```
pre-init-rule  THM

⊢  ∀i,a:Id, T:Type, ds:x:Id fp-> Type, P:(State(ds)→T→Prop),
|   init:x:Id fp-> ds(x)?Void.
|  (∀x:Id. x ∈ dom(ds) ⇒ x ∈ dom(init))
|  ⇒
|  @i (with ds: ds
|     init: init
|     action a:T
|     precondition a(v) is
|     P s v)
|  realizes es.(∃v:T. P((λx.init(x)?•),v)) ⇒ (∃e:E. loc(e) = i)
| by Auto
|
1. i : Id
2. a : Id
3. T : Type
4. ds : x:Id fp-> Type
5. P : State(ds)→T→Prop
6. init : x:Id fp-> ds(x)?Void
7. ∀x:Id. x ∈ dom(ds) ⇒ x ∈ dom(init)
⊢  @i (with ds: ds
|     init: init
|     action a:T
|     precondition a(v) is
|     P s v)
|  realizes es.(∃v:T. P((λx.init(x)?•),v)) ⇒ (∃e:E. loc(e) = i)
| by 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
| 6. init : x:Id fp-> ds(x)?Void
| 7. ∀x:Id. x ∈ dom(ds) ⇒ x ∈ dom(init)
| ⊢  (λes.(∃v:T. P((λx.init(x)?•),v)) ⇒ (∃e:E. loc(e) = i))
| |  ∈ {es:ES
| |     | es is an event system of @i (with ds: ds
| |                                    init: init
| |                                    action a:T
| |                                    precondition a(v) is
| |                                    P s 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. init : x:Id fp-> ds(x)?Void
| 7. ∀x:Id. x ∈ dom(ds) ⇒ x ∈ dom(init)
| 8. {es:ES
| |   | es is an event system of @i (with ds: ds
| |                                 init: init
| |                                 action a:T
| |                                 precondition a(v) is
| |                                 P s v) }
| 9. T
| ⊢  (λx.init(x)?•) ∈ State(ds)  by 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. init : x:Id fp-> ds(x)?Void
| | 7. ∀x:Id. x ∈ dom(ds) ⇒ x ∈ dom(init)
| | 8. {es:ES
| | |   | es is an event system of @i (with ds: ds
| | |                                 init: init
| | |                                 action a:T
| | |                                 precondition a(v) is
| | |                                 P s v) }
| | 9. T
| | 10. x : Id
| | ⊢  init(x)?• ∈ ds(x)?Top
| | | by RW (AddrC [2] (UnfoldC ‘fpf-cap‘)) 0 THEN SplitOnConclITE
| | |
| | |\
| | | .....truecase .....
| | | 1. i : Id
| | | 2. a : Id
| | | 3. T : Type
| | | 4. ds : x:Id fp-> Type
| | | 5. P : State(ds)→T→Prop
| | | 6. init : x:Id fp-> ds(x)?Void
| | | 7. ∀x:Id. x ∈ dom(ds) ⇒ x ∈ dom(init)
| | | 8. {es:ES
| | |     | es is an event system of @i (with ds: ds
| | |                                   init: init
| | |                                   action a:T
| | |                                   precondition a(v) is
| | |                                   P s v) }
| | | 9. T
| | | 10. x : Id
| | | 11. x ∈ dom(init)
| | | ⊢  init(x) ∈ ds(x)?Top  by DoSubsume
| | |
| | .\
```

```
| | . .....falsecase .....
| | . 1. i : Id
| | . 2. a : Id
| | . 3. T : Type
| | . 4. ds : x:Id fp-> Type
| | . 5. P : State(ds)→T→Prop
| | . 6. init : x:Id fp-> ds(x)?Void
| | . 7. ∀x:Id. x ∈ dom(ds) ⇒ x ∈ dom(init)
| | . 8. {es:ES
| | . |    | es is an event system of @i (with ds: ds
| | . |                                  init: init
| | . |                                  action a:T
| | . |                                  precondition a(v) is
| | . |                                  P s v) }
| | . 9. T
| | . 10. x : Id
| | . 11. ¬x ∈ dom(init)
| | . ⊢  · ∈ ds(x)?Top  by Unfold ‘fpf-cap‘ 0 THEN SplitOnConclITE
| | . |
| | . .....truecase .....
| | . 1. i : Id
| | . 2. a : Id
| | . 3. T : Type
| | . 4. ds : x:Id fp-> Type
| | . 5. P : State(ds)→T→Prop
| | . 6. init : x:Id fp-> ds(x)?Void
| | . 7. ∀x:Id. x ∈ dom(ds) ⇒ x ∈ dom(init)
| | . 8. {es:ES
| | .     | es is an event system of @i (with ds: ds
| | .                                  init: init
| | .                                  action a:T
| | .                                  precondition a(v) is
| | .                                  P s v) }
| | . 9. T
| | . 10. x : Id
| | . 11. ¬x ∈ dom(init)
| | . 12. x ∈ dom(ds)
| | . ⊢  · ∈ ds(x)  by Analyze -2 THEN BackThruSomeHyp
| |
| .\
| . .....eq aux .....
| . 1. i : Id
| . 2. a : Id
| . 3. T : Type
| . 4. ds : x:Id fp-> Type
| . 5. P : State(ds)→T→Prop
| . 6. init : x:Id fp-> ds(x)?Void
| . 7. ∀x:Id. x ∈ dom(ds) ⇒ x ∈ dom(init)
| . 8. {es:ES
| .     | es is an event system of @i (with ds: ds
| .                                  init: init
| .                                  action a:T
| .                                  precondition a(v) is
| .                                  P s v) }
| . 9. T
```

```
| . ⊢  Id ∈ 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. init : x:Id fp-> ds(x)?Void
. 7. ∀x:Id. x ∈ dom(ds) ⇒ x ∈ dom(init)
. ⊢  @i (with ds: ds
. |     init: init
. |     action a:T
. |     precondition a(v) is
. |     P s v) realizes2 es.(∃v:T. P((λx.init(x)?•),v))
. |                          ⇒
. |  (∃e:E. loc(e) = i)
. | 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. init : x:Id fp-> ds(x)?Void
```

```
. 7. ∀x:Id. x ∈ dom(ds) ⇒ x ∈ dom(init)
. 8. w : World
. 9. FairFifo
. 10. FairFifo
. 11. ∀l:IdLnk, tg:Id.
. |   (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. |                     (with ds: ds
. |                      init: init
. |                     action a:T
. |                      precondition a(v) is
. |                      P)
. |                  else  fi.da(rcv(l; tg))
. 12. (eqof(IdDeq)(i,i)) ∼ true₂
. 13. ∀a@0:Id, t:ℕ.
. |   ∃t':ℕ.
. |   t≤t'
. |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. |     ∨ ¬locl(a@0) ∈ dom(1of(2of((with ds: ds
. |                              init: init
. |                             action a:T
. |                              precondition a(v) is
. |                              P))))
. |     ∨ P@0 != 1of(2of(2of(2of((with ds: ds
. |                  init: init
. |                 action a:T
. |                  precondition a(v) is
. |                  P)))))(a@0) ==> ∀v:1of(2of((with ds: ds
. |                                          init: init
. |                                         action a:T
. |                                          precondition a(v) is
. |                                          P)))(locl(a@0))?Top.
. |       ¬P@0((λx.s(i;t').x),v)
. 14. ∀t:ℕ.
. |   ¬isnull(a(i;t))
. |   ⇒
. |   (islocal(kind(a(i;t)))
. |    ⇒
. |    deq-member(IdDeq;act(kind(a(i;t)));1of(1of(
. |                                       2of(2of(2of((with ds: ds
. |                                        init: init
. |                                       action a:T
. |                                        precondition a(v) is
. |                                        P)))))))
. |    ⇒
. |    2of(1of(2of(2of(2of((with ds: ds
. |             init: init
. |            action a:T
. |             precondition a(v) is
. |             P))))))
. |    (act(kind(a(i;t)))
. |    ,λx.s(i;t).x
. |    ,val(a(i;t))))
. |   & (∀x:Id.
. |      deq-member(product-deq(Knd;Id;KindDeq;IdDeq);...;1of(1of(
. |                                                      2of(2of(2of(
```

```
. |                                                          2of(
. |                                                          ...)))))))
. |      ⇒
. |      s(i;t+1).x
. |      =
. |      2of(1of(2of(2of(2of(2of((with ds: ds
. |                 init: init
. |                action a:T
. |                 precondition a(v) is
. |                 P)))))))
. |      (<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>;...)
