
. . . . . | . |      =
. . . . . | . |      if source(l) = i→
. . . . . | . |         concat(map(λtgf.map(λx.
. . . . . | . |         <1of(tgf)
. . . . . | . |         ,x>;2of(tgf)
. . . . . | . |             ((λx.s(i;t).x)
. . . . . | . |             ,val(a(i;t))));2of()(<kind(a(i;t)),l>)))
. . . . . | . |      else nil fi)
. . . . . | . |   & (∀x:Id.
. . . . . | . |      ¬(deq-member(IdDeq;x;1of())
. . . . . | . |        ⇒
. . . . . | . |        deq-member(KindDeq;kind(a(i;t));2of()(x)))
```

```
. . . . . | . |      ⇒
. . . . . | . |      s(i;t).x = s(i;t+1).x)
. . . . . | . |   & (∀l:IdLnk, tg:Id.
. . . . . | . |      ¬(deq-member(product-deq(...;Id;...;...);...;1of(
. . . . . | . |                                                  ))
. . . . . | . |        ⇒
. . . . . | . |        deq-member(KindDeq;kind(a(i;t));2of()(<l,tg>)))
. . . . . | . |      ⇒
. . . . . | . |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . | . 13. ∀x:Id.
. . . . . | . |   deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . . . . | . 14. ∀a@0:Action(i).
. . . . . | . |   ¬isnull(a@0)
. . . . . | . |   ⇒
. . . . . | . |   (valtype(i;a@0) ⊆r <[locl(a)],λx.T>(kind(a@0))?Top)
. . . . . | . 15. ∀x:Id.
. . . . . | . |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . . . . | . |                     2of(ds)(x)
. . . . . | . |                  else Top fi
. . . . . | . 16. IdDeq ∈ EqDecider(Id)
. . . . . | . 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . . | . 18. j : Id
. . . . . | . 19. t : ℕ
. . . . . | . 20. j = i
. . . . . | . 21. ¬isnull(a(j;t))
. . . . . | . 22. ¬isnull(a(i;t))
. . . . . | . 23. (λx.s(i;t).x) ∈ State(ds)
. . . . . | . 24. t' : ℕ
. . . . . | . 25. t+1≤t'
. . . . . | . 26. ¬isnull(a(i;t'))
. . . . . | . 27. kind(a(i;t')) = locl(a)
. . . . . | . 28. e' : E

. . . . . | . ⊢  ((<j,t> <loc e') ∨ <j,t> = e'
. . . . . | . |   & kind(e') = locl(a)
. . . . . | . |     ∨ (∀v:T. ¬P((λz.(z after e')),v)))
. . . . . | . |  ∈ Prop
. . . . . | . | by AssertBY (<j,t> ∈ E)
. . . . . | . |    (Unfold `w-E` 0 THEN Analyze THEN Try D_ES_Subtype
. . . . . | . |     THEN
. . . . . | . |     Reduce 0
. . . . . | . |     THEN
. . . . . | . |     Trivial)
. . . . . | . |
. . . . . | . 1. i : Id
. . . . . | . 2. a : Id
. . . . . | . 3. T : Type
. . . . . | . 4. ds : x:Id fp-> Type
. . . . . | . 5. P : State(ds)→T→Prop
. . . . . | . 6. w : World
. . . . . | . 7. p : FairFifo
. . . . . | . 8. FairFifo
. . . . . | . 9. ∀l:IdLnk, tg:Id.
. . . . . | . |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | . |                    <ds
. . . . . | . |                    ,<[locl(a)],λx.T>
```

```
. . . . . | . |                    ,
. . . . . | . |                    ,<[a],λx.P>
. . . . . | . |                    ,
. . . . . | . |                    ,
. . . . . | . |                    ,
. . . . . | . |                    ,
. . . . . | . |                    ,·>
. . . . . | . |                 else  fi.da(rcv(l; tg))
. . . . . | . 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . . | . 11. ∀a@0:Id, t:ℕ.
. . . . . | . |   ∃t':ℕ.
. . . . . | . |   t≤t'
. . . . . | . |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . . | . |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . . | . |     ∨ P@0 != <[a]
. . . . . | . |              ,λx.P>(a@0) ==> ∀v:<[locl(a)]
. . . . . | . |                                ,λx.T>(locl(a@0))?Top.
. . . . . | . |       ¬P@0((λx.s(i;t').x),v)
. . . . . | . 12. ∀t:ℕ.
. . . . . | . |   ¬isnull(a(i;t))
. . . . . | . |   ⇒
. . . . . | . |   (islocal(kind(a(i;t)))
. . . . . | . |    ⇒
. . . . . | . |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . . | . |    ⇒
. . . . . | . |    P((λx.s(i;t).x),val(a(i;t))))
. . . . . | . |   & (∀x:Id.
. . . . . | . |      deq-member(product-deq(Knd;Id;...;IdDeq);<...
. . . . . | . |                                              ,x>;1of(
. . . . . | . |                                                  ))
. . . . . | . |      ⇒
. . . . . | . |      s(i;t+1).x
. . . . . | . |      =
. . . . . | . |      2of()(<kind(a(i;t)),x>,λx.s(i;t).x,val(a(i;t))))
. . . . . | . |   & (∀l:IdLnk.
. . . . . | . |      deq-member(product-deq(Knd;...;...;...);<...
. . . . . | . |                                            ,l>;1of(
. . . . . | . |                                                ))
. . . . . | . |      ⇒
. . . . . | . |      withlnk(l;m(i;t))
. . . . . | . |      =
. . . . . | . |      if source(l) = i→
. . . . . | . |         concat(map(λtgf.map(λx.
. . . . . | . |         <1of(tgf)
. . . . . | . |         ,x>;2of(tgf)
. . . . . | . |             ((λx.s(i;t).x)
. . . . . | . |             ,val(a(i;t))));2of()(<kind(a(i;t)),l>)))
. . . . . | . |      else nil fi)
. . . . . | . |   & (∀x:Id.
. . . . . | . |      ¬(deq-member(IdDeq;x;1of())
. . . . . | . |        ⇒
. . . . . | . |        deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . . . . | . |      ⇒
. . . . . | . |      s(i;t).x = s(i;t+1).x)
. . . . . | . |   & (∀l:IdLnk, tg:Id.
```

```
. . . . . | . |      ¬(deq-member(product-deq(...;Id;...;...);...;1of(
. . . . . | . |                                                  ))
. . . . . | . |        ⇒
. . . . . | . |        deq-member(KindDeq;kind(a(i;t));2of()(<l,tg>)))
. . . . . | . |      ⇒
. . . . . | . |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . | . 13. ∀x:Id.
. . . . . | . |   deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . . . . | . 14. ∀a@0:Action(i).
. . . . . | . |   ¬isnull(a@0)
. . . . . | . |   ⇒
. . . . . | . |   (valtype(i;a@0) ⊆r <[locl(a)],λx.T>(kind(a@0))?Top)
. . . . . | . 15. ∀x:Id.
. . . . . | . |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . . . . | . |                      2of(ds)(x)
. . . . . | . |                  else Top fi
. . . . . | . 16. IdDeq ∈ EqDecider(Id)
. . . . . | . 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . . | . 18. j : Id
. . . . . | . 19. t : ℕ
. . . . . | . 20. j = i
. . . . . | . 21. ¬isnull(a(j;t))

. . . . . | . 22. ¬isnull(a(i;t))
. . . . . | . 23. (λx.s(i;t).x) ∈ State(ds)
. . . . . | . 24. t' : ℕ
. . . . . | . 25. t+1≤t'
. . . . . | . 26. ¬isnull(a(i;t'))
. . . . . | . 27. kind(a(i;t')) = locl(a)
. . . . . | . 28. e' : E
. . . . . | . 29. <j,t> ∈ E
. . . . . | . ⊢  ((<j,t> <loc e') ∨ <j,t> = e'
. . . . . | . |   & kind(e') = locl(a)
. . . . . | . |     ∨ (∀v:T. ¬P((λz.(z after e')),v)))
. . . . . | . |  ∈ Prop
. . . . . | . | by Repeat
. . . . . | . |    (Unfolds
. . . . . | . |     [‘es-Loc‘
. . . . . | . |     ;‘es-causl‘
. . . . . | . |     ;‘es-locl‘
. . . . . | . |     ;‘es-loc‘
. . . . . | . |     ;‘w-E‘
. . . . . | . |     ;‘w-locl‘]
. . . . . | . |     0
. . . . . | . |     THEN
. . . . . | . |     Reduce 0)
. . . . . | . |
. . . . . | . 1. i : Id
. . . . . | . 2. a : Id
. . . . . | . 3. T : Type
. . . . . | . 4. ds : x:Id fp-> Type
. . . . . | . 5. P : State(ds)→T→Prop
. . . . . | . 6. w : World
. . . . . | . 7. FairFifo
. . . . . | . 8. FairFifo
. . . . . | . 9. ∀l:IdLnk, tg:Id.
```

```
. . . . . | . |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | . |                    <ds
. . . . . | . |                    ,<[locl(a)],λx.T>
. . . . . | . |                    ,
. . . . . | . |                    ,<[a],λx.P>
. . . . . | . |                    ,
. . . . . | . |                    ,
. . . . . | . |                    ,
. . . . . | . |                    ,
. . . . . | . |                    ,·>
. . . . . | . |                 else  fi.da(rcv(l; tg))
. . . . . | . 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . . | . 11. ∀a@0:Id, t:ℕ.
. . . . . | . |   ∃t':ℕ.
. . . . . | . |   t≤t'
. . . . . | . |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . . | . |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . . | . |     ∨ P@0 != <[a]
. . . . . | . |              ,λx.P>(a@0) ==> ∀v:<[locl(a)]
. . . . . | . |                                ,λx.T>(locl(a@0))?Top.
. . . . . | . |       ¬P@0((λx.s(i;t').x),v)
. . . . . | . 12. ∀t:ℕ.
. . . . . | . |   ¬isnull(a(i;t))
. . . . . | . |   ⇒
. . . . . | . |   (islocal(kind(a(i;t)))
. . . . . | . |    ⇒
. . . . . | . |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . . | . |    ⇒
. . . . . | . |    P((λx.s(i;t).x),val(a(i;t))))
. . . . . | . |   & (∀x:Id.
. . . . . | . |      deq-member(product-deq(Knd;Id;...;IdDeq);<...
. . . . . | . |                                                ,x>;1of(
. . . . . | . |                                                    ))
. . . . . | . |      ⇒
. . . . . | . |      s(i;t+1).x
. . . . . | . |      =
. . . . . | . |      2of()(<kind(a(i;t)),x>,λx.s(i;t).x,val(a(i;t))))
. . . . . | . |   & (∀l:IdLnk.
. . . . . | . |      deq-member(product-deq(Knd;...;...;...);<...
. . . . . | . |                                              ,l>;1of(
. . . . . | . |                                                  ))
. . . . . | . |      ⇒
. . . . . | . |      withlnk(l;m(i;t))
. . . . . | . |      =
. . . . . | . |      if source(l) = i→
. . . . . | . |         concat(map(λtgf.map(λx.
. . . . . | . |         <1of(tgf)
. . . . . | . |         ,x>;2of(tgf)
. . . . . | . |             ((λx.s(i;t).x)
. . . . . | . |             ,val(a(i;t))));2of()(<kind(a(i;t)),l>)))
. . . . . | . |      else nil fi)
. . . . . | . |   & (∀x:Id.
. . . . . | . |      ¬(deq-member(IdDeq;x;1of())
. . . . . | . |        ⇒
. . . . . | . |        deq-member(KindDeq;kind(a(i;t));2of()(x)))
```

```
. . . . . | . |      ⇒
. . . . . | . |      s(i;t).x = s(i;t+1).x)
. . . . . | . |   & (∀l:IdLnk, tg:Id.
. . . . . | . |      ¬(deq-member(product-deq(...;Id;...;...);...;1of(
. . . . . | . |                                                  ))
. . . . . | . |        ⇒
. . . . . | . |        deq-member(KindDeq;kind(a(i;t));2of()(<l,tg>)))
. . . . . | . |      ⇒
. . . . . | . |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . | . 13. ∀x:Id.
. . . . . | . |   deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . . . . | . 14. ∀a@0:Action(i).
. . . . . | . |   ¬isnull(a@0)
. . . . . | . |   ⇒
. . . . . | . |   (valtype(i;a@0) ⊆r <[locl(a)],λx.T>(kind(a@0))?Top)
. . . . . | . 15. ∀x:Id.
. . . . . | . |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . . . . | . |                     2of(ds)(x)
. . . . . | . |                  else Top fi
. . . . . | . 16. IdDeq ∈ EqDecider(Id)
. . . . . | . 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . . | . 18. j : Id
. . . . . | . 19. t : ℕ
. . . . . | . 20. j = i
. . . . . | . 21. ¬isnull(a(j;t))
. . . . . | . 22. ¬isnull(a(i;t))
. . . . . | . 23. (λx.s(i;t).x) ∈ State(ds)
. . . . . | . 24. t' : ℕ
. . . . . | . 25. t+1≤t'
. . . . . | . 26. ¬isnull(a(i;t'))
. . . . . | . 27. kind(a(i;t')) = locl(a)
. . . . . | . 28. e' : E
. . . . . | . 29. <j,t> ∈ E
. . . . . | . ⊢  (j = loc(e') & <j,t> <c e' ∨ <j,t> = e'
. . . . . | . |   & kind(e') = locl(a)
. . . . . | . |     ∨ (∀v:T. ¬P((λz.(z after e')),v)))
. . . . . | . |  ∈ Prop  by Auto
. . . . . | . |
. . . . . | . |\
. . . . . | . | .....subterm .....
. . . . . | . | 1. i : Id
. . . . . | . | 2. a : Id
. . . . . | . | 3. T : Type
. . . . . | . | 4. ds : x:Id fp-> Type
. . . . . | . | 5. P : State(ds)→T→Prop
. . . . . | . | 6. w : World
. . . . . | . | 7. FairFifo
. . . . . | . | 8. FairFifo
. . . . . | . | 9. ∀l:IdLnk, tg:Id.
. . . . . | . |    (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | . |                      <ds
. . . . . | . |                      ,<[locl(a)],λx.T>
. . . . . | . |                      ,
. . . . . | . |                      ,<[a],λx.P>
. . . . . | . |                      ,
```

```
. . . . . | . |                      ,
. . . . . | . |                      ,
. . . . . | . |                      ,
. . . . . | . |                      ,·>
. . . . . | . |                   else  fi.da(rcv(l; tg))
. . . . . | . | 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . . | . | 11. ∀a@0:Id, t:ℕ.
. . . . . | . |     ∃t':ℕ.
. . . . . | . |     t≤t'
. . . . . | . |     & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . . | . |       ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . . | . |       ∨ P@0 != <[a]
. . . . . | . |                ,λx.P>(a@0) ==> ∀v:<[locl(a)]
. . . . . | . |                                ,λx.
. . . . . | . |                                 T>(locl(a@0))?Top.
. . . . . | . |         ¬P@0((λx.s(i;t').x),v)
. . . . . | . | 12. ∀t:ℕ.
. . . . . | . |     ¬isnull(a(i;t))
. . . . . | . |     ⇒
. . . . . | . |     (islocal(kind(a(i;t)))
. . . . . | . |      ⇒
. . . . . | . |      (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . . | . |      ⇒
. . . . . | . |      P((λx.s(i;t).x),val(a(i;t))))
. . . . . | . |     & (∀x:Id.
. . . . . | . |        deq-member(product-deq(Knd;Id;...;...);<...
. . . . . | . |                                              ,x>;1of(
. . . . . | . |                                                  ))
. . . . . | . |        ⇒
. . . . . | . |        s(i;t+1).x
. . . . . | . |        =
. . . . . | . |        2of()
. . . . . | . |        (<kind(a(i;t)),x>
. . . . . | . |        ,λx.s(i;t).x
. . . . . | . |        ,val(a(i;t))))
. . . . . | . |     & (∀l:IdLnk.
. . . . . | . |        deq-member(...;<kind(a(i;t)),l>;1of())
. . . . . | . |        ⇒
. . . . . | . |        withlnk(l;m(i;t))
. . . . . | . |        =
. . . . . | . |        if source(l) = i→
. . . . . | . |           concat(map(λtgf.map(λx.
. . . . . | . |           <1of(tgf),x>;2of(tgf)
. . . . . | . |                       ((λx.s(i;t).x)
. . . . . | . |                       ,val(a(i;t))));2of()
. . . . . | . |                                     (<kind(a(i;t))
. . . . . | . |                                      ,l>)))
. . . . . | . |        else nil fi)
. . . . . | . |     & (∀x:Id.
. . . . . | . |        ¬(deq-member(IdDeq;x;1of())
. . . . . | . |          ⇒
. . . . . | . |          deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . . . . | . |        ⇒
. . . . . | . |        s(i;t).x = s(i;t+1).x)
. . . . . | . |     & (∀l:IdLnk, tg:Id.
```

```
. . . . . | . |        ¬(deq-member(...;<l,tg>;1of())
. . . . . | . |          ⇒
. . . . . | . |          deq-member(KindDeq;kind(a(i;t));2of()
. . . . . | . |                                          (<l,tg>)))
. . . . . | . |        ⇒
. . . . . | . |        w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . | . | 13. ∀x:Id.
. . . . . | . |     deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . . . . | . | 14. ∀a@0:Action(i).
. . . . . | . |     ¬isnull(a@0)
. . . . . | . |     ⇒
. . . . . | . |     (valtype(i;a@0) ⊆r <[locl(a)]
. . . . . | . |                        ,λx.T>(kind(a@0))?Top)
. . . . . | . | 15. ∀x:Id.
. . . . . | . |     vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . . . . | . |                        2of(ds)(x)
. . . . . | . |                     else Top fi
. . . . . | . | 16. IdDeq ∈ EqDecider(Id)
. . . . . | . | 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . . | . | 18. j : Id
. . . . . | . | 19. t : ℕ
. . . . . | . | 20. j = i
. . . . . | . | 21. ¬isnull(a(j;t))
. . . . . | . | 22. ¬isnull(a(i;t))
. . . . . | . | 23. (λx.s(i;t).x) ∈ State(ds)
. . . . . | . | 24. t' : ℕ
. . . . . | . | 25. t+1≤t'
. . . . . | . | 26. ¬isnull(a(i;t'))
. . . . . | . | 27. kind(a(i;t')) = locl(a)
. . . . . | . | 28. E
. . . . . | . | 29. <j,t> ∈ E
. . . . . | . | ⊢  <j,t> ∈ {p:(Id×ℕ)| ¬isnull(a(1of(p);2of(p))) }
. . . . . | . |   by Analyze THEN Reduce 0
. . . . . | . |
. . . . . | . |\
. . . . . | . | .....subterm .....
. . . . . | . | 1. i : Id
. . . . . | . | 2. a : Id
. . . . . | . | 3. T : Type
. . . . . | . | 4. ds : x:Id fp-> Type
. . . . . | . | 5. P : State(ds)→T→Prop
. . . . . | . | 6. w : World
. . . . . | . | 7. FairFifo
. . . . . | . | 8. FairFifo
. . . . . | . | 9. ∀l:IdLnk, tg:Id.
. . . . . | . |    (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | . |                      <ds
. . . . . | . |                      ,<[locl(a)],λx.T>
. . . . . | . |                      ,
. . . . . | . |                      ,<[a],λx.P>
. . . . . | . |                      ,
. . . . . | . |                      ,
. . . . . | . |                      ,
. . . . . | . |                      ,
. . . . . | . |                      ,.>
```

```
. . . . . | . |                   else  fi.da(rcv(l; tg))
. . . . . | . | 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . . | . | 11. ∀a@0:Id, t:ℕ.
. . . . . | . |     ∃t':ℕ.
. . . . . | . |     t≤t'
. . . . . | . |     & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . . | . |       ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . . | . |       ∨ P@0 != <[a]
. . . . . | . |                ,λx.P>(a@0) ==> ∀v:<[locl(a)]
. . . . . | . |                                ,λx.
. . . . . | . |                                 T>(locl(a@0))?Top.
. . . . . | . |         ¬P@0((λx.s(i;t').x),v)
. . . . . | . | 12. ∀t:ℕ.
. . . . . | . |     ¬isnull(a(i;t))
. . . . . | . |     ⇒
. . . . . | . |     (islocal(kind(a(i;t)))
. . . . . | . |      ⇒
. . . . . | . |      (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . . | . |      ⇒
. . . . . | . |      P((λx.s(i;t).x),val(a(i;t))))
. . . . . | . |     & (∀x:Id.
. . . . . | . |        deq-member(product-deq(Knd;Id;...;...);<...
. . . . . | . |                                              ,x>;1of(
. . . . . | . |                                                  ))
. . . . . | . |        ⇒
. . . . . | . |        s(i;t+1).x
. . . . . | . |        =
. . . . . | . |        2of()
. . . . . | . |        (<kind(a(i;t)),x>
. . . . . | . |        ,λx.s(i;t).x
. . . . . | . |        ,val(a(i;t))))
. . . . . | . |     & (∀l:IdLnk.
. . . . . | . |        deq-member(...;<kind(a(i;t)),l>;1of())
. . . . . | . |        ⇒
. . . . . | . |        withlnk(l;m(i;t))
. . . . . | . |        =
. . . . . | . |        if source(l) = i→
. . . . . | . |           concat(map(λtgf.map(λx.
. . . . . | . |           <1of(tgf),x>;2of(tgf)
. . . . . | . |                       ((λx.s(i;t).x)
. . . . . | . |                       ,val(a(i;t))));2of()
. . . . . | . |                                      (<kind(a(i;t))
. . . . . | . |                                       ,l>)))
. . . . . | . |        else nil fi)
. . . . . | . |     & (∀x:Id.
. . . . . | . |        ¬(deq-member(IdDeq;x;1of())
. . . . . | . |          ⇒
. . . . . | . |          deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . . . . | . |        ⇒
. . . . . | . |        s(i;t).x = s(i;t+1).x)
. . . . . | . |     & (∀l:IdLnk, tg:Id.
. . . . . | . |        ¬(deq-member(...;<l,tg>;1of())
. . . . . | . |          ⇒
. . . . . | . |          deq-member(KindDeq;kind(a(i;t));2of()
. . . . . | . |                                          (<l,tg>)))
```

```
. . . . . | . |        ⇒
. . . . . | . |        w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . | . | 13. ∀x:Id.
. . . . . | . |     deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . . . . | . | 14. ∀a@0:Action(i).
. . . . . | . |     ¬isnull(a@0)
. . . . . | . |     ⇒
. . . . . | . |     (valtype(i;a@0) ⊆r <[locl(a)]
. . . . . | . |                        ,λx.T>(kind(a@0))?Top)
. . . . . | . | 15. ∀x:Id.
. . . . . | . |     vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . . . . | . |                        2of(ds)(x)
. . . . . | . |                    else Top fi
. . . . . | . | 16. IdDeq ∈ EqDecider(Id)
. . . . . | . | 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . . | . | 18. j : Id
. . . . . | . | 19. t : ℕ
. . . . . | . | 20. j = i
. . . . . | . | 21. ¬isnull(a(j;t))
. . . . . | . | 22. ¬isnull(a(i;t))
. . . . . | . | 23. (λx.s(i;t).x) ∈ State(ds)
. . . . . | . | 24. t' : ℕ
. . . . . | . | 25. t+1≤t'
. . . . . | . | 26. ¬isnull(a(i;t'))
. . . . . | . | 27. kind(a(i;t')) = locl(a)
. . . . . | . | 28. e' : E
. . . . . | . | 29. <j,t> ∈ E
. . . . . | . | ⊢  e' ∈ {p:(Id×ℕ)| ¬isnull(a(1of(p);2of(p))) }
. . . . . | . |   by Analyze -2 THEN Analyze
. . . . . | . |
. . . . . | . .\
. . . . . | . . .....subterm .....
. . . . . | . . 1. i : Id
. . . . . | . . 2. a : Id
. . . . . | . . 3. T : Type
. . . . . | . . 4. ds : x:Id fp-> Type
. . . . . | . . 5. P : State(ds)→T→Prop
. . . . . | . . 6. w : World
. . . . . | . . 7. FairFifo
. . . . . | . . 8. FairFifo
. . . . . | . . 9. ∀l:IdLnk, tg:Id.
. . . . . | . . |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | . . |                    <ds
. . . . . | . . |                    ,<[locl(a)],λx.T>
. . . . . | . . |                    ,
. . . . . | . . |                    ,<[a],λx.P>
. . . . . | . . |                    ,
. . . . . | . . |                    ,
. . . . . | . . |                    ,
. . . . . | . . |                    ,
. . . . . | . . |                    ,·>
. . . . . | . . |                else  fi.da(rcv(l; tg))
. . . . . | . . 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . . | . . 11. ∀a@0:Id, t:ℕ.
. . . . . | . . |   ∃t':ℕ.
```

```
. . . . . | . . |   t≤t'
. . . . . | . . |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . . | . . |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . . | . . |     ∨ P@0 != <[a]
. . . . . | . . |              ,λx.P>(a@0) ==> ∀v:<[locl(a)]
. . . . . | . . |                                ,λx.
. . . . . | . . |                                 T>(locl(a@0))?Top.
. . . . . | . . |       ¬P@0((λx.s(i;t').x),v)
. . . . . | . . 12. ∀t:ℕ.
. . . . . | . . |   ¬isnull(a(i;t))
. . . . . | . . |   ⇒
. . . . . | . . |   (islocal(kind(a(i;t)))
. . . . . | . . |    ⇒
. . . . . | . . |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . . | . . |    ⇒
. . . . . | . . |    P((λx.s(i;t).x),val(a(i;t))))
. . . . . | . . |   & (∀x:Id.
. . . . . | . . |      deq-member(product-deq(Knd;Id;...;...);<...
. . . . . | . . |                                            ,x>;1of(
. . . . . | . . |                                                ))
. . . . . | . . |      ⇒
. . . . . | . . |      s(i;t+1).x
. . . . . | . . |      =
. . . . . | . . |      2of()
. . . . . | . . |      (<kind(a(i;t)),x>
. . . . . | . . |      ,λx.s(i;t).x
. . . . . | . . |      ,val(a(i;t))))
. . . . . | . . |   & (∀l:IdLnk.
. . . . . | . . |      deq-member(...;<kind(a(i;t)),l>;1of())
. . . . . | . . |      ⇒
. . . . . | . . |      withlnk(l;m(i;t))
. . . . . | . . |      =
. . . . . | . . |      if source(l) = i→
. . . . . | . . |         concat(map(λtgf.map(λx.
. . . . . | . . |         <1of(tgf),x>;2of(tgf)
. . . . . | . . |                      ((λx.s(i;t).x)
. . . . . | . . |                      ,val(a(i;t))));2of()
. . . . . | . . |                                        (<kind(a(i;t))
. . . . . | . . |                                         ,l>)))
. . . . . | . . |      else nil fi)
. . . . . | . . |   & (∀x:Id.
. . . . . | . . |      ¬(deq-member(IdDeq;x;1of())
. . . . . | . . |        ⇒
. . . . . | . . |        deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . . . . | . . |      ⇒
. . . . . | . . |      s(i;t).x = s(i;t+1).x)
. . . . . | . . |   & (∀l:IdLnk, tg:Id.
. . . . . | . . |      ¬(deq-member(...;<l,tg>;1of())
. . . . . | . . |        ⇒
. . . . . | . . |        deq-member(KindDeq;kind(a(i;t));2of()
. . . . . | . . |                                        (<l,tg>)))
. . . . . | . . |      ⇒
. . . . . | . . |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . | . . 13. ∀x:Id.
. . . . . | . . |   deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
```

```
. . . . . | . . 14. ∀a@0:Action(i).
. . . . . | . . |   ¬isnull(a@0)
. . . . . | . . |   ⇒
. . . . . | . . |   (valtype(i;a@0) ⊆r <[locl(a)]
. . . . . | . . |                     ,λx.T>(kind(a@0))?Top)
. . . . . | . . 15. ∀x:Id.
. . . . . | . . |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . . . . | . . |                     2of(ds)(x)
. . . . . | . . |                  else Top fi
. . . . . | . . 16. IdDeq ∈ EqDecider(Id)
. . . . . | . . 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . . | . . 18. j : Id
. . . . . | . . 19. t : ℕ
. . . . . | . . 20. j = i
. . . . . | . . 21. ¬isnull(a(j;t))
. . . . . | . . 22. ¬isnull(a(i;t))
. . . . . | . . 23. (λx.s(i;t).x) ∈ State(ds)
. . . . . | . . 24. t' : ℕ
. . . . . | . . 25. t+1≤t'
. . . . . | . . 26. ¬isnull(a(i;t'))
. . . . . | . . 27. kind(a(i;t')) = locl(a)
. . . . . | . . 28. e' : E
. . . . . | . . 29. <j,t> ∈ E
. . . . . | . . 30. j = loc(e') & <j,t> <c e' ∨ <j,t> = e'
. . . . . | . . 31. T
. . . . . | . . ⊢  (λz.(z after e')) ∈ State(ds)
. . . . . | . . | by Analyze -4 THEN Analyze -5
. . . . . | . . |    THEN
. . . . . | . . |    Unfolds [`ma-state`;`w-after`] 0
. . . . . | . . |    THEN
. . . . . | . . |    Reduce 0
. . . . . | . . |
. . . . . | . . 1. i : Id
. . . . . | . . 2. a : Id
. . . . . | . . 3. T : Type
. . . . . | . . 4. ds : x:Id fp-> Type
. . . . . | . . 5. P : State(ds)→T→Prop
. . . . . | . . 6. w : World
. . . . . | . . 7. FairFifo
. . . . . | . . 8. FairFifo
. . . . . | . . 9. ∀l:IdLnk, tg:Id.
. . . . . | . . |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | . . |                   <ds
. . . . . | . . |                   ,<[locl(a)],λx.T>
. . . . . | . . |                   ,
. . . . . | . . |                   ,<[a],λx.P>
. . . . . | . . |                   ,
. . . . . | . . |                   ,
. . . . . | . . |                   ,
. . . . . | . . |                   ,
. . . . . | . . |                   ,•>
. . . . . | . . |                else  fi.da(rcv(l; tg))
. . . . . | . . 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . . | . . 11. ∀a@0:Id, t:ℕ.
. . . . . | . . |   ∃t':ℕ.
```

```
. . . . . | . . |   t≤t'
. . . . . | . . |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . . | . . |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . . | . . |     ∨ P@0 != <[a]
. . . . . | . . |              ,λx.P>(a@0) ==> ∀v:<[locl(a)]
. . . . . | . . |                                ,λx.
. . . . . | . . |                                 T>(locl(a@0))?Top.
. . . . . | . . |       ¬P@0((λx.s(i;t').x),v)
. . . . . | . . 12. ∀t:ℕ.
. . . . . | . . |   ¬isnull(a(i;t))
. . . . . | . . |   ⇒
. . . . . | . . |   (islocal(kind(a(i;t)))
. . . . . | . . |    ⇒
. . . . . | . . |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . . | . . |    ⇒
. . . . . | . . |    P((λx.s(i;t).x),val(a(i;t))))
. . . . . | . . |   & (∀x:Id.
. . . . . | . . |      deq-member(product-deq(Knd;Id;...;...);<...
. . . . . | . . |                                            ,x>;1of(
. . . . . | . . |                                                ))
. . . . . | . . |      ⇒
. . . . . | . . |      s(i;t+1).x
. . . . . | . . |      =
. . . . . | . . |      2of()
. . . . . | . . |      (<kind(a(i;t)),x>
. . . . . | . . |      ,λx.s(i;t).x
. . . . . | . . |      ,val(a(i;t))))
. . . . . | . . |   & (∀l:IdLnk.
. . . . . | . . |      deq-member(...;<kind(a(i;t)),l>;1of())
. . . . . | . . |      ⇒
. . . . . | . . |      withlnk(l;m(i;t))
. . . . . | . . |      =
. . . . . | . . |      if source(l) = i→
. . . . . | . . |         concat(map(λtgf.map(λx.
. . . . . | . . |         <1of(tgf),x>;2of(tgf)
. . . . . | . . |                     ((λx.s(i;t).x)
. . . . . | . . |                     ,val(a(i;t))));2of()
. . . . . | . . |                                    (<kind(a(i;t))
. . . . . | . . |                                     ,l>)))
. . . . . | . . |      else nil fi)
. . . . . | . . |   & (∀x:Id.
. . . . . | . . |      ¬(deq-member(IdDeq;x;1of())
. . . . . | . . |        ⇒
. . . . . | . . |        deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . . . . | . . |      ⇒
. . . . . | . . |      s(i;t).x = s(i;t+1).x)
. . . . . | . . |   & (∀l:IdLnk, tg:Id.
. . . . . | . . |      ¬(deq-member(...;<l,tg>;1of())
. . . . . | . . |        ⇒
. . . . . | . . |        deq-member(KindDeq;kind(a(i;t));2of()
. . . . . | . . |                                        (<l,tg>)))
. . . . . | . . |      ⇒
. . . . . | . . |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . | . . 13. ∀x:Id.
. . . . . | . . |   deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
```

```
. . . . . | . . 14. ∀a@0:Action(i).
. . . . . | . . |   ¬isnull(a@0)
. . . . . | . . |   ⇒
. . . . . | . . |   (valtype(i;a@0) ⊆r <[locl(a)]
. . . . . | . . |                     ,λx.T>(kind(a@0))?Top)
. . . . . | . . 15. ∀x:Id.
. . . . . | . . |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . . . . | . . |                     2of(ds)(x)
. . . . . | . . |                  else Top fi
. . . . . | . . 16. IdDeq ∈ EqDecider(Id)
. . . . . | . . 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . . | . . 18. j : Id
. . . . . | . . 19. t : ℕ
. . . . . | . . 20. j = i
. . . . . | . . 21. ¬isnull(a(j;t))
. . . . . | . . 22. ¬isnull(a(i;t))
. . . . . | . . 23. (λx.s(i;t).x) ∈ State(ds)
. . . . . | . . 24. t' : ℕ
. . . . . | . . 25. t+1≤t'
. . . . . | . . 26. ¬isnull(a(i;t'))
. . . . . | . . 27. kind(a(i;t')) = locl(a)
. . . . . | . . 28. e1 : Id
. . . . . | . . 29. e2 : ℕ
. . . . . | . . 30. ¬isnull(a(1of(<e1,e2>);2of(<e1,e2>)))
. . . . . | . . 31. <j,t> ∈ E
. . . . . | . . 32. j = loc(<e1,e2>) & <j,t> <c <e1,e2>
. . . . . | . . |   ∨ <j,t> = <e1,e2>
. . . . . | . . 33. T
. . . . . | . . ⊢  (λz.s(e1;e2+1).z) ∈ x:Id→ds(x)?Top
. . . . . | . . | by Auto THEN DoSubsume THEN Try BackThruSomeHyp
. . . . . | . . |    THEN
. . . . . | . . |    Try (Complete D_ES_Subtype)
. . . . . | . . |
. . . . . | . . .....subtype_rel .....
. . . . . | . . 1. i : Id
. . . . . | . . 2. a : Id
. . . . . | . . 3. T : Type
. . . . . | . . 4. ds : x:Id fp-> Type
. . . . . | . . 5. P : State(ds)→T→Prop
. . . . . | . . 6. w : World
. . . . . | . . 7. FairFifo
. . . . . | . . 8. FairFifo
. . . . . | . . 9. ∀l:IdLnk, tg:Id.
. . . . . | . . |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | . . |                  <ds
. . . . . | . . |                  ,<[locl(a)],λx.T>
. . . . . | . . |                  ,
. . . . . | . . |                  ,<[a],λx.P>
. . . . . | . . |                  ,
. . . . . | . . |                  ,
. . . . . | . . |                  ,
. . . . . | . . |                  ,
. . . . . | . . |                  ,.>
. . . . . | . . |               else  fi.da(rcv(l; tg))
. . . . . | . . 10. (eqof(IdDeq)(i,i)) ∼ true₂
```

```
. . . . . | . . 11. ∀a@0:Id, t:ℕ.
. . . . . | . .   |  ∃t':ℕ.
. . . . . | . .   |  t≤t'
. . . . . | . .   |  & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . . | . .   |    ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . . | . .   |    ∨ P@0 != <[a]
. . . . . | . .   |             ,λx.P>(a@0) ==> ∀v:<[locl(a)]
. . . . . | . .   |                                ,λx.
. . . . . | . .   |                                 T>(locl(a@0))?Top.
. . . . . | . .   |      ¬P@0((λx.s(i;t').x),v)
. . . . . | . . 12. ∀t:ℕ.
. . . . . | . .   |  ¬isnull(a(i;t))
. . . . . | . .   |  ⇒
. . . . . | . .   |  (islocal(kind(a(i;t)))
. . . . . | . .   |   ⇒
. . . . . | . .   |   (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . . | . .   |   ⇒
. . . . . | . .   |   P((λx.s(i;t).x),val(a(i;t))))
. . . . . | . .   |  & (∀x:Id.
. . . . . | . .   |     deq-member(product-deq(Knd;Id;...;...);<...
. . . . . | . .   |                                          ,x>;1of(
. . . . . | . .   |                                              ))
. . . . . | . .   |     ⇒
. . . . . | . .   |     s(i;t+1).x
. . . . . | . .   |     =
. . . . . | . .   |     2of()
. . . . . | . .   |     (<kind(a(i;t)),x>
. . . . . | . .   |     ,λx.s(i;t).x
. . . . . | . .   |     ,val(a(i;t))))
. . . . . | . .   |  & (∀l:IdLnk.
. . . . . | . .   |     deq-member(...;<kind(a(i;t)),l>;1of())
. . . . . | . .   |     ⇒
. . . . . | . .   |     withlnk(l;m(i;t))
. . . . . | . .   |     =
. . . . . | . .   |     if source(l) = i→
. . . . . | . .   |        concat(map(λtgf.map(λx.
. . . . . | . .   |        <1of(tgf),x>;2of(tgf)
. . . . . | . .   |                     ((λx.s(i;t).x)
. . . . . | . .   |                     ,val(a(i;t))));2of()
. . . . . | . .   |                                  (<kind(a(i;t))
. . . . . | . .   |                                   ,l>)))
. . . . . | . .   |     else nil fi)
. . . . . | . .   |  & (∀x:Id.
. . . . . | . .   |     ¬(deq-member(IdDeq;x;1of())
. . . . . | . .   |       ⇒
. . . . . | . .   |       deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . . . . | . .   |     ⇒
. . . . . | . .   |     s(i;t).x = s(i;t+1).x)
. . . . . | . .   |  & (∀l:IdLnk, tg:Id.
. . . . . | . .   |     ¬(deq-member(...;<l,tg>;1of())
. . . . . | . .   |       ⇒
. . . . . | . .   |       deq-member(KindDeq;kind(a(i;t));2of()
. . . . . | . .   |                                      (<l,tg>)))
. . . . . | . .   |     ⇒
. . . . . | . .   |     w-tagged(tg; onlnk(l;m(i;t))) = nil)
```

```
. . . . . | . . 13. ∀x:Id.
. . . . . | . . |   deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . . . . | . . 14. ∀a@0:Action(i).
. . . . . | . . |   ¬isnull(a@0)
. . . . . | . . |   ⇒
. . . . . | . . |   (valtype(i;a@0) ⊆r <[locl(a)]
. . . . . | . . |                      ,λx.T>(kind(a@0))?Top)
. . . . . | . . 15. ∀x:Id.
. . . . . | . . |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . . . . | . . |                      2of(ds)(x)
. . . . . | . . |                  else Top fi
. . . . . | . . 16. IdDeq ∈ EqDecider(Id)
. . . . . | . . 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . . | . . 18. j : Id
. . . . . | . . 19. t : ℕ
. . . . . | . . 20. j = i
. . . . . | . . 21. ¬isnull(a(j;t))
. . . . . | . . 22. ¬isnull(a(i;t))
. . . . . | . . 23. (λx.s(i;t).x) ∈ State(ds)
. . . . . | . . 24. t' : ℕ
. . . . . | . . 25. t+1≤t'
. . . . . | . . 26. ¬isnull(a(i;t'))
. . . . . | . . 27. kind(a(i;t')) = locl(a)
. . . . . | . . 28. e1 : Id
. . . . . | . . 29. e2 : ℕ
. . . . . | . . 30. ¬isnull(a(1of(<e1,e2>);2of(<e1,e2>)))
. . . . . | . . 31. <j,t> ∈ E
. . . . . | . . 32. j = loc(<e1,e2>) & <j,t> <c <e1,e2>
. . . . . | . . |   ∨ <j,t> = <e1,e2>
. . . . . | . . 33. T
. . . . . | . . 34. z : Id
. . . . . | . . ⊢  vartype(e1;z) ⊆r ds(z)?Top  by Subst (e1 = i) 0
. . . . . | . . |
. . . . . | . . |\
. . . . . | . . | .....equality .....
. . . . . | . . | 1. i : Id
. . . . . | . . | 2. a : Id
. . . . . | . . | 3. T : Type
. . . . . | . . | 4. ds : x:Id fp-> Type
. . . . . | . . | 5. P : State(ds)→T→Prop
. . . . . | . . | 6. w : World
. . . . . | . . | 7. FairFifo
. . . . . | . . | 8. FairFifo
. . . . . | . . | 9. ∀l:IdLnk, tg:Id.
. . . . . | . . | |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | . . | |                    <ds
. . . . . | . . | |                    ,<[locl(a)],λx.T>
. . . . . | . . | |                    ,
. . . . . | . . | |                    ,<[a],λx.P>
. . . . . | . . | |                    ,
. . . . . | . . | |                    ,
. . . . . | . . | |                    ,
. . . . . | . . | |                    ,
. . . . . | . . | |                    ,·>
. . . . . | . . | |                else  fi.da(rcv(l; tg))
```

```
. . . . . | . . | 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . . | . . | 11. ∀a@0:Id, t:ℕ.
. . . . . | . . | |   ∃t':ℕ.
. . . . . | . . | |   t≤t'
. . . . . | . . | |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . . | . . | |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . . | . . | |     ∨ P@0 != <[a]

. . . . . | . . | |              ,λx.
. . . . . | . . | |               P>(a@0) ==> ∀v:<[locl(a)]
. . . . . | . . | |                                ,λx.
. . . . . | . . | |                                 T>(locl(a@0))?Top.
. . . . . | . . | |       ¬P@0((λx.s(i;t').x),v)
. . . . . | . . | 12. ∀t:ℕ.
. . . . . | . . | |   ¬isnull(a(i;t))
. . . . . | . . | |   ⇒
. . . . . | . . | |   (islocal(kind(a(i;t)))
. . . . . | . . | |    ⇒
. . . . . | . . | |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . . | . . | |    ⇒
. . . . . | . . | |    P((λx.s(i;t).x),val(a(i;t))))
. . . . . | . . | |   & (∀x:Id.
. . . . . | . . | |      deq-member(...;<kind(a(i;t)),x>;1of())
. . . . . | . . | |      ⇒
. . . . . | . . | |      s(i;t+1).x
. . . . . | . . | |      =
. . . . . | . . | |      2of()
. . . . . | . . | |      (<kind(a(i;t)),x>
. . . . . | . . | |      ,λx.s(i;t).x
. . . . . | . . | |      ,val(a(i;t))))
. . . . . | . . | |   & (∀l:IdLnk.
. . . . . | . . | |      deq-member(...;<kind(a(i;t)),l>;1of())
. . . . . | . . | |      ⇒
. . . . . | . . | |      withlnk(l;m(i;t))
. . . . . | . . | |      =
. . . . . | . . | |      if source(l) = i→
. . . . . | . . | |         concat(map(λtgf.map(λx.
. . . . . | . . | |         <1of(tgf),x>;2of(tgf)
. . . . . | . . | |                      ((λx.s(i;t).x)
. . . . . | . . | |                      ,val(a(i;t))));2of()
. . . . . | . . | |                                    (<kind(a(i;t))
. . . . . | . . | |                                     ,l>)))
. . . . . | . . | |      else nil fi)
. . . . . | . . | |   & (∀x:Id.
. . . . . | . . | |      ¬(deq-member(IdDeq;x;1of())
. . . . . | . . | |        ⇒
. . . . . | . . | |        deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . . . . | . . | |      ⇒
. . . . . | . . | |      s(i;t).x = s(i;t+1).x)
. . . . . | . . | |   & (∀l:IdLnk, tg:Id.
. . . . . | . . | |      ¬(deq-member(...;<l,tg>;1of())
. . . . . | . . | |        ⇒
. . . . . | . . | |        deq-member(KindDeq;kind(a(i;t));2of()
. . . . . | . . | |                                       (<l,tg>)))
. . . . . | . . | |      ⇒
. . . . . | . . | |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
```

```
. . . . . | . . | 13. ∀x:Id.
. . . . . | . . | |   deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . . . . | . . | 14. ∀a@0:Action(i).
. . . . . | . . | |   ¬isnull(a@0)
. . . . . | . . | |   ⇒
. . . . . | . . | |   (valtype(i;a@0) ⊆r <[locl(a)]
. . . . . | . . | |                      ,λx.T>(kind(a@0))?Top)
. . . . . | . . | 15. ∀x:Id.
. . . . . | . . | |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . . . . | . . | |                      2of(ds)(x)
. . . . . | . . | |                   else Top fi
. . . . . | . . | 16. IdDeq ∈ EqDecider(Id)
. . . . . | . . | 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . . | . . | 18. j : Id
. . . . . | . . | 19. t : ℕ
. . . . . | . . | 20. j = i
. . . . . | . . | 21. ¬isnull(a(j;t))
. . . . . | . . | 22. ¬isnull(a(i;t))
. . . . . | . . | 23. (λx.s(i;t).x) ∈ State(ds)
. . . . . | . . | 24. t' : ℕ
. . . . . | . . | 25. t+1≤t'
. . . . . | . . | 26. ¬isnull(a(i;t'))
. . . . . | . . | 27. kind(a(i;t')) = locl(a)
. . . . . | . . | 28. e1 : Id
. . . . . | . . | 29. e2 : ℕ
. . . . . | . . | 30. ¬isnull(a(1of(<e1,e2>);2of(<e1,e2>)))
. . . . . | . . | 31. <j,t> ∈ E
. . . . . | . . | 32. j = loc(<e1,e2>) & <j,t> <c <e1,e2>
. . . . . | . . | |   ∨ <j,t> = <e1,e2>
. . . . . | . . | 33. T
. . . . . | . . | 34. Id
. . . . . | . . | ⊢  e1 = i  by Analyze -3
. . . . . | . . | |
. . . . . | . . | |\
. . . . . | . . | | 1. i : Id
. . . . . | . . | | 2. a : Id
. . . . . | . . | | 3. T : Type
. . . . . | . . | | 4. ds : x:Id fp-> Type
. . . . . | . . | | 5. P : State(ds)→T→Prop
. . . . . | . . | | 6. w : World
. . . . . | . . | | 7. FairFifo
. . . . . | . . | | 8. FairFifo
. . . . . | . . | | 9. ∀l:IdLnk, tg:Id.
. . . . . | . . | |    (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | . . | |                      <ds
. . . . . | . . | |                      ,<[locl(a)],λx.T>
. . . . . | . . | |                      ,
. . . . . | . . | |                      ,<[a],λx.P>
. . . . . | . . | |                      ,
. . . . . | . . | |                      ,
. . . . . | . . | |                      ,
. . . . . | . . | |                      ,
. . . . . | . . | |                      ,·>
. . . . . | . . | |                   else  fi.da(rcv(l; tg))
. . . . . | . . | | 10. (eqof(IdDeq)(i,i)) ∼ true₂
```

```
. . . . . | . . | | 11. ∀a@0:Id, t:ℕ.
. . . . . | . . | |     ∃t':ℕ.
. . . . . | . . | |     t≤t'
. . . . . | . . | |     & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . . | . . | |       ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . . | . . | |       ∨ P@0 != <[a]
. . . . . | . . | |                ,λx.
. . . . . | . . | |                 P>(a@0) ==> ∀v:<[locl(a)]
. . . . . | . . | |                                ,λx.
. . . . . | . . | |                                 T>(locl(a@0))?Top.
. . . . . | . . | |         ¬P@0((λx.s(i;t').x),v)
. . . . . | . . | | 12. ∀t:ℕ.
. . . . . | . . | |     ¬isnull(a(i;t))
. . . . . | . . | |     ⇒
. . . . . | . . | |     (islocal(kind(a(i;t)))
. . . . . | . . | |      ⇒
. . . . . | . . | |      (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . . | . . | |      ⇒
. . . . . | . . | |      P((λx.s(i;t).x),val(a(i;t))))
. . . . . | . . | |     & (∀x:Id.
. . . . . | . . | |        deq-member(...;<kind(a(i;t)),x>;1of())
. . . . . | . . | |        ⇒
. . . . . | . . | |        s(i;t+1).x
. . . . . | . . | |        =
. . . . . | . . | |        2of()
. . . . . | . . | |        (<kind(a(i;t)),x>
. . . . . | . . | |        ,λx.s(i;t).x
. . . . . | . . | |        ,val(a(i;t))))
. . . . . | . . | |     & (∀l:IdLnk.
. . . . . | . . | |        deq-member(...;<kind(a(i;t)),l>;1of())
. . . . . | . . | |        ⇒
. . . . . | . . | |        withlnk(l;m(i;t))
. . . . . | . . | |        =
. . . . . | . . | |        if source(l) = i→
. . . . . | . . | |           concat(map(λtgf.map(λx.
. . . . . | . . | |           <1of(tgf)
. . . . . | . . | |           ,x>;2of(tgf)
. . . . . | . . | |               ((λx.s(i;t).x)
. . . . . | . . | |               ,val(a(i;t))));2of()
. . . . . | . . | |                              (<kind(a(i;t)),l>)))
. . . . . | . . | |        else nil fi)
. . . . . | . . | |     & (∀x:Id.
. . . . . | . . | |        ¬(deq-member(IdDeq;x;1of())
. . . . . | . . | |          ⇒
. . . . . | . . | |          deq-member(KindDeq;kind(a(i;t));2of()
. . . . . | . . | |                                         (x)))
. . . . . | . . | |        ⇒
. . . . . | . . | |        s(i;t).x = s(i;t+1).x)
. . . . . | . . | |     & (∀l:IdLnk, tg:Id.
. . . . . | . . | |        ¬...
. . . . . | . . | |        ⇒
. . . . . | . . | |        w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . | . . | | 13. ∀x:Id.
. . . . . | . . | |     deq-member(IdDeq;x;1of())
. . . . . | . . | |     ⇒
```

```
. . . . . | . . | |     s(i;0).x = 2of()(x)
. . . . . | . . | | 14. ∀a@0:Action(i).
. . . . . | . . | |     ¬isnull(a@0)
. . . . . | . . | |     ⇒
. . . . . | . . | |     (valtype(i;a@0) ⊆r <[locl(a)]
. . . . . | . . | |                        ,λx.T>(kind(a@0))?Top)
. . . . . | . . | | 15. ∀x:Id.
. . . . . | . . | |     vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(
. . . . . | . . | |                                          ds))→
. . . . . | . . | |                        2of(ds)(x)
. . . . . | . . | |                    else Top fi
. . . . . | . . | | 16. IdDeq ∈ EqDecider(Id)
. . . . . | . . | | 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . . | . . | | 18. j : Id
. . . . . | . . | | 19. t : ℕ
. . . . . | . . | | 20. j = i
. . . . . | . . | | 21. ¬isnull(a(j;t))
. . . . . | . . | | 22. ¬isnull(a(i;t))
. . . . . | . . | | 23. (λx.s(i;t).x) ∈ State(ds)
. . . . . | . . | | 24. t' : ℕ
. . . . . | . . | | 25. t+1≤t'
. . . . . | . . | | 26. ¬isnull(a(i;t'))
. . . . . | . . | | 27. kind(a(i;t')) = locl(a)
. . . . . | . . | | 28. e1 : Id
. . . . . | . . | | 29. e2 : ℕ
. . . . . | . . | | 30. ¬isnull(a(1of(<e1,e2>);2of(<e1,e2>)))
. . . . . | . . | | 31. <j,t> ∈ E
. . . . . | . . | | 32. j = loc(<e1,e2>) & <j,t> <c <e1,e2>
. . . . . | . . | | 33. T
. . . . . | . . | | 34. Id
. . . . . | . . | | ⊢  e1 = i  by Reduce -3
. . . . . | . . | |
. . . . . | . . | .\
. . . . . | . . | . 1. i : Id
. . . . . | . . | . 2. a : Id
. . . . . | . . | . 3. T : Type
. . . . . | . . | . 4. ds : x:Id fp-> Type
. . . . . | . . | . 5. P : State(ds)→T→Prop
. . . . . | . . | . 6. w : World
. . . . . | . . | . 7. FairFifo
. . . . . | . . | . 8. FairFifo
. . . . . | . . | . 9. ∀l:IdLnk, tg:Id.
. . . . . | . . | .    (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | . . | .                      <ds
. . . . . | . . | .                      ,<[locl(a)],λx.T>
. . . . . | . . | .                      ,
. . . . . | . . | .                      ,<[a],λx.P>
. . . . . | . . | .                      ,
. . . . . | . . | .                      ,
. . . . . | . . | .                      ,
. . . . . | . . | .                      ,
. . . . . | . . | .                      ,.>
. . . . . | . . | .                  else  fi.da(rcv(l; tg))
. . . . . | . . | . 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . . | . . | . 11. ∀a@0:Id, t:ℕ.
```

```
. . . . . | . . | .     ∃t':ℕ.
. . . . . | . . | .     t≤t'
. . . . . | . . | .     & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . . | . . | .       ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . . | . . | .       ∨ P@0 != <[a]
. . . . . | . . | .                ,λx.
. . . . . | . . | .                 P>(a@0) ==> ∀v:<[locl(a)]
. . . . . | . . | .                                ,λx.
. . . . . | . . | .                                 T>(locl(a@0))?Top.
. . . . . | . . | .          ¬P@0((λx.s(i;t').x),v)
. . . . . | . . | . 12. ∀t:ℕ.
. . . . . | . . | .     ¬isnull(a(i;t))
. . . . . | . . | .     ⇒
. . . . . | . . | .     (islocal(kind(a(i;t)))
. . . . . | . . | .      ⇒
. . . . . | . . | .      (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . . | . . | .      ⇒
. . . . . | . . | .      P((λx.s(i;t).x),val(a(i;t))))
. . . . . | . . | .     & (∀x:Id.
. . . . . | . . | .        deq-member(...;<kind(a(i;t)),x>;1of())
. . . . . | . . | .        ⇒
. . . . . | . . | .        s(i;t+1).x
. . . . . | . . | .        =
. . . . . | . . | .        2of()
. . . . . | . . | .        (<kind(a(i;t)),x>
. . . . . | . . | .        ,λx.s(i;t).x
. . . . . | . . | .        ,val(a(i;t))))
. . . . . | . . | .     & (∀l:IdLnk.
. . . . . | . . | .        deq-member(...;<kind(a(i;t)),l>;1of())
. . . . . | . . | .        ⇒
. . . . . | . . | .        withlnk(l;m(i;t))
. . . . . | . . | .        =
. . . . . | . . | .        if source(l) = i→
. . . . . | . . | .           concat(map(λtgf.map(λx.
. . . . . | . . | .           <1of(tgf)
. . . . . | . . | .           ,x>;2of(tgf)
. . . . . | . . | .               ((λx.s(i;t).x)
. . . . . | . . | .               ,val(a(i;t))));2of()
. . . . . | . . | .                              (<kind(a(i;t)),l>)))
. . . . . | . . | .        else nil fi)
. . . . . | . . | .     & (∀x:Id.
. . . . . | . . | .        ¬(deq-member(IdDeq;x;1of())
. . . . . | . . | .          ⇒
. . . . . | . . | .          deq-member(KindDeq;kind(a(i;t));2of()
. . . . . | . . | .                                          (x)))
. . . . . | . . | .        ⇒
. . . . . | . . | .        s(i;t).x = s(i;t+1).x)
. . . . . | . . | .     & (∀l:IdLnk, tg:Id.
. . . . . | . . | .        ¬...
. . . . . | . . | .        ⇒
. . . . . | . . | .        w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . | . . | . 13. ∀x:Id.
. . . . . | . . | .     deq-member(IdDeq;x;1of())
. . . . . | . . | .     ⇒
. . . . . | . . | .     s(i;0).x = 2of()(x)
```

```
. . . . . | . . | . 14. ∀a@0:Action(i).
. . . . . | . . | .     ¬isnull(a@0)
. . . . . | . . | .     ⇒
. . . . . | . . | .     (valtype(i;a@0) ⊆r <[locl(a)]
. . . . . | . . | .                        ,λx.T>(kind(a@0))?Top)
. . . . . | . . | . 15. ∀x:Id.
. . . . . | . . | .     vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(
. . . . . | . . | .                                          ds))→
. . . . . | . . | .                          2of(ds)(x)
. . . . . | . . | .                       else Top fi
. . . . . | . . | . 16. IdDeq ∈ EqDecider(Id)
. . . . . | . . | . 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . . | . . | . 18. j : Id
. . . . . | . . | . 19. t : ℕ
. . . . . | . . | . 20. j = i
. . . . . | . . | . 21. ¬isnull(a(j;t))
. . . . . | . . | . 22. ¬isnull(a(i;t))
. . . . . | . . | . 23. (λx.s(i;t).x) ∈ State(ds)
. . . . . | . . | . 24. t' : ℕ
. . . . . | . . | . 25. t+1≤t'
. . . . . | . . | . 26. ¬isnull(a(i;t'))
. . . . . | . . | . 27. kind(a(i;t')) = locl(a)
. . . . . | . . | . 28. e1 : Id
. . . . . | . . | . 29. e2 : ℕ
. . . . . | . . | . 30. ¬isnull(a(1of(<e1,e2>);2of(<e1,e2>)))
. . . . . | . . | . 31. <j,t> ∈ E
. . . . . | . . | . 32. <j,t> = <e1,e2>
. . . . . | . . | . 33. T
. . . . . | . . | . 34. Id
. . . . . | . . | . ⊢  e1 = i
. . . . . | . . | .   by ApFunToHypEquands 'Z' 1of(Z) Id -3
. . . . . | . . | .      THEN

. . . . . | . . | .      Reduce -1
. . . . . | . . |
. . . . . | . . .\
. . . . . | . . . 1. i : Id
. . . . . | . . . 2. a : Id
. . . . . | . . . 3. T : Type
. . . . . | . . . 4. ds : x:Id fp-> Type
. . . . . | . . . 5. P : State(ds)→T→Prop
. . . . . | . . . 6. w : World
. . . . . | . . . 7. FairFifo
. . . . . | . . . 8. FairFifo
. . . . . | . . . 9. ∀l:IdLnk, tg:Id.
. . . . . | . . .    (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | . . .                      <ds
. . . . . | . . .                      ,<[locl(a)],λx.T>
. . . . . | . . .                      ,
. . . . . | . . .                      ,<[a],λx.P>
. . . . . | . . .                      ,
. . . . . | . . .                      ,
. . . . . | . . .                      ,
. . . . . | . . .                      ,
. . . . . | . . .                      ,·>
. . . . . | . . .                  else  fi.da(rcv(l; tg))
```

```
. . . . . | . . . 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . . | . . . 11. ∀a@0:Id, t:ℕ.
. . . . . | . . .     ∃t':ℕ.
. . . . . | . . .     t≤t'
. . . . . | . . .     & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . . | . . .       ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . . | . . .       ∨ P@0 != <[a]
. . . . . | . . .                ,λx.
. . . . . | . . .                 P>(a@0) ==> ∀v:<[locl(a)]
. . . . . | . . .                                ,λx.
. . . . . | . . .                                 T>(locl(a@0))?Top.
. . . . . | . . .         ¬P@0((λx.s(i;t').x),v)
. . . . . | . . . 12. ∀t:ℕ.
. . . . . | . . .     ¬isnull(a(i;t))
. . . . . | . . .     ⇒
. . . . . | . . .     (islocal(kind(a(i;t)))
. . . . . | . . .      ⇒
. . . . . | . . .      (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . . | . . .      ⇒
. . . . . | . . .      P((λx.s(i;t).x),val(a(i;t))))
. . . . . | . . .     & (∀x:Id.
. . . . . | . . .        deq-member(...;<kind(a(i;t)),x>;1of())
. . . . . | . . .        ⇒
. . . . . | . . .        s(i;t+1).x
. . . . . | . . .        =
. . . . . | . . .        2of()
. . . . . | . . .        (<kind(a(i;t)),x>
. . . . . | . . .        ,λx.s(i;t).x
. . . . . | . . .        ,val(a(i;t))))
. . . . . | . . .     & (∀l:IdLnk.
. . . . . | . . .        deq-member(...;<kind(a(i;t)),l>;1of())
. . . . . | . . .        ⇒
. . . . . | . . .        withlnk(l;m(i;t))
. . . . . | . . .        =
. . . . . | . . .        if source(l) = i→
. . . . . | . . .           concat(map(λtgf.map(λx.
. . . . . | . . .           <1of(tgf),x>;2of(tgf)
. . . . . | . . .                       ((λx.s(i;t).x)
. . . . . | . . .                       ,val(a(i;t))));2of()
. . . . . | . . .                                     (<kind(a(i;t))
. . . . . | . . .                                      ,l>)))
. . . . . | . . .        else nil fi)
. . . . . | . . .     & (∀x:Id.
. . . . . | . . .        ¬(deq-member(IdDeq;x;1of())
. . . . . | . . .          ⇒
. . . . . | . . .          deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . . . . | . . .        ⇒
. . . . . | . . .        s(i;t).x = s(i;t+1).x)
. . . . . | . . .     & (∀l:IdLnk, tg:Id.
. . . . . | . . .        ¬(deq-member(...;<l,tg>;1of())
. . . . . | . . .          ⇒
. . . . . | . . .          deq-member(KindDeq;kind(a(i;t));2of()
. . . . . | . . .                                          (<l,tg>)))
. . . . . | . . .        ⇒
. . . . . | . . .        w-tagged(tg; onlnk(l;m(i;t))) = nil)
```

```
. . . . . | . . . 13. ∀x:Id.
. . . . . | . . .     deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . . . . | . . . 14. ∀a@0:Action(i).
. . . . . | . . .     ¬isnull(a@0)
. . . . . | . . .     ⇒
. . . . . | . . .     (valtype(i;a@0) ⊆r <[locl(a)]
. . . . . | . . .                        ,λx.T>(kind(a@0))?Top)
. . . . . | . . . 15. ∀x:Id.
. . . . . | . . .     vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . . . . | . . .                        2of(ds)(x)
. . . . . | . . .                     else Top fi
. . . . . | . . . 16. IdDeq ∈ EqDecider(Id)
. . . . . | . . . 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . . | . . . 18. j : Id
. . . . . | . . . 19. t : ℕ
. . . . . | . . . 20. j = i
. . . . . | . . . 21. ¬isnull(a(j;t))
. . . . . | . . . 22. ¬isnull(a(i;t))
. . . . . | . . . 23. (λx.s(i;t).x) ∈ State(ds)
. . . . . | . . . 24. t' : ℕ
. . . . . | . . . 25. t+1≤t'
. . . . . | . . . 26. ¬isnull(a(i;t'))
. . . . . | . . . 27. kind(a(i;t')) = locl(a)
. . . . . | . . . 28. e1 : Id
. . . . . | . . . 29. e2 : ℕ
. . . . . | . . . 30. ¬isnull(a(1of(<e1,e2>);2of(<e1,e2>)))
. . . . . | . . . 31. <j,t> ∈ E
. . . . . | . . . 32. j = loc(<e1,e2>) & <j,t> <c <e1,e2>
. . . . . | . . .     ∨ <j,t> = <e1,e2>
. . . . . | . . . 33. T
. . . . . | . . . 34. z : Id
. . . . . | . . . ⊢  vartype(i;z) ⊆r ds(z)?Top  by BackThruSomeHyp
. . . . . |
. . . . . |\
. . . . . | 1. i : Id
. . . . . | 2. a : Id
. . . . . | 3. T : Type
. . . . . | 4. ds : x:Id fp-> Type
. . . . . | 5. P : State(ds)→T→Prop
. . . . . | 6. w : World
. . . . . | 7. p : FairFifo
. . . . . | 8. FairFifo
. . . . . | 9. ∀l:IdLnk, tg:Id.
. . . . . |    (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . |                       <ds
. . . . . |                       ,<[locl(a)],λx.T>
. . . . . |                       ,
. . . . . |                       ,<[a],λx.P>
. . . . . |                       ,
. . . . . |                       ,
. . . . . |                       ,
. . . . . |                       ,
. . . . . |                       ,·>
. . . . . |                    else  fi.da(rcv(l; tg))
. . . . . | 10. (eqof(IdDeq)(i,i)) ∼ true₂
```

```
. . . . . | 11. ∀a@0:Id, t:ℕ.
. . . . . |     ∃t':ℕ.
. . . . . |     t≤t'
. . . . . |     & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . . |       ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . . |       ∨ P@0 != <[a],λx.P>(a@0) ==> ∀v:<[locl(a)]
. . . . . |                                        ,λx.
. . . . . |                                         T>(locl(a@0))?Top.
. . . . . |         ¬P@0((λx.s(i;t').x),v)
. . . . . | 12. ∀t:ℕ.
. . . . . |     ¬isnull(a(i;t))
. . . . . |     ⇒
. . . . . |     (islocal(kind(a(i;t)))
. . . . . |      ⇒
. . . . . |      (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . . |      ⇒
. . . . . |      P((λx.s(i;t).x),val(a(i;t))))
. . . . . |     & (∀x:Id.
. . . . . |        deq-member(product-deq(Knd;Id;KindDeq;...);<...
. . . . . |                                                  ,x>;1of(
. . . . . |                                                      ))
. . . . . |        ⇒
. . . . . |        s(i;t+1).x
. . . . . |        =
. . . . . |        2of()(<kind(a(i;t)),x>,λx.s(i;t).x,val(a(i;t))))
. . . . . |     & (∀l:IdLnk.
. . . . . |        deq-member(product-deq(Knd;IdLnk;...;...);<...
. . . . . |                                                ,l>;1of(
. . . . . |                                                    ))
. . . . . |        ⇒
. . . . . |        withlnk(l;m(i;t))
. . . . . |        =
. . . . . |        if source(l) = i→
. . . . . |           concat(map(λtgf.map(λx.
. . . . . |           <1of(tgf),x>;2of(tgf)
. . . . . |                       ((λx.s(i;t).x)
. . . . . |                       ,val(a(i;t))));2of()
. . . . . |                                      (<kind(a(i;t)),l>)))
. . . . . |        else nil fi)
. . . . . |     & (∀x:Id.
. . . . . |        ¬(deq-member(IdDeq;x;1of())
. . . . . |          ⇒
. . . . . |          deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . . . . |        ⇒
. . . . . |        s(i;t).x = s(i;t+1).x)
. . . . . |     & (∀l:IdLnk, tg:Id.
. . . . . |        ¬(deq-member(product-deq(IdLnk;Id;...;...);...;1of(
. . . . . |                                                      ))
. . . . . |          ⇒
. . . . . |          deq-member(KindDeq;kind(a(i;t));2of()(<l,tg>)))
. . . . . |        ⇒
. . . . . |        w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . | 13. ∀x:Id.
. . . . . |     deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . . . . | 14. ∀a@0:Action(i).
```

```
. . . . . |     ¬isnull(a@0)
. . . . . |     ⇒
. . . . . |     (valtype(i;a@0) ⊆r <[locl(a)],λx.T>(kind(a@0))?Top)
. . . . . | 15. ∀x:Id.
. . . . . |     vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . . . . |                         2of(ds)(x)
. . . . . |                       else Top fi
. . . . . | 16. IdDeq ∈ EqDecider(Id)
. . . . . | 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . . | 18. j : Id
. . . . . | 19. t : ℕ
. . . . . | 20. j = i
. . . . . | 21. ¬isnull(a(j;t))
. . . . . | 22. ¬isnull(a(i;t))
. . . . . | 23. (λx.s(i;t).x) ∈ State(ds)
. . . . . | 24. t' : ℕ
. . . . . | 25. t+1≤t'
. . . . . | 26. ¬locl(a) ∈ dom(<[locl(a)],λx.T>)
. . . . . | ⊢  ∃e':E.
. . . . . |    (<j,t> <loc e') ∨ <j,t> = e'
. . . . . |    & kind(e') = locl(a) ∨ (∀v:T. ¬P((λz.(z after e')),v))
. . . . . |   by Analyze -1 THEN Unfold `fpf-dom` 0 THEN Reduce 0
. . . . . |      THEN
. . . . . |      RWO
. . . . . |      Thm* ∀d:EqDecider(A), i:A. (eqof(d)(i,i)) ∼ true₂
. . . . . |      {eqof_eq_btrue}
. . . . . |      0
. . . . . |      THEN
. . . . . |      Reduce 0
. . . . . |      THEN
. . . . . |      Try (Complete Auto)
. . . . . |
. . . . . .\
. . . . . . 1. i : Id
. . . . . . 2. a : Id
. . . . . . 3. T : Type
. . . . . . 4. ds : x:Id fp-> Type
. . . . . . 5. P : State(ds)→T→Prop
. . . . . . 6. w : World
. . . . . . 7. p : FairFifo
. . . . . . 8. FairFifo
. . . . . . 9. ∀l:IdLnk, tg:Id.
. . . . . . |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . . |                   <ds
. . . . . . |                   ,<[locl(a)],λx.T>
. . . . . . |                   ,
. . . . . . |                   ,<[a],λx.P>
. . . . . . |                   ,
. . . . . . |                   ,
. . . . . . |                   ,
. . . . . . |                   ,
. . . . . . |                   ,.>
. . . . . . |                 else  fi.da(rcv(l; tg))
. . . . . . 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . . . 11. ∀a@0:Id, t:ℕ.
```

```
. . . . . |   ∃t':ℕ.
. . . . . |   t≤t'
. . . . . |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . . |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . . |     ∨ P@0 != <[a],λx.P>(a@0) ==> ∀v:<[locl(a)]
. . . . . |                                      ,λx.
. . . . . |                                       T>(locl(a@0))?Top.
. . . . . |       ¬P@0((λx.s(i;t').x),v)
. . . . . 12. ∀t:ℕ.
. . . . . |   ¬isnull(a(i;t))
. . . . . |   ⇒
. . . . . |   (islocal(kind(a(i;t)))
. . . . . |    ⇒
. . . . . |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . . |    ⇒
. . . . . |    P((λx.s(i;t).x),val(a(i;t))))
. . . . . |   & (∀x:Id.
. . . . . |      deq-member(product-deq(Knd;Id;KindDeq;...);<...
. . . . . |                                                 ,x>;1of(
. . . . . |                                                     ))
. . . . . |      ⇒
. . . . . |      s(i;t+1).x
. . . . . |      =
. . . . . |      2of()(<kind(a(i;t)),x>,λx.s(i;t).x,val(a(i;t))))
. . . . . |   & (∀l:IdLnk.
. . . . . |      deq-member(product-deq(Knd;IdLnk;...;...);<...
. . . . . |                                               ,l>;1of(
. . . . . |                                                   ))
. . . . . |      ⇒
. . . . . |      withlnk(l;m(i;t))
. . . . . |      =
. . . . . |      if source(l) = i→
. . . . . |         concat(map(λtgf.map(λx.
. . . . . |         <1of(tgf),x>;2of(tgf)
. . . . . |                      ((λx.s(i;t).x)
. . . . . |                      ,val(a(i;t))));2of()
. . . . . |                                    (<kind(a(i;t)),l>)))
. . . . . |      else nil fi)
. . . . . |   & (∀x:Id.
. . . . . |      ¬(deq-member(IdDeq;x;1of())
. . . . . |        ⇒
. . . . . |        deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . . . . |      ⇒
. . . . . |      s(i;t).x = s(i;t+1).x)
. . . . . |   & (∀l:IdLnk, tg:Id.
. . . . . |      ¬(deq-member(product-deq(IdLnk;Id;...;...);...;1of(
. . . . . |                                                     ))
. . . . . |        ⇒
. . . . . |        deq-member(KindDeq;kind(a(i;t));2of()(<l,tg>)))
. . . . . |      ⇒
. . . . . |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . 13. ∀x:Id.
. . . . . |   deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . . . . 14. ∀a@0:Action(i).
. . . . . |   ¬isnull(a@0)
```

```
. . . . . | ⇒
. . . . . | (valtype(i;a@0) ⊆r <[locl(a)],λx.T>(kind(a@0))?Top)

. . . . . 15. ∀x:Id.
. . . . . | vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . . . . |                    2of(ds)(x)
. . . . . |                  else Top fi
. . . . . 16. IdDeq ∈ EqDecider(Id)
. . . . . 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . . 18. j : Id
. . . . . 19. t : ℕ
. . . . . 20. j = i
. . . . . 21. ¬isnull(a(j;t))
. . . . . 22. ¬isnull(a(i;t))
. . . . . 23. (λx.s(i;t).x) ∈ State(ds)
. . . . . 24. t' : ℕ
. . . . . 25. t+1≤t'
. . . . . 26. P@0 != <[a],λx.P>(a) ==> ∀v:<[locl(a)]
. . . . . |                                ,λx.T>(locl(a@0))?Top.
. . . . . | ¬P@0((λx.s(i;t').x),v)
. . . . . ⊢ ∃e':E.
. . . . . | (<j,t> <loc e') ∨ <j,t> = e'
. . . . . | & kind(e') = locl(a) ∨ (∀v:T. ¬P((λz.(z after e')),v))
. . . . . | by Fold `fpf-single` -1 THEN Reduce -1 THEN Analyze -1
. . . . . |
. . . . . 1. i : Id
. . . . . 2. a : Id
. . . . . 3. T : Type
. . . . . 4. ds : x:Id fp-> Type
. . . . . 5. P : State(ds)→T→Prop
. . . . . 6. w : World
. . . . . 7. p : FairFifo
. . . . . 8. FairFifo
. . . . . 9. ∀l:IdLnk, tg:Id.
. . . . . | (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . |                  <ds
. . . . . |                  ,<[locl(a)],λx.T>
. . . . . |                  ,
. . . . . |                  ,<[a],λx.P>
. . . . . |                  ,
. . . . . |                  ,
. . . . . |                  ,
. . . . . |                  ,
. . . . . |                  ,•>
. . . . . |               else  fi.da(rcv(l; tg))
. . . . . 10. (eqof(IdDeq)(i,i)) ~ true₂
. . . . . 11. ∀a@0:Id, t:ℕ.
. . . . . | ∃t':ℕ.
. . . . . | t≤t'
. . . . . | & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . . |   ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . . |   ∨ P@0 != <[a],λx.P>(a@0) ==> ∀v:<[locl(a)]
. . . . . |                                    ,λx.
. . . . . |                                     T>(locl(a@0))?Top.
. . . . . |     ¬P@0((λx.s(i;t').x),v)
. . . . . 12. ∀t:ℕ.
```

```
. . . . . |   ¬isnull(a(i;t))
. . . . . |   ⇒
. . . . . |   (islocal(kind(a(i;t)))
. . . . . |    ⇒
. . . . . |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . . |    ⇒
. . . . . |    P((λx.s(i;t).x),val(a(i;t))))
. . . . . |   & (∀x:Id.
. . . . . |      deq-member(product-deq(Knd;Id;KindDeq;...);<...
. . . . . |                                                ,x>;1of(
. . . . . |                                                    ))
. . . . . |      ⇒
. . . . . |      s(i;t+1).x
. . . . . |      =
. . . . . |      2of()(<kind(a(i;t)),x>,λx.s(i;t).x,val(a(i;t))))
. . . . . |   & (∀l:IdLnk.
. . . . . |      deq-member(product-deq(Knd;IdLnk;...;...);<...
. . . . . |                                              ,l>;1of(
. . . . . |                                                  ))
. . . . . |      ⇒
. . . . . |      withlnk(l;m(i;t))
. . . . . |      =
. . . . . |      if source(l) = i→
. . . . . |         concat(map(λtgf.map(λx.
. . . . . |         <1of(tgf),x>;2of(tgf)
. . . . . |                     ((λx.s(i;t).x)
. . . . . |                     ,val(a(i;t))));2of()
. . . . . |                                    (<kind(a(i;t)),l>)))
. . . . . |      else nil fi)
. . . . . |   & (∀x:Id.
. . . . . |      ¬(deq-member(IdDeq;x;1of())
. . . . . |        ⇒
. . . . . |        deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . . . . |      ⇒
. . . . . |      s(i;t).x = s(i;t+1).x)
. . . . . |   & (∀l:IdLnk, tg:Id.
. . . . . |      ¬(deq-member(product-deq(IdLnk;Id;...;...);...;1of(
. . . . . |                                                    ))
. . . . . |        ⇒
. . . . . |        deq-member(KindDeq;kind(a(i;t));2of()(<l,tg>)))
. . . . . |      ⇒
. . . . . |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . 13. ∀x:Id.
. . . . . |   deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . . . . 14. ∀a@0:Action(i).
. . . . . |   ¬isnull(a@0)
. . . . . |   ⇒
. . . . . |   (valtype(i;a@0) ⊆r <[locl(a)],λx.T>(kind(a@0))?Top)
. . . . . 15. ∀x:Id.
. . . . . |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . . . . |                      2of(ds)(x)
. . . . . |                  else Top fi
. . . . . 16. IdDeq ∈ EqDecider(Id)
. . . . . 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . . 18. j : Id
```

```
. . . . . 19. t : ℕ
. . . . . 20. j = i
. . . . . 21. ¬isnull(a(j;t))
. . . . . 22. ¬isnull(a(i;t))
. . . . . 23. (λx.s(i;t).x) ∈ State(ds)
. . . . . 24. t' : ℕ
. . . . . 25. t+1≤t'
. . . . . 26. ∀v:T. ¬P((λx.s(i;t').x),v)
. . . . . ⊢  ∃e':E.
. . . . . |  (<j,t> <loc e') ∨ <j,t> = e'
. . . . . |  & kind(e') = locl(a) ∨ (∀v:T. ¬P((λz.(z after e')),v))
. . . . . | by Assert
. . . . . |    (∃t2:ℕ.
. . . . . |     t2<t'
. . . . . |     & ¬isnull(a(i;t2))
. . . . . |     & (∀t3:ℕ. t2<t3 & t3<t' ⇒ isnull(a(i;t3))))
. . . . . |
. . . . . |\
. . . . . | .....assertion .....
. . . . . | 1. i : Id
. . . . . | 2. a : Id
. . . . . | 3. T : Type
. . . . . | 4. ds : x:Id fp-> Type
. . . . . | 5. P : State(ds)→T→Prop
. . . . . | 6. w : World
. . . . . | 7. FairFifo
. . . . . | 8. FairFifo
. . . . . | 9. ∀l:IdLnk, tg:Id.
. . . . . | |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | |                    <ds
. . . . . | |                    ,<[locl(a)],λx.T>
. . . . . | |                    ,
. . . . . | |                    ,<[a],λx.P>
. . . . . | |                    ,
. . . . . | |                    ,
. . . . . | |                    ,
. . . . . | |                    ,
. . . . . | |                    ,.>
. . . . . | |                 else  fi.da(rcv(l; tg))
. . . . . | 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . . | 11. ∀a@0:Id, t:ℕ.
. . . . . | |   ∃t':ℕ.
. . . . . | |   t≤t'
. . . . . | |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . . | |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . . | |     ∨ P@0 != <[a]
. . . . . | |              ,λx.P>(a@0) ==> ∀v:<[locl(a)]
. . . . . | |                                  ,λx.T>(locl(a@0))?Top.
. . . . . | |       ¬P@0((λx.s(i;t').x),v)
. . . . . | 12. ∀t:ℕ.
. . . . . | |   ¬isnull(a(i;t))
. . . . . | |   ⇒
. . . . . | |   (islocal(kind(a(i;t)))
. . . . . | |    ⇒
. . . . . | |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
```

```
. . . . . | |    ⇒
. . . . . | |    P((λx.s(i;t).x),val(a(i;t))))
. . . . . | |   & (∀x:Id.
. . . . . | |      deq-member(product-deq(Knd;Id;...;IdDeq);<...
. . . . . | |                                              ,x>;1of(
. . . . . | |                                                  ))
. . . . . | |      ⇒
. . . . . | |      s(i;t+1).x
. . . . . | |      =
. . . . . | |      2of()(<kind(a(i;t)),x>,λx.s(i;t).x,val(a(i;t))))
. . . . . | |   & (∀l:IdLnk.
. . . . . | |      deq-member(product-deq(Knd;...;...;...);<...
. . . . . | |                                             ,l>;1of(
. . . . . | |                                                 ))
. . . . . | |      ⇒
. . . . . | |      withlnk(l;m(i;t))
. . . . . | |      =
. . . . . | |      if source(l) = i→
. . . . . | |         concat(map(λtgf.map(λx.
. . . . . | |         <1of(tgf)
. . . . . | |         ,x>;2of(tgf)
. . . . . | |             ((λx.s(i;t).x)
. . . . . | |             ,val(a(i;t))));2of()(<kind(a(i;t)),l>)))
. . . . . | |      else nil fi)
. . . . . | |   & (∀x:Id.
. . . . . | |      ¬(deq-member(IdDeq;x;1of())
. . . . . | |        ⇒
. . . . . | |        deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . . . . | |      ⇒
. . . . . | |      s(i;t).x = s(i;t+1).x)
. . . . . | |   & (∀l:IdLnk, tg:Id.
. . . . . | |      ¬(deq-member(product-deq(...;Id;...;...);...;1of(
. . . . . | |                                                  ))
. . . . . | |        ⇒
. . . . . | |        deq-member(KindDeq;kind(a(i;t));2of()(<l,tg>)))
. . . . . | |      ⇒
. . . . . | |      w-tagged(tg; onlnk(l;m(i;t))) = nil)