. |      ⇒
. |      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(1of(2of(2of(2of(2of(2of(
. |                                           (with ds: ds
. |                                            init: init
. |                                           action a:T
. |                                            precondition a(v) is
. |                                            P)))))))
. |                                     (<kind(a(i;t)),l>)))
. |      else nil fi)
. |   & (∀x:Id.
. |      ¬(deq-member(IdDeq;x;1of(1of(2of(2of(2of(2of(2of(2of(
. |                                  (with ds: ds
. |                                   init: init
. |                                  action a:T
. |                                   precondition a(v) is
. |                                   P)))))))))
. |        ⇒
. |        deq-member(KindDeq;kind(a(i;t));2of(
. |                                       1of(2of(2of(2of(2of(2of(
. |                                           2of((with ds: ds
. |                                            init: init
. |                                           action a:T
. |                                            precondition a(v) is
. |                                            P)))))))))
. |                                       (x)))
. |      ⇒
. |      s(i;t).x = s(i;t+1).x)
. |   & (∀l:IdLnk, tg:Id.
. |      ¬(deq-member(product-deq(IdLnk;Id;IdLnkDeq;IdDeq);<l
. |                                                        ,tg>;...)
. |        ⇒
. |        deq-member(KindDeq;kind(a(i;t));2of(
. |                                       1of(2of(2of(2of(2of(2of(
```

```
. |                                              2of(2of((with ds: ds
. |                                               init: init
. |                                              action a:T
. |                                               precondition a(v) is
. |                                               P))))))))))
. |                                          (<l,tg>)))
. |      ⇒
. |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. 15. ∀x:Id.
. |   deq-member(IdDeq;x;1of(1of(2of(2of((with ds: ds
. |                                init: init
. |                               action a:T
. |                                precondition a(v) is
. |                                P))))))
. |   ⇒
. |   s(i;0).x
. |   =
. |   2of(1of(2of(2of((with ds: ds
. |            init: init
. |           action a:T
. |            precondition a(v) is
. |            P)))))
. |   (x)
. 16. ∀a@0:Action(i).
. |   ¬isnull(a@0)
. |   ⇒
. |   (valtype(i;a@0) ⊆r 1of(2of((with ds: ds
. |                            init: init
. |                           action a:T
. |                            precondition a(v) is
. |                            P)))(kind(a@0))?Top)
. 17. ∀x:Id.
. |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(1of((with ds: ds
. |                                           init: init
. |                                          action a:T
. |                                           precondition a(v) is
. |                                           P))))→
. |                       2of(1of((with ds: ds
. |                            init: init
. |                           action a:T
. |                            precondition a(v) is
. |                            P)))
. |                       (x)
. |                    else Top fi
. ⊢  (∃v:T. P((λx.init(x)?•),v)) ⇒ (∃e:E. loc(e) = i)
. | by Assert ((λx.init(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. init : x:Id fp-> ds(x)?Void
```

```
. | 7. ∀x:Id. x ∈ dom(ds) ⇒ x ∈ dom(init)
. | 8. w : World
. | 9. FairFifo
. | 10. FairFifo
. | 11. ∀l:IdLnk, tg:Id.
. | |   (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. | |                     (with ds: ds
. | |                      init: init
. | |                     action a:T
. | |                      precondition a(v) is
. | |                      P)
. | |                  else  fi.da(rcv(l; tg))
. | 12. (eqof(IdDeq)(i,i)) ∼ true₂
. | 13. ∀a@0:Id, t:ℕ.
. | |   ∃t':ℕ.
. | |   t≤t'
. | |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. | |     ∨ ¬locl(a@0) ∈ dom(1of(2of((with ds: ds
. | |                              init: init
. | |                             action a:T
. | |                              precondition a(v) is
. | |                              P))))
. | |     ∨ P@0 != 1of(2of(2of(2of((with ds: ds
. | |                    init: init
. | |                   action a:T
. | |                    precondition a(v) is
. | |                    P)))))(a@0) ==> ∀v:1of(2of((with ds: ds
. | |                                         init: init
. | |                                        action a:T
. | |                                         precondition a(v) is
. | |                                         P)))(locl(a@0))?Top.
. | |       ¬P@0((λx.s(i;t').x),v)
. | 14. ∀t:ℕ.
. | |   ¬isnull(a(i;t))
. | |   ⇒
. | |   (islocal(kind(a(i;t)))
. | |    ⇒
. | |    deq-member(IdDeq;act(kind(a(i;t)));1of(1of(
. | |                                       2of(2of(2of((with ds: ds
. | |                                        init: init
. | |                                       action a:T
. | |                                        precondition a(v) is
. | |                                        P)))))))
. | |    ⇒
. | |    2of(1of(2of(2of(2of((with ds: ds
. | |              init: init
. | |             action a:T
. | |              precondition a(v) is
. | |              P))))))
. | |    (act(kind(a(i;t)))
. | |    ,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(1of(
```

```
. | |                                                          2of(2of(
. | |                                                          2of(2of(
. | |                                                          ...)))))))
. | |      ⇒
. | |      s(i;t+1).x
. | |      =
. | |      2of(1of(2of(2of(2of(2of((with ds: ds
. | |                 init: init
. | |                action a:T
. | |                 precondition a(v) is
. | |                 P)))))))
. | |      (<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>;...)
. | |      ⇒
. | |      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(1of(2of(2of(2of(2of(2of(
. | |                                    (with ds: ds
. | |                                     init: init
. | |                                    action a:T
. | |                                     precondition a(v) is
. | |                                     P)))))))
. | |                              (<kind(a(i;t)),l>)))
. | |      else nil fi)
. | |   & (∀x:Id.
. | |      ¬(deq-member(IdDeq;x;1of(1of(2of(2of(2of(2of(2of(2of(
. | |                                   (with ds: ds
. | |                                    init: init
. | |                                   action a:T
. | |                                    precondition a(v) is
. | |                                    P)))))))))
. | |        ⇒
. | |        deq-member(KindDeq;kind(a(i;t));2of(
. | |                                        1of(2of(2of(2of(2of(2of(
. | |                                            2of((with ds: ds
. | |                                             init: init
. | |                                            action a:T
. | |                                             precondition a(v) is
. | |                                             P)))))))))
. | |                                        (x)))
. | |      ⇒
. | |      s(i;t).x = s(i;t+1).x)
. | |   & (∀l:IdLnk, tg:Id.
. | |      ¬(deq-member(product-deq(IdLnk;Id;IdLnkDeq;IdDeq);...;...)
. | |        ⇒
. | |        deq-member(KindDeq;kind(a(i;t));2of(
```

```
. | |                                          1of(2of(2of(2of(2of(2of(
. | |                                              2of(2of((with ds: ds
. | |                                               init: init
. | |                                              action a:T
. | |                                               precondition a(v) is
. | |                                               P))))))))))
. | |                                          (<1,tg>)))

. | |      ⇒
. | |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. | 15. ∀x:Id.
. | |   deq-member(IdDeq;x;1of(1of(2of(2of((with ds: ds
. | |                                  init: init
. | |                                 action a:T
. | |                                  precondition a(v) is
. | |                                  P))))))
. | |   ⇒
. | |   s(i;0).x
. | |   =
. | |   2of(1of(2of(2of((with ds: ds
. | |             init: init
. | |            action a:T
. | |             precondition a(v) is
. | |             P)))))
. | |   (x)
. | 16. ∀a@0:Action(i).
. | |   ¬isnull(a@0)
. | |   ⇒
. | |   (valtype(i;a@0) ⊆r 1of(2of((with ds: ds
. | |                              init: init
. | |                             action a:T
. | |                              precondition a(v) is
. | |                              P)))(kind(a@0))?Top)
. | 17. ∀x:Id.
. | |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(1of((with ds: ds
. | |                                                  init: init
. | |                                                 action a:T
. | |                                                  precondition a(v) is
. | |                                                  P))))→
. | |                       2of(1of((with ds: ds
. | |                            init: init
. | |                           action a:T
. | |                            precondition a(v) is
. | |                            P)))
. | |                         (x)
. | |                     else Top fi
. | ⊢  (λx.init(x)?·) ∈ State(ds)
. | | by 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. init : x:Id fp-> ds(x)?Void
. | | 7. ∀x:Id. x ∈ dom(ds) ⇒ x ∈ dom(init)
. | | 8. w : World
. | | 9. FairFifo
. | | 10. FairFifo
. | | 11. ∀l:IdLnk, tg:Id.