. . . . . | 13. ∀x:Id.
. . . . . | |   deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . . . . | 14. ∀a@0:Action(i).
. . . . . | |   ¬isnull(a@0)
. . . . . | |   ⇒
. . . . . | |   (valtype(i;a@0) ⊆r <[locl(a)],λx.T>(kind(a@0))?Top)
. . . . . | 15. ∀x:Id.
. . . . . | |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . . . . | |                      2of(ds)(x)
. . . . . | |                   else Top fi
. . . . . | 16. IdDeq ∈ EqDecider(Id)
. . . . . | 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . . | 18. j : Id
. . . . . | 19. t : ℕ
. . . . . | 20. j = i
. . . . . | 21. ¬isnull(a(j;t))
. . . . . | 22. ¬isnull(a(i;t))
. . . . . | 23. (λx.s(i;t).x) ∈ State(ds)
```

```
. . . . . | 24. t' : ℕ
. . . . . | 25. t+1≤t'
. . . . . | 26. ∀v:T. ¬P((λx.s(i;t').x),v)
. . . . . | ⊢  ∃t2:ℕ.
. . . . . | |  t2<t'
. . . . . | |  & ¬isnull(a(i;t2))
. . . . . | |  & (∀t3:ℕ. t2<t3 & t3<t' ⇒ isnull(a(i;t3)))
. . . . . | | by Thin -1 THEN MoveToConcl -1 THEN MoveToConcl -1
. . . . . | |    THEN
. . . . . | |    InductionOnNat
. . . . . | |
. . . . . | |\
. . . . . | | .....basecase .....
. . . . . | | 1. i : Id
. . . . . | | 2. a : Id
. . . . . | | 3. T : Type
. . . . . | | 4. ds : x:Id fp-> Type
. . . . . | | 5. P : State(ds)→T→Prop
. . . . . | | 6. w : World
. . . . . | | 7. FairFifo
. . . . . | | 8. FairFifo
. . . . . | | 9. ∀l:IdLnk, tg:Id.
. . . . . | |    (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | |                       <ds
. . . . . | |                       ,<[locl(a)],λx.T>
. . . . . | |                       ,
. . . . . | |                       ,<[a],λx.P>
. . . . . | |                       ,
. . . . . | |                       ,
. . . . . | |                       ,
. . . . . | |                       ,
. . . . . | |                       ,·>
. . . . . | |                    else  fi.da(rcv(l; tg))
. . . . . | | 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . . | | 11. ∀a@0:Id, t:ℕ.
. . . . . | |     ∃t':ℕ.
. . . . . | |     t≤t'
. . . . . | |     & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . . | |       ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . . | |       ∨ P@0 != <[a]
. . . . . | |                ,λx.P>(a@0) ==> ∀v:<[locl(a)]
. . . . . | |                                  ,λx.
. . . . . | |                                   T>(locl(a@0))?Top.
. . . . . | |         ¬P@0((λx.s(i;t').x),v)
. . . . . | | 12. ∀t:ℕ.
. . . . . | |     ¬isnull(a(i;t))
. . . . . | |     ⇒
. . . . . | |     (islocal(kind(a(i;t)))
. . . . . | |      ⇒
. . . . . | |      (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . . | |      ⇒
. . . . . | |      P((λx.s(i;t).x),val(a(i;t))))
. . . . . | |     & (∀x:Id.
. . . . . | |        deq-member(product-deq(Knd;Id;...;...);<...
. . . . . | |                                              ,x>;1of(
```

```
. . . . . | |                                                    ))
. . . . . | |        ⇒
. . . . . | |        s(i;t+1).x
. . . . . | |        =
. . . . . | |        2of()
. . . . . | |        (<kind(a(i;t)),x>
. . . . . | |        ,λx.s(i;t).x
. . . . . | |        ,val(a(i;t))))
. . . . . | |     & (∀l:IdLnk.
. . . . . | |        deq-member(...;<kind(a(i;t)),l>;1of())
. . . . . | |        ⇒
. . . . . | |        withlnk(l;m(i;t))
. . . . . | |        =
. . . . . | |        if source(l) = i→
. . . . . | |           concat(map(λtgf.map(λx.
. . . . . | |           <1of(tgf),x>;2of(tgf)
. . . . . | |                       ((λx.s(i;t).x)
. . . . . | |                       ,val(a(i;t))));2of()
. . . . . | |                                    (<kind(a(i;t))
. . . . . | |                                     ,l>)))
. . . . . | |        else nil fi)
. . . . . | |     & (∀x:Id.
. . . . . | |        ¬(deq-member(IdDeq;x;1of())
. . . . . | |          ⇒
. . . . . | |          deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . . . . | |        ⇒
. . . . . | |        s(i;t).x = s(i;t+1).x)
. . . . . | |     & (∀l:IdLnk, tg:Id.
. . . . . | |        ¬(deq-member(...;<l,tg>;1of())
. . . . . | |          ⇒
. . . . . | |          deq-member(KindDeq;kind(a(i;t));2of()
. . . . . | |                                          (<l,tg>)))
. . . . . | |        ⇒
. . . . . | |        w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . | | 13. ∀x:Id.
. . . . . | |     deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . . . . | | 14. ∀a@0:Action(i).
. . . . . | |     ¬isnull(a@0)
. . . . . | |     ⇒
. . . . . | |     (valtype(i;a@0) ⊆r <[locl(a)]
. . . . . | |                        ,λx.T>(kind(a@0))?Top)
. . . . . | | 15. ∀x:Id.
. . . . . | |     vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . . . . | |                        2of(ds)(x)
. . . . . | |                     else Top fi
. . . . . | | 16. IdDeq ∈ EqDecider(Id)
. . . . . | | 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . . | | 18. j : Id
. . . . . | | 19. t : ℕ
. . . . . | | 20. j = i
. . . . . | | 21. ¬isnull(a(j;t))
. . . . . | | 22. ¬isnull(a(i;t))
. . . . . | | 23. (λx.s(i;t).x) ∈ State(ds)
. . . . . | | ⊢  t+1≤0
. . . . . | |    ⇒
```

```
. . . . . | |    (∃t2:ℕ.
. . . . . | |     t2<0
. . . . . | |     & ¬isnull(a(i;t2))
. . . . . | |     & (∀t3:ℕ. t2<t3 & t3<0 ⇒ isnull(a(i;t3))))
. . . . . | |   by Auto
. . . . . | |
. . . . . | .\
. . . . . | . .....upcase .....
. . . . . | . 1. i : Id
. . . . . | . 2. a : Id
. . . . . | . 3. T : Type
. . . . . | . 4. ds : x:Id fp-> Type
. . . . . | . 5. P : State(ds)→T→Prop
. . . . . | . 6. w : World
. . . . . | . 7. FairFifo
. . . . . | . 8. FairFifo
. . . . . | . 9. ∀l:IdLnk, tg:Id.
. . . . . | . |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | . |                  <ds
. . . . . | . |                  ,<[locl(a)],λx.T>
. . . . . | . |                  ,
. . . . . | . |                  ,<[a],λx.P>
. . . . . | . |                  ,
. . . . . | . |                  ,
. . . . . | . |                  ,
. . . . . | . |                  ,
. . . . . | . |                  ,.>
. . . . . | . |               else  fi.da(rcv(l; tg))
. . . . . | . 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . . | . 11. ∀a@0:Id, t:ℕ.
. . . . . | . |   ∃t':ℕ.
. . . . . | . |   t≤t'
. . . . . | . |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . . | . |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . . | . |     ∨ P@0 != <[a]
. . . . . | . |             ,λx.P>(a@0) ==> ∀v:<[locl(a)]
. . . . . | . |                                ,λx.
. . . . . | . |                                 T>(locl(a@0))?Top.
. . . . . | . |       ¬P@0((λx.s(i;t').x),v)
. . . . . | . 12. ∀t:ℕ.
. . . . . | . |   ¬isnull(a(i;t))
. . . . . | . |   ⇒
. . . . . | . |   (islocal(kind(a(i;t)))
. . . . . | . |    ⇒
. . . . . | . |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . . | . |    ⇒
. . . . . | . |    P((λx.s(i;t).x),val(a(i;t))))
. . . . . | . |   & (∀x:Id.
. . . . . | . |      deq-member(product-deq(Knd;Id;...;...);<...
. . . . . | . |                                          ,x>;1of(
. . . . . | . |                                              ))
. . . . . | . |      ⇒
. . . . . | . |      s(i;t+1).x
. . . . . | . |      =
. . . . . | . |      2of()
```

```
. . . . . | . |      (<kind(a(i;t)),x>
. . . . . | . |      ,λx.s(i;t).x
. . . . . | . |      ,val(a(i;t))))
. . . . . | . |   & (∀l:IdLnk.
. . . . . | . |      deq-member(...;<kind(a(i;t)),l>;1of())
. . . . . | . |      ⇒
. . . . . | . |      withlnk(l;m(i;t))
. . . . . | . |      =
. . . . . | . |      if source(l) = i→
. . . . . | . |         concat(map(λtgf.map(λx.
. . . . . | . |         <1of(tgf),x>;2of(tgf)
. . . . . | . |                     ((λx.s(i;t).x)
. . . . . | . |                     ,val(a(i;t))));2of()
. . . . . | . |                                    (<kind(a(i;t))
. . . . . | . |                                     ,l>)))
. . . . . | . |      else nil fi)
. . . . . | . |   & (∀x:Id.

. . . . . | . |      ¬(deq-member(IdDeq;x;1of())
. . . . . | . |        ⇒
. . . . . | . |        deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . . . . | . |      ⇒
. . . . . | . |      s(i;t).x = s(i;t+1).x)
. . . . . | . |   & (∀l:IdLnk, tg:Id.
. . . . . | . |      ¬(deq-member(...;<l,tg>;1of())
. . . . . | . |        ⇒
. . . . . | . |        deq-member(KindDeq;kind(a(i;t));2of()
. . . . . | . |                                      (<l,tg>)))
. . . . . | . |      ⇒
. . . . . | . |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . | . 13. ∀x:Id.
. . . . . | . |   deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . . . . | . 14. ∀a@0:Action(i).
. . . . . | . |   ¬isnull(a@0)
. . . . . | . |   ⇒
. . . . . | . |   (valtype(i;a@0) ⊆r <[locl(a)]
. . . . . | . |                     ,λx.T>(kind(a@0))?Top)
. . . . . | . 15. ∀x:Id.
. . . . . | . |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . . . . | . |                     2of(ds)(x)
. . . . . | . |                  else Top fi
. . . . . | . 16. IdDeq ∈ EqDecider(Id)
. . . . . | . 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . . | . 18. j : Id
. . . . . | . 19. t : ℕ
. . . . . | . 20. j = i
. . . . . | . 21. ¬isnull(a(j;t))
. . . . . | . 22. ¬isnull(a(i;t))
. . . . . | . 23. (λx.s(i;t).x) ∈ State(ds)
. . . . . | . 24. t' : ℤ
. . . . . | . 25. 0<t'
. . . . . | . 26. t+1≤t'-1
. . . . . | . |   ⇒
. . . . . | . |   (∃t2:ℕ.
. . . . . | . |    t2<t'-1
. . . . . | . |    & ¬isnull(a(i;t2))
```

```
. . . . . | . |    & (∀t3:ℕ. t2<t3 & t3<t'-1 ⇒ isnull(a(i;t3))))
. . . . . | . ⊢  t+1≤t'
. . . . . | . |  ⇒
. . . . . | . |  (∃t2:ℕ.
. . . . . | . |   t2<t'
. . . . . | . |   & ¬isnull(a(i;t2))
. . . . . | . |   & (∀t3:ℕ. t2<t3 & t3<t' ⇒ isnull(a(i;t3))))
. . . . . | . | by Auto THEN Decide isnull(a(i;t'-1))
. . . . . | . |
. . . . . | . |\
. . . . . | . | 1. i : Id
. . . . . | . | 2. a : Id
. . . . . | . | 3. T : Type
. . . . . | . | 4. ds : x:Id fp-> Type
. . . . . | . | 5. P : State(ds)→T→Prop
. . . . . | . | 6. w : World
. . . . . | . | 7. FairFifo
. . . . . | . | 8. FairFifo
. . . . . | . | 9. ∀l:IdLnk, tg:Id.
. . . . . | . | |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | . | |                    <ds
. . . . . | . | |                    ,<[locl(a)],λx.T>
. . . . . | . | |                    ,
. . . . . | . | |                    ,<[a],λx.P>
. . . . . | . | |                    ,
. . . . . | . | |                    ,
. . . . . | . | |                    ,
. . . . . | . | |                    ,
. . . . . | . | |                    ,·>
. . . . . | . | |                else  fi.da(rcv(l; tg))
. . . . . | . | 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . . | . | 11. ∀a@0:Id, t:ℕ.
. . . . . | . | |   ∃t':ℕ.
. . . . . | . | |   t≤t'
. . . . . | . | |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . . | . | |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . . | . | |     ∨ P@0 != <[a]
. . . . . | . | |              ,λx.
. . . . . | . | |               P>(a@0) ==> ∀v:<[locl(a)]
. . . . . | . | |                                ,λx.
. . . . . | . | |                                 T>(locl(a@0))?Top.
. . . . . | . | |       ¬P@0((λx.s(i;t').x),v)
. . . . . | . | 12. ∀t:ℕ.
. . . . . | . | |   ¬isnull(a(i;t))
. . . . . | . | |   ⇒
. . . . . | . | |   (islocal(kind(a(i;t)))
. . . . . | . | |    ⇒
. . . . . | . | |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . . | . | |    ⇒
. . . . . | . | |    P((λx.s(i;t).x),val(a(i;t))))
. . . . . | . | |   & (∀x:Id.
. . . . . | . | |      deq-member(...;<kind(a(i;t)),x>;1of())
. . . . . | . | |      ⇒
. . . . . | . | |      s(i;t+1).x
. . . . . | . | |      =
```

```
. . . . . | . | |      2of()
. . . . . | . | |      (<kind(a(i;t)),x>
. . . . . | . | |      ,λx.s(i;t).x
. . . . . | . | |      ,val(a(i;t))))
. . . . . | . | |   & (∀l:IdLnk.
. . . . . | . | |      deq-member(...;<kind(a(i;t)),l>;1of())
. . . . . | . | |      ⇒
. . . . . | . | |      withlnk(l;m(i;t))
. . . . . | . | |      =
. . . . . | . | |      if source(l) = i→
. . . . . | . | |         concat(map(λtgf.map(λx.
. . . . . | . | |         <1of(tgf),x>;2of(tgf)
. . . . . | . | |                     ((λx.s(i;t).x)
. . . . . | . | |                     ,val(a(i;t))));2of()
. . . . . | . | |                                    (<kind(a(i;t))
. . . . . | . | |                                     ,l>)))
. . . . . | . | |      else nil fi)
. . . . . | . | |   & (∀x:Id.
. . . . . | . | |      ¬(deq-member(IdDeq;x;1of())
. . . . . | . | |        ⇒
. . . . . | . | |        deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . . . . | . | |      ⇒
. . . . . | . | |      s(i;t).x = s(i;t+1).x)
. . . . . | . | |   & (∀l:IdLnk, tg:Id.
. . . . . | . | |      ¬(deq-member(...;<l,tg>;1of())
. . . . . | . | |        ⇒
. . . . . | . | |        deq-member(KindDeq;kind(a(i;t));2of()
. . . . . | . | |                                      (<l,tg>)))
. . . . . | . | |      ⇒
. . . . . | . | |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . | . | 13. ∀x:Id.
. . . . . | . | |   deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . . . . | . | 14. ∀a@0:Action(i).
. . . . . | . | |   ¬isnull(a@0)
. . . . . | . | |   ⇒
. . . . . | . | |   (valtype(i;a@0) ⊆r <[locl(a)]
. . . . . | . | |                     ,λx.T>(kind(a@0))?Top)
. . . . . | . | 15. ∀x:Id.
. . . . . | . | |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . . . . | . | |                     2of(ds)(x)
. . . . . | . | |                  else Top fi
. . . . . | . | 16. IdDeq ∈ EqDecider(Id)
. . . . . | . | 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . . | . | 18. j : Id
. . . . . | . | 19. t : ℕ
. . . . . | . | 20. j = i
. . . . . | . | 21. ¬isnull(a(j;t))
. . . . . | . | 22. ¬isnull(a(i;t))
. . . . . | . | 23. (λx.s(i;t).x) ∈ State(ds)
. . . . . | . | 24. t' : ℤ
. . . . . | . | 25. 0<t'
. . . . . | . | 26. t+1≤t'-1
. . . . . | . | |   ⇒
. . . . . | . | |   (∃t2:ℕ.
. . . . . | . | |    t2<t'-1
```

```
. . . . . | . | |    & ¬isnull(a(i;t2))
. . . . . | . | |    & (∀t3:ℕ. t2<t3 & t3<t'-1 ⇒ isnull(a(i;t3))))
. . . . . | . | 27. t+1≤t'
. . . . . | . | 28. isnull(a(i;t'-1))
. . . . . | . | ⊢  ∃t2:ℕ.
. . . . . | . | |  t2<t'
. . . . . | . | |  & ¬isnull(a(i;t2))
. . . . . | . | |  & (∀t3:ℕ. t2<t3 & t3<t' ⇒ isnull(a(i;t3)))
. . . . . | . | | by Analyze -3
. . . . . | . | |
. . . . . | . | |\
. . . . . | . | | .....antecedent .....
. . . . . | . | | 1. i : Id
. . . . . | . | | 2. a : Id
. . . . . | . | | 3. T : Type
. . . . . | . | | 4. ds : x:Id fp-> Type
. . . . . | . | | 5. P : State(ds)→T→Prop
. . . . . | . | | 6. w : World
. . . . . | . | | 7. FairFifo
. . . . . | . | | 8. FairFifo
. . . . . | . | | 9. ∀l:IdLnk, tg:Id.
. . . . . | . | |    (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | . | |                      <ds
. . . . . | . | |                      ,<[locl(a)],λx.T>
. . . . . | . | |                      ,
. . . . . | . | |                      ,<[a],λx.P>
. . . . . | . | |                      ,
. . . . . | . | |                      ,
. . . . . | . | |                      ,
. . . . . | . | |                      ,
. . . . . | . | |                      ,.>
. . . . . | . | |                   else  fi.da(rcv(l; tg))
. . . . . | . | | 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . . | . | | 11. ∀a@0:Id, t:ℕ.
. . . . . | . | |     ∃t':ℕ.
. . . . . | . | |     t≤t'
. . . . . | . | |     & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . . | . | |       ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . . | . | |       ∨ P@0 != <[a]
. . . . . | . | |                ,λx.
. . . . . | . | |                 P>(a@0) ==> ∀v:<[locl(a)]
. . . . . | . | |                                ,λx.
. . . . . | . | |                                 T>(locl(a@0))?Top.
. . . . . | . | |         ¬P@0((λx.s(i;t').x),v)
. . . . . | . | | 12. ∀t:ℕ.
. . . . . | . | |     ¬isnull(a(i;t))
. . . . . | . | |     ⇒
. . . . . | . | |     (islocal(kind(a(i;t)))
. . . . . | . | |      ⇒
. . . . . | . | |      (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . . | . | |      ⇒
. . . . . | . | |      P((λx.s(i;t).x),val(a(i;t))))
. . . . . | . | |     & (∀x:Id.
. . . . . | . | |        deq-member(...;<kind(a(i;t)),x>;1of())
. . . . . | . | |        ⇒
```

```
. . . . . | . | |        s(i;t+1).x
. . . . . | . | |        =
. . . . . | . | |        2of()
. . . . . | . | |        (<kind(a(i;t)),x>
. . . . . | . | |        ,λx.s(i;t).x
. . . . . | . | |        ,val(a(i;t))))
. . . . . | . | |     & (∀l:IdLnk.
. . . . . | . | |        deq-member(...;<kind(a(i;t)),l>;1of())
. . . . . | . | |        ⇒
. . . . . | . | |        withlnk(l;m(i;t))
. . . . . | . | |        =
. . . . . | . | |        if source(l) = i→
. . . . . | . | |           concat(map(λtgf.map(λx.
. . . . . | . | |           <1of(tgf)
. . . . . | . | |           ,x>;2of(tgf)
. . . . . | . | |               ((λx.s(i;t).x)
. . . . . | . | |               ,val(a(i;t))));2of()
. . . . . | . | |                              (<kind(a(i;t)),l>)))
. . . . . | . | |        else nil fi)
. . . . . | . | |     & (∀x:Id.
. . . . . | . | |        ¬(deq-member(IdDeq;x;1of())
. . . . . | . | |          ⇒
. . . . . | . | |          deq-member(KindDeq;kind(a(i;t));2of()
. . . . . | . | |                                          (x)))
. . . . . | . | |        ⇒
. . . . . | . | |        s(i;t).x = s(i;t+1).x)
. . . . . | . | |     & (∀l:IdLnk, tg:Id.
. . . . . | . | |        ¬...
. . . . . | . | |        ⇒
. . . . . | . | |        w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . | . | | 13. ∀x:Id.
. . . . . | . | |     deq-member(IdDeq;x;1of())
. . . . . | . | |     ⇒
. . . . . | . | |     s(i;0).x = 2of()(x)
. . . . . | . | | 14. ∀a@0:Action(i).
. . . . . | . | |     ¬isnull(a@0)
. . . . . | . | |     ⇒
. . . . . | . | |     (valtype(i;a@0) ⊆r <[locl(a)]
. . . . . | . | |                        ,λx.T>(kind(a@0))?Top)
. . . . . | . | | 15. ∀x:Id.
. . . . . | . | |     vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(
. . . . . | . | |                                          ds))→
. . . . . | . | |                        2of(ds)(x)
. . . . . | . | |                    else Top fi
. . . . . | . | | 16. IdDeq ∈ EqDecider(Id)
. . . . . | . | | 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . . | . | | 18. j : Id
. . . . . | . | | 19. t : ℕ
. . . . . | . | | 20. j = i
. . . . . | . | | 21. ¬isnull(a(j;t))
. . . . . | . | | 22. ¬isnull(a(i;t))
. . . . . | . | | 23. (λx.s(i;t).x) ∈ State(ds)
. . . . . | . | | 24. t' : ℤ
. . . . . | . | | 25. 0<t'
. . . . . | . | | 26. t+1≤t'
```

```
. . . . . | . | | 27. isnull(a(i;t'-1))
. . . . . | . | | ⊢  t+1≤t'-1
. . . . . | . | |   by SupposeNot THEN Subst (t'-1 = t) -2
. . . . . | . | |
. . . . . | . | .\
. . . . . | . | . 1. i : Id
. . . . . | . | . 2. a : Id
. . . . . | . | . 3. T : Type
. . . . . | . | . 4. ds : x:Id fp-> Type
. . . . . | . | . 5. P : State(ds)→T→Prop
. . . . . | . | . 6. w : World
. . . . . | . | . 7. FairFifo
. . . . . | . | . 8. FairFifo
. . . . . | . | . 9. ∀l:IdLnk, tg:Id.
. . . . . | . | . |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | . | . |                    <ds
. . . . . | . | . |                    ,<[locl(a)],λx.T>
. . . . . | . | . |                    ,
. . . . . | . | . |                    ,<[a],λx.P>
. . . . . | . | . |                    ,
. . . . . | . | . |                    ,
. . . . . | . | . |                    ,
. . . . . | . | . |                    ,
. . . . . | . | . |                    ,.>
. . . . . | . | . |                 else  fi.da(rcv(l; tg))
. . . . . | . | . 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . . | . | . 11. ∀a@0:Id, t:ℕ.
. . . . . | . | . |   ∃t':ℕ.
. . . . . | . | . |   t≤t'
. . . . . | . | . |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . . | . | . |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . . | . | . |     ∨ P@0 != <[a]
. . . . . | . | . |              ,λx.
. . . . . | . | . |               P>(a@0) ==> ∀v:<[locl(a)]
. . . . . | . | . |                                ,λx.
. . . . . | . | . |                                 T>(locl(a@0))?Top.
. . . . . | . | . |       ¬P@0((λx.s(i;t').x),v)
. . . . . | . | . 12. ∀t:ℕ.
. . . . . | . | . |   ¬isnull(a(i;t))
. . . . . | . | . |   ⇒
. . . . . | . | . |   (islocal(kind(a(i;t)))
. . . . . | . | . |    ⇒
. . . . . | . | . |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . . | . | . |    ⇒
. . . . . | . | . |    P((λx.s(i;t).x),val(a(i;t))))
. . . . . | . | . |   & (∀x:Id.
. . . . . | . | . |      deq-member(...;<kind(a(i;t)),x>;1of())
. . . . . | . | . |      ⇒
. . . . . | . | . |      s(i;t+1).x
. . . . . | . | . |      =
. . . . . | . | . |      2of()
. . . . . | . | . |      (<kind(a(i;t)),x>
. . . . . | . | . |      ,λx.s(i;t).x
. . . . . | . | . |      ,val(a(i;t))))
. . . . . | . | . |   & (∀l:IdLnk.
```

```
. . . . . | . | . |      deq-member(...;<kind(a(i;t)),l>;1of())
. . . . . | . | . |      ⇒
. . . . . | . | . |      withlnk(l;m(i;t))
. . . . . | . | . |      =
. . . . . | . | . |      if source(l) = i→
. . . . . | . | . |         concat(map(λtgf.map(λx.
. . . . . | . | . |         <1of(tgf)
. . . . . | . | . |         ,x>;2of(tgf)
. . . . . | . | . |             ((λx.s(i;t).x)
. . . . . | . | . |             ,val(a(i;t))));2of()
. . . . . | . | . |                              (<kind(a(i;t)),l>)))
. . . . . | . | . |      else nil fi)
. . . . . | . | . |   & (∀x:Id.
. . . . . | . | . |      ¬(deq-member(IdDeq;x;1of())
. . . . . | . | . |        ⇒
. . . . . | . | . |        deq-member(KindDeq;kind(a(i;t));2of()
. . . . . | . | . |                                       (x)))
. . . . . | . | . |      ⇒
. . . . . | . | . |      s(i;t).x = s(i;t+1).x)
. . . . . | . | . |   & (∀l:IdLnk, tg:Id.
. . . . . | . | . |      ¬...
. . . . . | . | . |      ⇒
. . . . . | . | . |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . | . | . 13. ∀x:Id.
. . . . . | . | . |   deq-member(IdDeq;x;1of())
. . . . . | . | . |   ⇒
. . . . . | . | . |   s(i;0).x = 2of()(x)
. . . . . | . | . 14. ∀a@0:Action(i).
. . . . . | . | . |   ¬isnull(a@0)
. . . . . | . | . |   ⇒
. . . . . | . | . |   (valtype(i;a@0) ⊆r <[locl(a)]
. . . . . | . | . |                      ,λx.T>(kind(a@0))?Top)
. . . . . | . | . 15. ∀x:Id.
. . . . . | . | . |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(
. . . . . | . | . |                                        ds))→
. . . . . | . | . |                     2of(ds)(x)
. . . . . | . | . |                  else Top fi
. . . . . | . | . 16. IdDeq ∈ EqDecider(Id)
. . . . . | . | . 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . . | . | . 18. j : Id
. . . . . | . | . 19. t : ℕ
. . . . . | . | . 20. j = i
. . . . . | . | . 21. ¬isnull(a(j;t))
. . . . . | . | . 22. ¬isnull(a(i;t))
. . . . . | . | . 23. (λx.s(i;t).x) ∈ State(ds)
. . . . . | . | . 24. t' : ℤ
. . . . . | . | . 25. 0<t'
. . . . . | . | . 26. t+1≤t'
. . . . . | . | . 27. isnull(a(i;t'-1))
. . . . . | . | . 28. ∃t2:ℕ.
. . . . . | . | . |   t2<t'-1
. . . . . | . | . |   & ¬isnull(a(i;t2))
. . . . . | . | . |   & (∀t3:ℕ. t2<t3 & t3<t'-1 ⇒ isnull(a(i;t3)))
. . . . . | . | . ⊢  ∃t2:ℕ.
. . . . . | . | . |  t2<t'
```

```
. . . . . | . | . |  & ¬isnull(a(i;t2))
. . . . . | . | . |  & (∀t3:ℕ. t2<t3 & t3<t' ⇒ isnull(a(i;t3)))
. . . . . | . | . | by ParallelOp -1
. . . . . | . | . |
. . . . . | . | . 1. i : Id
. . . . . | . | . 2. a : Id
. . . . . | . | . 3. T : Type
. . . . . | . | . 4. ds : x:Id fp-> Type
. . . . . | . | . 5. P : State(ds)→T→Prop
. . . . . | . | . 6. w : World
. . . . . | . | . 7. FairFifo
. . . . . | . | . 8. FairFifo
. . . . . | . | . 9. ∀l:IdLnk, tg:Id.
. . . . . | . | . |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | . | . |                    <ds
. . . . . | . | . |                    ,<[locl(a)],λx.T>
. . . . . | . | . |                    ,
. . . . . | . | . |                    ,<[a],λx.P>
. . . . . | . | . |                    ,
. . . . . | . | . |                    ,
. . . . . | . | . |                    ,
. . . . . | . | . |                    ,
. . . . . | . | . |                    ,·>
. . . . . | . | . |                 else  fi.da(rcv(l; tg))
. . . . . | . | . 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . . | . | . 11. ∀a@0:Id, t:ℕ.
. . . . . | . | . |   ∃t':ℕ.
. . . . . | . | . |   t≤t'
. . . . . | . | . |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . . | . | . |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . . | . | . |     ∨ P@0 != <[a]
. . . . . | . | . |              ,λx.
. . . . . | . | . |               P>(a@0) ==> ∀v:<[locl(a)]
. . . . . | . | . |                                ,λx.
. . . . . | . | . |                                 T>(locl(a@0))?Top.
. . . . . | . | . |       ¬P@0((λx.s(i;t').x),v)
. . . . . | . | . 12. ∀t:ℕ.
. . . . . | . | . |   ¬isnull(a(i;t))
. . . . . | . | . |   ⇒
. . . . . | . | . |   (islocal(kind(a(i;t)))
. . . . . | . | . |    ⇒
. . . . . | . | . |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . . | . | . |    ⇒
. . . . . | . | . |    P((λx.s(i;t).x),val(a(i;t))))
. . . . . | . | . |   & (∀x:Id.
. . . . . | . | . |      deq-member(...;<kind(a(i;t)),x>;1of())
. . . . . | . | . |      ⇒
. . . . . | . | . |      s(i;t+1).x
. . . . . | . | . |      =
. . . . . | . | . |      2of()
. . . . . | . | . |      (<kind(a(i;t)),x>
. . . . . | . | . |      ,λx.s(i;t).x
. . . . . | . | . |      ,val(a(i;t))))
. . . . . | . | . |   & (∀l:IdLnk.
. . . . . | . | . |      deq-member(...;<kind(a(i;t)),l>;1of())
```

```
. . . . . | . | . |      ⇒
. . . . . | . | . |      withlnk(l;m(i;t))
. . . . . | . | . |      =
. . . . . | . | . |      if source(l) = i→
. . . . . | . | . |         concat(map(λtgf.map(λx.
. . . . . | . | . |         <1of(tgf)
. . . . . | . | . |         ,x>;2of(tgf)
. . . . . | . | . |             ((λx.s(i;t).x)
. . . . . | . | . |             ,val(a(i;t))));2of()
. . . . . | . | . |                           (<kind(a(i;t)),l>)))
. . . . . | . | . |      else nil fi)
. . . . . | . | . |   & (∀x:Id.
. . . . . | . | . |      ¬(deq-member(IdDeq;x;1of())
. . . . . | . | . |        ⇒
. . . . . | . | . |        deq-member(KindDeq;kind(a(i;t));2of()
. . . . . | . | . |                                       (x)))
. . . . . | . | . |      ⇒
. . . . . | . | . |      s(i;t).x = s(i;t+1).x)
. . . . . | . | . |   & (∀l:IdLnk, tg:Id.
. . . . . | . | . |      ¬...
. . . . . | . | . |      ⇒
. . . . . | . | . |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . | . | . 13. ∀x:Id.
. . . . . | . | . |   deq-member(IdDeq;x;1of())
. . . . . | . | . |   ⇒
. . . . . | . | . |   s(i;0).x = 2of()(x)
. . . . . | . | . 14. ∀a@0:Action(i).
. . . . . | . | . |   ¬isnull(a@0)
. . . . . | . | . |   ⇒
. . . . . | . | . |   (valtype(i;a@0) ⊆r <[locl(a)]
. . . . . | . | . |                      ,λx.T>(kind(a@0))?Top)
. . . . . | . | . 15. ∀x:Id.
. . . . . | . | . |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(
. . . . . | . | . |                                       ds))→
. . . . . | . | . |                     2of(ds)(x)
. . . . . | . | . |                  else Top fi
. . . . . | . | . 16. IdDeq ∈ EqDecider(Id)
. . . . . | . | . 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . . | . | . 18. j : Id
. . . . . | . | . 19. t : ℕ
. . . . . | . | . 20. j = i
. . . . . | . | . 21. ¬isnull(a(j;t))
. . . . . | . | . 22. ¬isnull(a(i;t))
. . . . . | . | . 23. (λx.s(i;t).x) ∈ State(ds)
. . . . . | . | . 24. t' : ℤ
. . . . . | . | . 25. 0<t'
. . . . . | . | . 26. t+1≤t'
. . . . . | . | . 27. isnull(a(i;t'-1))
. . . . . | . | . 28. t2 : ℕ
. . . . . | . | . 29. t2<t'-1
. . . . . | . | . 30. ¬isnull(a(i;t2))
. . . . . | . | . 31. ∀t3:ℕ. t2<t3 & t3<t'-1 ⇒ isnull(a(i;t3))
. . . . . | . | . 32. t3 : ℕ
. . . . . | . | . 33. t2<t3
. . . . . | . | . 34. t3<t'
```

```
. . . . . | . | . ⊢  isnull(a(i;t3))  by Decide (t3<t'-1)
. . . . . | . | . |
. . . . . | . | . |\
. . . . . | . | . | 1. i : Id
. . . . . | . | . | 2. a : Id
. . . . . | . | . | 3. T : Type
. . . . . | . | . | 4. ds : x:Id fp-> Type
. . . . . | . | . | 5. P : State(ds)→T→Prop
. . . . . | . | . | 6. w : World
. . . . . | . | . | 7. FairFifo
. . . . . | . | . | 8. FairFifo
. . . . . | . | . | 9. ∀l:IdLnk, tg:Id.
. . . . . | . | . |    (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | . | . |                      <ds
. . . . . | . | . |                      ,<[locl(a)],λx.T>
. . . . . | . | . |                      ,
. . . . . | . | . |                      ,<[a],λx.P>
. . . . . | . | . |                      ,
. . . . . | . | . |                      ,
. . . . . | . | . |                      ,
. . . . . | . | . |                      ,
. . . . . | . | . |                      ,·>
. . . . . | . | . |                    else  fi.da(rcv(l; tg))
. . . . . | . | . | 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . . | . | . | 11. ∀a@0:Id, t:ℕ.
. . . . . | . | . |     ∃t':ℕ.
. . . . . | . | . |     t≤t'
. . . . . | . | . |     & ¬isnull(a(i;t'))
. . . . . | . | . |       & kind(a(i;t')) = locl(a@0)
. . . . . | . | . |       ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . . | . | . |       ∨ P@0 != <[a]
. . . . . | . | . |                ,λx.
. . . . . | . | . |                 P>(a@0) ==> ∀v:<[locl(a)]
. . . . . | . | . |                                ,λx.
. . . . . | . | . |                                 T>(...)?Top.
. . . . . | . | . |          ¬P@0((λx.s(i;t').x),v)
. . . . . | . | . | 12. ∀t:ℕ.
. . . . . | . | . |     ¬isnull(a(i;t))
. . . . . | . | . |     ⇒
. . . . . | . | . |     (islocal(kind(a(i;t)))
. . . . . | . | . |      ⇒
. . . . . | . | . |      (eqof(IdDeq)(a,act(kind(a(i;t))))
. . . . . | . | . |       ∨₂ false₂)
. . . . . | . | . |      ⇒
. . . . . | . | . |      P((λx.s(i;t).x),val(a(i;t))))
. . . . . | . | . |     & (∀x:Id.
. . . . . | . | . |        deq-member(...;<kind(a(i;t)),x>;1of())
. . . . . | . | . |        ⇒
. . . . . | . | . |        s(i;t+1).x
. . . . . | . | . |        =
. . . . . | . | . |        2of()
. . . . . | . | . |        (<kind(a(i;t)),x>
. . . . . | . | . |        ,λx.s(i;t).x
. . . . . | . | . |        ,val(a(i;t))))
. . . . . | . | . |     & (∀l:IdLnk.
```

```
. . . . . | . | . |        deq-member(...;<kind(a(i;t)),l>;1of())
. . . . . | . | . |        ⇒
. . . . . | . | . |        withlnk(l;m(i;t))
. . . . . | . | . |        =
. . . . . | . | . |        if source(l) = i→
. . . . . | . | . |           concat(map(λtgf.map(λx.
. . . . . | . | . |           <1of(tgf)
. . . . . | . | . |           ,x>;2of(tgf)
. . . . . | . | . |               ((λx.s(i;t).x)
. . . . . | . | . |               ,val(a(i;t))));...))
. . . . . | . | . |        else nil fi)
. . . . . | . | . |     & (∀x:Id.
. . . . . | . | . |        ¬(deq-member(IdDeq;x;1of())
. . . . . | . | . |          ⇒
. . . . . | . | . |          deq-member(KindDeq;kind(a(i;t));2of()
. . . . . | . | . |                                          (x)))
. . . . . | . | . |        ⇒
. . . . . | . | . |        s(i;t).x = s(i;t+1).x)
. . . . . | . | . |     & (∀l:IdLnk, tg:Id.
. . . . . | . | . |        ¬(deq-member(...;<l,tg>;1of())
. . . . . | . | . |          ⇒
. . . . . | . | . |          deq-member(KindDeq;kind(a(i;t));...))
. . . . . | . | . |        ⇒
. . . . . | . | . |        w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . | . | . | 13. ∀x:Id.
. . . . . | . | . |     deq-member(IdDeq;x;1of())
. . . . . | . | . |     ⇒
. . . . . | . | . |     s(i;0).x = 2of()(x)
. . . . . | . | . | 14. ∀a@0:Action(i).
. . . . . | . | . |     ¬isnull(a@0)
. . . . . | . | . |     ⇒
. . . . . | . | . |     (valtype(i;a@0) ⊆r <[locl(a)]
. . . . . | . | . |                        ,λx.T>(kind(a@0))?Top)
. . . . . | . | . | 15. ∀x:Id.
. . . . . | . | . |     vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(
. . . . . | . | . |                                          ds))→
. . . . . | . | . |                        2of(ds)(x)
. . . . . | . | . |                    else Top fi
. . . . . | . | . | 16. IdDeq ∈ EqDecider(Id)
. . . . . | . | . | 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . . | . | . | 18. j : Id
. . . . . | . | . | 19. t : ℕ
. . . . . | . | . | 20. j = i
. . . . . | . | . | 21. ¬isnull(a(j;t))
. . . . . | . | . | 22. ¬isnull(a(i;t))
. . . . . | . | . | 23. (λx.s(i;t).x) ∈ State(ds)
. . . . . | . | . | 24. t' : ℤ
. . . . . | . | . | 25. 0<t'
. . . . . | . | . | 26. t+1≤t'
. . . . . | . | . | 27. isnull(a(i;t'-1))
. . . . . | . | . | 28. t2 : ℕ
. . . . . | . | . | 29. t2<t'-1
. . . . . | . | . | 30. ¬isnull(a(i;t2))
. . . . . | . | . | 31. ∀t3:ℕ. t2<t3 & t3<t'-1 ⇒ isnull(a(i;t3))
. . . . . | . | . | 32. t3 : ℕ
```