. | | |   (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. | | |                    (with ds: ds
. | | |                     init: init
. | | |                    action a:T
. | | |                     precondition a(v) is
. | | |                     P)
. | | |                  else  fi.da(rcv(l; tg))
. | | 12. (eqof(IdDeq)(i,i)) ∼ true₂
. | | 13. ∀a@0:Id, t:ℕ.
. | | |   ∃t':ℕ.
. | | |   t≤t'
. | | |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. | | |     ∨ ¬locl(a@0) ∈ dom(1of(2of((with ds: ds
. | | |                              init: init
. | | |                             action a:T
. | | |                              precondition a(v) is
. | | |                              P))))
. | | |     ∨ P@0 != 1of(2of(2of(2of((with ds: ds
. | | |                   init: init
. | | |                  action a:T
. | | |                   precondition a(v) is
. | | |                   P)))))(a@0) ==> ∀v:1of(2of((with ds: ds
. | | |                                               init: init
. | | |                                              action a:T
. | | |                                               precondition a(v) is
. | | |                                               P)))(locl(a@0))?Top.
. | | |       ¬P@0((λx.s(i;t').x),v)
. | | 14. ∀t:ℕ.
. | | |   ¬isnull(a(i;t))
. | | |   ⇒
. | | |   (islocal(kind(a(i;t)))
. | | |    ⇒
. | | |    deq-member(IdDeq;act(kind(a(i;t)));1of(1of(
. | | |                                          2of(2of(2of((with ds: ds
. | | |                                           init: init
. | | |                                          action a:T
. | | |                                           precondition a(v) is
. | | |                                           P)))))))
. | | |    ⇒
. | | |    2of(1of(2of(2of(2of((with ds: ds
. | | |             init: init
. | | |            action a:T
. | | |             precondition a(v) is
. | | |             P))))))
. | | |    (act(kind(a(i;t)))
. | | |    ,λx.s(i;t).x
. | | |    ,val(a(i;t))))
. | | |   & (∀x:Id.
. | | |      deq-member(product-deq(Knd;Id;KindDeq;IdDeq);<kind(...)
```

```
. | | |                                                    ,x>;...)
. | | |      ⇒
. | | |      s(i;t+1).x
. | | |      =
. | | |      2of(1of(2of(2of(2of(2of((with ds: ds
. | | |               init: init
. | | |              action a:T
. | | |               precondition a(v) is
. | | |               P)))))))
. | | |      (<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>;...)
. | | |      ⇒
. | | |      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(1of(2of(2of(2of(2of(2of(
. | | |                                  (with ds: ds
. | | |                                   init: init
. | | |                                  action a:T
. | | |                                   precondition a(v) is
. | | |                                   P)))))))
. | | |                             (<kind(a(i;t)),l>)))
. | | |      else nil fi)
. | | |   & (∀x:Id.
. | | |      ¬(deq-member(IdDeq;x;1of(1of(2of(2of(2of(2of(2of(2of(
. | | |                                  (with ds: ds
. | | |                                   init: init
. | | |                                  action a:T
. | | |                                   precondition a(v) is
. | | |                                   P)))))))))
. | | |        ⇒
. | | |        deq-member(KindDeq;kind(a(i;t));2of(
. | | |                                      1of(
. | | |                                      2of(2of(2of(2of(2of(
. | | |                                      2of((with ds: ds
. | | |                                       init: init
. | | |                                      action a:T
. | | |                                       precondition a(v) is
. | | |                                       P)))))))))
. | | |                                      (x)))
. | | |      ⇒
. | | |      s(i;t).x = s(i;t+1).x)
. | | |   & (∀l:IdLnk, tg:Id.
. | | |      ¬(deq-member(product-deq(IdLnk;Id;IdLnkDeq;...);...;...)
. | | |        ⇒
. | | |        deq-member(KindDeq;kind(a(i;t));2of(
. | | |                                      1of(
```

```
. | | |                                          2of(2of(2of(2of(2of(
. | | |                                          2of(2of((with ds: ds
. | | |                                           init: init
. | | |                                          action a:T
. | | |                                           precondition a(v) is
. | | |                                           P)))))))))))
. | | |                                          (<l,tg>)))
. | | |      ⇒
. | | |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. | | 15. ∀x:Id.
. | | |   deq-member(IdDeq;x;1of(1of(2of(2of((with ds: ds
. | | |                                  init: init
. | | |                                 action a:T
. | | |                                  precondition a(v) is
. | | |                                  P))))))
. | | |   ⇒
. | | |   s(i;0).x
. | | |   =
. | | |   2of(1of(2of(2of((with ds: ds
. | | |            init: init
. | | |           action a:T
. | | |            precondition a(v) is
. | | |            P)))))
. | | |   (x)
. | | 16. ∀a@0:Action(i).
. | | |   ¬isnull(a@0)
. | | |   ⇒
. | | |   (valtype(i;a@0) ⊆r 1of(2of((with ds: ds
. | | |                              init: init
. | | |                             action a:T
. | | |                              precondition a(v) is
. | | |                              P)))(kind(a@0))?Top)
. | | 17. ∀x:Id.
. | | |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(1of((with ds: ds
. | | |                                                  init: init
. | | |                                                 action a:T
. | | |                                                  precondition a(v) is
. | | |                                                  P))))→
. | | |                        2of(1of((with ds: ds
. | | |                             init: init
. | | |                            action a:T
. | | |                             precondition a(v) is
. | | |                             P)))
. | | |                        (x)
. | | |                    else Top fi
. | | 18. x : Id
. | | ⊢  init(x)?· ∈ ds(x)?Top
. | | | by RW (AddrC [2] (UnfoldC `fpf-cap`)) 0 THEN SplitOnConclITE
. | | |
. | | |\
. | | | .....truecase .....
. | | | 1. i : Id
. | | | 2. a : Id
. | | | 3. T : Type
. | | | 4. ds : x:Id fp-> Type
```

```
. | | | 5. P : State(ds)→T→Prop
. | | | 6. init : x:Id fp-> ds(x)?Void
. | | | 7. ∀x:Id. x ∈ dom(ds) ⇒ x ∈ dom(init)
. | | | 8. w : World
. | | | 9. FairFifo
. | | | 10. FairFifo
. | | | 11. ∀l:IdLnk, tg:Id.
. | | | |   (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. | | | |                    (with ds: ds
. | | | |                     init: init
. | | | |                    action a:T
. | | | |                     precondition a(v) is
. | | | |                     P)
. | | | |                 else  fi.da(rcv(l; tg))
. | | | 12. (eqof(IdDeq)(i,i)) ∼ true₂
. | | | 13. ∀a@0:Id, t:ℕ.
. | | | |   ∃t':ℕ.
. | | | |   t≤t'
. | | | |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. | | | |     ∨ ¬locl(a@0) ∈ dom(1of(2of((with ds: ds
. | | | |                              init: init
. | | | |                             action a:T
. | | | |                              precondition a(v) is
. | | | |                              P))))
. | | | |     ∨ P@0 != 1of(
. | | | |              2of(2of(2of((with ds: ds
. | | | |               init: init
. | | | |              action a:T
. | | | |               precondition a(v) is
. | | | |               P)))))(a@0) ==> ∀v:1of(2of((with ds: ds
. | | | |                                      init: init
. | | | |                                     action a:T
. | | | |                                      precondition a(v) is
. | | | |                                      P)))(locl(a@0))?Top.
. | | | |       ¬P@0((λx.s(i;t').x),v)
. | | | 14. ∀t:ℕ.
. | | | |   ¬isnull(a(i;t))
. | | | |   ⇒
. | | | |   (islocal(kind(a(i;t)))
. | | | |    ⇒
. | | | |    deq-member(IdDeq;act(kind(a(i;t)));1of(1of(
. | | | |                                      2of(2of(2of(
. | | | |                                      (with ds: ds
. | | | |                                       init: init
. | | | |                                      action a:T
. | | | |                                       precondition a(v) is
. | | | |                                       P)))))))
. | | | |    ⇒
. | | | |    2of(1of(2of(2of(2of((with ds: ds
. | | | |              init: init
. | | | |             action a:T
. | | | |              precondition a(v) is
. | | | |              P))))))
. | | | |    (act(kind(a(i;t)))
. | | | |    ,λx.s(i;t).x
```

```
. | | | | |    ,val(a(i;t))))
. | | | | |   & (∀x:Id.
. | | | | |      deq-member(product-deq(Knd;Id;KindDeq;IdDeq);<kind(...)
. | | | | |                                                   ,x>;...)