```
. . . . . | . | . | 33. t2<t3
. . . . . | . | . | 34. t3<t'
. . . . . | . | . | 35. t3<t'-1
. . . . . | . | . | ⊢  isnull(a(i;t3))  by BackThru -5
. . . . . | . | . |
. . . . . | . | . .\
. . . . . | . | . . 1. i : Id
. . . . . | . | . . 2. a : Id
. . . . . | . | . . 3. T : Type
. . . . . | . | . . 4. ds : x:Id fp-> Type
. . . . . | . | . . 5. P : State(ds)→T→Prop
. . . . . | . | . . 6. w : World
. . . . . | . | . . 7. FairFifo
. . . . . | . | . . 8. FairFifo
. . . . . | . | . . 9. ∀l:IdLnk, tg:Id.
. . . . . | . | . .    (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | . | . .                      <ds
. . . . . | . | . .                      ,<[locl(a)],λx.T>
. . . . . | . | . .                      ,
. . . . . | . | . .                      ,<[a],λx.P>
. . . . . | . | . .                      ,
. . . . . | . | . .                      ,
. . . . . | . | . .                      ,
. . . . . | . | . .                      ,
. . . . . | . | . .                      ,·>
. . . . . | . | . .                   else  fi.da(rcv(l; tg))
. . . . . | . | . . 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . . | . | . . 11. ∀a@0:Id, t:ℕ.
. . . . . | . | . .     ∃t':ℕ.
. . . . . | . | . .     t≤t'
. . . . . | . | . .     & ¬isnull(a(i;t'))
. . . . . | . | . .       & kind(a(i;t')) = locl(a@0)
. . . . . | . | . .       ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . . | . | . .       ∨ P@0 != <[a]
. . . . . | . | . .                ,λx.
. . . . . | . | . .                 P>(a@0) ==> ∀v:<[locl(a)]
. . . . . | . | . .                                ,λx.
. . . . . | . | . .                                 T>(...)?Top.
. . . . . | . | . .          ¬P@0((λx.s(i;t').x),v)
. . . . . | . | . . 12. ∀t:ℕ.
. . . . . | . | . .     ¬isnull(a(i;t))
. . . . . | . | . .     ⇒
. . . . . | . | . .     (islocal(kind(a(i;t)))
. . . . . | . | . .      ⇒
. . . . . | . | . .      (eqof(IdDeq)(a,act(kind(a(i;t))))
. . . . . | . | . .       ∨₂ false₂)
. . . . . | . | . .      ⇒
. . . . . | . | . .      P((λx.s(i;t).x),val(a(i;t))))
. . . . . | . | . .     & (∀x:Id.
. . . . . | . | . .        deq-member(...;<kind(a(i;t)),x>;1of())
. . . . . | . | . .        ⇒
. . . . . | . | . .        s(i;t+1).x
. . . . . | . | . .        =
. . . . . | . | . .        2of()
. . . . . | . | . .        (<kind(a(i;t)),x>
```

```
. . . . . | . | . .        ,λx.s(i;t).x
. . . . . | . | . .        ,val(a(i;t))))
. . . . . | . | . .     & (∀l:IdLnk.
. . . . . | . | . .        deq-member(...;<kind(a(i;t)),l>;1of())
. . . . . | . | . .        ⇒
. . . . . | . | . .        withlnk(l;m(i;t))
. . . . . | . | . .        =
. . . . . | . | . .        if source(l) = i→
. . . . . | . | . .           concat(map(λtgf.map(λx.
. . . . . | . | . .           <1of(tgf)
. . . . . | . | . .           ,x>;2of(tgf)
. . . . . | . | . .               ((λx.s(i;t).x)
. . . . . | . | . .               ,val(a(i;t))));...))
. . . . . | . | . .        else nil fi)
. . . . . | . | . .     & (∀x:Id.
. . . . . | . | . .        ¬(deq-member(IdDeq;x;1of())
. . . . . | . | . .          ⇒
. . . . . | . | . .          deq-member(KindDeq;kind(a(i;t));2of()
. . . . . | . | . .                                          (x)))
. . . . . | . | . .        ⇒
. . . . . | . | . .        s(i;t).x = s(i;t+1).x)
. . . . . | . | . .     & (∀l:IdLnk, tg:Id.
. . . . . | . | . .        ¬(deq-member(...;<l,tg>;1of())
. . . . . | . | . .          ⇒
. . . . . | . | . .          deq-member(KindDeq;kind(a(i;t));...))
. . . . . | . | . .        ⇒
. . . . . | . | . .        w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . | . | . . 13. ∀x:Id.
. . . . . | . | . .     deq-member(IdDeq;x;1of())
. . . . . | . | . .     ⇒
. . . . . | . | . .     s(i;0).x = 2of()(x)
. . . . . | . | . . 14. ∀a@0:Action(i).
. . . . . | . | . .     ¬isnull(a@0)
. . . . . | . | . .     ⇒
. . . . . | . | . .     (valtype(i;a@0) ⊆r <[locl(a)]
. . . . . | . | . .                        ,λx.T>(kind(a@0))?Top)
. . . . . | . | . . 15. ∀x:Id.
. . . . . | . | . .     vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(
. . . . . | . | . .                                          ds))→
. . . . . | . | . .                          2of(ds)(x)
. . . . . | . | . .                       else Top fi
. . . . . | . | . . 16. IdDeq ∈ EqDecider(Id)
. . . . . | . | . . 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . . | . | . . 18. j : Id
. . . . . | . | . . 19. t : ℕ
. . . . . | . | . . 20. j = i
. . . . . | . | . . 21. ¬isnull(a(j;t))
. . . . . | . | . . 22. ¬isnull(a(i;t))
. . . . . | . | . . 23. (λx.s(i;t).x) ∈ State(ds)
. . . . . | . | . . 24. t' : ℤ
. . . . . | . | . . 25. 0<t'
. . . . . | . | . . 26. t+1≤t'
. . . . . | . | . . 27. isnull(a(i;t'-1))
. . . . . | . | . . 28. t2 : ℕ
. . . . . | . | . . 29. t2<t'-1
```

```
. . . . . | . | . . 30. ¬isnull(a(i;t2))
. . . . . | . | . . 31. ∀t3:ℕ. t2<t3 & t3<t'-1 ⇒ isnull(a(i;t3))

. . . . . | . | . . 32. t3 : ℕ
. . . . . | . | . . 33. t2<t3
. . . . . | . | . . 34. t3<t'
. . . . . | . | . . 35. ¬t3<t'-1
. . . . . | . | . . ⊢  isnull(a(i;t3))  by Subst (t3 = t'-1) 0
. . . . . | . |
. . . . . | . .\
. . . . . | . . 1. i : Id
. . . . . | . . 2. a : Id
. . . . . | . . 3. T : Type
. . . . . | . . 4. ds : x:Id fp-> Type
. . . . . | . . 5. P : State(ds)→T→Prop
. . . . . | . . 6. w : World
. . . . . | . . 7. FairFifo
. . . . . | . . 8. FairFifo
. . . . . | . . 9. ∀l:IdLnk, tg:Id.
. . . . . | . .    (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | . .                      <ds
. . . . . | . .                      ,<[locl(a)],λx.T>
. . . . . | . .                      ,
. . . . . | . .                      ,<[a],λx.P>
. . . . . | . .                      ,
. . . . . | . .                      ,
. . . . . | . .                      ,
. . . . . | . .                      ,
. . . . . | . .                      ,·>
. . . . . | . .                   else  fi.da(rcv(l; tg))
. . . . . | . . 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . . | . . 11. ∀a@0:Id, t:ℕ.
. . . . . | . .     ∃t':ℕ.
. . . . . | . .     t≤t'
. . . . . | . .     & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . . | . .       ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . . | . .       ∨ P@0 != <[a]
. . . . . | . .                ,λx.
. . . . . | . .                 P>(a@0) ==> ∀v:<[locl(a)]
. . . . . | . .                                ,λx.
. . . . . | . .                                 T>(locl(a@0))?Top.
. . . . . | . .         ¬P@0((λx.s(i;t').x),v)
. . . . . | . . 12. ∀t:ℕ.
. . . . . | . .     ¬isnull(a(i;t))
. . . . . | . .     ⇒
. . . . . | . .     (islocal(kind(a(i;t)))
. . . . . | . .      ⇒
. . . . . | . .      (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . . | . .      ⇒
. . . . . | . .      P((λx.s(i;t).x),val(a(i;t))))
. . . . . | . .     & (∀x:Id.
. . . . . | . .        deq-member(...;<kind(a(i;t)),x>;1of())
. . . . . | . .        ⇒
. . . . . | . .        s(i;t+1).x
. . . . . | . .        =
. . . . . | . .        2of()
```

```
. . . . . | . .        (<kind(a(i;t)),x>
. . . . . | . .        ,λx.s(i;t).x
. . . . . | . .        ,val(a(i;t))))
. . . . . | . .     & (∀l:IdLnk.
. . . . . | . .        deq-member(...;<kind(a(i;t)),l>;1of())
. . . . . | . .        ⇒
. . . . . | . .        withlnk(l;m(i;t))
. . . . . | . .        =
. . . . . | . .        if source(l) = i→
. . . . . | . .           concat(map(λtgf.map(λx.
. . . . . | . .           <1of(tgf),x>;2of(tgf)
. . . . . | . .                       ((λx.s(i;t).x)
. . . . . | . .                       ,val(a(i;t))));2of()
. . . . . | . .                                    (<kind(a(i;t))
. . . . . | . .                                     ,l>)))
. . . . . | . .        else nil fi)
. . . . . | . .     & (∀x:Id.
. . . . . | . .        ¬(deq-member(IdDeq;x;1of())
. . . . . | . .          ⇒
. . . . . | . .          deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . . . . | . .        ⇒
. . . . . | . .        s(i;t).x = s(i;t+1).x)
. . . . . | . .     & (∀l:IdLnk, tg:Id.
. . . . . | . .        ¬(deq-member(...;<l,tg>;1of())
. . . . . | . .          ⇒
. . . . . | . .          deq-member(KindDeq;kind(a(i;t));2of()
. . . . . | . .                                          (<l,tg>)))
. . . . . | . .        ⇒
. . . . . | . .        w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . | . . 13. ∀x:Id.
. . . . . | . .     deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . . . . | . . 14. ∀a@0:Action(i).
. . . . . | . .     ¬isnull(a@0)
. . . . . | . .     ⇒
. . . . . | . .     (valtype(i;a@0) ⊆r <[locl(a)]
. . . . . | . .                        ,λx.T>(kind(a@0))?Top)
. . . . . | . . 15. ∀x:Id.
. . . . . | . .     vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . . . . | . .                        2of(ds)(x)
. . . . . | . .                    else Top fi
. . . . . | . . 16. IdDeq ∈ EqDecider(Id)
. . . . . | . . 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . . | . . 18. j : Id
. . . . . | . . 19. t : ℕ
. . . . . | . . 20. j = i
. . . . . | . . 21. ¬isnull(a(j;t))
. . . . . | . . 22. ¬isnull(a(i;t))
. . . . . | . . 23. (λx.s(i;t).x) ∈ State(ds)
. . . . . | . . 24. t' : ℤ
. . . . . | . . 25. 0<t'
. . . . . | . . 26. t+1≤t'-1
. . . . . | . .     ⇒
. . . . . | . .     (∃t2:ℕ.
. . . . . | . .      t2<t'-1
. . . . . | . .      & ¬isnull(a(i;t2))
```

```
. . . . . | . .      & (∀t3:ℕ. t2<t3 & t3<t'-1 ⇒ isnull(a(i;t3))))
. . . . . | . . 27. t+1≤t'
. . . . . | . . 28. ¬isnull(a(i;t'-1))
. . . . . | . . ⊢  ∃t2:ℕ.
. . . . . | . .    t2<t'
. . . . . | . .    & ¬isnull(a(i;t2))
. . . . . | . .    & (∀t3:ℕ. t2<t3 & t3<t' ⇒ isnull(a(i;t3)))
. . . . . | . .   by InstConcl [t'-1]
. . . . . |
. . . . . .\
. . . . . . 1. i : Id
. . . . . . 2. a : Id
. . . . . . 3. T : Type
. . . . . . 4. ds : x:Id fp-> Type
. . . . . . 5. P : State(ds)→T→Prop
. . . . . . 6. w : World
. . . . . . 7. p : FairFifo
. . . . . . 8. FairFifo
. . . . . . 9. ∀l:IdLnk, tg:Id.
. . . . . . | (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . . |                  <ds
. . . . . . |                  ,<[locl(a)],λx.T>
. . . . . . |                  ,
. . . . . . |                  ,<[a],λx.P>
. . . . . . |                  ,
. . . . . . |                  ,
. . . . . . |                  ,
. . . . . . |                  ,
. . . . . . |                  ,·>
. . . . . . |               else  fi.da(rcv(l; tg))
. . . . . . 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . . . 11. ∀a@0:Id, t:ℕ.
. . . . . . |   ∃t':ℕ.
. . . . . . |   t≤t'
. . . . . . |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . . . |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . . . |     ∨ P@0 != <[a]
. . . . . . |              ,λx.P>(a@0) ==> ∀v:<[locl(a)]
. . . . . . |                                  ,λx.T>(locl(a@0))?Top.
. . . . . . |       ¬P@0((λx.s(i;t').x),v)
. . . . . . 12. ∀t:ℕ.
. . . . . . |   ¬isnull(a(i;t))
. . . . . . |   ⇒
. . . . . . |   (islocal(kind(a(i;t)))
. . . . . . |    ⇒
. . . . . . |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . . . |    ⇒
. . . . . . |    P((λx.s(i;t).x),val(a(i;t))))
. . . . . . |   & (∀x:Id.
. . . . . . |      deq-member(product-deq(Knd;Id;...;IdDeq);<...
. . . . . . |                                                ,x>;1of(
. . . . . . |                                                    ))
. . . . . . |      ⇒
. . . . . . |      s(i;t+1).x
. . . . . . |      =
```

```
. . . . . | .     2of()(<kind(a(i;t)),x>,λx.s(i;t).x,val(a(i;t))))
. . . . . | .  & (∀l:IdLnk.
. . . . . | .     deq-member(product-deq(Knd;...;...;...);<...
. . . . . | .                                          ,l>;1of(
. . . . . | .                                              ))
. . . . . | .     ⇒
. . . . . | .     withlnk(l;m(i;t))
. . . . . | .     =
. . . . . | .     if source(l) = i→
. . . . . | .        concat(map(λtgf.map(λx.
. . . . . | .        <1of(tgf)
. . . . . | .        ,x>;2of(tgf)
. . . . . | .            ((λx.s(i;t).x)
. . . . . | .            ,val(a(i;t))));2of()(<kind(a(i;t)),l>)))
. . . . . | .     else nil fi)
. . . . . | .  & (∀x:Id.
. . . . . | .     ¬(deq-member(IdDeq;x;1of())
. . . . . | .       ⇒
. . . . . | .       deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . . . . | .     ⇒
. . . . . | .     s(i;t).x = s(i;t+1).x)
. . . . . | .  & (∀l:IdLnk, tg:Id.
. . . . . | .     ¬(deq-member(product-deq(...;Id;...;...);...;1of(
. . . . . | .                                               ))
. . . . . | .       ⇒
. . . . . | .       deq-member(KindDeq;kind(a(i;t));2of()(<l,tg>)))
. . . . . | .     ⇒
. . . . . | .     w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . 13. ∀x:Id.
. . . . . | .  deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . . . . 14. ∀a@0:Action(i).
. . . . . | .  ¬isnull(a@0)
. . . . . | .  ⇒
. . . . . | .  (valtype(i;a@0) ⊆r <[locl(a)],λx.T>(kind(a@0))?Top)
. . . . . 15. ∀x:Id.
. . . . . | .  vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . . . . | .                      2of(ds)(x)
. . . . . | .                  else Top fi
. . . . . 16. IdDeq ∈ EqDecider(Id)
. . . . . 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . . 18. j : Id
. . . . . 19. t : ℕ
. . . . . 20. j = i
. . . . . 21. ¬isnull(a(j;t))
. . . . . 22. ¬isnull(a(i;t))
. . . . . 23. (λx.s(i;t).x) ∈ State(ds)
. . . . . 24. t' : ℕ
. . . . . 25. t+1≤t'
. . . . . 26. ∀v:T. ¬P((λx.s(i;t').x),v)
. . . . . 27. ∃t2:ℕ.
. . . . . | .  t2<t'
. . . . . | .  & ¬isnull(a(i;t2))
. . . . . | .  & (∀t3:ℕ. t2<t3 & t3<t' ⇒ isnull(a(i;t3)))
. . . . . ⊢  ∃e':E.
. . . . . |  (<j,t> <loc e') ∨ <j,t> = e'
```

```
. . . . . | & kind(e') = locl(a)
. . . . . |   ∨ (∀v:T. ¬P((λz.(z after e')),v))
. . . . . | by ExRepD THEN Assert (t≤t2)
. . . . . |
. . . . . |\
. . . . . | .....assertion .....
. . . . . | 1. i : Id
. . . . . | 2. a : Id
. . . . . | 3. T : Type
. . . . . | 4. ds : x:Id fp-> Type
. . . . . | 5. P : State(ds)→T→Prop
. . . . . | 6. w : World
. . . . . | 7. FairFifo
. . . . . | 8. FairFifo
. . . . . | 9. ∀l:IdLnk, tg:Id.
. . . . . | |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | |                    <ds
. . . . . | |                    ,<[locl(a)],λx.T>
. . . . . | |                    ,
. . . . . | |                    ,<[a],λx.P>
. . . . . | |                    ,
. . . . . | |                    ,
. . . . . | |                    ,
. . . . . | |                    ,
. . . . . | |                    ,·>
. . . . . | |                 else  fi.da(rcv(l; tg))
. . . . . | 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . . | 11. ∀a@0:Id, t:ℕ.
. . . . . | |   ∃t':ℕ.
. . . . . | |   t≤t'
. . . . . | |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . . | |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . . | |     ∨ P@0 != <[a]
. . . . . | |              ,λx.P>(a@0) ==> ∀v:<[locl(a)]
. . . . . | |                                  ,λx.
. . . . . | |                                   T>(locl(a@0))?Top.
. . . . . | |       ¬P@0((λx.s(i;t').x),v)
. . . . . | 12. ∀t:ℕ.
. . . . . | |   ¬isnull(a(i;t))
. . . . . | |   ⇒
. . . . . | |   (islocal(kind(a(i;t)))
. . . . . | |    ⇒
. . . . . | |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . . | |    ⇒
. . . . . | |    P((λx.s(i;t).x),val(a(i;t))))
. . . . . | |   & (∀x:Id.
. . . . . | |      deq-member(product-deq(Knd;Id;...;...);<...
. . . . . | |                                              ,x>;1of(
. . . . . | |                                                  ))
. . . . . | |      ⇒
. . . . . | |      s(i;t+1).x
. . . . . | |      =
. . . . . | |      2of()
. . . . . | |      (<kind(a(i;t)),x>
. . . . . | |      ,λx.s(i;t).x
```

```
. . . . . | |      ,val(a(i;t))))
. . . . . | |   & (∀l:IdLnk.
. . . . . | |      deq-member(...;<kind(a(i;t)),l>;1of())
. . . . . | |      ⇒
. . . . . | |      withlnk(l;m(i;t))
. . . . . | |      =
. . . . . | |      if source(l) = i→
. . . . . | |         concat(map(λtgf.map(λx.
. . . . . | |         <1of(tgf),x>;2of(tgf)
. . . . . | |                     ((λx.s(i;t).x)
. . . . . | |                     ,val(a(i;t))));2of()
. . . . . | |                                   (<kind(a(i;t))
. . . . . | |                                    ,l>)))
. . . . . | |      else nil fi)
. . . . . | |   & (∀x:Id.
. . . . . | |      ¬(deq-member(IdDeq;x;1of())
. . . . . | |        ⇒
. . . . . | |        deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . . . . | |      ⇒
. . . . . | |      s(i;t).x = s(i;t+1).x)
. . . . . | |   & (∀l:IdLnk, tg:Id.
. . . . . | |      ¬(deq-member(...;<l,tg>;1of())
. . . . . | |        ⇒
. . . . . | |        deq-member(KindDeq;kind(a(i;t));2of()
. . . . . | |                                      (<l,tg>)))
. . . . . | |      ⇒
. . . . . | |      w-tagged(tg; onlnk(l;m(i;t))) = nil)

. . . . . | 13. ∀x:Id.
. . . . . | |   deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . . . . | 14. ∀a@0:Action(i).
. . . . . | |   ¬isnull(a@0)
. . . . . | |   ⇒
. . . . . | |   (valtype(i;a@0) ⊆r <[locl(a)]
. . . . . | |                     ,λx.T>(kind(a@0))?Top)
. . . . . | 15. ∀x:Id.
. . . . . | |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . . . . | |                     2of(ds)(x)
. . . . . | |                   else Top fi
. . . . . | 16. IdDeq ∈ EqDecider(Id)
. . . . . | 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . . | 18. j : Id
. . . . . | 19. t : ℕ
. . . . . | 20. j = i
. . . . . | 21. ¬isnull(a(j;t))
. . . . . | 22. ¬isnull(a(i;t))
. . . . . | 23. (λx.s(i;t).x) ∈ State(ds)
. . . . . | 24. t' : ℕ
. . . . . | 25. t+1≤t'
. . . . . | 26. ∀v:T. ¬P((λx.s(i;t').x),v)
. . . . . | 27. t2 : ℕ
. . . . . | 28. t2<t'
. . . . . | 29. ¬isnull(a(i;t2))
. . . . . | 30. ∀t3:ℕ. t2<t3 & t3<t' ⇒ isnull(a(i;t3))
. . . . . | ⊢  t≤t2  by SupposeNot
. . . . . | |
```

```
. . . . . | 1. i : Id
. . . . . | 2. a : Id
. . . . . | 3. T : Type
. . . . . | 4. ds : x:Id fp-> Type
. . . . . | 5. P : State(ds)→T→Prop
. . . . . | 6. w : World
. . . . . | 7. FairFifo
. . . . . | 8. FairFifo
. . . . . | 9. ∀l:IdLnk, tg:Id.
. . . . . |    (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . |                       <ds
. . . . . |                       ,<[locl(a)],λx.T>
. . . . . |                       ,
. . . . . |                       ,<[a],λx.P>
. . . . . |                       ,
. . . . . |                       ,
. . . . . |                       ,
. . . . . |                       ,
. . . . . |                       ,·>
. . . . . |                    else  fi.da(rcv(l; tg))
. . . . . | 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . . | 11. ∀a@0:Id, t:ℕ.
. . . . . |     ∃t':ℕ.
. . . . . |     t≤t'
. . . . . |     & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . . |       ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . . |       ∨ P@0 != <[a]
. . . . . |                ,λx.P>(a@0) ==> ∀v:<[locl(a)]
. . . . . |                                  ,λx.
. . . . . |                                   T>(locl(a@0))?Top.
. . . . . |         ¬P@0((λx.s(i;t').x),v)
. . . . . | 12. ∀t:ℕ.
. . . . . |     ¬isnull(a(i;t))
. . . . . |     ⇒
. . . . . |     (islocal(kind(a(i;t)))
. . . . . |      ⇒
. . . . . |      (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . . |      ⇒
. . . . . |      P((λx.s(i;t).x),val(a(i;t))))
. . . . . |     & (∀x:Id.
. . . . . |        deq-member(product-deq(Knd;Id;...;...);<...
. . . . . |                                                ,x>;1of(
. . . . . |                                                    ))
. . . . . |        ⇒
. . . . . |        s(i;t+1).x
. . . . . |        =
. . . . . |        2of()
. . . . . |        (<kind(a(i;t)),x>
. . . . . |        ,λx.s(i;t).x
. . . . . |        ,val(a(i;t))))
. . . . . |     & (∀l:IdLnk.
. . . . . |        deq-member(...;<kind(a(i;t)),l>;1of())
. . . . . |        ⇒
. . . . . |        withlnk(l;m(i;t))
. . . . . |        =
```

```
. . . . . | .       if source(l) = i→
. . . . . | .          concat(map(λtgf.map(λx.
. . . . . | .          <1of(tgf),x>;2of(tgf)
. . . . . | .                      ((λx.s(i;t).x)
. . . . . | .                      ,val(a(i;t))));2of()
. . . . . | .                                    (<kind(a(i;t))
. . . . . | .                                     ,l>)))
. . . . . | .       else nil fi)
. . . . . | .    & (∀x:Id.
. . . . . | .       ¬(deq-member(IdDeq;x;1of())
. . . . . | .         ⇒
. . . . . | .         deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . . . . | .       ⇒
. . . . . | .       s(i;t).x = s(i;t+1).x)
. . . . . | .    & (∀l:IdLnk, tg:Id.
. . . . . | .       ¬(deq-member(...;<l,tg>;1of())
. . . . . | .         ⇒

. . . . . | .         deq-member(KindDeq;kind(a(i;t));2of()
. . . . . | .                                       (<l,tg>)))
. . . . . | .       ⇒
. . . . . | .       w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . | 13. ∀x:Id.
. . . . . | .    deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . . . . | 14. ∀a@0:Action(i).
. . . . . | .    ¬isnull(a@0)
. . . . . | .    ⇒
. . . . . | .    (valtype(i;a@0) ⊆r <[locl(a)]
. . . . . | .                       ,λx.T>(kind(a@0))?Top)
. . . . . | 15. ∀x:Id.
. . . . . | .    vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . . . . | .                       2of(ds)(x)
. . . . . | .                    else Top fi
. . . . . | 16. IdDeq ∈ EqDecider(Id)
. . . . . | 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . . | 18. j : Id
. . . . . | 19. t : ℕ
. . . . . | 20. j = i
. . . . . | 21. ¬isnull(a(j;t))
. . . . . | 22. ¬isnull(a(i;t))
. . . . . | 23. (λx.s(i;t).x) ∈ State(ds)
. . . . . | 24. t' : ℕ
. . . . . | 25. t+1≤t'
. . . . . | 26. ∀v:T. ¬P((λx.s(i;t').x),v)
. . . . . | 27. t2 : ℕ
. . . . . | 28. t2<t'
. . . . . | 29. ¬isnull(a(i;t2))
. . . . . | 30. ∀t3:ℕ. t2<t3 & t3<t' ⇒ isnull(a(i;t3))
. . . . . | 31. ¬t≤t2
. . . . . | ⊢  t≤t2  by InstHyp [t] -2
. . . . . |
. . . . . .\
. . . . . . 1. i : Id
. . . . . . 2. a : Id
. . . . . . 3. T : Type
. . . . . . 4. ds : x:Id fp-> Type
```

```
. . . . . 5. P : State(ds)→T→Prop
. . . . . 6. w : World
. . . . . 7. p : FairFifo
. . . . . 8. FairFifo
. . . . . 9. ∀l:IdLnk, tg:Id.
. . . . . |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . |                    <ds
. . . . . |                    ,<[locl(a)],λx.T>
. . . . . |                    ,
. . . . . |                    ,<[a],λx.P>
. . . . . |                    ,
. . . . . |                    ,
. . . . . |                    ,
. . . . . |                    ,
. . . . . |                    ,·>
. . . . . |                 else  fi.da(rcv(l; tg))
. . . . . 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . . 11. ∀a@0:Id, t:ℕ.
. . . . . |   ∃t':ℕ.
. . . . . |   t≤t'
. . . . . |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . . |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . . |     ∨ P@0 != <[a]
. . . . . |              ,λx.P>(a@0) ==> ∀v:<[locl(a)]
. . . . . |                                  ,λx.
. . . . . |                                   T>(locl(a@0))?Top.
. . . . . |       ¬P@0((λx.s(i;t').x),v)
. . . . . 12. ∀t:ℕ.
. . . . . |   ¬isnull(a(i;t))
. . . . . |   ⇒
. . . . . |   (islocal(kind(a(i;t)))
. . . . . |    ⇒
. . . . . |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . . |    ⇒
. . . . . |    P((λx.s(i;t).x),val(a(i;t))))
. . . . . |   & (∀x:Id.
. . . . . |      deq-member(product-deq(Knd;Id;...;...);<...
. . . . . |                                              ,x>;1of(
. . . . . |                                                  ))
. . . . . |      ⇒
. . . . . |      s(i;t+1).x
. . . . . |      =
. . . . . |      2of()
. . . . . |      (<kind(a(i;t)),x>
. . . . . |      ,λx.s(i;t).x
. . . . . |      ,val(a(i;t))))
. . . . . |   & (∀l:IdLnk.
. . . . . |      deq-member(...;<kind(a(i;t)),l>;1of())
. . . . . |      ⇒
. . . . . |      withlnk(l;m(i;t))
. . . . . |      =
. . . . . |      if source(l) = i→
. . . . . |         concat(map(λtgf.map(λx.
. . . . . |         <1of(tgf),x>;2of(tgf)
. . . . . |                       ((λx.s(i;t).x)
```

```
. . . . . | ,val(a(i;t))));2of()
. . . . . | (<kind(a(i;t))
. . . . . | ,l>)))
. . . . . | else nil fi)
. . . . . | & (∀x:Id.
. . . . . | ¬(deq-member(IdDeq;x;1of())
. . . . . | ⇒
. . . . . | deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . . . . | ⇒
. . . . . | s(i;t).x = s(i;t+1).x)
. . . . . | & (∀l:IdLnk, tg:Id.
. . . . . | ¬(deq-member(...;<l,tg>;1of())
. . . . . | ⇒
. . . . . | deq-member(KindDeq;kind(a(i;t));2of()
. . . . . | (<l,tg>)))
. . . . . | ⇒
. . . . . | w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . 13. ∀x:Id.
. . . . . | deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . . . . 14. ∀a@0:Action(i).
. . . . . | ¬isnull(a@0)
. . . . . | ⇒
. . . . . | (valtype(i;a@0) ⊆r <[locl(a)]
. . . . . | ,λx.T>(kind(a@0))?Top)
. . . . . 15. ∀x:Id.
. . . . . | vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . . . . | 2of(ds)(x)
. . . . . | else Top fi
. . . . . 16. IdDeq ∈ EqDecider(Id)
. . . . . 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . . 18. j : Id
. . . . . 19. t : ℕ
. . . . . 20. j = i
. . . . . 21. ¬isnull(a(j;t))
. . . . . 22. ¬isnull(a(i;t))
. . . . . 23. (λx.s(i;t).x) ∈ State(ds)
. . . . . 24. t' : ℕ
. . . . . 25. t+1≤t'
. . . . . 26. ∀v:T. ¬P((λx.s(i;t').x),v)
. . . . . 27. t2 : ℕ
. . . . . 28. t2<t'
. . . . . 29. ¬isnull(a(i;t2))
. . . . . 30. ∀t3:ℕ. t2<t3 & t3<t' ⇒ isnull(a(i;t3))
. . . . . 31. t≤t2
. . . . . ⊢ ∃e':E.
. . . . . | (<j,t> <loc e') ∨ <j,t> = e'
. . . . . | & kind(e') = locl(a)
. . . . . | ∨ (∀v:T. ¬P((λz.(z after e')),v))
. . . . . | by Unfold ‘es-locl‘ 0
. . . . . | THEN
. . . . . | Unfolds [‘w-ekind‘;‘w-when‘;‘w-after‘;‘w-locl‘] 0
. . . . . | THEN
. . . . . | Reduce 0
. . . . . | THEN
. . . . . | InstConcl [<i,t2>]
```

```
. . . . . |
. . . . . |\
. . . . . | .....wf .....
. . . . . | 1. i : Id
. . . . . | 2. a : Id
. . . . . | 3. T : Type
. . . . . | 4. ds : x:Id fp-> Type
. . . . . | 5. P : State(ds)→T→Prop
. . . . . | 6. w : World
. . . . . | 7. FairFifo
. . . . . | 8. FairFifo
. . . . . | 9. ∀l:IdLnk, tg:Id.
. . . . . |    (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . |                       <ds
. . . . . |                       ,<[locl(a)],λx.T>
. . . . . |                       ,
. . . . . |                       ,<[a],λx.P>
. . . . . |                       ,
. . . . . |                       ,
. . . . . |                       ,
. . . . . |                       ,
. . . . . |                       ,·>
. . . . . |                    else  fi.da(rcv(l; tg))
. . . . . | 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . . | 11. ∀a@0:Id, t:ℕ.
. . . . . |     ∃t':ℕ.
. . . . . |     t≤t'
. . . . . |     & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . . |       ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . . |       ∨ P@0 != <[a]
. . . . . |                 ,λx.
. . . . . |                  P>(a@0) ==> ∀v:<[locl(a)]
. . . . . |                                 ,λx.
. . . . . |                                  T>(locl(a@0))?Top.
. . . . . |          ¬P@0((λx.s(i;t').x),v)
. . . . . | 12. ∀t:ℕ.
. . . . . |     ¬isnull(a(i;t))
. . . . . |     ⇒
. . . . . |     (islocal(kind(a(i;t)))
. . . . . |      ⇒
. . . . . |      (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . . |      ⇒
. . . . . |      P((λx.s(i;t).x),val(a(i;t))))
. . . . . |     & (∀x:Id.
. . . . . |        deq-member(...;<kind(a(i;t)),x>;1of())
. . . . . |        ⇒
. . . . . |        s(i;t+1).x
. . . . . |        =
. . . . . |        2of()
. . . . . |        (<kind(a(i;t)),x>
. . . . . |        ,λx.s(i;t).x
. . . . . |        ,val(a(i;t))))
. . . . . |     & (∀l:IdLnk.
. . . . . |        deq-member(...;<kind(a(i;t)),l>;1of())
. . . . . |        ⇒
```

```
. . . . . |       withlnk(l;m(i;t))
. . . . . |       =
. . . . . |       if source(l) = i→
. . . . . |          concat(map(λtgf.map(λx.
. . . . . |          <1of(tgf),x>;2of(tgf)
. . . . . |                        ((λx.s(i;t).x)
. . . . . |                        ,val(a(i;t))));2of()
. . . . . |                                      (<kind(a(i;t))
. . . . . |                                       ,l>)))
. . . . . |       else nil fi)
. . . . . |    & (∀x:Id.
. . . . . |       ¬(deq-member(IdDeq;x;1of())
. . . . . |         ⇒
. . . . . |         deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . . . . |       ⇒
. . . . . |       s(i;t).x = s(i;t+1).x)
. . . . . |    & (∀l:IdLnk, tg:Id.
. . . . . |       ¬(deq-member(...;<l,tg>;1of())
. . . . . |         ⇒
. . . . . |         deq-member(KindDeq;kind(a(i;t));2of()
. . . . . |                                          (<l,tg>)))
. . . . . |       ⇒
. . . . . |       w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . | 13. ∀x:Id.
. . . . . |     deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . . . . | 14. ∀a@0:Action(i).
. . . . . |     ¬isnull(a@0)
. . . . . |     ⇒
. . . . . |     (valtype(i;a@0) ⊆r <[locl(a)]
. . . . . |                        ,λx.T>(kind(a@0))?Top)
. . . . . | 15. ∀x:Id.
. . . . . |     vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . . . . |                         2of(ds)(x)
. . . . . |                      else Top fi
. . . . . | 16. IdDeq ∈ EqDecider(Id)
. . . . . | 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . . | 18. j : Id
. . . . . | 19. t : ℕ
. . . . . | 20. j = i
. . . . . | 21. ¬isnull(a(j;t))
. . . . . | 22. ¬isnull(a(i;t))
. . . . . | 23. (λx.s(i;t).x) ∈ State(ds)
. . . . . | 24. t' : ℕ
. . . . . | 25. t+1≤t'
. . . . . | 26. ∀v:T. ¬P((λx.s(i;t').x),v)
. . . . . | 27. t2 : ℕ
. . . . . | 28. t2<t'
. . . . . | 29. ¬isnull(a(i;t2))
. . . . . | 30. ∀t3:ℕ. t2<t3 & t3<t' ⇒ isnull(a(i;t3))
. . . . . | 31. t≤t2
. . . . . | ⊢  <i,t2> ∈ E
. . . . . |   by Unfold `w-E` 0 THEN Analyze
. . . . . |      THEN
. . . . . |      Try D_ES_Subtype
. . . . . |      THEN
```

```
. . . . . | |      Reduce 0
. . . . . | |      THEN
. . . . . | |      Trivial
. . . . . |
. . . . . |\
. . . . . | 1. i : Id
. . . . . | 2. a : Id
. . . . . | 3. T : Type
. . . . . | 4. ds : x:Id fp-> Type
. . . . . | 5. P : State(ds)→T→Prop
. . . . . | 6. w : World
. . . . . | 7. p : FairFifo
. . . . . | 8. FairFifo
. . . . . | 9. ∀l:IdLnk, tg:Id.
. . . . . | |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | |                    <ds
. . . . . | |                    ,<[locl(a)],λx.T>
. . . . . | |                    ,
. . . . . | |                    ,<[a],λx.P>
. . . . . | |                    ,
. . . . . | |                    ,
. . . . . | |                    ,
. . . . . | |                    ,
. . . . . | |                    ,.>
. . . . . | |                 else  fi.da(rcv(l; tg))
. . . . . | 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . . | 11. ∀a@0:Id, t:ℕ.
. . . . . | |   ∃t':ℕ.
. . . . . | |   t≤t'
. . . . . | |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . . | |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . . | |     ∨ P@0 != <[a]
. . . . . | |              ,λx.
. . . . . | |               P>(a@0) ==> ∀v:<[locl(a)]
. . . . . | |                                ,λx.
. . . . . | |                                 T>(locl(a@0))?Top.
. . . . . | |       ¬P@0((λx.s(i;t').x),v)
. . . . . | 12. ∀t:ℕ.
. . . . . | |   ¬isnull(a(i;t))
. . . . . | |   ⇒
. . . . . | |   (islocal(kind(a(i;t)))
. . . . . | |    ⇒
. . . . . | |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . . | |    ⇒
. . . . . | |    P((λx.s(i;t).x),val(a(i;t))))
. . . . . | |   & (∀x:Id.
. . . . . | |      deq-member(...;<kind(a(i;t)),x>;1of())
. . . . . | |      ⇒
. . . . . | |      s(i;t+1).x
. . . . . | |      =
. . . . . | |      2of()
. . . . . | |      (<kind(a(i;t)),x>
. . . . . | |      ,λx.s(i;t).x
. . . . . | |      ,val(a(i;t))))
. . . . . | |   & (∀l:IdLnk.
```

```
. . . . . | | |     deq-member(...;<kind(a(i;t)),l>;1of())
. . . . . | | |     ⇒
. . . . . | | |     withlnk(l;m(i;t))
. . . . . | | |     =
. . . . . | | |     if source(l) = i→
. . . . . | | |        concat(map(λtgf.map(λx.
. . . . . | | |        <1of(tgf),x>;2of(tgf)
. . . . . | | |                     ((λx.s(i;t).x)
. . . . . | | |                     ,val(a(i;t))));2of()
. . . . . | | |                                   (<kind(a(i;t))
. . . . . | | |                                    ,l>)))
. . . . . | | |     else nil fi)
. . . . . | | |   & (∀x:Id.
. . . . . | | |     ¬(deq-member(IdDeq;x;1of())
. . . . . | | |       ⇒
. . . . . | | |       deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . . . . | | |     ⇒
. . . . . | | |     s(i;t).x = s(i;t+1).x)
. . . . . | | |   & (∀l:IdLnk, tg:Id.
. . . . . | | |     ¬(deq-member(...;<l,tg>;1of())
. . . . . | | |       ⇒
. . . . . | | |       deq-member(KindDeq;kind(a(i;t));2of()
. . . . . | | |                                     (<l,tg>)))
. . . . . | | |     ⇒
. . . . . | | |     w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . | | 13. ∀x:Id.
. . . . . | | |   deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . . . . | | 14. ∀a@0:Action(i).
. . . . . | | |   ¬isnull(a@0)
. . . . . | | |   ⇒
. . . . . | | |   (valtype(i;a@0) ⊆r <[locl(a)]
. . . . . | | |                     ,λx.T>(kind(a@0))?Top)
. . . . . | | 15. ∀x:Id.
. . . . . | | |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . . . . | | |                     2of(ds)(x)
. . . . . | | |                   else Top fi
. . . . . | | 16. IdDeq ∈ EqDecider(Id)
. . . . . | | 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . . | | 18. j : Id
. . . . . | | 19. t : ℕ
. . . . . | | 20. j = i
. . . . . | | 21. ¬isnull(a(j;t))
. . . . . | | 22. ¬isnull(a(i;t))
. . . . . | | 23. (λx.s(i;t).x) ∈ State(ds)
. . . . . | | 24. t' : ℕ
. . . . . | | 25. t+1≤t'
. . . . . | | 26. ∀v:T. ¬P((λx.s(i;t').x),v)
. . . . . | | 27. t2 : ℕ
. . . . . | | 28. t2<t'
. . . . . | | 29. ¬isnull(a(i;t2))
. . . . . | | 30. ∀t3:ℕ. t2<t3 & t3<t' ⇒ isnull(a(i;t3))
. . . . . | | 31. t≤t2
. . . . . | | ⊢  loc(<j,t>) = loc(<i,t2>) & (<j,t> < <i,t2>)
. . . . . | | |  ∨ <j,t> = <i,t2>
. . . . . | | |  & kind(act(<i,t2>)) = locl(a)
```