. | | | | |      ⇒
. | | | | |      s(i;t+1).x
. | | | | |      =
. | | | | |      2of(1of(2of(2of(2of(2of((with ds: ds
. | | | | |               init: init
. | | | | |              action a:T
. | | | | |               precondition a(v) is
. | | | | |               P)))))))
. | | | | |      (<kind(a(i;t)),x>
. | | | | |      ,λx.s(i;t).x
. | | | | |      ,val(a(i;t))))
. | | | | |   & (∀l:IdLnk.
. | | | | |      deq-member(product-deq(Knd;IdLnk;KindDeq;...);<...
. | | | | |                                                    ,l>;...)
. | | | | |      ⇒
. | | | | |      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(1of(2of(2of(2of(2of(2of(
. | | | | |                                  (with ds: ds
. | | | | |                                   init: init
. | | | | |                                  action a:T
. | | | | |                                   precondition a(v) is
. | | | | |                                   P)))))))))

. | | | | |                             (<kind(a(i;t)),l>)))
. | | | | |      else nil fi)
. | | | | |   & (∀x:Id.
. | | | | |      ¬(deq-member(IdDeq;x;1of(1of(2of(2of(2of(2of(2of(2of(
. | | | | |                                  (with ds: ds
. | | | | |                                   init: init
. | | | | |                                  action a:T
. | | | | |                                   precondition a(v) is
. | | | | |                                   P)))))))))))
. | | | | |        ⇒
. | | | | |        deq-member(KindDeq;kind(a(i;t));2of(
. | | | | |                                      1of(
. | | | | |                                      2of(2of(2of(2of(2of(
. | | | | |                                      2of((with ds: ds
. | | | | |                                       init: init
. | | | | |                                      action a:T
. | | | | |                                       precondition a(v) is
. | | | | |                                       P)))))))))
. | | | | |                                      (x)))
. | | | | |      ⇒
. | | | | |      s(i;t).x = s(i;t+1).x)
. | | | | |   & (∀l:IdLnk, tg:Id.
. | | | | |      ¬(deq-member(product-deq(IdLnk;Id;...;IdDeq);...;...)
```

```
. | | | |        ⇒
. | | | |        deq-member(KindDeq;kind(a(i;t));2of(
. | | | |                                          1of(
. | | | |                                          2of(2of(2of(2of(2of(
. | | | |                                          2of(2of((with ds: ds
. | | | |                                           init: init
. | | | |                                          action a:T
. | | | |                                           precondition a(v) is
. | | | |                                           P))))))))))
. | | | |                                          (<l,tg>)))
. | | | |      ⇒
. | | | |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. | | | 15. ∀x:Id.
. | | | |   deq-member(IdDeq;x;1of(1of(2of(2of((with ds: ds
. | | | |                                 init: init
. | | | |                                action a:T
. | | | |                                 precondition a(v) is
. | | | |                                 P))))))
. | | | |   ⇒
. | | | |   s(i;0).x
. | | | |   =
. | | | |   2of(1of(2of(2of((with ds: ds
. | | | |            init: init
. | | | |           action a:T
. | | | |            precondition a(v) is
. | | | |            P)))))
. | | | |   (x)
. | | | 16. ∀a@0:Action(i).
. | | | |   ¬isnull(a@0)
. | | | |   ⇒
. | | | |   (valtype(i;a@0) ⊆r 1of(2of((with ds: ds
. | | | |                              init: init
. | | | |                             action a:T
. | | | |                              precondition a(v) is
. | | | |                              P)))(kind(a@0))?Top)
. | | | 17. ∀x:Id.
. | | | |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(1of(...)))→
. | | | |                       2of(1of((with ds: ds
. | | | |                            init: init
. | | | |                           action a:T
. | | | |                            precondition a(v) is
. | | | |                            P)))
. | | | |                       (x)
. | | | |                   else Top fi
. | | | 18. x : Id
. | | | 19. x ∈ dom(init)
. | | | ⊢  init(x) ∈ ds(x)?Top  by Auto
. | | | |
. | | | .....truecase .....
. | | | 1. i : Id
. | | | 2. a : Id
. | | | 3. T : Type
. | | | 4. ds : x:Id fp-> Type
. | | | 5. P : State(ds)→T→Prop
. | | | 6. init : x:Id fp-> ds(x)?Void
```

```
. | | | 7. ∀x:Id. x ∈ dom(ds) ⇒ x ∈ dom(init)
. | | | 8. w : World
. | | | 9. FairFifo
. | | | 10. FairFifo
. | | | 11. ∀l:IdLnk, tg:Id.
. | | |     (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. | | |                       (with ds: ds
. | | |                        init: init
. | | |                       action a:T
. | | |                        precondition a(v) is
. | | |                        P)
. | | |                    else  fi.da(rcv(l; tg))
. | | | 12. (eqof(IdDeq)(i,i)) ∼ true₂
. | | | 13. ∀a@0:Id, t:ℕ.
. | | |     ∃t':ℕ.
. | | |     t≤t'
. | | |     & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. | | |       ∨ ¬locl(a@0) ∈ dom(1of(2of((with ds: ds
. | | |                                  init: init
. | | |                                 action a:T
. | | |                                  precondition a(v) is
. | | |                                  P))))

. | | |       ∨ P@0 != 1of(
. | | |                 2of(2of(2of((with ds: ds
. | | |                  init: init
. | | |                 action a:T
. | | |                  precondition a(v) is
. | | |                  P)))))(a@0) ==> ∀v:1of(2of((with ds: ds
. | | |                                              init: init
. | | |                                             action a:T
. | | |                                              precondition a(v) is
. | | |                                              P)))(locl(a@0))?Top.
. | | |         ¬P@0((λx.s(i;t').x),v)
. | | | 14. ∀t:ℕ.
. | | |     ¬isnull(a(i;t))
. | | |     ⇒
. | | |     (islocal(kind(a(i;t)))
. | | |      ⇒
. | | |      deq-member(IdDeq;act(kind(a(i;t)));1of(1of(
. | | |                                           2of(2of(2of(
. | | |                                           (with ds: ds
. | | |                                            init: init
. | | |                                           action a:T
. | | |                                            precondition a(v) is
. | | |                                            P)))))))
. | | |      ⇒
. | | |      2of(1of(2of(2of(2of((with ds: ds
. | | |                 init: init
. | | |                action a:T
. | | |                 precondition a(v) is
. | | |                 P))))))
. | | |      (act(kind(a(i;t)))
. | | |      ,λx.s(i;t).x
. | | |      ,val(a(i;t))))
. | | |     & (∀x:Id.
```

```
. | | |        deq-member(product-deq(Knd;Id;KindDeq;IdDeq);<kind(...)
. | | |                                                    ,x>;...)
. | | |        ⇒
. | | |        s(i;t+1).x
. | | |        =
. | | |        2of(1of(2of(2of(2of(2of((with ds: ds
. | | |                  init: init
. | | |                 action a:T
. | | |                  precondition a(v) is
. | | |                  P)))))))
. | | |        (<kind(a(i;t)),x>
. | | |        ,λx.s(i;t).x
. | | |        ,val(a(i;t))))
. | | |     & (∀l:IdLnk.
. | | |        deq-member(product-deq(Knd;IdLnk;KindDeq;...);<...
. | | |                                                     ,l>;...)
. | | |        ⇒
. | | |        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(1of(2of(2of(2of(2of(2of(
. | | |                                    (with ds: ds
. | | |                                     init: init
. | | |                                    action a:T
. | | |                                     precondition a(v) is
. | | |                                     P)))))))))
. | | |                               (<kind(a(i;t)),l>)))
. | | |        else nil fi)
. | | |     & (∀x:Id.
. | | |        ¬(deq-member(IdDeq;x;1of(1of(2of(2of(2of(2of(2of(2of(
. | | |                                    (with ds: ds
. | | |                                     init: init
. | | |                                    action a:T
. | | |                                     precondition a(v) is
. | | |                                     P)))))))))))
. | | |          ⇒
. | | |          deq-member(KindDeq;kind(a(i;t));2of(
. | | |                                        1of(
. | | |                                        2of(2of(2of(2of(2of(
. | | |                                        2of((with ds: ds
. | | |                                         init: init
. | | |                                        action a:T
. | | |                                         precondition a(v) is
. | | |                                         P)))))))))
. | | |                                        (x)))
. | | |        ⇒
. | | |        s(i;t).x = s(i;t+1).x)
. | | |     & (∀l:IdLnk, tg:Id.
. | | |        ¬(deq-member(product-deq(IdLnk;Id;...;IdDeq);...;...)
. | | |          ⇒
. | | |          deq-member(KindDeq;kind(a(i;t));2of(
```

```
. | | |                                          1of(
. | | |                                          2of(2of(2of(2of(2of(
. | | |                                          2of(2of((with ds: ds
. | | |                                           init: init
. | | |                                          action a:T
. | | |                                           precondition a(v) is
. | | |                                           P))))))))))
. | | |                                          (<l,tg>)))
. | | |       ⇒
. | | |       w-tagged(tg; onlnk(l;m(i;t))) = nil)
. | | | 15. ∀x:Id.
. | | |     deq-member(IdDeq;x;1of(1of(2of(2of((with ds: ds
. | | |                                  init: init
. | | |                                 action a:T
. | | |                                  precondition a(v) is
. | | |                                  P))))))
. | | |     ⇒
. | | |     s(i;0).x
. | | |     =
. | | |     2of(1of(2of(2of((with ds: ds
. | | |              init: init
. | | |             action a:T
. | | |              precondition a(v) is
. | | |              P)))))
. | | |     (x)
. | | | 16. ∀a@0:Action(i).
. | | |     ¬isnull(a@0)
. | | |     ⇒
. | | |     (valtype(i;a@0) ⊆r 1of(2of((with ds: ds
. | | |                               init: init
. | | |                              action a:T
. | | |                               precondition a(v) is
. | | |                               P)))(kind(a@0))?Top)
. | | | 17. ∀x:Id.
. | | |     vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(1of(...)))→
. | | |                        2of(1of((with ds: ds
. | | |                             init: init
. | | |                            action a:T
. | | |                             precondition a(v) is
. | | |                             P)))
. | | |                        (x)
. | | |                     else Top fi
. | | | 18. x : Id
. | | | 19. x ∈ dom(init)
. | | | ⊢  init(x) ∈ ds(x)?Top  by DoSubsume
. | | |
. | | .\
. | | . .....falsecase .....
. | | . 1. i : Id
. | | . 2. a : Id
. | | . 3. T : Type
. | | . 4. ds : x:Id fp-> Type
. | | . 5. P : State(ds)→T→Prop
. | | . 6. init : x:Id fp-> ds(x)?Void
. | | . 7. ∀x:Id. x ∈ dom(ds) ⇒ x ∈ dom(init)
```

```
. | | . 8. w : World
. | | . 9. FairFifo
. | | . 10. FairFifo
. | | . 11. ∀l:IdLnk, tg:Id.
. | | . |   (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. | | . |                    (with ds: ds
. | | . |                     init: init
. | | . |                    action a:T
. | | . |                     precondition a(v) is
. | | . |                     P)
. | | . |                 else  fi.da(rcv(l; tg))
. | | . 12. (eqof(IdDeq)(i,i)) ∼ true₂
. | | . 13. ∀a@0:Id, t:ℕ.
. | | . |   ∃t':ℕ.
. | | . |   t≤t'
. | | . |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. | | . |     ∨ ¬locl(a@0) ∈ dom(1of(2of((with ds: ds
. | | . |                              init: init
. | | . |                             action a:T
. | | . |                              precondition a(v) is
. | | . |                              P))))
. | | . |     ∨ P@0 != 1of(
. | | . |              2of(2of(2of((with ds: ds
. | | . |               init: init
. | | . |              action a:T
. | | . |               precondition a(v) is
. | | . |               P)))))(a@0) ==> ∀v:1of(2of((with ds: ds
. | | . |                                        init: init
. | | . |                                       action a:T
. | | . |                                        precondition a(v) is
. | | . |                                        P)))(locl(a@0))?Top.
. | | . |       ¬P@0((λx.s(i;t').x),v)
. | | . 14. ∀t:ℕ.
. | | . |   ¬isnull(a(i;t))
. | | . |   ⇒
. | | . |   (islocal(kind(a(i;t)))
. | | . |    ⇒
. | | . |    deq-member(IdDeq;act(kind(a(i;t)));1of(1of(
. | | . |                                        2of(2of(2of(
. | | . |                                        (with ds: ds
. | | . |                                         init: init
. | | . |                                        action a:T
. | | . |                                         precondition a(v) is
. | | . |                                         P)))))))
. | | . |    ⇒
. | | . |    2of(1of(2of(2of(2of((with ds: ds
. | | . |              init: init
. | | . |             action a:T
. | | . |              precondition a(v) is
. | | . |              P))))))
. | | . |    (act(kind(a(i;t)))
. | | . |    ,λx.s(i;t).x
. | | . |    ,val(a(i;t))))
. | | . |   & (∀x:Id.
. | | . |      deq-member(product-deq(Knd;Id;KindDeq;IdDeq);<kind(...)
```

```
. | | . |                                                    ,x>;...)
. | | . |      ⇒
. | | . |      s(i;t+1).x
. | | . |      =
. | | . |      2of(1of(2of(2of(2of(2of((with ds: ds
. | | . |               init: init
. | | . |              action a:T
. | | . |               precondition a(v) is
. | | . |               P)))))))
. | | . |      (<kind(a(i;t)),x>
. | | . |      ,λx.s(i;t).x
. | | . |      ,val(a(i;t))))
. | | . |   & (∀l:IdLnk.
. | | . |      deq-member(product-deq(Knd;IdLnk;KindDeq;...);<...
. | | . |                                                     ,l>;...)
. | | . |      ⇒
. | | . |      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(1of(2of(2of(2of(2of(2of(
. | | . |                                  (with ds: ds
. | | . |                                   init: init
. | | . |                                  action a:T
. | | . |                                   precondition a(v) is
. | | . |                                   P)))))))))
. | | . |                             (<kind(a(i;t)),l>)))
. | | . |      else nil fi)
. | | . |   & (∀x:Id.
. | | . |      ¬(deq-member(IdDeq;x;1of(1of(2of(2of(2of(2of(2of(2of(2of(
. | | . |                                  (with ds: ds
. | | . |                                   init: init
. | | . |                                  action a:T
. | | . |                                   precondition a(v) is
. | | . |                                   P)))))))))))
. | | . |        ⇒
. | | . |        deq-member(KindDeq;kind(a(i;t));2of(
. | | . |                                      1of(
. | | . |                                      2of(2of(2of(2of(2of(2of(
. | | . |                                      2of((with ds: ds
. | | . |                                       init: init
. | | . |                                      action a:T
. | | . |                                       precondition a(v) is
. | | . |                                       P)))))))))
. | | . |                                      (x)))
. | | . |      ⇒
. | | . |      s(i;t).x = s(i;t+1).x)
. | | . |   & (∀l:IdLnk, tg:Id.
. | | . |      ¬(deq-member(product-deq(IdLnk;Id;...;IdDeq);...;...)
. | | . |        ⇒
. | | . |        deq-member(KindDeq;kind(a(i;t));2of(
. | | . |                                      1of(
```

```
. | | . |                                          2of(2of(2of(2of(2of(
. | | . |                                          2of(2of((with ds: ds
. | | . |                                           init: init
. | | . |                                          action a:T
. | | . |                                           precondition a(v) is
. | | . |                                           P))))))))))
. | | . |                                          (<l,tg>)))
. | | . |      ⇒
. | | . |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. | | . 15. ∀x:Id.
. | | . |   deq-member(IdDeq;x;1of(1of(2of(2of((with ds: ds
. | | . |                                  init: init
. | | . |                                 action a:T
. | | . |                                  precondition a(v) is
. | | . |                                  P))))))
. | | . |   ⇒
. | | . |   s(i;0).x
. | | . |   =
. | | . |   2of(1of(2of(2of((with ds: ds
. | | . |            init: init
. | | . |           action a:T
. | | . |            precondition a(v) is
. | | . |            P)))))
. | | . |   (x)
. | | . 16. ∀a@0:Action(i).
. | | . |   ¬isnull(a@0)
. | | . |   ⇒
. | | . |   (valtype(i;a@0) ⊆r 1of(2of((with ds: ds
. | | . |                              init: init
. | | . |                             action a:T
. | | . |                              precondition a(v) is
. | | . |                              P)))(kind(a@0))?Top)
. | | . 17. ∀x:Id.
. | | . |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(1of(...)))→
. | | . |                       2of(1of((with ds: ds
. | | . |                            init: init
. | | . |                           action a:T
. | | . |                            precondition a(v) is
. | | . |                            P)))
. | | . |                       (x)
. | | . |                   else Top fi
. | | . 18. x : Id
. | | . 19. ¬x ∈ dom(init)
. | | . ⊢  · ∈ ds(x)?Top  by Unfold ‘fpf-cap‘ 0 THEN SplitOnConclITE
. | | . |
. | | . .....truecase .....