```
. . . . . | |    ∨ (∀v:T.
. . . . . | |       ¬P((λz.s(1of(<i,t2>);2of(<i,t2>)+1).z),v))
. . . . . | | by Analyze 0
. . . . . | |
. . . . . | |\
. . . . . | | 1. i : Id
. . . . . | | 2. a : Id
. . . . . | | 3. T : Type
. . . . . | | 4. ds : x:Id fp-> Type
. . . . . | | 5. P : State(ds)→T→Prop
. . . . . | | 6. w : World
. . . . . | | 7. p : FairFifo
. . . . . | | 8. FairFifo
. . . . . | | 9. ∀l:IdLnk, tg:Id.
. . . . . | | |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | | |                    <ds
. . . . . | | |                    ,<[locl(a)],λx.T>
. . . . . | | |                    ,
. . . . . | | |                    ,<[a],λx.P>
. . . . . | | |                    ,
. . . . . | | |                    ,
. . . . . | | |                    ,
. . . . . | | |                    ,
. . . . . | | |                    ,.>
. . . . . | | |                 else  fi.da(rcv(l; tg))
. . . . . | | 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . . | | 11. ∀a@0:Id, t:ℕ.
. . . . . | | |   ∃t':ℕ.
. . . . . | | |   t≤t'
. . . . . | | |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . . | | |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . . | | |     ∨ P@0 != <[a]
. . . . . | | |              ,λx.
. . . . . | | |               P>(a@0) ==> ∀v:<[locl(a)]
. . . . . | | |                                ,λx.
. . . . . | | |                                 T>(locl(a@0))?Top.
. . . . . | | |       ¬P@0((λx.s(i;t').x),v)
. . . . . | | 12. ∀t:ℕ.
. . . . . | | |   ¬isnull(a(i;t))
. . . . . | | |   ⇒
. . . . . | | |   (islocal(kind(a(i;t)))
. . . . . | | |    ⇒
. . . . . | | |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . . | | |    ⇒
. . . . . | | |    P((λx.s(i;t).x),val(a(i;t))))
. . . . . | | |   & (∀x:Id.
. . . . . | | |      deq-member(...;<kind(a(i;t)),x>;1of())
. . . . . | | |      ⇒
. . . . . | | |      s(i;t+1).x
. . . . . | | |      =
. . . . . | | |      2of()
. . . . . | | |      (<kind(a(i;t)),x>
. . . . . | | |      ,λx.s(i;t).x
. . . . . | | |      ,val(a(i;t))))
. . . . . | | |   & (∀l:IdLnk.
```

```
. . . . . | | |      deq-member(...;<kind(a(i;t)),l>;1of())
. . . . . | | |      ⇒
. . . . . | | |      withlnk(l;m(i;t))
. . . . . | | |      =
. . . . . | | |      if source(l) = i→
. . . . . | | |         concat(map(λtgf.map(λx.
. . . . . | | |         <1of(tgf)
. . . . . | | |         ,x>;2of(tgf)
. . . . . | | |             ((λx.s(i;t).x)
. . . . . | | |             ,val(a(i;t))));2of()
. . . . . | | |                              (<kind(a(i;t)),l>)))
. . . . . | | |      else nil fi)
. . . . . | | |   & (∀x:Id.
. . . . . | | |      ¬(deq-member(IdDeq;x;1of())
. . . . . | | |        ⇒
. . . . . | | |        deq-member(KindDeq;kind(a(i;t));2of()
. . . . . | | |                                        (x)))
. . . . . | | |      ⇒
. . . . . | | |      s(i;t).x = s(i;t+1).x)
. . . . . | | |   & (∀l:IdLnk, tg:Id.
. . . . . | | |      ¬...
. . . . . | | |      ⇒
. . . . . | | |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . | | 13. ∀x:Id.
. . . . . | | |   deq-member(IdDeq;x;1of())
. . . . . | | |   ⇒
. . . . . | | |   s(i;0).x = 2of()(x)
. . . . . | | 14. ∀a@0:Action(i).
. . . . . | | |   ¬isnull(a@0)
. . . . . | | |   ⇒
. . . . . | | |   (valtype(i;a@0) ⊆r <[locl(a)]
. . . . . | | |                      ,λx.T>(kind(a@0))?Top)
. . . . . | | 15. ∀x:Id.
. . . . . | | |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(
. . . . . | | |                                        ds))→
. . . . . | | |                      2of(ds)(x)
. . . . . | | |                   else Top fi
. . . . . | | 16. IdDeq ∈ EqDecider(Id)
. . . . . | | 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . . | | 18. j : Id
. . . . . | | 19. t : ℕ
. . . . . | | 20. j = i
. . . . . | | 21. ¬isnull(a(j;t))
. . . . . | | 22. ¬isnull(a(i;t))
. . . . . | | 23. (λx.s(i;t).x) ∈ State(ds)
. . . . . | | 24. t' : ℕ
. . . . . | | 25. t+1≤t'
. . . . . | | 26. ∀v:T. ¬P((λx.s(i;t').x),v)
. . . . . | | 27. t2 : ℕ
. . . . . | | 28. t2<t'
. . . . . | | 29. ¬isnull(a(i;t2))
. . . . . | | 30. ∀t3:ℕ. t2<t3 & t3<t' ⇒ isnull(a(i;t3))
. . . . . | | 31. t≤t2
. . . . . | | ⊢  loc(<j,t>) = loc(<i,t2>) & (<j,t> < <i,t2>)
. . . . . | | |  ∨ <j,t> = <i,t2>
```

```
. . . . . | | | by Repeat
. . . . . | | |    (Unfolds
. . . . . | | |     [‘es-Loc‘
. . . . . | | |     ;‘es-causl‘
. . . . . | | |     ;‘es-locl‘
. . . . . | | |     ;‘es-loc‘
. . . . . | | |     ;‘w-E‘
. . . . . | | |     ;‘w-locl‘]
. . . . . | | |     0
. . . . . | | |     THEN
. . . . . | | |     Reduce 0)
. . . . . | | |    THEN
. . . . . | | |    Decide (t<t2)
. . . . . | | |
. . . . . | | |\
. . . . . | | | 1. i : Id
. . . . . | | | 2. a : Id
. . . . . | | | 3. T : Type
. . . . . | | | 4. ds : x:Id fp-> Type
. . . . . | | | 5. P : State(ds)→T→Prop
. . . . . | | | 6. w : World
. . . . . | | | 7. FairFifo
. . . . . | | | 8. FairFifo
. . . . . | | | 9. ∀l:IdLnk, tg:Id.
. . . . . | | | |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | | | |                  <ds
. . . . . | | | |                  ,<[locl(a)],λx.T>
. . . . . | | | |                  ,
. . . . . | | | |                  ,<[a],λx.P>
. . . . . | | | |                  ,
. . . . . | | | |                  ,
. . . . . | | | |                  ,
. . . . . | | | |                  ,
. . . . . | | | |                  ,.>
. . . . . | | | |               else  fi.da(rcv(l; tg))
. . . . . | | | 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . . | | | 11. ∀a@0:Id, t:ℕ.
. . . . . | | | |   ∃t’:ℕ.
. . . . . | | | |   t≤t’
. . . . . | | | |   & ¬isnull(a(i;t’))
. . . . . | | | |     & kind(a(i;t’)) = locl(a@0)
. . . . . | | | |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . . | | | |     ∨ P@0 != <[a]
. . . . . | | | |              ,λx.
. . . . . | | | |               P>(a@0) ==> ∀v:<[locl(a)]
. . . . . | | | |                                ,λx.
. . . . . | | | |                                 T>(...)?Top.
. . . . . | | | |       ¬P@0((λx.s(i;t’).x),v)
. . . . . | | | 12. ∀t:ℕ.
. . . . . | | | |   ¬isnull(a(i;t))
. . . . . | | | |   ⇒
. . . . . | | | |   (islocal(kind(a(i;t)))
. . . . . | | | |    ⇒
. . . . . | | | |    (eqof(IdDeq)(a,act(kind(a(i;t))))
. . . . . | | | |     ∨₂ false₂)
```

```
. . . . . | | | |    ⇒
. . . . . | | | |    P((λx.s(i;t).x),val(a(i;t))))
. . . . . | | | |   & (∀x:Id.
. . . . . | | | |      deq-member(...;<kind(a(i;t)),x>;1of())
. . . . . | | | |      ⇒
. . . . . | | | |      s(i;t+1).x
. . . . . | | | |      =
. . . . . | | | |      2of()
. . . . . | | | |      (<kind(a(i;t)),x>
. . . . . | | | |      ,λx.s(i;t).x
. . . . . | | | |      ,val(a(i;t))))
. . . . . | | | |   & (∀l:IdLnk.
. . . . . | | | |      deq-member(...;<kind(a(i;t)),l>;1of())
. . . . . | | | |      ⇒
. . . . . | | | |      withlnk(l;m(i;t))
. . . . . | | | |      =
. . . . . | | | |      if source(l) = i→
. . . . . | | | |         concat(map(λtgf.map(λx.
. . . . . | | | |         <1of(tgf)
. . . . . | | | |         ,x>;2of(tgf)
. . . . . | | | |             ((λx.s(i;t).x)
. . . . . | | | |             ,val(a(i;t))));...))
. . . . . | | | |      else nil fi)
. . . . . | | | |   & (∀x:Id.
. . . . . | | | |      ¬(deq-member(IdDeq;x;1of())
. . . . . | | | |        ⇒
. . . . . | | | |        deq-member(KindDeq;kind(a(i;t));2of()
. . . . . | | | |                                        (x)))
. . . . . | | | |      ⇒
. . . . . | | | |      s(i;t).x = s(i;t+1).x)
. . . . . | | | |   & (∀l:IdLnk, tg:Id.
. . . . . | | | |      ¬(deq-member(...;<l,tg>;1of())
. . . . . | | | |        ⇒
. . . . . | | | |        deq-member(KindDeq;kind(a(i;t));...))
. . . . . | | | |      ⇒
. . . . . | | | |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . | | | 13. ∀x:Id.
. . . . . | | | |   deq-member(IdDeq;x;1of())
. . . . . | | | |   ⇒
. . . . . | | | |   s(i;0).x = 2of()(x)
. . . . . | | | 14. ∀a@0:Action(i).
. . . . . | | | |   ¬isnull(a@0)
. . . . . | | | |   ⇒
. . . . . | | | |   (valtype(i;a@0) ⊆r <[locl(a)]
. . . . . | | | |                      ,λx.T>(kind(a@0))?Top)
. . . . . | | | 15. ∀x:Id.
. . . . . | | | |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(
. . . . . | | | |                                        ds))→
. . . . . | | | |                     2of(ds)(x)
. . . . . | | | |                  else Top fi
. . . . . | | | 16. IdDeq ∈ EqDecider(Id)
. . . . . | | | 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . . | | | 18. j : Id
. . . . . | | | 19. t : ℕ
. . . . . | | | 20. j = i
```

```
. . . . . | | | 21. ¬isnull(a(j;t))
. . . . . | | | 22. ¬isnull(a(i;t))
. . . . . | | | 23. (λx.s(i;t).x) ∈ State(ds)
. . . . . | | | 24. t' : ℕ
. . . . . | | | 25. t+1≤t'
. . . . . | | | 26. ∀v:T. ¬P((λx.s(i;t').x),v)
. . . . . | | | 27. t2 : ℕ
. . . . . | | | 28. t2<t'
. . . . . | | | 29. ¬isnull(a(i;t2))
. . . . . | | | 30. ∀t3:ℕ. t2<t3 & t3<t' ⇒ isnull(a(i;t3))
. . . . . | | | 31. t≤t2
. . . . . | | | 32. t<t2
. . . . . | | | ⊢  j = i & <j,t> <c <i,t2> ∨ <j,t> = <i,t2>
. . . . . | | | | by OrLeft THEN Try (Analyze THEN Reduce 0)
. . . . . | | | |
. . . . . | | | 1. i : Id
. . . . . | | | 2. a : Id
. . . . . | | | 3. T : Type
. . . . . | | | 4. ds : x:Id fp-> Type
. . . . . | | | 5. P : State(ds)→T→Prop
. . . . . | | | 6. w : World
. . . . . | | | 7. FairFifo
. . . . . | | | 8. FairFifo
. . . . . | | | 9. ∀l:IdLnk, tg:Id.
. . . . . | | | |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | | | |                  <ds
. . . . . | | | |                  ,<[locl(a)],λx.T>
. . . . . | | | |                  ,
. . . . . | | | |                  ,<[a],λx.P>
. . . . . | | | |                  ,
. . . . . | | | |                  ,
. . . . . | | | |                  ,
. . . . . | | | |                  ,
. . . . . | | | |                  ,.>
. . . . . | | | |               else  fi.da(rcv(l; tg))
. . . . . | | | 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . . | | | 11. ∀a@0:Id, t:ℕ.
. . . . . | | | |   ∃t':ℕ.
. . . . . | | | |   t≤t'
. . . . . | | | |   & ¬isnull(a(i;t'))
. . . . . | | | |     & kind(a(i;t')) = locl(a@0)
. . . . . | | | |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . . | | | |     ∨ P@0 != <[a]
. . . . . | | | |              ,λx.
. . . . . | | | |               P>(a@0) ==> ∀v:<[locl(a)]
. . . . . | | | |                                ,λx.
. . . . . | | | |                                 T>(...)?Top.
. . . . . | | | |       ¬P@0((λx.s(i;t').x),v)
. . . . . | | | 12. ∀t:ℕ.
. . . . . | | | |   ¬isnull(a(i;t))
. . . . . | | | |   ⇒
. . . . . | | | |   (islocal(kind(a(i;t)))
. . . . . | | | |    ⇒
. . . . . | | | |    (eqof(IdDeq)(a,act(kind(a(i;t))))
. . . . . | | | |     ∨₂ false₂)
```

```
. . . . . | | | |    ⇒
. . . . . | | | |    P((λx.s(i;t).x),val(a(i;t))))
. . . . . | | | |   & (∀x:Id.
. . . . . | | | |      deq-member(...;<kind(a(i;t)),x>;1of())
. . . . . | | | |      ⇒
. . . . . | | | |      s(i;t+1).x
. . . . . | | | |      =
. . . . . | | | |      2of()
. . . . . | | | |      (<kind(a(i;t)),x>
. . . . . | | | |      ,λx.s(i;t).x
. . . . . | | | |      ,val(a(i;t))))
. . . . . | | | |   & (∀l:IdLnk.
. . . . . | | | |      deq-member(...;<kind(a(i;t)),l>;1of())
. . . . . | | | |      ⇒
. . . . . | | | |      withlnk(l;m(i;t))
. . . . . | | | |      =
. . . . . | | | |      if source(l) = i→
. . . . . | | | |         concat(map(λtgf.map(λx.
. . . . . | | | |         <1of(tgf)
. . . . . | | | |         ,x>;2of(tgf)
. . . . . | | | |             ((λx.s(i;t).x)
. . . . . | | | |             ,val(a(i;t))));...))
. . . . . | | | |      else nil fi)
. . . . . | | | |   & (∀x:Id.
. . . . . | | | |      ¬(deq-member(IdDeq;x;1of())
. . . . . | | | |        ⇒
. . . . . | | | |        deq-member(KindDeq;kind(a(i;t));2of()
. . . . . | | | |                                        (x)))
. . . . . | | | |      ⇒
. . . . . | | | |      s(i;t).x = s(i;t+1).x)
. . . . . | | | |   & (∀l:IdLnk, tg:Id.
. . . . . | | | |      ¬(deq-member(...;<l,tg>;1of())
. . . . . | | | |        ⇒
. . . . . | | | |        deq-member(KindDeq;kind(a(i;t));...))
. . . . . | | | |      ⇒
. . . . . | | | |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . | | | 13. ∀x:Id.
. . . . . | | | |   deq-member(IdDeq;x;1of())
. . . . . | | | |   ⇒
. . . . . | | | |   s(i;0).x = 2of()(x)
. . . . . | | | 14. ∀a@0:Action(i).
. . . . . | | | |   ¬isnull(a@0)
. . . . . | | | |   ⇒
. . . . . | | | |   (valtype(i;a@0) ⊆r <[locl(a)]
. . . . . | | | |                       ,λx.T>(kind(a@0))?Top)
. . . . . | | | 15. ∀x:Id.
. . . . . | | | |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(
. . . . . | | | |                                          ds))→
. . . . . | | | |                      2of(ds)(x)
. . . . . | | | |                   else Top fi
. . . . . | | | 16. IdDeq ∈ EqDecider(Id)
. . . . . | | | 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . . | | | 18. j : Id
. . . . . | | | 19. t : ℕ
. . . . . | | | 20. j = i
```

```
. . . . . | | | 21. ¬isnull(a(j;t))
. . . . . | | | 22. ¬isnull(a(i;t))

. . . . . | | | 23. (λx.s(i;t).x) ∈ State(ds)
. . . . . | | | 24. t' : ℕ
. . . . . | | | 25. t+1≤t'
. . . . . | | | 26. ∀v:T. ¬P((λx.s(i;t').x),v)
. . . . . | | | 27. t2 : ℕ
. . . . . | | | 28. t2<t'
. . . . . | | | 29. ¬isnull(a(i;t2))
. . . . . | | | 30. ∀t3:ℕ. t2<t3 & t3<t' ⇒ isnull(a(i;t3))
. . . . . | | | 31. t≤t2
. . . . . | | | 32. t<t2
. . . . . | | | ⊢  <j,t> <c <i,t2>
. . . . . | | | | by ((Unfold `w-causl` 0
. . . . . | | | |      THEN
. . . . . | | | |      Unfold `rel_plus` 0
. . . . . | | | |      THEN
. . . . . | | | |      Reduce 0
. . . . . | | | |      THEN
. . . . . | | | |      InstConcl [1])
. . . . . | | | |     THEN
. . . . . | | | |     (Repeat
. . . . . | | | |      (RecUnfold `rel_exp` 0 THEN Reduce 0))
. . . . . | | | |     THEN
. . . . . | | | |     (InstConcl [<i,t2>]))
. . . . . | | | |    THEN
. . . . . | | | |    Try
. . . . . | | | |    (Unfold `w-E` 0 THEN Analyze THEN Reduce 0)
. . . . . | | | |    THEN
. . . . . | | | |    OrLeft
. . . . . | | | |    THENA
. . . . . | | | |    (Auto
. . . . . | | | |     THEN
. . . . . | | | |     Try
. . . . . | | | |     (Unfold `w-E` 0 THEN Analyze
. . . . . | | | |      THEN
. . . . . | | | |      Reduce 0))
. . . . . | | | |
. . . . . | | | 1. i : Id
. . . . . | | | 2. a : Id
. . . . . | | | 3. T : Type
. . . . . | | | 4. ds : x:Id fp-> Type
. . . . . | | | 5. P : State(ds)→T→Prop
. . . . . | | | 6. w : World
. . . . . | | | 7. FairFifo
. . . . . | | | 8. FairFifo
. . . . . | | | 9. ∀l:IdLnk, tg:Id.
. . . . . | | |    (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | | |                    <ds
. . . . . | | |                    ,<[locl(a)],λx.T>
. . . . . | | |                    ,
. . . . . | | |                    ,<[a],λx.P>
. . . . . | | |                    ,
. . . . . | | |                    ,
. . . . . | | |                    ,
```

```
. . . . . | | |                        ,
. . . . . | | |                        ,.>
. . . . . | | |                    else  fi.da(rcv(l; tg))
. . . . . | | | 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . . | | | 11. ∀a@0:Id, t:ℕ.
. . . . . | | |     ∃t':ℕ.
. . . . . | | |     t≤t'
. . . . . | | |     & ¬isnull(a(i;t'))
. . . . . | | |       & kind(a(i;t')) = locl(a@0)
. . . . . | | |       ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . . | | |       ∨ P@0 != <[a]
. . . . . | | |                ,λx.
. . . . . | | |                 P>(a@0) ==> ∀v:<[locl(a)]
. . . . . | | |                                ,λx.
. . . . . | | |                                 T>(...)?Top.
. . . . . | | |         ¬P@0((λx.s(i;t').x),v)
. . . . . | | | 12. ∀t:ℕ.
. . . . . | | |     ¬isnull(a(i;t))
. . . . . | | |     ⇒
. . . . . | | |     (islocal(kind(a(i;t)))
. . . . . | | |      ⇒
. . . . . | | |      (eqof(IdDeq)(a,act(kind(a(i;t))))
. . . . . | | |       ∨₂ false₂)
. . . . . | | |      ⇒
. . . . . | | |      P((λx.s(i;t).x),val(a(i;t))))
. . . . . | | |     & (∀x:Id.
. . . . . | | |        deq-member(...;<kind(a(i;t)),x>;1of())
. . . . . | | |        ⇒
. . . . . | | |        s(i;t+1).x
. . . . . | | |        =
. . . . . | | |        2of()
. . . . . | | |        (<kind(a(i;t)),x>
. . . . . | | |        ,λx.s(i;t).x
. . . . . | | |        ,val(a(i;t))))
. . . . . | | |     & (∀l:IdLnk.
. . . . . | | |        deq-member(...;<kind(a(i;t)),l>;1of())
. . . . . | | |        ⇒
. . . . . | | |        withlnk(l;m(i;t))
. . . . . | | |        =
. . . . . | | |        if source(l) = i→
. . . . . | | |           concat(map(λtgf.map(λx.
. . . . . | | |           <1of(tgf)
. . . . . | | |           ,x>;2of(tgf)
. . . . . | | |               ((λx.s(i;t).x)
. . . . . | | |               ,val(a(i;t))));...))
. . . . . | | |        else nil fi)
. . . . . | | |     & (∀x:Id.
. . . . . | | |        ¬(deq-member(IdDeq;x;1of())
. . . . . | | |          ⇒
. . . . . | | |          deq-member(KindDeq;kind(a(i;t));2of()
. . . . . | | |                                          (x)))
. . . . . | | |        ⇒
. . . . . | | |        s(i;t).x = s(i;t+1).x)
. . . . . | | |     & (∀l:IdLnk, tg:Id.
. . . . . | | |        ¬(deq-member(...;<l,tg>;1of())
```

```
. . . . . | | |          ⇒
. . . . . | | |          deq-member(KindDeq;kind(a(i;t));...))
. . . . . | | |        ⇒
. . . . . | | |        w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . | | | 13. ∀x:Id.
. . . . . | | |     deq-member(IdDeq;x;1of())
. . . . . | | |     ⇒
. . . . . | | |     s(i;0).x = 2of()(x)
. . . . . | | | 14. ∀a@0:Action(i).
. . . . . | | |     ¬isnull(a@0)
. . . . . | | |     ⇒
. . . . . | | |     (valtype(i;a@0) ⊆r <[locl(a)]
. . . . . | | |                         ,λx.T>(kind(a@0))?Top)
. . . . . | | | 15. ∀x:Id.
. . . . . | | |     vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(
. . . . . | | |                                          ds))→
. . . . . | | |                          2of(ds)(x)
. . . . . | | |                       else Top fi
. . . . . | | | 16. IdDeq ∈ EqDecider(Id)
. . . . . | | | 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . . | | | 18. j : Id
. . . . . | | | 19. t : ℕ
. . . . . | | | 20. j = i
. . . . . | | | 21. ¬isnull(a(j;t))
. . . . . | | | 22. ¬isnull(a(i;t))
. . . . . | | | 23. (λx.s(i;t).x) ∈ State(ds)
. . . . . | | | 24. t' : ℕ
. . . . . | | | 25. t+1≤t'
. . . . . | | | 26. ∀v:T. ¬P((λx.s(i;t').x),v)
. . . . . | | | 27. t2 : ℕ
. . . . . | | | 28. t2<t'
. . . . . | | | 29. ¬isnull(a(i;t2))
. . . . . | | | 30. ∀t3:ℕ. t2<t3 & t3<t' ⇒ isnull(a(i;t3))
. . . . . | | | 31. t≤t2
. . . . . | | | 32. t<t2
. . . . . | | | ⊢  <j,t> <loc <i,t2>
. . . . . | | |   by Unfold `w-locl` 0 THEN Reduce 0
. . . . . | | |
. . . . . | | .\
. . . . . | | . 1. i : Id
. . . . . | | . 2. a : Id
. . . . . | | . 3. T : Type
. . . . . | | . 4. ds : x:Id fp-> Type
. . . . . | | . 5. P : State(ds)→T→Prop
. . . . . | | . 6. w : World
. . . . . | | . 7. FairFifo
. . . . . | | . 8. FairFifo
. . . . . | | . 9. ∀l:IdLnk, tg:Id.
. . . . . | | . |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | | . |                    <ds
. . . . . | | . |                    ,<[locl(a)],λx.T>
. . . . . | | . |                    ,
. . . . . | | . |                    ,<[a],λx.P>
. . . . . | | . |                    ,
. . . . . | | . |                    ,
```

```
. . . . . | | . |                    ,
. . . . . | | . |                    ,
. . . . . | | . |                    ,·>
. . . . . | | . |                 else  fi.da(rcv(l; tg))
. . . . . | | . 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . . | | . 11. ∀a@0:Id, t:ℕ.
. . . . . | | . |   ∃t':ℕ.
. . . . . | | . |   t≤t'
. . . . . | | . |   & ¬isnull(a(i;t'))
. . . . . | | . |     & kind(a(i;t')) = locl(a@0)
. . . . . | | . |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . . | | . |     ∨ P@0 != <[a]
. . . . . | | . |              ,λx.
. . . . . | | . |               P>(a@0) ==> ∀v:<[locl(a)]
. . . . . | | . |                                ,λx.
. . . . . | | . |                                 T>(...)?Top.
. . . . . | | . |       ¬P@0((λx.s(i;t').x),v)
. . . . . | | . 12. ∀t:ℕ.
. . . . . | | . |   ¬isnull(a(i;t))
. . . . . | | . |   ⇒
. . . . . | | . |   (islocal(kind(a(i;t)))
. . . . . | | . |    ⇒
. . . . . | | . |    (eqof(IdDeq)(a,act(kind(a(i;t))))
. . . . . | | . |     ∨₂ false₂)
. . . . . | | . |    ⇒
. . . . . | | . |    P((λx.s(i;t).x),val(a(i;t))))
. . . . . | | . |   & (∀x:Id.
. . . . . | | . |      deq-member(...;<kind(a(i;t)),x>;1of())
. . . . . | | . |      ⇒
. . . . . | | . |      s(i;t+1).x
. . . . . | | . |      =
. . . . . | | . |      2of()
. . . . . | | . |      (<kind(a(i;t)),x>
. . . . . | | . |      ,λx.s(i;t).x
. . . . . | | . |      ,val(a(i;t))))
. . . . . | | . |   & (∀l:IdLnk.
. . . . . | | . |      deq-member(...;<kind(a(i;t)),l>;1of())
. . . . . | | . |      ⇒
. . . . . | | . |      withlnk(l;m(i;t))
. . . . . | | . |      =
. . . . . | | . |      if source(l) = i→
. . . . . | | . |         concat(map(λtgf.map(λx.
. . . . . | | . |         <1of(tgf)
. . . . . | | . |         ,x>;2of(tgf)
. . . . . | | . |             ((λx.s(i;t).x)
. . . . . | | . |             ,val(a(i;t))));...))
. . . . . | | . |      else nil fi)
. . . . . | | . |   & (∀x:Id.
. . . . . | | . |      ¬(deq-member(IdDeq;x;1of())
. . . . . | | . |        ⇒
. . . . . | | . |        deq-member(KindDeq;kind(a(i;t));2of()
. . . . . | | . |                                        (x)))
. . . . . | | . |      ⇒
. . . . . | | . |      s(i;t).x = s(i;t+1).x)
. . . . . | | . |   & (∀l:IdLnk, tg:Id.
```

```
. . . . . | | . |      ¬(deq-member(...;<l,tg>;1of())
. . . . . | | . |        ⇒
. . . . . | | . |        deq-member(KindDeq;kind(a(i;t));...))
. . . . . | | . |      ⇒
. . . . . | | . |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . | | . 13. ∀x:Id.
. . . . . | | . |   deq-member(IdDeq;x;1of())
. . . . . | | . |   ⇒
. . . . . | | . |   s(i;0).x = 2of()(x)
. . . . . | | . 14. ∀a@0:Action(i).
. . . . . | | . |   ¬isnull(a@0)
. . . . . | | . |   ⇒
. . . . . | | . |   (valtype(i;a@0) ⊆r <[locl(a)]
. . . . . | | . |                      ,λx.T>(kind(a@0))?Top)
. . . . . | | . 15. ∀x:Id.
. . . . . | | . |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(
. . . . . | | . |                                        ds))→
. . . . . | | . |                      2of(ds)(x)
. . . . . | | . |                  else Top fi
. . . . . | | . 16. IdDeq ∈ EqDecider(Id)
. . . . . | | . 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . . | | . 18. j : Id
. . . . . | | . 19. t : ℕ
. . . . . | | . 20. j = i
. . . . . | | . 21. ¬isnull(a(j;t))
. . . . . | | . 22. ¬isnull(a(i;t))
. . . . . | | . 23. (λx.s(i;t).x) ∈ State(ds)
. . . . . | | . 24. t' : ℕ
. . . . . | | . 25. t+1≤t'
. . . . . | | . 26. ∀v:T. ¬P((λx.s(i;t').x),v)
. . . . . | | . 27. t2 : ℕ
. . . . . | | . 28. t2<t'
. . . . . | | . 29. ¬isnull(a(i;t2))
. . . . . | | . 30. ∀t3:ℕ. t2<t3 & t3<t' ⇒ isnull(a(i;t3))
. . . . . | | . 31. t≤t2
. . . . . | | . 32. ¬t<t2
. . . . . | | . ⊢  j = i & <j,t> <c <i,t2> ∨ <j,t> = <i,t2>
. . . . . | | . | by OrRight
. . . . . | | . |    THENA
. . . . . | | . |    (Auto THEN Unfold `w-E` 0 THEN Analyze
. . . . . | | . |     THEN
. . . . . | | . |     Reduce 0)
. . . . . | | . |
. . . . . | | . 1. i : Id
. . . . . | | . 2. a : Id
. . . . . | | . 3. T : Type
. . . . . | | . 4. ds : x:Id fp-> Type
. . . . . | | . 5. P : State(ds)→T→Prop
. . . . . | | . 6. w : World
. . . . . | | . 7. FairFifo
. . . . . | | . 8. FairFifo
. . . . . | | . 9. ∀l:IdLnk, tg:Id.
. . . . . | | .    (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | | .                     <ds
. . . . . | | .                     ,<[locl(a)],λx.T>
```

```
. . . . . | | .                    ,
. . . . . | | .                    ,<[a],λx.P>
. . . . . | | .                    ,
. . . . . | | .                    ,
. . . . . | | .                    ,
. . . . . | | .                    ,
. . . . . | | .                    ,·>
. . . . . | | .                  else  fi.da(rcv(l; tg))
. . . . . | | . 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . . | | . 11. ∀a@0:Id, t:ℕ.
. . . . . | | .     ∃t':ℕ.
. . . . . | | .     t≤t'
. . . . . | | .     & ¬isnull(a(i;t'))
. . . . . | | .       & kind(a(i;t')) = locl(a@0)
. . . . . | | .       ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . . | | .       ∨ P@0 != <[a]
. . . . . | | .                ,λx.
. . . . . | | .                 P>(a@0) ==> ∀v:<[locl(a)]
. . . . . | | .                                ,λx.
. . . . . | | .                                 T>(...)?Top.
. . . . . | | .         ¬P@0((λx.s(i;t').x),v)
. . . . . | | . 12. ∀t:ℕ.
. . . . . | | .     ¬isnull(a(i;t))
. . . . . | | .     ⇒
. . . . . | | .     (islocal(kind(a(i;t)))
. . . . . | | .      ⇒
. . . . . | | .      (eqof(IdDeq)(a,act(kind(a(i;t))))
. . . . . | | .       ∨₂ false₂)
. . . . . | | .      ⇒
. . . . . | | .      P((λx.s(i;t).x),val(a(i;t))))
. . . . . | | .     & (∀x:Id.
. . . . . | | .        deq-member(...;<kind(a(i;t)),x>;1of())
. . . . . | | .        ⇒
. . . . . | | .        s(i;t+1).x
. . . . . | | .        =
. . . . . | | .        2of()
. . . . . | | .        (<kind(a(i;t)),x>
. . . . . | | .        ,λx.s(i;t).x
. . . . . | | .        ,val(a(i;t))))
. . . . . | | .     & (∀l:IdLnk.
. . . . . | | .        deq-member(...;<kind(a(i;t)),l>;1of())
. . . . . | | .        ⇒
. . . . . | | .        withlnk(l;m(i;t))
. . . . . | | .        =
. . . . . | | .        if source(l) = i→
. . . . . | | .           concat(map(λtgf.map(λx.
. . . . . | | .           <1of(tgf)
. . . . . | | .           ,x>;2of(tgf)
. . . . . | | .               ((λx.s(i;t).x)
. . . . . | | .               ,val(a(i;t))));...))
. . . . . | | .        else nil fi)
. . . . . | | .     & (∀x:Id.
. . . . . | | .        ¬(deq-member(IdDeq;x;1of())
. . . . . | | .          ⇒
. . . . . | | .          deq-member(KindDeq;kind(a(i;t));2of()
```

```
. . . . . | | .                                              (x)))
. . . . . | | .        ⇒
. . . . . | | .        s(i;t).x = s(i;t+1).x)
. . . . . | | .     & (∀l:IdLnk, tg:Id.
. . . . . | | .        ¬(deq-member(...;<l,tg>;1of())
. . . . . | | .          ⇒
. . . . . | | .          deq-member(KindDeq;kind(a(i;t));...))
. . . . . | | .        ⇒
. . . . . | | .        w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . | | . 13. ∀x:Id.
. . . . . | | .     deq-member(IdDeq;x;1of())
. . . . . | | .     ⇒
. . . . . | | .     s(i;0).x = 2of()(x)
. . . . . | | . 14. ∀a@0:Action(i).
. . . . . | | .     ¬isnull(a@0)
. . . . . | | .     ⇒
. . . . . | | .     (valtype(i;a@0) ⊆r <[locl(a)]
. . . . . | | .                        ,λx.T>(kind(a@0))?Top)
. . . . . | | . 15. ∀x:Id.
. . . . . | | .     vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(
. . . . . | | .                                          ds))→
. . . . . | | .                        2of(ds)(x)
. . . . . | | .                     else Top fi
. . . . . | | . 16. IdDeq ∈ EqDecider(Id)
. . . . . | | . 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . . | | . 18. j : Id
. . . . . | | . 19. t : ℕ
. . . . . | | . 20. j = i
. . . . . | | . 21. ¬isnull(a(j;t))
. . . . . | | . 22. ¬isnull(a(i;t))
. . . . . | | . 23. (λx.s(i;t).x) ∈ State(ds)
. . . . . | | . 24. t' : ℕ
. . . . . | | . 25. t+1≤t'
. . . . . | | . 26. ∀v:T. ¬P((λx.s(i;t').x),v)
. . . . . | | . 27. t2 : ℕ
. . . . . | | . 28. t2<t'
. . . . . | | . 29. ¬isnull(a(i;t2))
. . . . . | | . 30. ∀t3:ℕ. t2<t3 & t3<t' ⇒ isnull(a(i;t3))
. . . . . | | . 31. t≤t2
. . . . . | | . 32. ¬t<t2
. . . . . | | . ⊢  <j,t> = <i,t2>
. . . . . | | .   by Analyze THEN Reduce 0 THEN Analyze
. . . . . | |
. . . . . | .\
. . . . . | . 1. i : Id
. . . . . | . 2. a : Id
. . . . . | . 3. T : Type
. . . . . | . 4. ds : x:Id fp-> Type
. . . . . | . 5. P : State(ds)→T→Prop
. . . . . | . 6. w : World
. . . . . | . 7. p : FairFifo
. . . . . | . 8. FairFifo
. . . . . | . 9. ∀l:IdLnk, tg:Id.
. . . . . | . |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | . |                    <ds
```

```
. . . . . | . |                    ,<[locl(a)],λx.T>
. . . . . | . |                    ,
. . . . . | . |                    ,<[a],λx.P>
. . . . . | . |                    ,
. . . . . | . |                    ,
. . . . . | . |                    ,
. . . . . | . |                    ,
. . . . . | . |                    ,·>
. . . . . | . |                 else  fi.da(rcv(l; tg))
. . . . . | . 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . . | . 11. ∀a@0:Id, t:ℕ.
. . . . . | . |   ∃t':ℕ.
. . . . . | . |   t≤t'
. . . . . | . |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . . | . |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . . | . |     ∨ P@0 != <[a]
. . . . . | . |              ,λx.
. . . . . | . |               P>(a@0) ==> ∀v:<[locl(a)]
. . . . . | . |                                ,λx.
. . . . . | . |                                 T>(locl(a@0))?Top.
. . . . . | . |       ¬P@0((λx.s(i;t').x),v)
. . . . . | . 12. ∀t:ℕ.
. . . . . | . |   ¬isnull(a(i;t))
. . . . . | . |   ⇒
. . . . . | . |   (islocal(kind(a(i;t)))
. . . . . | . |    ⇒
. . . . . | . |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . . | . |    ⇒
. . . . . | . |    P((λx.s(i;t).x),val(a(i;t))))
. . . . . | . |   & (∀x:Id.
. . . . . | . |      deq-member(...;<kind(a(i;t)),x>;1of())
. . . . . | . |      ⇒
. . . . . | . |      s(i;t+1).x
. . . . . | . |      =
. . . . . | . |      2of()
. . . . . | . |      (<kind(a(i;t)),x>
. . . . . | . |      ,λx.s(i;t).x
. . . . . | . |      ,val(a(i;t))))
. . . . . | . |   & (∀l:IdLnk.
. . . . . | . |      deq-member(...;<kind(a(i;t)),l>;1of())
. . . . . | . |      ⇒
. . . . . | . |      withlnk(l;m(i;t))
. . . . . | . |      =
. . . . . | . |      if source(l) = i→
. . . . . | . |         concat(map(λtgf.map(λx.
. . . . . | . |         <1of(tgf)
. . . . . | . |         ,x>;2of(tgf)
. . . . . | . |             ((λx.s(i;t).x)
. . . . . | . |             ,val(a(i;t))));2of()
. . . . . | . |                              (<kind(a(i;t)),l>)))
. . . . . | . |      else nil fi)
. . . . . | . |   & (∀x:Id.
. . . . . | . |      ¬(deq-member(IdDeq;x;1of())
. . . . . | . |        ⇒
. . . . . | . |        deq-member(KindDeq;kind(a(i;t));2of()
```

```
. . . . . | . |                                          (x)))
. . . . . | . |      ⇒
. . . . . | . |      s(i;t).x = s(i;t+1).x)
. . . . . | . |   & (∀l:IdLnk, tg:Id.
. . . . . | . |      ¬...
. . . . . | . |      ⇒
. . . . . | . |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . | . 13. ∀x:Id.
. . . . . | . |   deq-member(IdDeq;x;1of())
. . . . . | . |   ⇒
. . . . . | . |   s(i;0).x = 2of()(x)
. . . . . | . 14. ∀a@0:Action(i).
. . . . . | . |   ¬isnull(a@0)
. . . . . | . |   ⇒
. . . . . | . |   (valtype(i;a@0) ⊆r <[locl(a)]
. . . . . | . |                      ,λx.T>(kind(a@0))?Top)
. . . . . | . 15. ∀x:Id.
. . . . . | . |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(
. . . . . | . |                                        ds))→
. . . . . | . |                    2of(ds)(x)
. . . . . | . |                 else Top fi
. . . . . | . 16. IdDeq ∈ EqDecider(Id)
. . . . . | . 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . . | . 18. j : Id
. . . . . | . 19. t : ℕ
. . . . . | . 20. j = i
. . . . . | . 21. ¬isnull(a(j;t))
. . . . . | . 22. ¬isnull(a(i;t))
. . . . . | . 23. (λx.s(i;t).x) ∈ State(ds)
. . . . . | . 24. t' : ℕ
. . . . . | . 25. t+1≤t'
. . . . . | . 26. ∀v:T. ¬P((λx.s(i;t').x),v)
. . . . . | . 27. t2 : ℕ
. . . . . | . 28. t2<t'
. . . . . | . 29. ¬isnull(a(i;t2))
. . . . . | . 30. ∀t3:ℕ. t2<t3 & t3<t' ⇒ isnull(a(i;t3))
. . . . . | . 31. t≤t2
. . . . . | . 32. loc(<j,t>) = loc(<i,t2>) & (<j,t> < <i,t2>)
. . . . . | . |   ∨ <j,t> = <i,t2>
. . . . . | . ⊢  kind(act(<i,t2>)) = locl(a)
. . . . . | . |  ∨ (∀v:T.
. . . . . | . |     ¬P((λz.s(1of(<i,t2>);2of(<i,t2>)+1).z),v))
. . . . . | . | by Unfold `w-act` 0 THEN Reduce 0 THEN OrRight
. . . . . | . |
. . . . . | . 1. i : Id
. . . . . | . 2. a : Id
. . . . . | . 3. T : Type
. . . . . | . 4. ds : x:Id fp-> Type
. . . . . | . 5. P : State(ds)→T→Prop
. . . . . | . 6. w : World
. . . . . | . 7. p : FairFifo
. . . . . | . 8. FairFifo
. . . . . | . 9. ∀l:IdLnk, tg:Id.
. . . . . | . |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | . |                    <ds
```