. | | . 1. i : Id
. | | . 2. a : Id
. | | . 3. T : Type
. | | . 4. ds : x:Id fp-> Type
. | | . 5. P : State(ds)→T→Prop
. | | . 6. init : x:Id fp-> ds(x)?Void
. | | . 7. ∀x:Id. x ∈ dom(ds) ⇒ x ∈ dom(init)
. | | . 8. w : World
. | | . 9. FairFifo
```

```
. | | . 10. FairFifo
. | | . 11. ∀l:IdLnk, tg:Id.
. | | .     (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. | | .                         (with ds: ds
. | | .                          init: init
. | | .                         action a:T
. | | .                          precondition a(v) is
. | | .                          P)
. | | .                     else  fi.da(rcv(l; tg))
. | | . 12. (eqof(IdDeq)(i,i)) ∼ true₂
. | | . 13. ∀a@0:Id, t:ℕ.
. | | .     ∃t':ℕ.
. | | .     t≤t'
. | | .     & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. | | .       ∨ ¬locl(a@0) ∈ dom(1of(2of((with ds: ds
. | | .                                  init: init
. | | .                                 action a:T
. | | .                                  precondition a(v) is
. | | .                                  P))))
. | | .       ∨ P@0 != 1of(
. | | .                 2of(2of(2of((with ds: ds
. | | .                  init: init
. | | .                 action a:T
. | | .                  precondition a(v) is
. | | .                  P)))))(a@0) ==> ∀v:1of(2of((with ds: ds
. | | .                                              init: init
. | | .                                             action a:T
. | | .                                              precondition a(v) is
. | | .                                              P)))(locl(a@0))?Top.
. | | .          ¬P@0((λx.s(i;t').x),v)
. | | . 14. ∀t:ℕ.
. | | .     ¬isnull(a(i;t))
. | | .     ⇒
. | | .     (islocal(kind(a(i;t)))
. | | .      ⇒
. | | .      deq-member(IdDeq;act(kind(a(i;t)));1of(1of(
. | | .                                             2of(2of(2of(
. | | .                                             (with ds: ds
. | | .                                              init: init
. | | .                                             action a:T
. | | .                                              precondition a(v) is
. | | .                                              P)))))))
. | | .      ⇒
. | | .      2of(1of(2of(2of(2of((with ds: ds
. | | .                 init: init
. | | .                action a:T
. | | .                 precondition a(v) is
. | | .                 P))))))
. | | .      (act(kind(a(i;t)))
. | | .      ,λx.s(i;t).x
. | | .      ,val(a(i;t))))
. | | .     & (∀x:Id.
. | | .        deq-member(product-deq(Knd;Id;KindDeq;IdDeq);<kind(...)
. | | .                                                    ,x>;...)
. | | .          ⇒
```

```
. | | .        s(i;t+1).x
. | | .        =
. | | .        2of(1of(2of(2of(2of(2of((with ds: ds
. | | .                 init: init
. | | .                action a:T
. | | .                 precondition a(v) is
. | | .                 P)))))))
. | | .        (<kind(a(i;t)),x>
. | | .        ,λx.s(i;t).x
. | | .        ,val(a(i;t))))
. | | .     & (∀l:IdLnk.
. | | .        deq-member(product-deq(Knd;IdLnk;KindDeq;...);<...
. | | .                                                    ,l>;...)
. | | .        ⇒
. | | .        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(1of(2of(2of(2of(2of(2of(
. | | .                                    (with ds: ds
. | | .                                     init: init
. | | .                                    action a:T
. | | .                                     precondition a(v) is
. | | .                                     P)))))))))
. | | .                               (<kind(a(i;t)),l>)))
. | | .        else nil fi)
. | | .     & (∀x:Id.
. | | .        ¬(deq-member(IdDeq;x;1of(1of(2of(2of(2of(2of(2of(2of(
. | | .                                    (with ds: ds
. | | .                                     init: init
. | | .                                    action a:T
. | | .                                     precondition a(v) is
. | | .                                     P)))))))))))
. | | .          ⇒
. | | .          deq-member(KindDeq;kind(a(i;t));2of(
. | | .                                          1of(
. | | .                                          2of(2of(2of(2of(2of(
. | | .                                          2of((with ds: ds
. | | .                                           init: init
. | | .                                          action a:T
. | | .                                           precondition a(v) is
. | | .                                           P)))))))))
. | | .                                          (x)))
. | | .        ⇒
. | | .        s(i;t).x = s(i;t+1).x)
. | | .     & (∀l:IdLnk, tg:Id.
. | | .        ¬(deq-member(product-deq(IdLnk;Id;...;IdDeq);...;...)
. | | .          ⇒
. | | .          deq-member(KindDeq;kind(a(i;t));2of(
. | | .                                          1of(
. | | .                                          2of(2of(2of(2of(2of(
. | | .                                          2of(2of((with ds: ds
```

```
. | | .                                          init: init
. | | .                                         action a:T
. | | .                                          precondition a(v) is
. | | .                                          P))))))))))
. | | .                                         (<l,tg>)))
. | | .        ⇒
. | | .        w-tagged(tg; onlnk(l;m(i;t))) = nil)
. | | . 15. ∀x:Id.
. | | .     deq-member(IdDeq;x;1of(1of(2of(2of((with ds: ds
. | | .                                  init: init
. | | .                                 action a:T
. | | .                                  precondition a(v) is
. | | .                                  P))))))
. | | .     ⇒
. | | .     s(i;0).x
. | | .     =
. | | .     2of(1of(2of(2of((with ds: ds
. | | .              init: init
. | | .             action a:T
. | | .              precondition a(v) is
. | | .              P)))))
. | | .     (x)
. | | . 16. ∀a@0:Action(i).
. | | .     ¬isnull(a@0)
. | | .     ⇒
. | | .     (valtype(i;a@0) ⊆r 1of(2of((with ds: ds
. | | .                               init: init
. | | .                              action a:T
. | | .                               precondition a(v) is
. | | .                               P)))(kind(a@0))?Top)
. | | . 17. ∀x:Id.
. | | .     vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(1of(...)))→
. | | .                          2of(1of((with ds: ds
. | | .                               init: init
. | | .                              action a:T
. | | .                               precondition a(v) is
. | | .                               P)))
. | | .                          (x)
. | | .                       else Top fi
. | | . 18. x : Id
. | | . 19. ¬x ∈ dom(init)
. | | . 20. x ∈ dom(ds)
. | | . ⊢  · ∈ ds(x)  by Analyze -2 THEN BackThruSomeHyp
. | |
. | .\
. | . .....eq aux .....
. | . 1. i : Id
. | . 2. a : Id
. | . 3. T : Type
. | . 4. ds : x:Id fp-> Type
. | . 5. P : State(ds)→T→Prop
. | . 6. init : x:Id fp-> ds(x)?Void
. | . 7. ∀x:Id. x ∈ dom(ds) ⇒ x ∈ dom(init)
. | . 8. w : World
. | . 9. FairFifo
```

```
. | . 10. FairFifo
. | . 11. ∀l:IdLnk, tg:Id.
. | .     (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. | .                       (with ds: ds
. | .                        init: init
. | .                       action a:T
. | .                        precondition a(v) is
. | .                        P)
. | .                     else  fi.da(rcv(l; tg))
. | . 12. (eqof(IdDeq)(i,i)) ∼ true₂
. | . 13. ∀a@0:Id, t:ℕ.
. | .     ∃t':ℕ.
. | .     t≤t'
. | .     & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. | .       ∨ ¬locl(a@0) ∈ dom(1of(2of((with ds: ds
. | .                                  init: init
. | .                                 action a:T
. | .                                  precondition a(v) is
. | .                                  P))))
. | .       ∨ P@0 != 1of(2of(2of(2of((with ds: ds
. | .                         init: init
. | .                        action a:T
. | .                         precondition a(v) is
. | .                         P)))))(a@0) ==> ∀v:1of(2of((with ds: ds
. | .                                                    init: init
. | .                                                   action a:T
. | .                                                    precondition a(v) is
. | .                                                    P)))(locl(a@0))?Top.
. | .          ¬P@0((λx.s(i;t').x),v)
. | . 14. ∀t:ℕ.