```
. . . . . | . |                    ,<[locl(a)],λx.T>
. . . . . | . |                    ,
. . . . . | . |                    ,<[a],λx.P>
. . . . . | . |                    ,
. . . . . | . |                    ,
. . . . . | . |                    ,
. . . . . | . |                    ,
. . . . . | . |                    ,·>
. . . . . | . |                 else  fi.da(rcv(l; tg))
. . . . . | . 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . . | . 11. ∀a@0:Id, t:ℕ.
. . . . . | . |   ∃t':ℕ.
. . . . . | . |   t≤t'
. . . . . | . |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . . | . |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . . | . |     ∨ P@0 != <[a]
. . . . . | . |              ,λx.
. . . . . | . |               P>(a@0) ==> ∀v:<[locl(a)]
. . . . . | . |                                ,λx.
. . . . . | . |                                 T>(locl(a@0))?Top.
. . . . . | . |       ¬P@0((λx.s(i;t').x),v)
. . . . . | . 12. ∀t:ℕ.
. . . . . | . |   ¬isnull(a(i;t))
. . . . . | . |   ⇒
. . . . . | . |   (islocal(kind(a(i;t)))
. . . . . | . |    ⇒
. . . . . | . |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . . | . |    ⇒
. . . . . | . |    P((λx.s(i;t).x),val(a(i;t))))
. . . . . | . |   & (∀x:Id.
. . . . . | . |      deq-member(...;<kind(a(i;t)),x>;1of())
. . . . . | . |      ⇒
. . . . . | . |      s(i;t+1).x
. . . . . | . |      =
. . . . . | . |      2of()
. . . . . | . |      (<kind(a(i;t)),x>
. . . . . | . |      ,λx.s(i;t).x
. . . . . | . |      ,val(a(i;t))))
. . . . . | . |   & (∀l:IdLnk.
. . . . . | . |      deq-member(...;<kind(a(i;t)),l>;1of())
. . . . . | . |      ⇒
. . . . . | . |      withlnk(l;m(i;t))
. . . . . | . |      =
. . . . . | . |      if source(l) = i→
. . . . . | . |         concat(map(λtgf.map(λx.
. . . . . | . |         <1of(tgf)
. . . . . | . |         ,x>;2of(tgf)
. . . . . | . |             ((λx.s(i;t).x)
. . . . . | . |             ,val(a(i;t))));2of()
. . . . . | . |                              (<kind(a(i;t)),l>)))
. . . . . | . |      else nil fi)
. . . . . | . |   & (∀x:Id.
. . . . . | . |      ¬(deq-member(IdDeq;x;1of())
. . . . . | . |        ⇒
. . . . . | . |        deq-member(KindDeq;kind(a(i;t));2of()
```

```
. . . . . | . |                                          (x)))
. . . . . | . |      ⇒
. . . . . | . |      s(i;t).x = s(i;t+1).x)
. . . . . | . |   & (∀l:IdLnk, tg:Id.
. . . . . | . |      ¬...
. . . . . | . |      ⇒
. . . . . | . |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . | . 13. ∀x:Id.
. . . . . | . |   deq-member(IdDeq;x;1of())
. . . . . | . |   ⇒
. . . . . | . |   s(i;0).x = 2of()(x)
. . . . . | . 14. ∀a@0:Action(i).
. . . . . | . |   ¬isnull(a@0)
. . . . . | . |   ⇒
. . . . . | . |   (valtype(i;a@0) ⊆r <[locl(a)]
. . . . . | . |                      ,λx.T>(kind(a@0))?Top)
. . . . . | . 15. ∀x:Id.
. . . . . | . |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(
. . . . . | . |                                          ds))→
. . . . . | . |                     2of(ds)(x)
. . . . . | . |                  else Top fi
. . . . . | . 16. IdDeq ∈ EqDecider(Id)
. . . . . | . 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . . | . 18. j : Id
. . . . . | . 19. t : ℕ
. . . . . | . 20. j = i
. . . . . | . 21. ¬isnull(a(j;t))
. . . . . | . 22. ¬isnull(a(i;t))
. . . . . | . 23. (λx.s(i;t).x) ∈ State(ds)
. . . . . | . 24. t' : ℕ
. . . . . | . 25. t+1≤t'
. . . . . | . 26. ∀v:T. ¬P((λx.s(i;t').x),v)
. . . . . | . 27. t2 : ℕ
. . . . . | . 28. t2<t'
. . . . . | . 29. ¬isnull(a(i;t2))
. . . . . | . 30. ∀t3:ℕ. t2<t3 & t3<t' ⇒ isnull(a(i;t3))
. . . . . | . 31. t≤t2
. . . . . | . 32. loc(<j,t>) = loc(<i,t2>) & (<j,t> < <i,t2>)
. . . . . | . |   ∨ <j,t> = <i,t2>
. . . . . | . 33. v : T
. . . . . | . ⊢  ¬P((λz.s(i;t2+1).z),v)
. . . . . | . | by AllHyps
. . . . . | . |    (λh.InstHyp [v] h THENA Complete Auto)
. . . . . | . |    THEN
. . . . . | . |    NthHypEq -1
. . . . . | . |
. . . . . | . .....assertion .....
. . . . . | . 1. i : Id
. . . . . | . 2. a : Id
. . . . . | . 3. T : Type
. . . . . | . 4. ds : x:Id fp-> Type
. . . . . | . 5. P : State(ds)→T→Prop
. . . . . | . 6. w : World
. . . . . | . 7. p : FairFifo
. . . . . | . 8. FairFifo
```

```
. . . . . | . 9. ∀l:IdLnk, tg:Id.
. . . . . | . |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | . |                   <ds
. . . . . | . |                   ,<[locl(a)],λx.T>
. . . . . | . |                   ,
. . . . . | . |                   ,<[a],λx.P>
. . . . . | . |                   ,
. . . . . | . |                   ,
. . . . . | . |                   ,
. . . . . | . |                   ,
. . . . . | . |                   ,·>
. . . . . | . |                else  fi.da(rcv(l; tg))
. . . . . | . 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . . | . 11. ∀a@0:Id, t:ℕ.
. . . . . | . |   ∃t':ℕ.
. . . . . | . |   t≤t'
. . . . . | . |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . . | . |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . . | . |     ∨ P@0 != <[a]
. . . . . | . |              ,λx.
. . . . . | . |               P>(a@0) ==> ∀v:<[locl(a)]
. . . . . | . |                                ,λx.
. . . . . | . |                                 T>(locl(a@0))?Top.
. . . . . | . |       ¬P@0((λx.s(i;t').x),v)
. . . . . | . 12. ∀t:ℕ.
. . . . . | . |   ¬isnull(a(i;t))
. . . . . | . |   ⇒
. . . . . | . |   (islocal(kind(a(i;t)))
. . . . . | . |    ⇒
. . . . . | . |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . . | . |    ⇒
. . . . . | . |    P((λx.s(i;t).x),val(a(i;t))))
. . . . . | . |   & (∀x:Id.
. . . . . | . |      deq-member(...;<kind(a(i;t)),x>;1of())
. . . . . | . |      ⇒
. . . . . | . |      s(i;t+1).x
. . . . . | . |      =
. . . . . | . |      2of()
. . . . . | . |      (<kind(a(i;t)),x>
. . . . . | . |      ,λx.s(i;t).x
. . . . . | . |      ,val(a(i;t))))
. . . . . | . |   & (∀l:IdLnk.
. . . . . | . |      deq-member(...;<kind(a(i;t)),l>;1of())
. . . . . | . |      ⇒
. . . . . | . |      withlnk(l;m(i;t))
. . . . . | . |      =
. . . . . | . |      if source(l) = i→
. . . . . | . |         concat(map(λtgf.map(λx.
. . . . . | . |         <1of(tgf)
. . . . . | . |         ,x>;2of(tgf)
. . . . . | . |             ((λx.s(i;t).x)
. . . . . | . |             ,val(a(i;t))));2of()
. . . . . | . |                            (<kind(a(i;t)),l>)))
. . . . . | . |      else nil fi)
. . . . . | . |   & (∀x:Id.
```

```
. . . . . | . |      ¬(deq-member(IdDeq;x;1of())
. . . . . | . |        ⇒
. . . . . | . |        deq-member(KindDeq;kind(a(i;t));2of()
. . . . . | . |                                        (x)))
. . . . . | . |      ⇒
. . . . . | . |      s(i;t).x = s(i;t+1).x)
. . . . . | . |   & (∀l:IdLnk, tg:Id.
. . . . . | . |      ¬...
. . . . . | . |      ⇒
. . . . . | . |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . | . 13. ∀x:Id.
. . . . . | . |   deq-member(IdDeq;x;1of())
. . . . . | . |   ⇒
. . . . . | . |   s(i;0).x = 2of()(x)
. . . . . | . 14. ∀a@0:Action(i).
. . . . . | . |   ¬isnull(a@0)
. . . . . | . |   ⇒
. . . . . | . |   (valtype(i;a@0) ⊆r <[locl(a)]
. . . . . | . |                      ,λx.T>(kind(a@0))?Top)
. . . . . | . 15. ∀x:Id.
. . . . . | . |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(
. . . . . | . |                                        ds))→
. . . . . | . |                     2of(ds)(x)
. . . . . | . |                  else Top fi
. . . . . | . 16. IdDeq ∈ EqDecider(Id)
. . . . . | . 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . . | . 18. j : Id
. . . . . | . 19. t : ℕ
. . . . . | . 20. j = i
. . . . . | . 21. ¬isnull(a(j;t))
. . . . . | . 22. ¬isnull(a(i;t))
. . . . . | . 23. (λx.s(i;t).x) ∈ State(ds)
. . . . . | . 24. t' : ℕ
. . . . . | . 25. t+1≤t'
. . . . . | . 26. ∀v:T. ¬P((λx.s(i;t').x),v)
. . . . . | . 27. t2 : ℕ
. . . . . | . 28. t2<t'
. . . . . | . 29. ¬isnull(a(i;t2))
. . . . . | . 30. ∀t3:ℕ. t2<t3 & t3<t' ⇒ isnull(a(i;t3))
. . . . . | . 31. t≤t2
. . . . . | . 32. loc(<j,t>) = loc(<i,t2>) & (<j,t> < <i,t2>)
. . . . . | . |   ∨ <j,t> = <i,t2>
. . . . . | . 33. v : T
. . . . . | . 34. ¬P((λx.s(i;t').x),v)
. . . . . | . ⊢  (¬P((λz.s(i;t2+1).z),v))
. . . . . | . |  =
. . . . . | . |  (¬P((λx.s(i;t').x),v))
. . . . . | . | by RepeatFor 3 Analyze THEN Unfold `ma-state` 0
. . . . . | . |    THEN
. . . . . | . |    Analyze
. . . . . | . |
. . . . . | . .....subterm .....
. . . . . | . 1. i : Id
. . . . . | . 2. a : Id
. . . . . | . 3. T : Type
```

```
. . . . . | . 4. ds : x:Id fp-> Type
. . . . . | . 5. P : State(ds)→T→Prop
. . . . . | . 6. w : World
. . . . . | . 7. p : FairFifo
. . . . . | . 8. FairFifo
. . . . . | . 9. ∀l:IdLnk, tg:Id.
. . . . . | . |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | . |                   <ds
. . . . . | . |                   ,<[locl(a)],λx.T>
. . . . . | . |                   ,
. . . . . | . |                   ,<[a],λx.P>
. . . . . | . |                   ,
. . . . . | . |                   ,
. . . . . | . |                   ,
. . . . . | . |                   ,
. . . . . | . |                   ,·>
. . . . . | . |               else  fi.da(rcv(l; tg))
. . . . . | . 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . . | . 11. ∀a@0:Id, t:ℕ.
. . . . . | . |   ∃t':ℕ.
. . . . . | . |   t≤t'
. . . . . | . |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . . | . |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . . | . |     ∨ P@0 != <[a]
. . . . . | . |              ,λx.
. . . . . | . |               P>(a@0) ==> ∀v:<[locl(a)]
. . . . . | . |                                ,λx.
. . . . . | . |                                 T>(locl(a@0))?Top.
. . . . . | . |       ¬P@0((λx.s(i;t').x),v)
. . . . . | . 12. ∀t:ℕ.
. . . . . | . |   ¬isnull(a(i;t))
. . . . . | . |   ⇒
. . . . . | . |   (islocal(kind(a(i;t)))
. . . . . | . |    ⇒
. . . . . | . |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . . | . |    ⇒
. . . . . | . |    P((λx.s(i;t).x),val(a(i;t))))
. . . . . | . |   & (∀x:Id.
. . . . . | . |      deq-member(...;<kind(a(i;t)),x>;1of())
. . . . . | . |      ⇒
. . . . . | . |      s(i;t+1).x
. . . . . | . |      =
. . . . . | . |      2of()
. . . . . | . |      (<kind(a(i;t)),x>
. . . . . | . |      ,λx.s(i;t).x
. . . . . | . |      ,val(a(i;t))))
. . . . . | . |   & (∀l:IdLnk.
. . . . . | . |      deq-member(...;<kind(a(i;t)),l>;1of())
. . . . . | . |      ⇒
. . . . . | . |      withlnk(l;m(i;t))
. . . . . | . |      =
. . . . . | . |      if source(l) = i→
. . . . . | . |         concat(map(λtgf.map(λx.
. . . . . | . |         <1of(tgf)
. . . . . | . |         ,x>;2of(tgf)
```

```
. . . . . | . |            ((λx.s(i;t).x)
. . . . . | . |            ,val(a(i;t))));2of()
. . . . . | . |                          (<kind(a(i;t)),l>)))
. . . . . | . |     else nil fi)
. . . . . | . |   & (∀x:Id.
. . . . . | . |     ¬(deq-member(IdDeq;x;1of())
. . . . . | . |       ⇒
. . . . . | . |       deq-member(KindDeq;kind(a(i;t));2of()
. . . . . | . |                                    (x)))
. . . . . | . |     ⇒
. . . . . | . |     s(i;t).x = s(i;t+1).x)
. . . . . | . |   & (∀l:IdLnk, tg:Id.
. . . . . | . |     ¬...
. . . . . | . |     ⇒
. . . . . | . |     w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . | . 13. ∀x:Id.
. . . . . | . |   deq-member(IdDeq;x;1of())
. . . . . | . |   ⇒
. . . . . | . |   s(i;0).x = 2of()(x)
. . . . . | . 14. ∀a@0:Action(i).
. . . . . | . |   ¬isnull(a@0)
. . . . . | . |   ⇒
. . . . . | . |   (valtype(i;a@0) ⊆r <[locl(a)]
. . . . . | . |                      ,λx.T>(kind(a@0))?Top)
. . . . . | . 15. ∀x:Id.
. . . . . | . |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(
. . . . . | . |                                    ds))→
. . . . . | . |                     2of(ds)(x)
. . . . . | . |                  else Top fi
. . . . . | . 16. IdDeq ∈ EqDecider(Id)
. . . . . | . 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . . | . 18. j : Id
. . . . . | . 19. t : ℕ
. . . . . | . 20. j = i
. . . . . | . 21. ¬isnull(a(j;t))
. . . . . | . 22. ¬isnull(a(i;t))
. . . . . | . 23. (λx.s(i;t).x) ∈ State(ds)
. . . . . | . 24. t' : ℕ
. . . . . | . 25. t+1≤t'
. . . . . | . 26. ∀v:T. ¬P((λx.s(i;t').x),v)
. . . . . | . 27. t2 : ℕ
. . . . . | . 28. t2<t'
. . . . . | . 29. ¬isnull(a(i;t2))
. . . . . | . 30. ∀t3:ℕ. t2<t3 & t3<t' ⇒ isnull(a(i;t3))
. . . . . | . 31. t≤t2
. . . . . | . 32. loc(<j,t>) = loc(<i,t2>) & (<j,t> < <i,t2>)
. . . . . | . |   ∨ <j,t> = <i,t2>
. . . . . | . 33. v : T
. . . . . | . 34. ¬P((λx.s(i;t').x),v)
. . . . . | . 35. z : Id
. . . . . | . ⊢  s(i;t2+1).z = s(i;t').z
. . . . . | . | by Assert
. . . . . | . |    (∀t:ℕ.
. . . . . | . |     t2+1≤t ⇒ t≤t' ⇒ s(i;t2+1).z = s(i;t).z)
. . . . . | . |    THEN
```

```
. . . . . | . |    Try (InstHyp [t'] -1)
. . . . . | . |
. . . . . | . .....assertion .....
. . . . . | . 1. i : Id
. . . . . | . 2. a : Id
. . . . . | . 3. T : Type
. . . . . | . 4. ds : x:Id fp-> Type
. . . . . | . 5. P : State(ds)→T→Prop
. . . . . | . 6. w : World
. . . . . | . 7. p : FairFifo
. . . . . | . 8. FairFifo
. . . . . | . 9. ∀l:IdLnk, tg:Id.
. . . . . | . |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | . |                    <ds
. . . . . | . |                    ,<[locl(a)],λx.T>
. . . . . | . |                    ,
. . . . . | . |                    ,<[a],λx.P>
. . . . . | . |                    ,
. . . . . | . |                    ,
. . . . . | . |                    ,
. . . . . | . |                    ,
. . . . . | . |                    ,·>
. . . . . | . |                else  fi.da(rcv(l; tg))
. . . . . | . 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . . | . 11. ∀a@0:Id, t:ℕ.
. . . . . | . |   ∃t':ℕ.
. . . . . | . |   t≤t'
. . . . . | . |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . . | . |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . . | . |     ∨ P@0 != <[a]
. . . . . | . |              ,λx.
. . . . . | . |               P>(a@0) ==> ∀v:<[locl(a)]
. . . . . | . |                                ,λx.
. . . . . | . |                                 T>(locl(a@0))?Top.
. . . . . | . |       ¬P@0((λx.s(i;t').x),v)
. . . . . | . 12. ∀t:ℕ.
. . . . . | . |   ¬isnull(a(i;t))
. . . . . | . |   ⇒
. . . . . | . |   (islocal(kind(a(i;t)))
. . . . . | . |    ⇒
. . . . . | . |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . . | . |    ⇒
. . . . . | . |    P((λx.s(i;t).x),val(a(i;t))))
. . . . . | . |   & (∀x:Id.
. . . . . | . |      deq-member(...;<kind(a(i;t)),x>;1of())
. . . . . | . |      ⇒
. . . . . | . |      s(i;t+1).x
. . . . . | . |      =
. . . . . | . |      2of()
. . . . . | . |      (<kind(a(i;t)),x>
. . . . . | . |      ,λx.s(i;t).x
. . . . . | . |      ,val(a(i;t))))
. . . . . | . |   & (∀l:IdLnk.
. . . . . | . |      deq-member(...;<kind(a(i;t)),l>;1of())
. . . . . | . |      ⇒
```

```
. . . . . | . |      withlnk(l;m(i;t))
. . . . . | . |      =
. . . . . | . |      if source(l) = i→
. . . . . | . |         concat(map(λtgf.map(λx.
. . . . . | . |         <1of(tgf)
. . . . . | . |         ,x>;2of(tgf)
. . . . . | . |             ((λx.s(i;t).x)
. . . . . | . |             ,val(a(i;t))));2of()
. . . . . | . |                           (<kind(a(i;t)),l>)))
. . . . . | . |      else nil fi)
. . . . . | . |   & (∀x:Id.
. . . . . | . |      ¬(deq-member(IdDeq;x;1of())
. . . . . | . |        ⇒
. . . . . | . |        deq-member(KindDeq;kind(a(i;t));2of()
. . . . . | . |                                        (x)))
. . . . . | . |      ⇒
. . . . . | . |      s(i;t).x = s(i;t+1).x)
. . . . . | . |   & (∀l:IdLnk, tg:Id.
. . . . . | . |      ¬...
. . . . . | . |      ⇒
. . . . . | . |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . | . 13. ∀x:Id.

. . . . . | . |   deq-member(IdDeq;x;1of())
. . . . . | . |   ⇒
. . . . . | . |   s(i;0).x = 2of()(x)
. . . . . | . 14. ∀a@0:Action(i).
. . . . . | . |   ¬isnull(a@0)
. . . . . | . |   ⇒
. . . . . | . |   (valtype(i;a@0) ⊆r <[locl(a)]
. . . . . | . |                        ,λx.T>(kind(a@0))?Top)
. . . . . | . 15. ∀x:Id.
. . . . . | . |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(
. . . . . | . |                                          ds))→
. . . . . | . |                        2of(ds)(x)
. . . . . | . |                    else Top fi
. . . . . | . 16. IdDeq ∈ EqDecider(Id)
. . . . . | . 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . . | . 18. j : Id
. . . . . | . 19. t : ℕ
. . . . . | . 20. j = i
. . . . . | . 21. ¬isnull(a(j;t))
. . . . . | . 22. ¬isnull(a(i;t))
. . . . . | . 23. (λx.s(i;t).x) ∈ State(ds)
. . . . . | . 24. t' : ℕ
. . . . . | . 25. t+1≤t'
. . . . . | . 26. ∀v:T. ¬P((λx.s(i;t').x),v)
. . . . . | . 27. t2 : ℕ
. . . . . | . 28. t2<t'
. . . . . | . 29. ¬isnull(a(i;t2))
. . . . . | . 30. ∀t3:ℕ. t2<t3 & t3<t' ⇒ isnull(a(i;t3))
. . . . . | . 31. t≤t2
. . . . . | . 32. loc(<j,t>) = loc(<i,t2>) & (<j,t> < <i,t2>)
. . . . . | . |   ∨ <j,t> = <i,t2>
. . . . . | . 33. v : T
. . . . . | . 34. ¬P((λx.s(i;t').x),v)
```

```
. . . . . | . 35. z : Id
. . . . . | . ⊢  ∀t:ℕ. t2+1≤t ⇒ t≤t' ⇒ s(i;t2+1).z = s(i;t).z
. . . . . | . | by InductionOnNat THEN Decide (t2+1≤t3-1)
. . . . . | . |
. . . . . | . |\
. . . . . | . | 1. i : Id
. . . . . | . | 2. a : Id
. . . . . | . | 3. T : Type
. . . . . | . | 4. ds : x:Id fp-> Type
. . . . . | . | 5. P : State(ds)→T→Prop
. . . . . | . | 6. w : World
. . . . . | . | 7. p : FairFifo
. . . . . | . | 8. FairFifo
. . . . . | . | 9. ∀l:IdLnk, tg:Id.
. . . . . | . | |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | . | |                    <ds
. . . . . | . | |                    ,<[locl(a)],λx.T>
. . . . . | . | |                    ,
. . . . . | . | |                    ,<[a],λx.P>
. . . . . | . | |                    ,
. . . . . | . | |                    ,
. . . . . | . | |                    ,
. . . . . | . | |                    ,
. . . . . | . | |                    ,.>
. . . . . | . | |                 else  fi.da(rcv(l; tg))
. . . . . | . | 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . . | . | 11. ∀a@0:Id, t:ℕ.
. . . . . | . | |   ∃t':ℕ.
. . . . . | . | |   t≤t'
. . . . . | . | |   & ¬isnull(a(i;t'))
. . . . . | . | |     & kind(a(i;t')) = locl(a@0)
. . . . . | . | |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . . | . | |     ∨ P@0 != <[a]
. . . . . | . | |              ,λx.
. . . . . | . | |               P>(a@0) ==> ∀v:<[locl(a)]
. . . . . | . | |                                ,λx.
. . . . . | . | |                                 T>(...)?Top.
. . . . . | . | |       ¬P@0((λx.s(i;t').x),v)
. . . . . | . | 12. ∀t:ℕ.
. . . . . | . | |   ¬isnull(a(i;t))
. . . . . | . | |   ⇒
. . . . . | . | |   (islocal(kind(a(i;t)))
. . . . . | . | |    ⇒
. . . . . | . | |    (eqof(IdDeq)(a,act(kind(a(i;t))))
. . . . . | . | |     ∨₂ false₂)
. . . . . | . | |    ⇒
. . . . . | . | |    P((λx.s(i;t).x),val(a(i;t))))
. . . . . | . | |   & (∀x:Id.
. . . . . | . | |      deq-member(...;<kind(a(i;t)),x>;1of())
. . . . . | . | |      ⇒
. . . . . | . | |      s(i;t+1).x
. . . . . | . | |      =
. . . . . | . | |      2of()
. . . . . | . | |      (<kind(a(i;t)),x>
. . . . . | . | |      ,λx.s(i;t).x
```

```
. . . . . | . | |      ,val(a(i;t))))
. . . . . | . | |   & (∀l:IdLnk.
. . . . . | . | |      deq-member(...;<kind(a(i;t)),l>;1of())
. . . . . | . | |      ⇒
. . . . . | . | |      withlnk(l;m(i;t))
. . . . . | . | |      =
. . . . . | . | |      if source(l) = i⟶
. . . . . | . | |         concat(map(λtgf.map(λx.
. . . . . | . | |         <1of(tgf)
. . . . . | . | |         ,x>;2of(tgf)
. . . . . | . | |             ((λx.s(i;t).x)
. . . . . | . | |             ,val(a(i;t))));...))
. . . . . | . | |      else nil fi)
. . . . . | . | |   & (∀x:Id.
. . . . . | . | |      ¬(deq-member(IdDeq;x;1of())
. . . . . | . | |        ⇒
. . . . . | . | |        deq-member(KindDeq;kind(a(i;t));2of()
. . . . . | . | |                                        (x)))
. . . . . | . | |      ⇒
. . . . . | . | |      s(i;t).x = s(i;t+1).x)
. . . . . | . | |   & (∀l:IdLnk, tg:Id.
. . . . . | . | |      ¬(deq-member(...;<l,tg>;1of())
. . . . . | . | |        ⇒
. . . . . | . | |        deq-member(KindDeq;kind(a(i;t));...))
. . . . . | . | |      ⇒
. . . . . | . | |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . | . | 13. ∀x:Id.
. . . . . | . | |   deq-member(IdDeq;x;1of())
. . . . . | . | |   ⇒
. . . . . | . | |   s(i;0).x = 2of()(x)
. . . . . | . | 14. ∀a@0:Action(i).
. . . . . | . | |   ¬isnull(a@0)
. . . . . | . | |   ⇒
. . . . . | . | |   (valtype(i;a@0) ⊆r <[locl(a)]
. . . . . | . | |                      ,λx.T>(kind(a@0))?Top)
. . . . . | . | 15. ∀x:Id.
. . . . . | . | |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(
. . . . . | . | |                                        ds))⟶
. . . . . | . | |                     2of(ds)(x)
. . . . . | . | |                  else Top fi
. . . . . | . | 16. IdDeq ∈ EqDecider(Id)
. . . . . | . | 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . . | . | 18. j : Id
. . . . . | . | 19. t : ℕ
. . . . . | . | 20. j = i
. . . . . | . | 21. ¬isnull(a(j;t))
. . . . . | . | 22. ¬isnull(a(i;t))
. . . . . | . | 23. (λx.s(i;t).x) ∈ State(ds)
. . . . . | . | 24. t' : ℕ
. . . . . | . | 25. t+1≤t'
. . . . . | . | 26. ∀v:T. ¬P((λx.s(i;t').x),v)
. . . . . | . | 27. t2 : ℕ
. . . . . | . | 28. t2<t'
. . . . . | . | 29. ¬isnull(a(i;t2))
. . . . . | . | 30. ∀t3:ℕ. t2<t3 & t3<t' ⇒ isnull(a(i;t3))
```

```
. . . . . | . | 31. t≤t2
. . . . . | . | 32. loc(<j,t>) = loc(<i,t2>) & (<j,t> < <i,t2>)
. . . . . | . | |   ∨ <j,t> = <i,t2>
. . . . . | . | 33. v : T
. . . . . | . | 34. ¬P((λx.s(i;t').x),v)
. . . . . | . | 35. z : Id
. . . . . | . | 36. t3 : ℤ
. . . . . | . | 37. 0<t3
. . . . . | . | 38. t2+1≤t3-1
. . . . . | . | |   ⇒
. . . . . | . | |   t3-1≤t' ⇒ s(i;t2+1).z = s(i;t3-1).z
. . . . . | . | 39. t2+1≤t3
. . . . . | . | 40. t3≤t'
. . . . . | . | 41. t2+1≤t3-1
. . . . . | . | ⊢  s(i;t2+1).z = s(i;t3).z
. . . . . | . | | by Analyze -4 THEN Analyze -1
. . . . . | . | |
. . . . . | . | 1. i : Id
. . . . . | . | 2. a : Id
. . . . . | . | 3. T : Type
. . . . . | . | 4. ds : x:Id fp-> Type
. . . . . | . | 5. P : State(ds)→T→Prop
. . . . . | . | 6. w : World
. . . . . | . | 7. p : FairFifo
. . . . . | . | 8. FairFifo
. . . . . | . | 9. ∀l:IdLnk, tg:Id.
. . . . . | . | |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | . | |                    <ds
. . . . . | . | |                    ,<[locl(a)],λx.T>
. . . . . | . | |                    ,
. . . . . | . | |                    ,<[a],λx.P>
. . . . . | . | |                    ,
. . . . . | . | |                    ,
. . . . . | . | |                    ,
. . . . . | . | |                    ,
. . . . . | . | |                    ,·>
. . . . . | . | |                 else  fi.da(rcv(l; tg))
. . . . . | . | 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . . | . | 11. ∀a@0:Id, t:ℕ.
. . . . . | . | |   ∃t':ℕ.
. . . . . | . | |   t≤t'
. . . . . | . | |   & ¬isnull(a(i;t'))
. . . . . | . | |     & kind(a(i;t')) = locl(a@0)
. . . . . | . | |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . . | . | |     ∨ P@0 != <[a]
. . . . . | . | |               ,λx.
. . . . . | . | |                P>(a@0) ==> ∀v:<[locl(a)]
. . . . . | . | |                                ,λx.
. . . . . | . | |                                 T>(...)?Top.
. . . . . | . | |       ¬P@0((λx.s(i;t').x),v)
. . . . . | . | 12. ∀t:ℕ.
. . . . . | . | |   ¬isnull(a(i;t))
. . . . . | . | |   ⇒
. . . . . | . | |   (islocal(kind(a(i;t)))
. . . . . | . | |    ⇒
```

```
. . . . . | . | |    (eqof(IdDeq)(a,act(kind(a(i;t))))
. . . . . | . | |     ∨₂ false₂)

. . . . . | . | |    ⇒
. . . . . | . | |    P((λx.s(i;t).x),val(a(i;t))))
. . . . . | . | |   & (∀x:Id.
. . . . . | . | |      deq-member(...;<kind(a(i;t)),x>;1of())
. . . . . | . | |      ⇒
. . . . . | . | |      s(i;t+1).x
. . . . . | . | |      =
. . . . . | . | |      2of()
. . . . . | . | |      (<kind(a(i;t)),x>
. . . . . | . | |      ,λx.s(i;t).x
. . . . . | . | |      ,val(a(i;t))))
. . . . . | . | |   & (∀l:IdLnk.
. . . . . | . | |      deq-member(...;<kind(a(i;t)),l>;1of())
. . . . . | . | |      ⇒
. . . . . | . | |      withlnk(l;m(i;t))
. . . . . | . | |      =
. . . . . | . | |      if source(l) = i→
. . . . . | . | |         concat(map(λtgf.map(λx.
. . . . . | . | |         <1of(tgf)
. . . . . | . | |         ,x>;2of(tgf)
. . . . . | . | |             ((λx.s(i;t).x)
. . . . . | . | |             ,val(a(i;t))));...))
. . . . . | . | |      else nil fi)
. . . . . | . | |   & (∀x:Id.
. . . . . | . | |      ¬(deq-member(IdDeq;x;1of())
. . . . . | . | |        ⇒
. . . . . | . | |        deq-member(KindDeq;kind(a(i;t));2of()
. . . . . | . | |                                        (x)))
. . . . . | . | |      ⇒
. . . . . | . | |      s(i;t).x = s(i;t+1).x)
. . . . . | . | |   & (∀l:IdLnk, tg:Id.
. . . . . | . | |      ¬(deq-member(...;<l,tg>;1of())
. . . . . | . | |        ⇒
. . . . . | . | |        deq-member(KindDeq;kind(a(i;t));...))
. . . . . | . | |      ⇒
. . . . . | . | |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . | . | 13. ∀x:Id.
. . . . . | . | |   deq-member(IdDeq;x;1of())
. . . . . | . | |   ⇒
. . . . . | . | |   s(i;0).x = 2of()(x)
. . . . . | . | 14. ∀a@0:Action(i).
. . . . . | . | |   ¬isnull(a@0)
. . . . . | . | |   ⇒
. . . . . | . | |   (valtype(i;a@0) ⊆r <[locl(a)]
. . . . . | . | |                      ,λx.T>(kind(a@0))?Top)
. . . . . | . | 15. ∀x:Id.
. . . . . | . | |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(
. . . . . | . | |                                        ds))→
. . . . . | . | |                     2of(ds)(x)
. . . . . | . | |                  else Top fi
. . . . . | . | 16. IdDeq ∈ EqDecider(Id)
. . . . . | . | 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . . | . | 18. j : Id
```

```
. . . . . | . | 19. t : ℕ
. . . . . | . | 20. j = i
. . . . . | . | 21. ¬isnull(a(j;t))
. . . . . | . | 22. ¬isnull(a(i;t))
. . . . . | . | 23. (λx.s(i;t).x) ∈ State(ds)
. . . . . | . | 24. t' : ℕ
. . . . . | . | 25. t+1≤t'
. . . . . | . | 26. ∀v:T. ¬P((λx.s(i;t').x),v)
. . . . . | . | 27. t2 : ℕ
. . . . . | . | 28. t2<t'
. . . . . | . | 29. ¬isnull(a(i;t2))
. . . . . | . | 30. ∀t3:ℕ. t2<t3 & t3<t' ⇒ isnull(a(i;t3))
. . . . . | . | 31. t≤t2
. . . . . | . | 32. loc(<j,t>) = loc(<i,t2>) & (<j,t> < <i,t2>)
. . . . . | . | |   ∨ <j,t> = <i,t2>
. . . . . | . | 33. v : T
. . . . . | . | 34. ¬P((λx.s(i;t').x),v)
. . . . . | . | 35. z : Id
. . . . . | . | 36. t3 : ℤ
. . . . . | . | 37. 0<t3
. . . . . | . | 38. t2+1≤t3
. . . . . | . | 39. t3≤t'
. . . . . | . | 40. t2+1≤t3-1
. . . . . | . | 41. s(i;t2+1).z = s(i;t3-1).z
. . . . . | . | ⊢  s(i;t2+1).z = s(i;t3).z
. . . . . | . | | by AllHyps
. . . . . | . | |    (λh.InstHyp [t3-1] h THENA Complete Auto)
. . . . . | . | |
. . . . . | . | 1. i : Id
. . . . . | . | 2. a : Id
. . . . . | . | 3. T : Type
. . . . . | . | 4. ds : x:Id fp-> Type
. . . . . | . | 5. P : State(ds)→T→Prop
. . . . . | . | 6. w : World
. . . . . | . | 7. p : FairFifo
. . . . . | . | 8. FairFifo
. . . . . | . | 9. ∀l:IdLnk, tg:Id.
. . . . . | . | |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | . | |                    <ds
. . . . . | . | |                    ,<[locl(a)],λx.T>
. . . . . | . | |                    ,
. . . . . | . | |                    ,<[a],λx.P>
. . . . . | . | |                    ,
. . . . . | . | |                    ,
. . . . . | . | |                    ,
. . . . . | . | |                    ,
. . . . . | . | |                    ,·>

. . . . . | . | |                 else  fi.da(rcv(l; tg))
. . . . . | . | 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . . | . | 11. ∀a@0:Id, t:ℕ.
. . . . . | . | |   ∃t':ℕ.
. . . . . | . | |   t≤t'
. . . . . | . | |   & ¬isnull(a(i;t'))
. . . . . | . | |     & kind(a(i;t')) = locl(a@0)
. . . . . | . | |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
```

```
. . . . . | . | |     ∨ P@0 != <[a]
. . . . . | . | |              ,λx.
. . . . . | . | |               P>(a@0) ==> ∀v:<[locl(a)]
. . . . . | . | |                                ,λx.
. . . . . | . | |                                 T>(...)?Top.
. . . . . | . | |       ¬P@0((λx.s(i;t').x),v)
. . . . . | . | 12. ∀t:ℕ.
. . . . . | . | |   ¬isnull(a(i;t))
. . . . . | . | |   ⇒
. . . . . | . | |   (islocal(kind(a(i;t)))
. . . . . | . | |    ⇒
. . . . . | . | |    (eqof(IdDeq)(a,act(kind(a(i;t))))
. . . . . | . | |     ∨₂ false₂)
. . . . . | . | |    ⇒
. . . . . | . | |    P((λx.s(i;t).x),val(a(i;t))))
. . . . . | . | |   & (∀x:Id.
. . . . . | . | |      deq-member(...;<kind(a(i;t)),x>;1of())
. . . . . | . | |      ⇒
. . . . . | . | |      s(i;t+1).x
. . . . . | . | |      =
. . . . . | . | |      2of()
. . . . . | . | |      (<kind(a(i;t)),x>
. . . . . | . | |      ,λx.s(i;t).x
. . . . . | . | |      ,val(a(i;t))))
. . . . . | . | |   & (∀l:IdLnk.
. . . . . | . | |      deq-member(...;<kind(a(i;t)),l>;1of())
. . . . . | . | |      ⇒
. . . . . | . | |      withlnk(l;m(i;t))
. . . . . | . | |      =
. . . . . | . | |      if source(l) = i→
. . . . . | . | |         concat(map(λtgf.map(λx.
. . . . . | . | |         <1of(tgf)
. . . . . | . | |         ,x>;2of(tgf)
. . . . . | . | |             ((λx.s(i;t).x)
. . . . . | . | |             ,val(a(i;t))));...))
. . . . . | . | |      else nil fi)
. . . . . | . | |   & (∀x:Id.
. . . . . | . | |      ¬(deq-member(IdDeq;x;1of())
. . . . . | . | |        ⇒
. . . . . | . | |        deq-member(KindDeq;kind(a(i;t));2of()
. . . . . | . | |                                        (x)))
. . . . . | . | |      ⇒
. . . . . | . | |      s(i;t).x = s(i;t+1).x)
. . . . . | . | |   & (∀l:IdLnk, tg:Id.
. . . . . | . | |      ¬(deq-member(...;<l,tg>;1of())
. . . . . | . | |        ⇒
. . . . . | . | |        deq-member(KindDeq;kind(a(i;t));...))
. . . . . | . | |      ⇒
. . . . . | . | |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . | . | 13. ∀x:Id.
. . . . . | . | |   deq-member(IdDeq;x;1of())
. . . . . | . | |   ⇒
. . . . . | . | |   s(i;0).x = 2of()(x)
. . . . . | . | 14. ∀a@0:Action(i).
. . . . . | . | |   ¬isnull(a@0)
```

```
. . . . . | . | |   ⇒
. . . . . | . | |   (valtype(i;a@0) ⊆r <[locl(a)]
. . . . . | . | |                     ,λx.T>(kind(a@0))?Top)
. . . . . | . | 15. ∀x:Id.
. . . . . | . | |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(
. . . . . | . | |                                        ds))→
. . . . . | . | |                     2of(ds)(x)
. . . . . | . | |                  else Top fi
. . . . . | . | 16. IdDeq ∈ EqDecider(Id)
. . . . . | . | 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . . | . | 18. j : Id
. . . . . | . | 19. t : ℕ
. . . . . | . | 20. j = i
. . . . . | . | 21. ¬isnull(a(j;t))
. . . . . | . | 22. ¬isnull(a(i;t))
. . . . . | . | 23. (λx.s(i;t).x) ∈ State(ds)
. . . . . | . | 24. t' : ℕ
. . . . . | . | 25. t+1≤t'
. . . . . | . | 26. ∀v:T. ¬P((λx.s(i;t').x),v)
. . . . . | . | 27. t2 : ℕ
. . . . . | . | 28. t2<t'
. . . . . | . | 29. ¬isnull(a(i;t2))
. . . . . | . | 30. ∀t3:ℕ. t2<t3 & t3<t' ⇒ isnull(a(i;t3))
. . . . . | . | 31. t≤t2
. . . . . | . | 32. loc(<j,t>) = loc(<i,t2>) & (<j,t> < <i,t2>)
. . . . . | . | |   ∨ <j,t> = <i,t2>
. . . . . | . | 33. v : T
. . . . . | . | 34. ¬P((λx.s(i;t').x),v)
. . . . . | . | 35. z : Id
. . . . . | . | 36. t3 : ℤ
. . . . . | . | 37. 0<t3
. . . . . | . | 38. t2+1≤t3
. . . . . | . | 39. t3≤t'
. . . . . | . | 40. t2+1≤t3-1
. . . . . | . | 41. s(i;t2+1).z = s(i;t3-1).z
. . . . . | . | 42. isnull(a(i;t3-1))
. . . . . | . | ⊢  s(i;t2+1).z = s(i;t3).z

. . . . . | . | | by AllHyps
. . . . . | . | |    (λh.
. . . . . | . | |     Analyze h THEN Analyze h+1
. . . . . | . | |     THEN
. . . . . | . | |     InstHyp [i;t3-1] h+1
. . . . . | . | |     THEN
. . . . . | . | |     Analyze -1
. . . . . | . | |     THEN
. . . . . | . | |     InstHyp [z] -2
. . . . . | . | |     THENA
. . . . . | . | |     (Auto THEN D_ES_Subtype))
. . . . . | . | |
. . . . . | . | 1. i : Id
. . . . . | . | 2. a : Id
. . . . . | . | 3. T : Type
. . . . . | . | 4. ds : x:Id fp-> Type
. . . . . | . | 5. P : State(ds)→T→Prop
. . . . . | . | 6. w : World
```

```
. . . . . | . | 7. p1 :
. . . . . | . | | ∀i:Id, t:ℕ, l:IdLnk.
. . . . . | . | | ¬source(l) = i ⇒ onlnk(l;m(i;t)) = nil
. . . . . | . | 8. p3 :
. . . . . | . | | ∀i:Id, t:ℕ.
. . . . . | . | | isnull(a(i;t))
. . . . . | . | | ⇒
. . . . . | . | | (∀x:Id. s(i;t+1).x = s(i;t).x) & m(i;t) = nil
. . . . . | . | 9. p4 :
. . . . . | . | | (∀i:Id, t:ℕ, l:IdLnk.
. . . . . | . | |  isrcv(l;a(i;t))
. . . . . | . | |  ⇒
. . . . . | . | |  destination(l) = i
. . . . . | . | |  & ||queue(l;t)||≥1
. . . . . | . | |    & hd(queue(l;t)) = msg(a(i;t)))
. . . . . | . | | & (∀l:IdLnk, t:ℕ.
. . . . . | . | |    ∃t':ℕ.
. . . . . | . | |    t≤t'
. . . . . | . | |    & isrcv(l;a(destination(l);t'))
. . . . . | . | |      ∨ queue(l;t') = nil)
. . . . . | . | 10. ∀i:Id, t:ℕ, l:IdLnk.
. . . . . | . | |  ¬source(l) = i ⇒ onlnk(l;m(i;t)) = nil
. . . . . | . | 11. ∀i:Id, t:ℕ.
. . . . . | . | |  isnull(a(i;t))
. . . . . | . | |  ⇒
. . . . . | . | |  (∀x:Id. s(i;t+1).x = s(i;t).x)
. . . . . | . | |  & m(i;t) = nil
. . . . . | . | 12. (∀i:Id, t:ℕ, l:IdLnk.
. . . . . | . | |  isrcv(l;a(i;t))
. . . . . | . | |  ⇒
. . . . . | . | |  destination(l) = i
. . . . . | . | |  & ||queue(l;t)||≥1
. . . . . | . | |    & hd(queue(l;t)) = msg(a(i;t)))
. . . . . | . | |  & (∀l:IdLnk, t:ℕ.
. . . . . | . | |    ∃t':ℕ.
. . . . . | . | |    t≤t'
. . . . . | . | |    & isrcv(l;a(destination(l);t'))
. . . . . | . | |      ∨ queue(l;t') = nil)
. . . . . | . | 13. ∀l:IdLnk, tg:Id.
. . . . . | . | |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | . | |                  <ds
. . . . . | . | |                  ,<[locl(a)],λx.T>
. . . . . | . | |                  ,
. . . . . | . | |                  ,<[a],λx.P>
. . . . . | . | |                  ,
. . . . . | . | |                  ,
. . . . . | . | |                  ,
. . . . . | . | |                  ,
. . . . . | . | |                  ,.>
. . . . . | . | |               else  fi.da(rcv(l; tg))
. . . . . | . | 14. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . . | . | 15. ∀a@0:Id, t:ℕ.
. . . . . | . | |  ∃t':ℕ.
. . . . . | . | |  t≤t'
. . . . . | . | |  & ¬isnull(a(i;t'))
```

```
. . . . . | . | |     & kind(a(i;t')) = locl(a@0)
. . . . . | . | |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . . | . | |     ∨ P@0 != <[a]
. . . . . | . | |              ,λx.
. . . . . | . | |               P>(a@0) ==> ∀v:<[locl(a)]
. . . . . | . | |                                ,λx.
. . . . . | . | |                                 T>(...)?Top.
. . . . . | . | |       ¬P@0((λx.s(i;t').x),v)
. . . . . | . | 16. ∀t:ℕ.
. . . . . | . | |   ¬isnull(a(i;t))
. . . . . | . | |   ⇒
. . . . . | . | |   (islocal(kind(a(i;t)))
. . . . . | . | |    ⇒
. . . . . | . | |    (eqof(IdDeq)(a,act(kind(a(i;t))))
. . . . . | . | |     ∨₂ false₂)
. . . . . | . | |    ⇒
. . . . . | . | |    P((λx.s(i;t).x),val(a(i;t))))
. . . . . | . | |   & (∀x:Id.
. . . . . | . | |      deq-member(...;<kind(a(i;t)),x>;1of())
. . . . . | . | |      ⇒
. . . . . | . | |      s(i;t+1).x
. . . . . | . | |      =
. . . . . | . | |      2of()
. . . . . | . | |      (<kind(a(i;t)),x>
. . . . . | . | |      ,λx.s(i;t).x
. . . . . | . | |      ,val(a(i;t))))
. . . . . | . | |   & (∀l:IdLnk.
. . . . . | . | |      deq-member(...;<kind(a(i;t)),l>;1of())
. . . . . | . | |      ⇒
. . . . . | . | |      withlnk(l;m(i;t))
. . . . . | . | |      =
. . . . . | . | |      if source(l) = i→
. . . . . | . | |         concat(map(λtgf.map(λx.
. . . . . | . | |         <1of(tgf)
. . . . . | . | |         ,x>;2of(tgf)
. . . . . | . | |             ((λx.s(i;t).x)
. . . . . | . | |             ,val(a(i;t))));...))
. . . . . | . | |      else nil fi)
. . . . . | . | |   & (∀x:Id.
. . . . . | . | |      ¬(deq-member(IdDeq;x;1of())
. . . . . | . | |        ⇒
. . . . . | . | |        deq-member(KindDeq;kind(a(i;t));2of()
. . . . . | . | |                                        (x)))
. . . . . | . | |      ⇒
. . . . . | . | |      s(i;t).x = s(i;t+1).x)
. . . . . | . | |   & (∀l:IdLnk, tg:Id.
. . . . . | . | |      ¬(deq-member(...;<l,tg>;1of())
. . . . . | . | |        ⇒
. . . . . | . | |        deq-member(KindDeq;kind(a(i;t));...))
. . . . . | . | |      ⇒
. . . . . | . | |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . | . | 17. ∀x:Id.
. . . . . | . | |   deq-member(IdDeq;x;1of())
. . . . . | . | |   ⇒
. . . . . | . | |   s(i;0).x = 2of()(x)
```

```
. . . . . | . | 18. ∀a@0:Action(i).
. . . . . | . | |   ¬isnull(a@0)
. . . . . | . | |   ⇒
. . . . . | . | |   (valtype(i;a@0) ⊆r <[locl(a)]
. . . . . | . | |                      ,λx.T>(kind(a@0))?Top)
. . . . . | . | 19. ∀x:Id.
. . . . . | . | |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(
. . . . . | . | |                                        ds))→
. . . . . | . | |                     2of(ds)(x)
. . . . . | . | |                  else Top fi
. . . . . | . | 20. IdDeq ∈ EqDecider(Id)
. . . . . | . | 21. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . . | . | 22. j : Id
. . . . . | . | 23. t : ℕ
. . . . . | . | 24. j = i
. . . . . | . | 25. ¬isnull(a(j;t))
. . . . . | . | 26. ¬isnull(a(i;t))
. . . . . | . | 27. (λx.s(i;t).x) ∈ State(ds)
. . . . . | . | 28. t' : ℕ
. . . . . | . | 29. t+1≤t'
. . . . . | . | 30. ∀v:T. ¬P((λx.s(i;t').x),v)
. . . . . | . | 31. t2 : ℕ
. . . . . | . | 32. t2<t'
. . . . . | . | 33. ¬isnull(a(i;t2))
. . . . . | . | 34. ∀t3:ℕ. t2<t3 & t3<t' ⇒ isnull(a(i;t3))
. . . . . | . | 35. t≤t2
. . . . . | . | 36. loc(<j,t>) = loc(<i,t2>) & (<j,t> < <i,t2>)
. . . . . | . | |   ∨ <j,t> = <i,t2>
. . . . . | . | 37. v : T
. . . . . | . | 38. ¬P((λx.s(i;t').x),v)
. . . . . | . | 39. z : Id
. . . . . | . | 40. t3 : ℤ
. . . . . | . | 41. 0<t3
. . . . . | . | 42. t2+1≤t3
. . . . . | . | 43. t3≤t'
. . . . . | . | 44. t2+1≤t3-1
. . . . . | . | 45. s(i;t2+1).z = s(i;t3-1).z
. . . . . | . | 46. isnull(a(i;t3-1))
. . . . . | . | 47. ∀x:Id. s(i;t3-1+1).x = s(i;t3-1).x
. . . . . | . | 48. m(i;t3-1) = nil
. . . . . | . | 49. s(i;t3-1+1).z = s(i;t3-1).z
. . . . . | . | 50. ∀x:Id. s(i;t3-1+1).x = s(i;t3-1).x
. . . . . | . | 51. m(i;t3-1) = nil
. . . . . | . | 52. s(i;t3-1+1).z = s(i;t3-1).z
. . . . . | . | ⊢  s(i;t2+1).z = s(i;t3).z
. . . . . | . | | by Subst ((t3-1+1) ∼ t3) -1
. . . . . | . | |
. . . . . | . | |\
. . . . . | . | | .....equality .....
. . . . . | . | | 1. i : Id
. . . . . | . | | 2. a : Id
. . . . . | . | | 3. T : Type
. . . . . | . | | 4. ds : x:Id fp-> Type
. . . . . | . | | 5. P : State(ds)→T→Prop
. . . . . | . | | 6. w : World
```

```
. . . . . | . | 7. p1 :
. . . . . | . |    ∀i:Id, t:ℕ, l:IdLnk.
. . . . . | . |    ¬source(l) = i ⇒ onlnk(l;m(i;t)) = nil
. . . . . | . | 8. p3 :
. . . . . | . |    ∀i:Id, t:ℕ.
. . . . . | . |    isnull(a(i;t))
. . . . . | . |    ⇒
. . . . . | . |    (∀x:Id. s(i;t+1).x = s(i;t).x)
. . . . . | . |    & m(i;t) = nil
. . . . . | . | 9. p4 :
. . . . . | . |    (∀i:Id, t:ℕ, l:IdLnk.
. . . . . | . |     isrcv(l;a(i;t))
. . . . . | . |     ⇒
. . . . . | . |     destination(l) = i
. . . . . | . |     & ||queue(l;t)||≥1
. . . . . | . |       & hd(queue(l;t)) = msg(a(i;t)))
. . . . . | . |    & (∀l:IdLnk, t:ℕ.
. . . . . | . |       ∃t':ℕ.
. . . . . | . |       t≤t'
. . . . . | . |       & isrcv(l;a(destination(l);t'))
. . . . . | . |         ∨ queue(l;t') = nil)
. . . . . | . | 10. ∀i:Id, t:ℕ, l:IdLnk.
. . . . . | . |     ¬source(l) = i ⇒ onlnk(l;m(i;t)) = nil
. . . . . | . | 11. ∀i:Id, t:ℕ.
. . . . . | . |     isnull(a(i;t))
. . . . . | . |     ⇒
. . . . . | . |     (∀x:Id. s(i;t+1).x = s(i;t).x)
. . . . . | . |     & m(i;t) = nil
. . . . . | . | 12. (∀i:Id, t:ℕ, l:IdLnk.
. . . . . | . |      isrcv(l;a(i;t))
. . . . . | . |      ⇒
. . . . . | . |      destination(l) = i
. . . . . | . |      & ||queue(l;t)||≥1
. . . . . | . |        & hd(queue(l;t)) = msg(a(i;t)))
. . . . . | . |     & (∀l:IdLnk, t:ℕ.
. . . . . | . |        ∃t':ℕ.
. . . . . | . |        t≤t'
. . . . . | . |        & isrcv(l;a(destination(l);t'))
. . . . . | . |          ∨ queue(l;t') = nil)
. . . . . | . | 13. ∀l:IdLnk, tg:Id.
. . . . . | . |     (w.M
. . . . . | . |      (l
. . . . . | . |      ,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | . |                   <ds
. . . . . | . |                   ,<[locl(a)],λx.T>
. . . . . | . |                   ,
. . . . . | . |                   ,<[a],λx.P>
. . . . . | . |                   ,
. . . . . | . |                   ,
. . . . . | . |                   ,
. . . . . | . |                   ,
. . . . . | . |                   ,.>
. . . . . | . |                else  fi.da(rcv(l; tg))
. . . . . | . | 14. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . . | . | 15. ∀a@0:Id, t:ℕ.
```

```
. . . . . | . | |     ∃t':ℕ.
. . . . . | . | |     t≤t'
. . . . . | . | |     & ¬isnull(a(i;t'))
. . . . . | . | |       & kind(a(i;t')) = locl(a@0)
. . . . . | . | |       ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . . | . | |       ∨ P@0 != <[a]
. . . . . | . | |                ,λx.
. . . . . | . | |                 P>(a@0) ==> ∀v:<[locl(a)]
. . . . . | . | |                                ,λx.
. . . . . | . | |                                 T>(...)?Top.
. . . . . | . | |         ¬P@0((λx.s(i;t').x),v)
. . . . . | . | | 16. ∀t:ℕ.
. . . . . | . | |     ¬isnull(a(i;t))
. . . . . | . | |     ⇒
. . . . . | . | |     (islocal(kind(a(i;t)))
. . . . . | . | |      ⇒
. . . . . | . | |      (eqof(IdDeq)(a,act(kind(a(i;t))))
. . . . . | . | |       ∨₂ false₂)
. . . . . | . | |      ⇒
. . . . . | . | |      P((λx.s(i;t).x),val(a(i;t))))
. . . . . | . | |     & (∀x:Id.
. . . . . | . | |        deq-member(...;<kind(a(i;t)),x>;1of())
. . . . . | . | |        ⇒
. . . . . | . | |        s(i;t+1).x
. . . . . | . | |        =
. . . . . | . | |        2of()
. . . . . | . | |        (<kind(a(i;t)),x>
. . . . . | . | |        ,λx.s(i;t).x
. . . . . | . | |        ,val(a(i;t))))
. . . . . | . | |     & (∀l:IdLnk.
. . . . . | . | |        deq-member(...;<kind(a(i;t)),l>;1of())
. . . . . | . | |        ⇒
. . . . . | . | |        withlnk(l;m(i;t))
. . . . . | . | |        =
. . . . . | . | |        if source(l) = i→
. . . . . | . | |           concat(map(λtgf.map(λx.
. . . . . | . | |           <1of(tgf)
. . . . . | . | |           ,x>;2of(tgf)
. . . . . | . | |               ((λx.s(i;t).x)
. . . . . | . | |               ,val(a(i;t))));...))
. . . . . | . | |        else nil fi)
. . . . . | . | |     & (∀x:Id.
. . . . . | . | |        ¬(deq-member(IdDeq;x;1of())
. . . . . | . | |          ⇒
. . . . . | . | |          deq-member(KindDeq;kind(a(i;t));2of()
. . . . . | . | |                                        (x)))
. . . . . | . | |        ⇒
. . . . . | . | |        s(i;t).x = s(i;t+1).x)
. . . . . | . | |     & (∀l:IdLnk, tg:Id.
. . . . . | . | |        ¬(deq-member(...;<l,tg>;1of())
. . . . . | . | |          ⇒
. . . . . | . | |          deq-member(KindDeq;kind(a(i;t));...))
. . . . . | . | |        ⇒
. . . . . | . | |        w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . | . | | 17. ∀x:Id.
```

```
. . . . . | . | |     deq-member(IdDeq;x;1of())
. . . . . | . | |     ⇒
. . . . . | . | |     s(i;0).x = 2of()(x)
. . . . . | . | | 18. ∀a@0:Action(i).
. . . . . | . | |     ¬isnull(a@0)
. . . . . | . | |     ⇒
. . . . . | . | |     (valtype(i;a@0) ⊆r <[locl(a)]
. . . . . | . | |                         ,λx.T>(kind(a@0))?Top)
. . . . . | . | | 19. ∀x:Id.
. . . . . | . | |     vartype(i;x) ⊆r if deq-member(...;x;1of(
. . . . . | . | |                                        ds))→
. . . . . | . | |                         2of(ds)(x)
. . . . . | . | |                       else Top fi
. . . . . | . | | 20. IdDeq ∈ EqDecider(Id)
. . . . . | . | | 21. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . . | . | | 22. j : Id
. . . . . | . | | 23. t : ℕ
. . . . . | . | | 24. j = i
. . . . . | . | | 25. ¬isnull(a(j;t))
. . . . . | . | | 26. ¬isnull(a(i;t))
. . . . . | . | | 27. (λx.s(i;t).x) ∈ State(ds)
. . . . . | . | | 28. t' : ℕ
. . . . . | . | | 29. t+1≤t'
. . . . . | . | | 30. ∀v:T. ¬P((λx.s(i;t').x),v)
. . . . . | . | | 31. t2 : ℕ
. . . . . | . | | 32. t2<t'
. . . . . | . | | 33. ¬isnull(a(i;t2))
. . . . . | . | | 34. ∀t3:ℕ. t2<t3 & t3<t' ⇒ isnull(a(i;t3))
. . . . . | . | | 35. t≤t2
. . . . . | . | | 36. loc(<j,t>) = loc(<i,t2>)
. . . . . | . | |     & (<j,t> < <i,t2>)
. . . . . | . | |     ∨ <j,t> = <i,t2>
. . . . . | . | | 37. v : T
. . . . . | . | | 38. ¬P((λx.s(i;t').x),v)
. . . . . | . | | 39. z : Id
. . . . . | . | | 40. t3 : ℤ
. . . . . | . | | 41. 0<t3
. . . . . | . | | 42. t2+1≤t3
. . . . . | . | | 43. t3≤t'
. . . . . | . | | 44. t2+1≤t3-1
. . . . . | . | | 45. s(i;t2+1).z = s(i;t3-1).z
. . . . . | . | | 46. isnull(a(i;t3-1))
. . . . . | . | | 47. ∀x:Id. s(i;t3-1+1).x = s(i;t3-1).x
. . . . . | . | | 48. m(i;t3-1) = nil
. . . . . | . | | 49. s(i;t3-1+1).z = s(i;t3-1).z
. . . . . | . | | 50. ∀x:Id. s(i;t3-1+1).x = s(i;t3-1).x
. . . . . | . | | 51. m(i;t3-1) = nil
. . . . . | . | | 52. s(i;t3-1+1).z = s(i;t3-1).z
. . . . . | . | | ⊢  (t3-1+1) ∼ t3  by Auto
. . . . . | . | |
. . . . . | . | .\
. . . . . | . | . 1. i : Id
. . . . . | . | . 2. a : Id
. . . . . | . | . 3. T : Type
. . . . . | . | . 4. ds : x:Id fp-> Type
```

```
. . . . . | . | . 5. P : State(ds)→T→Prop
. . . . . | . | . 6. w : World
. . . . . | . | . 7. p1 :
. . . . . | . | . |  ∀i:Id, t:ℕ, l:IdLnk.
. . . . . | . | . |  ¬source(l) = i ⇒ onlnk(l;m(i;t)) = nil
. . . . . | . | . 8. p3 :
. . . . . | . | . |  ∀i:Id, t:ℕ.
. . . . . | . | . |  isnull(a(i;t))
. . . . . | . | . |  ⇒
. . . . . | . | . |  (∀x:Id. s(i;t+1).x = s(i;t).x)
. . . . . | . | . |  & m(i;t) = nil
. . . . . | . | . 9. p4 :
. . . . . | . | . |  (∀i:Id, t:ℕ, l:IdLnk.
. . . . . | . | . |   isrcv(l;a(i;t))
. . . . . | . | . |   ⇒
. . . . . | . | . |   destination(l) = i
. . . . . | . | . |   & ||queue(l;t)||≥1
. . . . . | . | . |     & hd(queue(l;t)) = msg(a(i;t)))
. . . . . | . | . |  & (∀l:IdLnk, t:ℕ.
. . . . . | . | . |     ∃t':ℕ.
. . . . . | . | . |     t≤t'
. . . . . | . | . |     & isrcv(l;a(destination(l);t'))
. . . . . | . | . |       ∨ queue(l;t') = nil)
. . . . . | . | . 10. ∀i:Id, t:ℕ, l:IdLnk.
. . . . . | . | . |   ¬source(l) = i ⇒ onlnk(l;m(i;t)) = nil
. . . . . | . | . 11. ∀i:Id, t:ℕ.
. . . . . | . | . |   isnull(a(i;t))
. . . . . | . | . |   ⇒
. . . . . | . | . |   (∀x:Id. s(i;t+1).x = s(i;t).x)
. . . . . | . | . |   & m(i;t) = nil
. . . . . | . | . 12. (∀i:Id, t:ℕ, l:IdLnk.
. . . . . | . | . |    isrcv(l;a(i;t))
. . . . . | . | . |    ⇒
. . . . . | . | . |    destination(l) = i
. . . . . | . | . |    & ||queue(l;t)||≥1
. . . . . | . | . |      & hd(queue(l;t)) = msg(a(i;t)))
. . . . . | . | . |   & (∀l:IdLnk, t:ℕ.
. . . . . | . | . |      ∃t':ℕ.
. . . . . | . | . |      t≤t'
. . . . . | . | . |      & isrcv(l;a(destination(l);t'))
. . . . . | . | . |        ∨ queue(l;t') = nil)
. . . . . | . | . 13. ∀l:IdLnk, tg:Id.
. . . . . | . | . |   (w.M
. . . . . | . | . |    (l
. . . . . | . | . |    ,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | . | . |                <ds
. . . . . | . | . |                ,<[locl(a)],λx.T>
. . . . . | . | . |                ,
. . . . . | . | . |                ,<[a],λx.P>
. . . . . | . | . |                ,
. . . . . | . | . |                ,
. . . . . | . | . |                ,
. . . . . | . | . |                ,
. . . . . | . | . |                ,•>
. . . . . | . | . |            else  fi.da(rcv(l; tg))
```

```
. . . . . | . | . 14. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . . | . | . 15. ∀a@0:Id, t:ℕ.
. . . . . | . | . |   ∃t':ℕ.
. . . . . | . | . |   t≤t'
. . . . . | . | . |   & ¬isnull(a(i;t'))
. . . . . | . | . |     & kind(a(i;t')) = locl(a@0)
. . . . . | . | . |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . . | . | . |     ∨ P@0 != <[a]
. . . . . | . | . |               ,λx.
. . . . . | . | . |                P>(a@0) ==> ∀v:<[locl(a)]
. . . . . | . | . |                                ,λx.
. . . . . | . | . |                                 T>(...)?Top.
. . . . . | . | . |       ¬P@0((λx.s(i;t').x),v)
. . . . . | . | . 16. ∀t:ℕ.
. . . . . | . | . |   ¬isnull(a(i;t))
. . . . . | . | . |   ⇒
. . . . . | . | . |   (islocal(kind(a(i;t)))
. . . . . | . | . |    ⇒
. . . . . | . | . |    (eqof(IdDeq)(a,act(kind(a(i;t))))
. . . . . | . | . |     ∨₂ false₂)
. . . . . | . | . |    ⇒
. . . . . | . | . |    P((λx.s(i;t).x),val(a(i;t))))
. . . . . | . | . |   & (∀x:Id.
. . . . . | . | . |      deq-member(...;<kind(a(i;t)),x>;1of())
. . . . . | . | . |      ⇒
. . . . . | . | . |      s(i;t+1).x
. . . . . | . | . |      =
. . . . . | . | . |      2of()
. . . . . | . | . |      (<kind(a(i;t)),x>
. . . . . | . | . |      ,λx.s(i;t).x
. . . . . | . | . |      ,val(a(i;t))))
. . . . . | . | . |   & (∀l:IdLnk.
. . . . . | . | . |      deq-member(...;<kind(a(i;t)),l>;1of())
. . . . . | . | . |      ⇒
. . . . . | . | . |      withlnk(l;m(i;t))
. . . . . | . | . |      =
. . . . . | . | . |      if source(l) = i→
. . . . . | . | . |         concat(map(λtgf.map(λx.
. . . . . | . | . |         <1of(tgf)
. . . . . | . | . |         ,x>;2of(tgf)
. . . . . | . | . |             ((λx.s(i;t).x)
. . . . . | . | . |             ,val(a(i;t))));...))
. . . . . | . | . |      else nil fi)
. . . . . | . | . |   & (∀x:Id.
. . . . . | . | . |      ¬(deq-member(IdDeq;x;1of())
. . . . . | . | . |        ⇒
. . . . . | . | . |        deq-member(KindDeq;kind(a(i;t));2of()
. . . . . | . | . |                                       (x)))
. . . . . | . | . |      ⇒
. . . . . | . | . |      s(i;t).x = s(i;t+1).x)
. . . . . | . | . |   & (∀l:IdLnk, tg:Id.
. . . . . | . | . |      ¬(deq-member(...;<l,tg>;1of())
. . . . . | . | . |        ⇒
. . . . . | . | . |        deq-member(KindDeq;kind(a(i;t));...))
. . . . . | . | . |      ⇒
```

```
. . . . . | . | . |     w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . | . | . 17. ∀x:Id.
. . . . . | . | . |   deq-member(IdDeq;x;1of())
. . . . . | . | . |   ⇒
. . . . . | . | . |   s(i;0).x = 2of()(x)
. . . . . | . | . 18. ∀a@0:Action(i).
. . . . . | . | . |   ¬isnull(a@0)
. . . . . | . | . |   ⇒
. . . . . | . | . |   (valtype(i;a@0) ⊆r <[locl(a)]
. . . . . | . | . |                      ,λx.T>(kind(a@0))?Top)
. . . . . | . | . 19. ∀x:Id.
. . . . . | . | . |   vartype(i;x) ⊆r if deq-member(...;x;1of(
. . . . . | . | . |                                      ds))→
. . . . . | . | . |                     2of(ds)(x)
. . . . . | . | . |                  else Top fi
. . . . . | . | . 20. IdDeq ∈ EqDecider(Id)
. . . . . | . | . 21. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . . | . | . 22. j : Id
. . . . . | . | . 23. t : ℕ
. . . . . | . | . 24. j = i
. . . . . | . | . 25. ¬isnull(a(j;t))
. . . . . | . | . 26. ¬isnull(a(i;t))
. . . . . | . | . 27. (λx.s(i;t).x) ∈ State(ds)
. . . . . | . | . 28. t' : ℕ
. . . . . | . | . 29. t+1≤t'
. . . . . | . | . 30. ∀v:T. ¬P((λx.s(i;t').x),v)
. . . . . | . | . 31. t2 : ℕ
. . . . . | . | . 32. t2<t'
. . . . . | . | . 33. ¬isnull(a(i;t2))
. . . . . | . | . 34. ∀t3:ℕ. t2<t3 & t3<t' ⇒ isnull(a(i;t3))
. . . . . | . | . 35. t≤t2
. . . . . | . | . 36. loc(<j,t>) = loc(<i,t2>)
. . . . . | . | . |   & (<j,t> < <i,t2>)
. . . . . | . | . |   ∨ <j,t> = <i,t2>
. . . . . | . | . 37. v : T
. . . . . | . | . 38. ¬P((λx.s(i;t').x),v)
. . . . . | . | . 39. z : Id
. . . . . | . | . 40. t3 : ℤ
. . . . . | . | . 41. 0<t3
. . . . . | . | . 42. t2+1≤t3
. . . . . | . | . 43. t3≤t'
. . . . . | . | . 44. t2+1≤t3-1
. . . . . | . | . 45. s(i;t2+1).z = s(i;t3-1).z
. . . . . | . | . 46. isnull(a(i;t3-1))
. . . . . | . | . 47. ∀x:Id. s(i;t3-1+1).x = s(i;t3-1).x
. . . . . | . | . 48. m(i;t3-1) = nil
. . . . . | . | . 49. s(i;t3-1+1).z = s(i;t3-1).z
. . . . . | . | . 50. ∀x:Id. s(i;t3-1+1).x = s(i;t3-1).x
. . . . . | . | . 51. m(i;t3-1) = nil
. . . . . | . | . 52. s(i;t3).z = s(i;t3-1).z
. . . . . | . | . ⊢  s(i;t2+1).z = s(i;t3).z  by HypSubst -1 0
. . . . . | . | . |
. . . . . | . | . .....subterm .....
. . . . . | . | . 1. i : Id
. . . . . | . | . 2. a : Id
```

```
. . . . . | . | . 3. T : Type
. . . . . | . | . 4. ds : x:Id fp-> Type
. . . . . | . | . 5. P : State(ds)→T→Prop
. . . . . | . | . 6. w : World
. . . . . | . | . 7. p1 :
. . . . . | . | . |  ∀i:Id, t:ℕ, l:IdLnk.
. . . . . | . | . |  ¬source(l) = i ⇒ onlnk(l;m(i;t)) = nil
. . . . . | . | . 8. p3 :
. . . . . | . | . |  ∀i:Id, t:ℕ.
. . . . . | . | . |  isnull(a(i;t))
. . . . . | . | . |  ⇒
. . . . . | . | . |  (∀x:Id. s(i;t+1).x = s(i;t).x)
. . . . . | . | . |  & m(i;t) = nil
. . . . . | . | . 9. p5 :
. . . . . | . | . |  ∀i:Id, t:ℕ, l:IdLnk.
. . . . . | . | . |  isrcv(l;a(i;t))
. . . . . | . | . |  ⇒
. . . . . | . | . |  destination(l) = i
. . . . . | . | . |  & ||queue(l;t)||≥1
. . . . . | . | . |    & hd(queue(l;t)) = msg(a(i;t))
. . . . . | . | . 10. p6 :
. . . . . | . | . |   ∀l:IdLnk, t:ℕ.
. . . . . | . | . |   ∃t':ℕ.
. . . . . | . | . |   t≤t'
. . . . . | . | . |   & isrcv(l;a(destination(l);t'))
. . . . . | . | . |     ∨ queue(l;t') = nil
. . . . . | . | . 11. ∀i:Id, t:ℕ, l:IdLnk.
. . . . . | . | . |   ¬source(l) = i ⇒ onlnk(l;m(i;t)) = nil
. . . . . | . | . 12. ∀i:Id, t:ℕ.
. . . . . | . | . |   isnull(a(i;t))
. . . . . | . | . |   ⇒
. . . . . | . | . |   (∀x:Id. s(i;t+1).x = s(i;t).x)
. . . . . | . | . |   & m(i;t) = nil
. . . . . | . | . 13. ∀i:Id, t:ℕ, l:IdLnk.
. . . . . | . | . |   isrcv(l;a(i;t))
. . . . . | . | . |   ⇒
. . . . . | . | . |   destination(l) = i
. . . . . | . | . |   & ||queue(l;t)||≥1
. . . . . | . | . |     & hd(queue(l;t)) = msg(a(i;t))
. . . . . | . | . 14. ∀l:IdLnk, t:ℕ.
. . . . . | . | . |   ∃t':ℕ.
. . . . . | . | . |   t≤t'
. . . . . | . | . |   & isrcv(l;a(destination(l);t'))
. . . . . | . | . |     ∨ queue(l;t') = nil
. . . . . | . | . 15. ∀l:IdLnk, tg:Id.
. . . . . | . | . |   (w.M
. . . . . | . | . |    (l
. . . . . | . | . |    ,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | . | . |                <ds
. . . . . | . | . |                ,<[locl(a)],λx.T>
. . . . . | . | . |                ,
. . . . . | . | . |                ,<[a],λx.P>
. . . . . | . | . |                ,
. . . . . | . | . |                ,
. . . . . | . | . |                ,
```

```
. . . . . | . | . |                ,
. . . . . | . | . |                ,.>
. . . . . | . | . |             else  fi.da(rcv(l; tg))
. . . . . | . | . 16. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . . | . | . 17. ∀a@0:Id, t:ℕ.
. . . . . | . | . |   ∃t':ℕ.
. . . . . | . | . |   t≤t'
. . . . . | . | . |   & ¬isnull(a(i;t'))
. . . . . | . | . |     & kind(a(i;t')) = locl(a@0)
. . . . . | . | . |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . . | . | . |     ∨ P@0 != <[a]
. . . . . | . | . |              ,λx.
. . . . . | . | . |               P>(a@0) ==> ∀v:<[locl(a)]
. . . . . | . | . |                                ,λx.
. . . . . | . | . |                                 T>(...)?Top.
. . . . . | . | . |       ¬P@0((λx.s(i;t').x),v)
. . . . . | . | . 18. ∀t:ℕ.
. . . . . | . | . |   ¬isnull(a(i;t))
. . . . . | . | . |   ⇒
. . . . . | . | . |   (islocal(kind(a(i;t)))
. . . . . | . | . |    ⇒
. . . . . | . | . |    (eqof(IdDeq)(a,act(kind(a(i;t))))
. . . . . | . | . |     ∨₂ false₂)
. . . . . | . | . |    ⇒
. . . . . | . | . |    P((λx.s(i;t).x),val(a(i;t))))
. . . . . | . | . |   & (∀x:Id.
. . . . . | . | . |      deq-member(...;<kind(a(i;t)),x>;1of())
. . . . . | . | . |      ⇒
. . . . . | . | . |      s(i;t+1).x
. . . . . | . | . |      =
. . . . . | . | . |      2of()
. . . . . | . | . |      (<kind(a(i;t)),x>
. . . . . | . | . |      ,λx.s(i;t).x
. . . . . | . | . |      ,val(a(i;t))))
. . . . . | . | . |   & (∀l:IdLnk.
. . . . . | . | . |      deq-member(...;<kind(a(i;t)),l>;1of())
. . . . . | . | . |      ⇒
. . . . . | . | . |      withlnk(l;m(i;t))
. . . . . | . | . |      =
. . . . . | . | . |      if source(l) = i→
. . . . . | . | . |         concat(map(λtgf.map(λx.
. . . . . | . | . |         <1of(tgf)
. . . . . | . | . |         ,x>;2of(tgf)
. . . . . | . | . |             ((λx.s(i;t).x)
. . . . . | . | . |             ,val(a(i;t))));...))
. . . . . | . | . |      else nil fi)
. . . . . | . | . |   & (∀x:Id.
. . . . . | . | . |      ¬(deq-member(IdDeq;x;1of())
. . . . . | . | . |        ⇒
. . . . . | . | . |        deq-member(KindDeq;kind(a(i;t));2of()
. . . . . | . | . |                                        (x)))
. . . . . | . | . |      ⇒
. . . . . | . | . |      s(i;t).x = s(i;t+1).x)
. . . . . | . | . |   & (∀l:IdLnk, tg:Id.
. . . . . | . | . |      ¬(deq-member(...;<l,tg>;1of())
```

```
. . . . . | . | . |       ⇒
. . . . . | . | . |       deq-member(KindDeq;kind(a(i;t));...))
. . . . . | . | . |     ⇒
. . . . . | . | . |     w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . | . | . 19. ∀x:Id.
. . . . . | . | . |   deq-member(IdDeq;x;1of())
. . . . . | . | . |   ⇒
. . . . . | . | . |   s(i;0).x = 2of()(x)
. . . . . | . | . 20. ∀a@0:Action(i).
. . . . . | . | . |   ¬isnull(a@0)
. . . . . | . | . |   ⇒
. . . . . | . | . |   (valtype(i;a@0) ⊆r <[locl(a)]
. . . . . | . | . |                      ,λx.T>(kind(a@0))?Top)
. . . . . | . | . 21. ∀x:Id.
. . . . . | . | . |   vartype(i;x) ⊆r if deq-member(...;x;1of(
. . . . . | . | . |                                      ds))→
. . . . . | . | . |                      2of(ds)(x)
. . . . . | . | . |                  else Top fi
. . . . . | . | . 22. IdDeq ∈ EqDecider(Id)
. . . . . | . | . 23. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . . | . | . 24. j : Id
. . . . . | . | . 25. t : ℕ
. . . . . | . | . 26. j = i
. . . . . | . | . 27. ¬isnull(a(j;t))
. . . . . | . | . 28. ¬isnull(a(i;t))
. . . . . | . | . 29. (λx.s(i;t).x) ∈ State(ds)
. . . . . | . | . 30. t' : ℕ
. . . . . | . | . 31. t+1≤t'
. . . . . | . | . 32. ∀v:T. ¬P((λx.s(i;t').x),v)
. . . . . | . | . 33. t2 : ℕ
. . . . . | . | . 34. t2<t'
. . . . . | . | . 35. ¬isnull(a(i;t2))
. . . . . | . | . 36. ∀t3:ℕ. t2<t3 & t3<t' ⇒ isnull(a(i;t3))
. . . . . | . | . 37. t≤t2
. . . . . | . | . 38. loc(<j,t>) = loc(<i,t2>)
. . . . . | . | . |   & (<j,t> < <i,t2>)
. . . . . | . | . |   ∨ <j,t> = <i,t2>
. . . . . | . | . 39. v : T
. . . . . | . | . 40. ¬P((λx.s(i;t').x),v)
. . . . . | . | . 41. z : Id
. . . . . | . | . 42. t3 : ℤ
. . . . . | . | . 43. 0<t3
. . . . . | . | . 44. t2+1≤t3
. . . . . | . | . 45. t3≤t'
. . . . . | . | . 46. t2+1≤t3-1
. . . . . | . | . 47. s(i;t2+1).z = s(i;t3-1).z
. . . . . | . | . 48. isnull(a(i;t3-1))
. . . . . | . | . 49. ∀x:Id. s(i;t3-1+1).x = s(i;t3-1).x
. . . . . | . | . 50. m(i;t3-1) = nil
. . . . . | . | . 51. s(i;t3-1+1).z = s(i;t3-1).z
. . . . . | . | . 52. ∀x:Id. s(i;t3-1+1).x = s(i;t3-1).x
. . . . . | . | . 53. m(i;t3-1) = nil
. . . . . | . | . 54. s(i;t3).z = s(i;t3-1).z
. . . . . | . | . 55. z1 : vartype(i;z)
. . . . . | . | . ⊢  z1 ∈ ds(z)?Top  by DoSubsume
```