. | .     ¬isnull(a(i;t))
. | .     ⇒
. | .     (islocal(kind(a(i;t)))
. | .      ⇒
. | .      deq-member(IdDeq;act(kind(a(i;t)));1of(1of(
. | .                                           2of(2of(2of((with ds: ds
. | .                                            init: init
. | .                                           action a:T
. | .                                            precondition a(v) is
. | .                                            P)))))))
. | .      ⇒
. | .      2of(1of(2of(2of(2of((with ds: ds
. | .                          init: init
. | .                         action a:T
. | .                          precondition a(v) is
. | .                          P))))))
. | .      (act(kind(a(i;t)))
. | .      ,λx.s(i;t).x
. | .      ,val(a(i;t))))
. | .     & (∀x:Id.
. | .        deq-member(product-deq(Knd;Id;KindDeq;IdDeq);<kind(...)
. | .                                                     ,x>;...)
. | .        ⇒
. | .        s(i;t+1).x
. | .        =
```

```
. | .        2of(1of(2of(2of(2of(2of((with ds: ds
. | .                 init: init
. | .                action a:T
. | .                 precondition a(v) is
. | .                 P)))))))
. | .        (<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>;...)
. | .        ⇒
. | .        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(1of(2of(2of(2of(2of(2of(
. | .                                    (with ds: ds
. | .                                     init: init
. | .                                    action a:T
. | .                                     precondition a(v) is
. | .                                     P)))))))
. | .                               (<kind(a(i;t)),l>)))
. | .        else nil fi)
. | .     & (∀x:Id.
. | .        ¬(deq-member(IdDeq;x;1of(1of(2of(2of(2of(2of(2of(2of(
. | .                                   (with ds: ds
. | .                                    init: init
. | .                                   action a:T
. | .                                    precondition a(v) is
. | .                                    P)))))))))
. | .          ⇒
. | .          deq-member(KindDeq;kind(a(i;t));2of(
. | .                                       1of(
. | .                                       2of(2of(2of(2of(2of(
. | .                                       2of((with ds: ds
. | .                                        init: init
. | .                                       action a:T
. | .                                        precondition a(v) is
. | .                                        P)))))))))
. | .                                       (x)))
. | .        ⇒
. | .        s(i;t).x = s(i;t+1).x)
. | .     & (∀l:IdLnk, tg:Id.
. | .        ¬(deq-member(product-deq(IdLnk;Id;IdLnkDeq;...);...;...)
. | .          ⇒
. | .          deq-member(KindDeq;kind(a(i;t));2of(
. | .                                       1of(
. | .                                       2of(2of(2of(2of(2of(
. | .                                       2of(2of((with ds: ds
. | .                                        init: init
. | .                                       action a:T
```

```
. | .                                          precondition a(v) is
. | .                                          P))))))))))
. | .                                         (<l,tg>)))
. | .       ⇒
. | .       w-tagged(tg; onlnk(l;m(i;t))) = nil)
. | . 15. ∀x:Id.
. | .     deq-member(IdDeq;x;1of(1of(2of(2of((with ds: ds
. | .                                 init: init
. | .                                action a:T
. | .                                 precondition a(v) is
. | .                                 P))))))
. | .     ⇒
. | .     s(i;0).x
. | .     =
. | .     2of(1of(2of(2of((with ds: ds
. | .              init: init
. | .             action a:T
. | .              precondition a(v) is
. | .              P)))))
. | .     (x)
. | . 16. ∀a@0:Action(i).
. | .     ¬isnull(a@0)
. | .     ⇒
. | .     (valtype(i;a@0) ⊆r 1of(2of((with ds: ds
. | .                               init: init
. | .                              action a:T
. | .                               precondition a(v) is
. | .                               P)))(kind(a@0))?Top)
. | . 17. ∀x:Id.
. | .     vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(1of((with ds: ds
. | .                                              init: init
. | .                                             action a:T
. | .                                              precondition a(v) is
. | .                                              P))))→
. | .                         2of(1of((with ds: ds
. | .                              init: init
. | .                             action a:T
. | .                              precondition a(v) is
. | .                              P)))
. | .                         (x)
. | .                       else Top fi
. | . ⊢  Id ∈ 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. init : x:Id fp-> ds(x)?Void
. . 7. ∀x:Id. x ∈ dom(ds) ⇒ x ∈ dom(init)
. . 8. w : World
. . 9. FairFifo
. . 10. FairFifo
. . 11. ∀l:IdLnk, tg:Id.
```

```
. . |   (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . |                     (with ds: ds
. . |                      init: init
. . |                     action a:T
. . |                      precondition a(v) is
. . |                      P)
. . |                  else  fi.da(rcv(l; tg))
. . 12. (eqof(IdDeq)(i,i)) ∼ true₂
. . 13. ∀a@0:Id, t:ℕ.
. . |   ∃t':ℕ.
. . |   t≤t'
. . |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . |     ∨ ¬locl(a@0) ∈ dom(1of(2of((with ds: ds
. . |                              init: init
. . |                             action a:T
. . |                              precondition a(v) is
. . |                              P))))
. . |     ∨ P@0 != 1of(2of(2of(2of((with ds: ds
. . |                    init: init
. . |                   action a:T
. . |                    precondition a(v) is
. . |                    P)))))(a@0) ==> ∀v:1of(2of((with ds: ds
. . |                                         init: init
. . |                                        action a:T
. . |                                         precondition a(v) is
. . |                                         P)))(locl(a@0))?Top.
. . |       ¬P@0((λx.s(i;t').x),v)
. . 14. ∀t:ℕ.
. . |   ¬isnull(a(i;t))
. . |   ⇒
. . |   (islocal(kind(a(i;t)))
. . |    ⇒
. . |    deq-member(IdDeq;act(kind(a(i;t)));1of(1of(
. . |                                       2of(2of(2of((with ds: ds
. . |                                        init: init
. . |                                       action a:T
. . |                                        precondition a(v) is
. . |                                        P)))))))
. . |    ⇒
. . |    2of(1of(2of(2of(2of((with ds: ds
. . |              init: init
. . |             action a:T
. . |              precondition a(v) is
. . |              P))))))
. . |    (act(kind(a(i;t)))
. . |    ,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(1of(
. . |                                                       2of(2of(
. . |                                                       2of(2of(
. . |                                                       ...)))))))
. . |      ⇒
. . |      s(i;t+1).x
```

```
. . |      =
. . |      2of(1of(2of(2of(2of(2of((with ds: ds
. . |               init: init
. . |              action a:T
. . |               precondition a(v) is
. . |               P)))))))
. . |      (<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>;...)
. . |      ⇒
. . |      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(1of(2of(2of(2of(2of(2of(
. . |                                  (with ds: ds
. . |                                   init: init
. . |                                  action a:T
. . |                                   precondition a(v) is
. . |                                   P)))))))
. . |                            (<kind(a(i;t)),l>)))
. . |      else nil fi)
. . |   & (∀x:Id.
. . |      ¬(deq-member(IdDeq;x;1of(1of(2of(2of(2of(2of(2of(2of(
. . |                                  (with ds: ds
. . |                                   init: init
. . |                                  action a:T
. . |                                   precondition a(v) is
. . |                                   P)))))))))))
. . |        ⇒
. . |        deq-member(KindDeq;kind(a(i;t));2of(
. . |                                      1of(2of(2of(2of(2of(2of(
. . |                                          2of((with ds: ds
. . |                                           init: init
. . |                                          action a:T
. . |                                           precondition a(v) is
. . |                                           P)))))))))
. . |                                      (x)))
. . |      ⇒
. . |      s(i;t).x = s(i;t+1).x)
. . |   & (∀l:IdLnk, tg:Id.
. . |      ¬(deq-member(product-deq(IdLnk;Id;IdLnkDeq;IdDeq);...;...)
. . |        ⇒
. . |        deq-member(KindDeq;kind(a(i;t));2of(
. . |                                      1of(2of(2of(2of(2of(2of(
. . |                                          2of(2of((with ds: ds
. . |                                           init: init
. . |                                          action a:T
. . |                                           precondition a(v) is
```

```
. . |                                                P))))))))))
. . |                                           (<l,tg>)))
. . |      ⇒
. . |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . 15. ∀x:Id.
. . |   deq-member(IdDeq;x;1of(1of(2of(2of((with ds: ds
. . |                                  init: init
. . |                                action a:T
. . |                                 precondition a(v) is
. . |                                 P))))))
. . |   ⇒
. . |   s(i;0).x
. . |   =
. . |   2of(1of(2of(2of((with ds: ds
. . |            init: init
. . |           action a:T
. . |            precondition a(v) is
. . |            P)))))
. . |   (x)
. . 16. ∀a@0:Action(i).