```
. . . . . | . | . |
. . . . . | . | . .....subtype_rel .....
. . . . . | . | . 1. i : Id
. . . . . | . | . 2. a : Id
. . . . . | . | . 3. T : Type
. . . . . | . | . 4. ds : x:Id fp-> Type
. . . . . | . | . 5. P : State(ds)→T→Prop
. . . . . | . | . 6. w : World
. . . . . | . | . 7. p1 :
. . . . . | . | .    ∀i:Id, t:ℕ, l:IdLnk.
. . . . . | . | .    ¬source(l) = i ⇒ onlnk(l;m(i;t)) = nil
. . . . . | . | . 8. p3 :
. . . . . | . | .    ∀i:Id, t:ℕ.
. . . . . | . | .    isnull(a(i;t))
. . . . . | . | .    ⇒
. . . . . | . | .    (∀x:Id. s(i;t+1).x = s(i;t).x)
. . . . . | . | .    & m(i;t) = nil
. . . . . | . | . 9. p5 :
. . . . . | . | .    ∀i:Id, t:ℕ, l:IdLnk.
. . . . . | . | .    isrcv(l;a(i;t))
. . . . . | . | .    ⇒
. . . . . | . | .    destination(l) = i
. . . . . | . | .    & ||queue(l;t)||≥1
. . . . . | . | .      & hd(queue(l;t)) = msg(a(i;t))
. . . . . | . | . 10. p6 :
. . . . . | . | .     ∀l:IdLnk, t:ℕ.
. . . . . | . | .     ∃t':ℕ.
. . . . . | . | .     t≤t'
. . . . . | . | .     & isrcv(l;a(destination(l);t'))
. . . . . | . | .       ∨ queue(l;t') = nil
. . . . . | . | . 11. ∀i:Id, t:ℕ, l:IdLnk.
. . . . . | . | .     ¬source(l) = i ⇒ onlnk(l;m(i;t)) = nil
. . . . . | . | . 12. ∀i:Id, t:ℕ.
. . . . . | . | .     isnull(a(i;t))
. . . . . | . | .     ⇒
. . . . . | . | .     (∀x:Id. s(i;t+1).x = s(i;t).x)
. . . . . | . | .     & m(i;t) = nil
. . . . . | . | . 13. ∀i:Id, t:ℕ, l:IdLnk.
. . . . . | . | .     isrcv(l;a(i;t))
. . . . . | . | .     ⇒
. . . . . | . | .     destination(l) = i
. . . . . | . | .     & ||queue(l;t)||≥1
. . . . . | . | .       & hd(queue(l;t)) = msg(a(i;t))
. . . . . | . | . 14. ∀l:IdLnk, t:ℕ.
. . . . . | . | .     ∃t':ℕ.
. . . . . | . | .     t≤t'
. . . . . | . | .     & isrcv(l;a(destination(l);t'))
. . . . . | . | .       ∨ queue(l;t') = nil
. . . . . | . | . 15. ∀l:IdLnk, tg:Id.
. . . . . | . | .     (w.M
. . . . . | . | .      (l
. . . . . | . | .      ,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | . | .                  <ds
. . . . . | . | .                  ,<[locl(a)],λx.T>
. . . . . | . | .                  ,
```

```
. . . . . | . | .                  ,<[a],λx.P>
. . . . . | . | .                  ,
. . . . . | . | .                  ,
. . . . . | . | .                  ,
. . . . . | . | .                  ,
. . . . . | . | .                  ,.>
. . . . . | . | .                else  fi.da(rcv(l; tg))
. . . . . | . | . 16. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . . | . | . 17. ∀a@0:Id, t:ℕ.
. . . . . | . | .     ∃t':ℕ.
. . . . . | . | .     t≤t'
. . . . . | . | .     & ¬isnull(a(i;t'))
. . . . . | . | .       & kind(a(i;t')) = locl(a@0)
. . . . . | . | .       ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . . | . | .       ∨ P@0 != <[a]
. . . . . | . | .                ,λx.
. . . . . | . | .                 P>(a@0) ==> ∀v:<[locl(a)]
. . . . . | . | .                                ,λx.
. . . . . | . | .                                 T>(...)?Top.
. . . . . | . | .         ¬P@0((λx.s(i;t').x),v)
. . . . . | . | . 18. ∀t:ℕ.
. . . . . | . | .     ¬isnull(a(i;t))
. . . . . | . | .     ⇒
. . . . . | . | .     (islocal(kind(a(i;t)))
. . . . . | . | .      ⇒
. . . . . | . | .      (eqof(IdDeq)(a,act(kind(a(i;t))))
. . . . . | . | .       ∨₂ false₂)
. . . . . | . | .      ⇒
. . . . . | . | .      P((λx.s(i;t).x),val(a(i;t))))
. . . . . | . | .     & (∀x:Id.
. . . . . | . | .        deq-member(...;<kind(a(i;t)),x>;1of())
. . . . . | . | .        ⇒
. . . . . | . | .        s(i;t+1).x
. . . . . | . | .        =
. . . . . | . | .        2of()
. . . . . | . | .        (<kind(a(i;t)),x>
. . . . . | . | .        ,λx.s(i;t).x
. . . . . | . | .        ,val(a(i;t))))
. . . . . | . | .     & (∀l:IdLnk.
. . . . . | . | .        deq-member(...;<kind(a(i;t)),l>;1of())
. . . . . | . | .        ⇒
. . . . . | . | .        withlnk(l;m(i;t))
. . . . . | . | .        =
. . . . . | . | .        if source(l) = i→
. . . . . | . | .           concat(map(λtgf.map(λx.
. . . . . | . | .           <1of(tgf)
. . . . . | . | .           ,x>;2of(tgf)
. . . . . | . | .               ((λx.s(i;t).x)
. . . . . | . | .               ,val(a(i;t))));...))
. . . . . | . | .        else nil fi)
. . . . . | . | .     & (∀x:Id.
. . . . . | . | .        ¬(deq-member(IdDeq;x;1of())
. . . . . | . | .          ⇒
. . . . . | . | .          deq-member(KindDeq;kind(a(i;t));2of()
. . . . . | . | .                                          (x)))
```

```
. . . . . | . | .        ⇒
. . . . . | . | .        s(i;t).x = s(i;t+1).x)
. . . . . | . | .     & (∀l:IdLnk, tg:Id.
. . . . . | . | .        ¬(deq-member(...;<l,tg>;1of())
. . . . . | . | .          ⇒
. . . . . | . | .          deq-member(KindDeq;kind(a(i;t));...))
. . . . . | . | .        ⇒
. . . . . | . | .        w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . | . | . 19. ∀x:Id.
. . . . . | . | .     deq-member(IdDeq;x;1of())
. . . . . | . | .     ⇒
. . . . . | . | .     s(i;0).x = 2of()(x)
. . . . . | . | . 20. ∀a@0:Action(i).
. . . . . | . | .     ¬isnull(a@0)
. . . . . | . | .     ⇒
. . . . . | . | .     (valtype(i;a@0) ⊆r <[locl(a)]
. . . . . | . | .                        ,λx.T>(kind(a@0))?Top)
. . . . . | . | . 21. ∀x:Id.
. . . . . | . | .     vartype(i;x) ⊆r if deq-member(...;x;1of(
. . . . . | . | .                                      ds))→
. . . . . | . | .                        2of(ds)(x)
. . . . . | . | .                    else Top fi
. . . . . | . | . 22. IdDeq ∈ EqDecider(Id)
. . . . . | . | . 23. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . . | . | . 24. j : Id
. . . . . | . | . 25. t : ℕ
. . . . . | . | . 26. j = i
. . . . . | . | . 27. ¬isnull(a(j;t))
. . . . . | . | . 28. ¬isnull(a(i;t))
. . . . . | . | . 29. (λx.s(i;t).x) ∈ State(ds)
. . . . . | . | . 30. t' : ℕ
. . . . . | . | . 31. t+1≤t'
. . . . . | . | . 32. ∀v:T. ¬P((λx.s(i;t').x),v)
. . . . . | . | . 33. t2 : ℕ
. . . . . | . | . 34. t2<t'
. . . . . | . | . 35. ¬isnull(a(i;t2))
. . . . . | . | . 36. ∀t3:ℕ. t2<t3 & t3<t' ⇒ isnull(a(i;t3))
. . . . . | . | . 37. t≤t2
. . . . . | . | . 38. loc(<j,t>) = loc(<i,t2>)
. . . . . | . | .     & (<j,t> < <i,t2>)
. . . . . | . | .     ∨ <j,t> = <i,t2>
. . . . . | . | . 39. v : T
. . . . . | . | . 40. ¬P((λx.s(i;t').x),v)
. . . . . | . | . 41. z : Id
. . . . . | . | . 42. t3 : ℤ
. . . . . | . | . 43. 0<t3
. . . . . | . | . 44. t2+1≤t3
. . . . . | . | . 45. t3≤t'
. . . . . | . | . 46. t2+1≤t3-1
. . . . . | . | . 47. s(i;t2+1).z = s(i;t3-1).z
. . . . . | . | . 48. isnull(a(i;t3-1))
. . . . . | . | . 49. ∀x:Id. s(i;t3-1+1).x = s(i;t3-1).x
. . . . . | . | . 50. m(i;t3-1) = nil
. . . . . | . | . 51. s(i;t3-1+1).z = s(i;t3-1).z
. . . . . | . | . 52. ∀x:Id. s(i;t3-1+1).x = s(i;t3-1).x
```

```
. . . . . | . | . 53. m(i;t3-1) = nil
. . . . . | . | . 54. s(i;t3).z = s(i;t3-1).z
. . . . . | . | . 55. vartype(i;z)
. . . . . | . | . ⊢  vartype(i;z) ⊆r ds(z)?Top
. . . . . | . | .   by BackThruSomeHyp
. . . . . | . |
. . . . . | . .\
. . . . . | . . 1. i : Id
. . . . . | . . 2. a : Id
. . . . . | . . 3. T : Type
. . . . . | . . 4. ds : x:Id fp-> Type
. . . . . | . . 5. P : State(ds)→T→Prop
. . . . . | . . 6. w : World
. . . . . | . . 7. p : FairFifo
. . . . . | . . 8. FairFifo
. . . . . | . . 9. ∀l:IdLnk, tg:Id.
. . . . . | . .    (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | . .                      <ds
. . . . . | . .                      ,<[locl(a)],λx.T>
. . . . . | . .                      ,
. . . . . | . .                      ,<[a],λx.P>
. . . . . | . .                      ,
. . . . . | . .                      ,
. . . . . | . .                      ,
. . . . . | . .                      ,
. . . . . | . .                      ,·>
. . . . . | . .                    else  fi.da(rcv(l; tg))
. . . . . | . . 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . . | . . 11. ∀a@0:Id, t:ℕ.
. . . . . | . .     ∃t':ℕ.
. . . . . | . .     t≤t'
. . . . . | . .     & ¬isnull(a(i;t'))
. . . . . | . .       & kind(a(i;t')) = locl(a@0)
. . . . . | . .       ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . . | . .       ∨ P@0 != <[a]
. . . . . | . .                ,λx.
. . . . . | . .                 P>(a@0) ==> ∀v:<[locl(a)]
. . . . . | . .                                ,λx.
. . . . . | . .                                 T>(...)?Top.
. . . . . | . .         ¬P@0((λx.s(i;t').x),v)
. . . . . | . . 12. ∀t:ℕ.
. . . . . | . .     ¬isnull(a(i;t))
. . . . . | . .     ⇒
. . . . . | . .     (islocal(kind(a(i;t)))
. . . . . | . .      ⇒
. . . . . | . .      (eqof(IdDeq)(a,act(kind(a(i;t))))
. . . . . | . .       ∨₂ false₂)
. . . . . | . .      ⇒
. . . . . | . .      P((λx.s(i;t).x),val(a(i;t))))
. . . . . | . .     & (∀x:Id.
. . . . . | . .        deq-member(...;<kind(a(i;t)),x>;1of())
. . . . . | . .        ⇒
. . . . . | . .        s(i;t+1).x
. . . . . | . .        =
. . . . . | . .        2of()
```

```
. . . . . | . .        (<kind(a(i;t)),x>
. . . . . | . .        ,λx.s(i;t).x

. . . . . | . .        ,val(a(i;t))))
. . . . . | . .     & (∀l:IdLnk.
. . . . . | . .        deq-member(...;<kind(a(i;t)),l>;1of())
. . . . . | . .        ⇒
. . . . . | . .        withlnk(l;m(i;t))
. . . . . | . .        =
. . . . . | . .        if source(l) = i→
. . . . . | . .           concat(map(λtgf.map(λx.
. . . . . | . .           <1of(tgf)
. . . . . | . .           ,x>;2of(tgf)
. . . . . | . .               ((λx.s(i;t).x)
. . . . . | . .               ,val(a(i;t))));...))
. . . . . | . .        else nil fi)
. . . . . | . .     & (∀x:Id.
. . . . . | . .        ¬(deq-member(IdDeq;x;1of())
. . . . . | . .          ⇒
. . . . . | . .          deq-member(KindDeq;kind(a(i;t));2of()
. . . . . | . .                                          (x)))
. . . . . | . .        ⇒
. . . . . | . .        s(i;t).x = s(i;t+1).x)
. . . . . | . .     & (∀l:IdLnk, tg:Id.
. . . . . | . .        ¬(deq-member(...;<l,tg>;1of())
. . . . . | . .          ⇒
. . . . . | . .          deq-member(KindDeq;kind(a(i;t));...))
. . . . . | . .        ⇒
. . . . . | . .        w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . | . . 13. ∀x:Id.
. . . . . | . .     deq-member(IdDeq;x;1of())
. . . . . | . .     ⇒
. . . . . | . .     s(i;0).x = 2of()(x)
. . . . . | . . 14. ∀a@0:Action(i).
. . . . . | . .     ¬isnull(a@0)
. . . . . | . .     ⇒
. . . . . | . .     (valtype(i;a@0) ⊆r <[locl(a)]
. . . . . | . .                        ,λx.T>(kind(a@0))?Top)
. . . . . | . . 15. ∀x:Id.
. . . . . | . .     vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(
. . . . . | . .                                          ds))→
. . . . . | . .                        2of(ds)(x)
. . . . . | . .                    else Top fi
. . . . . | . . 16. IdDeq ∈ EqDecider(Id)
. . . . . | . . 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . . | . . 18. j : Id
. . . . . | . . 19. t : ℕ
. . . . . | . . 20. j = i
. . . . . | . . 21. ¬isnull(a(j;t))
. . . . . | . . 22. ¬isnull(a(i;t))
. . . . . | . . 23. (λx.s(i;t).x) ∈ State(ds)
. . . . . | . . 24. t' : ℕ
. . . . . | . . 25. t+1≤t'
. . . . . | . . 26. ∀v:T. ¬P((λx.s(i;t').x),v)
. . . . . | . . 27. t2 : ℕ
. . . . . | . . 28. t2<t'
```

```
. . . . . | . . 29. ¬isnull(a(i;t2))
. . . . . | . . 30. ∀t3:ℕ. t2<t3 & t3<t' ⇒ isnull(a(i;t3))
. . . . . | . . 31. t≤t2
. . . . . | . . 32. loc(<j,t>) = loc(<i,t2>) & (<j,t> < <i,t2>)
. . . . . | . .     ∨ <j,t> = <i,t2>
. . . . . | . . 33. v : T
. . . . . | . . 34. ¬P((λx.s(i;t').x),v)
. . . . . | . . 35. z : Id
. . . . . | . . 36. t3 : ℤ
. . . . . | . . 37. 0<t3
. . . . . | . . 38. t2+1≤t3-1
. . . . . | . .     ⇒
. . . . . | . .     t3-1≤t' ⇒ s(i;t2+1).z = s(i;t3-1).z
. . . . . | . . 39. t2+1≤t3
. . . . . | . . 40. t3≤t'
. . . . . | . . 41. ¬t2+1≤t3-1
. . . . . | . . ⊢  s(i;t2+1).z = s(i;t3).z
. . . . . | . .   by Subst (t3 = t2+1) 0
. . . . . | . .      THEN
. . . . . | . .      Try (Fold `member` 0)
. . . . . | . .      THEN
. . . . . | . .      DoSubsume
. . . . . | . .      THEN
. . . . . | . .      Try BackThruSomeHyp
. . . . . | . .      THEN
. . . . . | . .      Try D_ES_Subtype
. . . . . |
. . . . . .\
. . . . . .....wf .....
. . . . . . 1. i : Id
. . . . . . 2. a : Id
. . . . . . 3. T : Type
. . . . . . 4. ds : x:Id fp-> Type
. . . . . . 5. P : State(ds)→T→Prop
. . . . . . 6. w : World
. . . . . . 7. p : FairFifo
. . . . . . 8. FairFifo
. . . . . . 9. ∀l:IdLnk, tg:Id.
. . . . . . | (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . . |                  <ds
. . . . . . |                  ,<[locl(a)],λx.T>
. . . . . . |                  ,
. . . . . . |                  ,<[a],λx.P>
. . . . . . |                  ,
. . . . . . |                  ,
. . . . . . |                  ,
. . . . . . |                  ,
. . . . . . |                  ,.>
. . . . . . |              else  fi.da(rcv(l; tg))
. . . . . . 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . . . 11. ∀a@0:Id, t:ℕ.
. . . . . . |   ∃t':ℕ.
. . . . . . |   t≤t'
. . . . . . |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . . . |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
```

```
. . . . . |     ∨ P@0 != <[a]
. . . . . |               ,λx.
. . . . . |                P>(a@0) ==> ∀v:<[locl(a)]
. . . . . |                                ,λx.
. . . . . |                                 T>(locl(a@0))?Top.
. . . . . |       ¬P@0((λx.s(i;t').x),v)
. . . . . 12. ∀t:ℕ.
. . . . . |   ¬isnull(a(i;t))
. . . . . |   ⇒
. . . . . |   (islocal(kind(a(i;t)))
. . . . . |    ⇒
. . . . . |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . . |    ⇒
. . . . . |    P((λx.s(i;t).x),val(a(i;t))))
. . . . . |   & (∀x:Id.
. . . . . |      deq-member(...;<kind(a(i;t)),x>;1of())
. . . . . |      ⇒
. . . . . |      s(i;t+1).x
. . . . . |      =
. . . . . |      2of()
. . . . . |      (<kind(a(i;t)),x>
. . . . . |      ,λx.s(i;t).x
. . . . . |      ,val(a(i;t))))
. . . . . |   & (∀l:IdLnk.
. . . . . |      deq-member(...;<kind(a(i;t)),l>;1of())
. . . . . |      ⇒
. . . . . |      withlnk(l;m(i;t))
. . . . . |      =
. . . . . |      if source(l) = i→
. . . . . |         concat(map(λtgf.map(λx.
. . . . . |         <1of(tgf),x>;2of(tgf)
. . . . . |                      ((λx.s(i;t).x)
. . . . . |                      ,val(a(i;t))));2of()
. . . . . |                                    (<kind(a(i;t))
. . . . . |                                     ,l>)))
. . . . . |      else nil fi)
. . . . . |   & (∀x:Id.
. . . . . |      ¬(deq-member(IdDeq;x;1of())
. . . . . |        ⇒
. . . . . |        deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . . . . |      ⇒
. . . . . |      s(i;t).x = s(i;t+1).x)
. . . . . |   & (∀l:IdLnk, tg:Id.
. . . . . |      ¬(deq-member(...;<l,tg>;1of())
. . . . . |        ⇒
. . . . . |        deq-member(KindDeq;kind(a(i;t));2of()
. . . . . |                                         (<l,tg>)))
. . . . . |      ⇒
. . . . . |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . 13. ∀x:Id.
. . . . . |   deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . . . . 14. ∀a@0:Action(i).
. . . . . |   ¬isnull(a@0)
. . . . . |   ⇒
. . . . . |   (valtype(i;a@0) ⊆r <[locl(a)]
```

```
. . . . . | .λx.T>(kind(a@0))?Top)
. . . . . 15. ∀x:Id.
. . . . . |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . . . . |                     2of(ds)(x)
. . . . . |                  else Top fi
. . . . . 16. IdDeq ∈ EqDecider(Id)
. . . . . 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . . 18. j : Id
. . . . . 19. t : ℕ
. . . . . 20. j = i
. . . . . 21. ¬isnull(a(j;t))
. . . . . 22. ¬isnull(a(i;t))
. . . . . 23. (λx.s(i;t).x) ∈ State(ds)
. . . . . 24. t' : ℕ
. . . . . 25. t+1≤t'
. . . . . 26. ∀v:T. ¬P((λx.s(i;t').x),v)
. . . . . 27. t2 : ℕ
. . . . . 28. t2<t'
. . . . . 29. ¬isnull(a(i;t2))
. . . . . 30. ∀t3:ℕ. t2<t3 & t3<t' ⇒ isnull(a(i;t3))
. . . . . 31. t≤t2
. . . . . 32. e' : E
. . . . . ⊢  (loc(<j,t>) = loc(e') & (<j,t> < e') ∨ <j,t> = e'
. . . . . |   & kind(act(e')) = locl(a)
. . . . . |     ∨ (∀v:T. ¬P((λz.s(1of(e');2of(e')+1).z),v)))
. . . . . |  ∈ Type
. . . . . | by Analyze -1 THEN Analyze -2
. . . . . |    THEN
. . . . . |    Unfolds [‘w-act‘] 0
. . . . . |    THEN
. . . . . |    All Reduce
. . . . . |
. . . . . 1. i : Id
. . . . . 2. a : Id
. . . . . 3. T : Type
. . . . . 4. ds : x:Id fp-> Type
. . . . . 5. P : State(ds)→T→Prop

. . . . . 6. w : World
. . . . . 7. p : FairFifo
. . . . . 8. FairFifo
. . . . . 9. ∀l:IdLnk, tg:Id.
. . . . . |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . |                   <ds
. . . . . |                   ,<[locl(a)],λx.T>
. . . . . |                   ,
. . . . . |                   ,<[a],λx.P>
. . . . . |                   ,
. . . . . |                   ,
. . . . . |                   ,
. . . . . |                   ,
. . . . . |                   ,·>
. . . . . |                else  fi.da(rcv(l; tg))
. . . . . 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . . 11. ∀a@0:Id, t:ℕ.
. . . . . |   ∃t':ℕ.
```

```
. . . . . |   t≤t'
. . . . . |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . . |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . . |     ∨ P@0 != <[a]
. . . . . |              ,λx.
. . . . . |               P>(a@0) ==> ∀v:<[locl(a)]
. . . . . |                                ,λx.
. . . . . |                                 T>(locl(a@0))?Top.
. . . . . |       ¬P@0((λx.s(i;t').x),v)
. . . . . 12. ∀t:ℕ.
. . . . . |   ¬isnull(a(i;t))
. . . . . |   ⇒
. . . . . |   (islocal(kind(a(i;t)))
. . . . . |    ⇒
. . . . . |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . . |    ⇒
. . . . . |    P((λx.s(i;t).x),val(a(i;t))))
. . . . . |   & (∀x:Id.
. . . . . |      deq-member(...;<kind(a(i;t)),x>;1of())
. . . . . |      ⇒
. . . . . |      s(i;t+1).x
. . . . . |      =
. . . . . |      2of()
. . . . . |      (<kind(a(i;t)),x>
. . . . . |      ,λx.s(i;t).x
. . . . . |      ,val(a(i;t))))
. . . . . |   & (∀l:IdLnk.
. . . . . |      deq-member(...;<kind(a(i;t)),l>;1of())
. . . . . |      ⇒
. . . . . |      withlnk(l;m(i;t))
. . . . . |      =
. . . . . |      if source(l) = i→
. . . . . |         concat(map(λtgf.map(λx.
. . . . . |         <1of(tgf),x>;2of(tgf)
. . . . . |                      ((λx.s(i;t).x)
. . . . . |                      ,val(a(i;t))));2of()
. . . . . |                                    (<kind(a(i;t))
. . . . . |                                     ,l>)))
. . . . . |      else nil fi)
. . . . . |   & (∀x:Id.
. . . . . |      ¬(deq-member(IdDeq;x;1of())
. . . . . |        ⇒
. . . . . |        deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . . . . |      ⇒
. . . . . |      s(i;t).x = s(i;t+1).x)
. . . . . |   & (∀l:IdLnk, tg:Id.
. . . . . |      ¬(deq-member(...;<l,tg>;1of())
. . . . . |        ⇒
. . . . . |        deq-member(KindDeq;kind(a(i;t));2of()
. . . . . |                                        (<l,tg>)))
. . . . . |      ⇒
. . . . . |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . 13. ∀x:Id.
. . . . . |   deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . . . . 14. ∀a@0:Action(i).
```

```
. . . . . | ¬isnull(a@0)
. . . . . | ⇒
. . . . . | (valtype(i;a@0) ⊆r <[locl(a)]
. . . . . |                    ,λx.T>(kind(a@0))?Top)
. . . . . 15. ∀x:Id.
. . . . . | vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . . . . |                    2of(ds)(x)
. . . . . |                 else Top fi
. . . . . 16. IdDeq ∈ EqDecider(Id)
. . . . . 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . . 18. j : Id
. . . . . 19. t : ℕ
. . . . . 20. j = i
. . . . . 21. ¬isnull(a(j;t))
. . . . . 22. ¬isnull(a(i;t))
. . . . . 23. (λx.s(i;t).x) ∈ State(ds)
. . . . . 24. t' : ℕ
. . . . . 25. t+1≤t'
. . . . . 26. ∀v:T. ¬P((λx.s(i;t').x),v)
. . . . . 27. t2 : ℕ
. . . . . 28. t2<t'
. . . . . 29. ¬isnull(a(i;t2))
. . . . . 30. ∀t3:ℕ. t2<t3 & t3<t' ⇒ isnull(a(i;t3))
. . . . . 31. t≤t2
. . . . . 32. e1 : Id
. . . . . 33. e2 : ℕ
. . . . . 34. ¬isnull(a(e1;e2))

. . . . . ⊢ (loc(<j,t>) = loc(<e1,e2>) & (<j,t> < <e1,e2>)
. . . . . | ∨ <j,t> = <e1,e2>
. . . . . | & kind(a(e1;e2)) = locl(a)
. . . . . |   ∨ (∀v:T. ¬P((λz.s(e1;e2+1).z),v)))
. . . . . | ∈ Type
. . . . . | by Repeat
. . . . . |  (Unfolds [`w-E`;`es-loc`;`es-causl`;`es-Loc`] 0
. . . . . |   THEN
. . . . . |   Reduce 0)
. . . . . |  THEN
. . . . . |  Try (Analyze THEN Reduce 0 THEN Complete Auto)
. . . . . |  THEN
. . . . . |  Try (Complete D_ES_Subtype)
. . . . . |

. . . . . .....subterm .....
. . . . . 1. i : Id
. . . . . 2. a : Id
. . . . . 3. T : Type
. . . . . 4. ds : x:Id fp-> Type
. . . . . 5. P : State(ds)→T→Prop
. . . . . 6. w : World
. . . . . 7. FairFifo
. . . . . 8. FairFifo
. . . . . 9. ∀l:IdLnk, tg:Id.
. . . . . | (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . |                  <ds
. . . . . |                  ,<[locl(a)],λx.T>
. . . . . |                  ,
```

```
. . . . . | ,<[a],λx.P>
. . . . . | ,
. . . . . | ,
. . . . . | ,
. . . . . | ,
. . . . . | ,.>
. . . . . | else  fi.da(rcv(l; tg))
. . . . . 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . . 11. ∀a@0:Id, t:ℕ.
. . . . . |   ∃t':ℕ.
. . . . . |   t≤t'
. . . . . |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . . |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . . |     ∨ P@0 != <[a]
. . . . . |              ,λx.
. . . . . |               P>(a@0) ==> ∀v:<[locl(a)]
. . . . . |                                ,λx.
. . . . . |                                 T>(locl(a@0))?Top.
. . . . . |       ¬P@0((λx.s(i;t').x),v)
. . . . . 12. ∀t:ℕ.
. . . . . |   ¬isnull(a(i;t))
. . . . . |   ⇒
. . . . . |   (islocal(kind(a(i;t)))
. . . . . |    ⇒
. . . . . |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . . |    ⇒
. . . . . |    P((λx.s(i;t).x),val(a(i;t))))
. . . . . |   & (∀x:Id.
. . . . . |      deq-member(...;<kind(a(i;t)),x>;1of())
. . . . . |      ⇒
. . . . . |      s(i;t+1).x
. . . . . |      =
. . . . . |      2of()
. . . . . |      (<kind(a(i;t)),x>
. . . . . |      ,λx.s(i;t).x
. . . . . |      ,val(a(i;t))))
. . . . . |   & (∀l:IdLnk.
. . . . . |      deq-member(...;<kind(a(i;t)),l>;1of())
. . . . . |      ⇒
. . . . . |      withlnk(l;m(i;t))
. . . . . |      =
. . . . . |      if source(l) = i→
. . . . . |         concat(map(λtgf.map(λx.
. . . . . |         <1of(tgf),x>;2of(tgf)
. . . . . |                      ((λx.s(i;t).x)
. . . . . |                      ,val(a(i;t))));2of()
. . . . . |                                    (<kind(a(i;t))
. . . . . |                                     ,l>)))
. . . . . |      else nil fi)
. . . . . |   & (∀x:Id.
. . . . . |      ¬(deq-member(IdDeq;x;1of())
. . . . . |        ⇒
. . . . . |        deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . . . . |      ⇒
. . . . . |      s(i;t).x = s(i;t+1).x)
```

```
. . . . . |   & (∀l:IdLnk, tg:Id.
. . . . . |      ¬(deq-member(...;<l,tg>;1of())
. . . . . |        ⇒
. . . . . |        deq-member(KindDeq;kind(a(i;t));2of()
. . . . . |                                        (<l,tg>)))
. . . . . |      ⇒
. . . . . |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . 13. ∀x:Id.
. . . . . |   deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . . . . 14. ∀a@0:Action(i).
. . . . . |   ¬isnull(a@0)
. . . . . |   ⇒
. . . . . |   (valtype(i;a@0) ⊆r <[locl(a)]
. . . . . |                      ,λx.T>(kind(a@0))?Top)
. . . . . 15. ∀x:Id.
. . . . . |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . . . . |                      2of(ds)(x)
. . . . . |                   else Top fi
. . . . . 16. IdDeq ∈ EqDecider(Id)
. . . . . 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . . 18. j : Id
. . . . . 19. t : ℕ
. . . . . 20. j = i
. . . . . 21. ¬isnull(a(j;t))
. . . . . 22. ¬isnull(a(i;t))
. . . . . 23. (λx.s(i;t).x) ∈ State(ds)
. . . . . 24. t' : ℕ
. . . . . 25. t+1≤t'
. . . . . 26. ∀v:T. ¬P((λx.s(i;t').x),v)
. . . . . 27. t2 : ℕ
. . . . . 28. t2<t'
. . . . . 29. ¬isnull(a(i;t2))
. . . . . 30. ∀t3:ℕ. t2<t3 & t3<t' ⇒ isnull(a(i;t3))
. . . . . 31. t≤t2
. . . . . 32. e1 : Id
. . . . . 33. e2 : ℕ
. . . . . 34. ¬isnull(a(e1;e2))
. . . . . 35. j = e1 & <j,t> <c <e1,e2> ∨ <j,t> = <e1,e2>
. . . . . 36. T
. . . . . ⊢  (λz.s(e1;e2+1).z) ∈ State(ds)
. . . . . | by Unfold `ma-state` 0 THEN DoSubsume
. . . . . |
. . . . . .....subtype_rel .....
. . . . . 1. i : Id
. . . . . 2. a : Id
. . . . . 3. T : Type
. . . . . 4. ds : x:Id fp-> Type
. . . . . 5. P : State(ds)→T→Prop
. . . . . 6. w : World
. . . . . 7. FairFifo
. . . . . 8. FairFifo
. . . . . 9. ∀l:IdLnk, tg:Id.
. . . . . |  (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . |                    <ds
. . . . . |                    ,<[locl(a)],λx.T>
```

```
. . . . . |                    ,
. . . . . |                    ,<[a],λx.P>
. . . . . |                    ,
. . . . . |                    ,
. . . . . |                    ,
. . . . . |                    ,
. . . . . |                    ,·>
. . . . . |                 else  fi.da(rcv(l; tg))
. . . . . 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . . 11. ∀a@0:Id, t:ℕ.
. . . . . |   ∃t':ℕ.
. . . . . |   t≤t'
. . . . . |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . . |     ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . . |     ∨ P@0 != <[a]
. . . . . |               ,λx.
. . . . . |                P>(a@0) ==> ∀v:<[locl(a)]
. . . . . |                                ,λx.
. . . . . |                                 T>(locl(a@0))?Top.
. . . . . |       ¬P@0((λx.s(i;t').x),v)
. . . . . 12. ∀t:ℕ.
. . . . . |   ¬isnull(a(i;t))
. . . . . |   ⇒
. . . . . |   (islocal(kind(a(i;t)))
. . . . . |    ⇒
. . . . . |    (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . . |    ⇒
. . . . . |    P((λx.s(i;t).x),val(a(i;t))))
. . . . . |   & (∀x:Id.
. . . . . |      deq-member(...;<kind(a(i;t)),x>;1of())
. . . . . |      ⇒
. . . . . |      s(i;t+1).x
. . . . . |      =
. . . . . |      2of()
. . . . . |      (<kind(a(i;t)),x>
. . . . . |      ,λx.s(i;t).x
. . . . . |      ,val(a(i;t))))
. . . . . |   & (∀l:IdLnk.
. . . . . |      deq-member(...;<kind(a(i;t)),l>;1of())
. . . . . |      ⇒
. . . . . |      withlnk(l;m(i;t))
. . . . . |      =
. . . . . |      if source(l) = i→
. . . . . |         concat(map(λtgf.map(λx.
. . . . . |         <1of(tgf),x>;2of(tgf)
. . . . . |                      ((λx.s(i;t).x)
. . . . . |                      ,val(a(i;t))));2of()
. . . . . |                                    (<kind(a(i;t))
. . . . . |                                     ,l>)))
. . . . . |      else nil fi)
. . . . . |   & (∀x:Id.
. . . . . |      ¬(deq-member(IdDeq;x;1of())
. . . . . |        ⇒
. . . . . |        deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . . . . |      ⇒
```

```
. . . . . |      s(i;t).x = s(i;t+1).x)
. . . . . |   & (∀l:IdLnk, tg:Id.
. . . . . |      ¬(deq-member(...;<l,tg>;1of())
. . . . . |        ⇒
. . . . . |        deq-member(KindDeq;kind(a(i;t));2of()
. . . . . |                                        (<l,tg>)))
. . . . . |      ⇒
. . . . . |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . 13. ∀x:Id.
. . . . . |   deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . . . . 14. ∀a@0:Action(i).
. . . . . |   ¬isnull(a@0)
. . . . . |   ⇒
. . . . . |   (valtype(i;a@0) ⊆r <[locl(a)]
. . . . . |                        ,λx.T>(kind(a@0))?Top)
. . . . . 15. ∀x:Id.
. . . . . |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . . . . |                       2of(ds)(x)
. . . . . |                    else Top fi
. . . . . 16. IdDeq ∈ EqDecider(Id)
. . . . . 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . . 18. j : Id
. . . . . 19. t : ℕ
. . . . . 20. j = i
. . . . . 21. ¬isnull(a(j;t))
. . . . . 22. ¬isnull(a(i;t))
. . . . . 23. (λx.s(i;t).x) ∈ State(ds)
. . . . . 24. t' : ℕ
. . . . . 25. t+1≤t'
. . . . . 26. ∀v:T. ¬P((λx.s(i;t').x),v)
. . . . . 27. t2 : ℕ
. . . . . 28. t2<t'
. . . . . 29. ¬isnull(a(i;t2))
. . . . . 30. ∀t3:ℕ. t2<t3 & t3<t' ⇒ isnull(a(i;t3))
. . . . . 31. t≤t2
. . . . . 32. e1 : Id
. . . . . 33. e2 : ℕ
. . . . . 34. ¬isnull(a(e1;e2))
. . . . . 35. j = e1 & <j,t> <c <e1,e2> ∨ <j,t> = <e1,e2>
. . . . . 36. T
. . . . . 37. z : Id
. . . . . ⊢  vartype(e1;z) ⊆r ds(z)?Top
. . . . . | by Subst (e1 = i) 0 THEN Try BackThruSomeHyp
. . . . . |    THEN
. . . . . |    SplitOrHyps
. . . . . |
. . . . . 1. i : Id
. . . . . 2. a : Id
. . . . . 3. T : Type
. . . . . 4. ds : x:Id fp-> Type
. . . . . 5. P : State(ds)→T→Prop
. . . . . 6. w : World
. . . . . 7. FairFifo
. . . . . 8. FairFifo
. . . . . 9. ∀l:IdLnk, tg:Id.
```

```
. . . . . (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . .                  <ds
. . . . . .                  ,<[locl(a)],λx.T>
. . . . . .                  ,
. . . . . .                  ,<[a],λx.P>
. . . . . .                  ,
. . . . . .                  ,
. . . . . .                  ,
. . . . . .                  ,
. . . . . .                  ,·>
. . . . . .               else  fi.da(rcv(l; tg))
. . . . . 10. (eqof(IdDeq)(i,i)) ∼ true₂
. . . . . 11. ∀a@0:Id, t:ℕ.
. . . . . .    ∃t':ℕ.
. . . . . .    t≤t'
. . . . . .    & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . . . . .      ∨ ¬locl(a@0) ∈ dom(<[locl(a)],λx.T>)
. . . . . .      ∨ P@0 != <[a]
. . . . . .              ,λx.
. . . . . .               P>(a@0) ==> ∀v:<[locl(a)]
. . . . . .                                ,λx.
. . . . . .                                 T>(locl(a@0))?Top.
. . . . . .        ¬P@0((λx.s(i;t').x),v)
. . . . . 12. ∀t:ℕ.
. . . . . .    ¬isnull(a(i;t))
. . . . . .    ⇒
. . . . . .    (islocal(kind(a(i;t)))
. . . . . .     ⇒
. . . . . .     (eqof(IdDeq)(a,act(kind(a(i;t)))) ∨₂ false₂)
. . . . . .     ⇒
. . . . . .     P((λx.s(i;t).x),val(a(i;t))))
. . . . . .    & (∀x:Id.
. . . . . .       deq-member(...;<kind(a(i;t)),x>;1of())
. . . . . .       ⇒
. . . . . .       s(i;t+1).x
. . . . . .       =
. . . . . .       2of()
. . . . . .       (<kind(a(i;t)),x>
. . . . . .       ,λx.s(i;t).x
. . . . . .       ,val(a(i;t))))
. . . . . .    & (∀l:IdLnk.
. . . . . .       deq-member(...;<kind(a(i;t)),l>;1of())
. . . . . .       ⇒
. . . . . .       withlnk(l;m(i;t))
. . . . . .       =
. . . . . .       if source(l) = i→
. . . . . .          concat(map(λtgf.map(λx.
. . . . . .          <1of(tgf),x>;2of(tgf)
. . . . . .                       ((λx.s(i;t).x)
. . . . . .                       ,val(a(i;t))));2of()
. . . . . .                                    (<kind(a(i;t))
. . . . . .                                     ,l>)))

. . . . . .       else nil fi)
. . . . . .    & (∀x:Id.
. . . . . .       ¬(deq-member(IdDeq;x;1of())
```

```
. . . . . .          ⇒
. . . . . .          deq-member(KindDeq;kind(a(i;t));2of()(x)))
. . . . . .        ⇒
. . . . . .        s(i;t).x = s(i;t+1).x)
. . . . . .     & (∀l:IdLnk, tg:Id.
. . . . . .        ¬(deq-member(...;<l,tg>;1of())
. . . . . .          ⇒
. . . . . .          deq-member(KindDeq;kind(a(i;t));2of()
. . . . . .                                          (<l,tg>)))
. . . . . .        ⇒
. . . . . .        w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . . 13. ∀x:Id.
. . . . . .     deq-member(IdDeq;x;1of()) ⇒ s(i;0).x = 2of()(x)
. . . . . . 14. ∀a@0:Action(i).
. . . . . .     ¬isnull(a@0)
. . . . . .     ⇒
. . . . . .     (valtype(i;a@0) ⊆r <[locl(a)]
. . . . . .                        ,λx.T>(kind(a@0))?Top)
. . . . . . 15. ∀x:Id.
. . . . . .     vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(ds))→
. . . . . .                        2of(ds)(x)
. . . . . .                     else Top fi
. . . . . . 16. IdDeq ∈ EqDecider(Id)
. . . . . . 17. ∀x:Id. vartype(i;x) ⊆r ds(x)?Top
. . . . . . 18. j : Id
. . . . . . 19. t : ℕ
. . . . . . 20. j = i
. . . . . . 21. ¬isnull(a(j;t))
. . . . . . 22. ¬isnull(a(i;t))
. . . . . . 23. (λx.s(i;t).x) ∈ State(ds)
. . . . . . 24. t' : ℕ
. . . . . . 25. t+1≤t'
. . . . . . 26. ∀v:T. ¬P((λx.s(i;t').x),v)
. . . . . . 27. t2 : ℕ
. . . . . . 28. t2<t'
. . . . . . 29. ¬isnull(a(i;t2))
. . . . . . 30. ∀t3:ℕ. t2<t3 & t3<t' ⇒ isnull(a(i;t3))
. . . . . . 31. t≤t2
. . . . . . 32. e1 : Id
. . . . . . 33. e2 : ℕ
. . . . . . 34. ¬isnull(a(e1;e2))
. . . . . . 35. <j,t> = <e1,e2>
. . . . . . 36. T
. . . . . . 37. Id
. . . . . . ⊢  e1 = i
. . . . . .   by Analyze -3 THEN Analyze -4 THEN All Reduce
END
```