. . |   ¬isnull(a@0)
. . |   ⇒
. . |   (valtype(i;a@0) ⊆r 1of(2of((with ds: ds
. . |                             init: init
. . |                            action a:T
. . |                             precondition a(v) is
. . |                             P)))(kind(a@0))?Top)
. . 17. ∀x:Id.
. . |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(1of((with ds: ds
. . |                                                 init: init
. . |                                                action a:T
. . |                                                 precondition a(v) is
. . |                                                 P))))→
. . |                       2of(1of((with ds: ds
. . |                            init: init
. . |                           action a:T
. . |                            precondition a(v) is
. . |                            P)))
. . |                      (x)
. . |                   else Top fi
. . 18. (λx.init(x)?·) ∈ State(ds)
. . ⊢  (∃v:T. P((λx.init(x)?·),v)) ⇒ (∃e:E. loc(e) = i)
. . | 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. init : x:Id fp-> ds(x)?Void
. . 7. ∀x:Id. x ∈ dom(ds) ⇒ x ∈ dom(init)
. . 8. w : World
. . 9. FairFifo
. . 10. FairFifo
. . 11. ∀l:IdLnk, tg:Id.
```

```
. . |   (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . |                     (with ds: ds
. . |                      init: init
. . |                     action a:T
. . |                      precondition a(v) is
. . |                      P)
. . |                  else  fi.da(rcv(l; tg))
. . 12. (eqof(IdDeq)(i,i)) ∼ true₂
. . 13. ∀a@0:Id, t:ℕ.
. . |   ∃t':ℕ.
. . |   t≤t'
. . |   & ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a@0)
. . |     ∨ ¬locl(a@0) ∈ dom(1of(2of((with ds: ds
. . |                              init: init
. . |                             action a:T
. . |                              precondition a(v) is
. . |                              P))))
. . |     ∨ P@0 != 1of(2of(2of(2of((with ds: ds
. . |                    init: init
. . |                   action a:T
. . |                    precondition a(v) is
. . |                    P)))))(a@0) ==> ∀v:1of(2of((with ds: ds
. . |                                         init: init
. . |                                        action a:T
. . |                                         precondition a(v) is
. . |                                         P)))(locl(a@0))?Top.
. . |       ¬P@0((λx.s(i;t').x),v)
. . 14. ∀t:ℕ.
. . |   ¬isnull(a(i;t))
. . |   ⇒
. . |   (islocal(kind(a(i;t)))
. . |    ⇒
. . |    deq-member(IdDeq;act(kind(a(i;t)));1of(1of(
. . |                                       2of(2of(2of((with ds: ds
. . |                                        init: init
. . |                                       action a:T
. . |                                        precondition a(v) is
. . |                                        P)))))))
. . |    ⇒
. . |    2of(1of(2of(2of(2of((with ds: ds
. . |              init: init
. . |             action a:T
. . |              precondition a(v) is
. . |              P))))))
. . |    (act(kind(a(i;t)))
. . |    ,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(1of(
. . |                                                       2of(2of(
. . |                                                       2of(2of(
. . |                                                       ...)))))))
. . |      ⇒
. . |      s(i;t+1).x
```

```
. . |      =
. . |      2of(1of(2of(2of(2of(2of((with ds: ds
. . |               init: init
. . |              action a:T
. . |               precondition a(v) is
. . |               P)))))))
. . |      (<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>;...)
. . |      ⇒
. . |      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(1of(2of(2of(2of(2of(2of(
. . |                                  (with ds: ds
. . |                                   init: init
. . |                                  action a:T
. . |                                   precondition a(v) is
. . |                                   P)))))))
. . |                            (<kind(a(i;t)),l>)))
. . |      else nil fi)
. . |   & (∀x:Id.
. . |      ¬(deq-member(IdDeq;x;1of(1of(2of(2of(2of(2of(2of(2of(
. . |                                  (with ds: ds
. . |                                   init: init
. . |                                  action a:T
. . |                                   precondition a(v) is
. . |                                   P)))))))))
. . |        ⇒
. . |        deq-member(KindDeq;kind(a(i;t));2of(
. . |                                      1of(2of(2of(2of(2of(2of(
. . |                                          2of((with ds: ds
. . |                                           init: init
. . |                                          action a:T
. . |                                           precondition a(v) is
. . |                                           P)))))))))
. . |                                      (x)))
. . |      ⇒
. . |      s(i;t).x = s(i;t+1).x)
. . |   & (∀l:IdLnk, tg:Id.
. . |      ¬(deq-member(product-deq(IdLnk;Id;IdLnkDeq;IdDeq);...;...)
. . |        ⇒
. . |        deq-member(KindDeq;kind(a(i;t));2of(
. . |                                      1of(2of(2of(2of(2of(2of(
. . |                                          2of(2of((with ds: ds
. . |                                           init: init
. . |                                          action a:T
. . |                                           precondition a(v) is
```

```
. . |                                                P))))))))))
. . |                                           (<l,tg>)))
. . |      ⇒
. . |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . 15. ∀x:Id.
. . |   deq-member(IdDeq;x;1of(1of(2of(2of((with ds: ds
. . |                                  init: init
. . |                                 action a:T
. . |                                  precondition a(v) is
. . |                                  P))))))
. . |   ⇒
. . |   s(i;0).x
. . |   =
. . |   2of(1of(2of(2of((with ds: ds
. . |            init: init
. . |           action a:T
. . |            precondition a(v) is
. . |            P)))))
. . |   (x)
. . 16. ∀a@0:Action(i).
. . |   ¬isnull(a@0)
. . |   ⇒
. . |   (valtype(i;a@0) ⊆r 1of(2of((with ds: ds
. . |                           init: init
. . |                          action a:T
. . |                           precondition a(v) is
. . |                           P)))(kind(a@0))?Top)
. . 17. ∀x:Id.
. . |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(1of((with ds: ds
. . |                                              init: init
. . |                                             action a:T
. . |                                              precondition a(v) is
. . |                                              P))))→
. . |                       2of(1of((with ds: ds
. . |                            init: init
. . |                           action a:T
. . |                            precondition a(v) is
. . |                            P)))
. . |                         (x)
. . |                     else Top fi
. . 18. (λx.init(x)?•) ∈ State(ds)
. . 19. ∃v:T. P((λx.init(x)?•),v)
. . ⊢  ∃e:E. loc(e) = i  by MoveToHyp 8 -1 THEN ExRepD
. . |
. . 1. i : Id
. . 2. a : Id
. . 3. T : Type
. . 4. ds : x:Id fp-> Type
. . 5. P : State(ds)→T→Prop
. . 6. init : x:Id fp-> ds(x)?Void
. . 7. ∀x:Id. x ∈ dom(ds) ⇒ x ∈ dom(init)
. . 8. v : T
. . 9. P((λx.init(x)?•),v)
. . 10. w : World
. . 11. FairFifo
```

```
. . 12. FairFifo
. . 13. ∀l:IdLnk, tg:Id.
. . |   (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . |                     (with ds: ds
. . |                      init: init
. . |                     action a:T
. . |                      precondition a(v) is
. . |                      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(1of(2of((with ds: ds
. . |                              init: init
. . |                             action a:T
. . |                              precondition a(v) is
. . |                              P))))
. . |     ∨ P@0 != 1of(2of(2of(2of((with ds: ds
. . |                    init: init
. . |                   action a:T
. . |                    precondition a(v) is
. . |                    P)))))(a@0) ==> ∀v:1of(2of((with ds: ds
. . |                                                init: init
. . |                                               action a:T
. . |                                                precondition a(v) is
. . |                                                P)))(locl(a@0))?Top.
. . |       ¬P@0((λx.s(i;t').x),v)
. . 16. ∀t:ℕ.
. . |   ¬isnull(a(i;t))
. . |   ⇒
. . |   (islocal(kind(a(i;t)))
. . |    ⇒
. . |    deq-member(IdDeq;act(kind(a(i;t)));1of(1of(
. . |                                        2of(2of(2of((with ds: ds
. . |                                         init: init
. . |                                        action a:T
. . |                                         precondition a(v) is
. . |                                         P)))))))
. . |    ⇒
. . |    2of(1of(2of(2of(2of((with ds: ds
. . |              init: init
. . |             action a:T
. . |              precondition a(v) is
. . |              P))))))
. . |    (act(kind(a(i;t)))
. . |    ,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(1of(
. . |                                                        2of(2of(
. . |                                                        2of(2of(
. . |                                                        ...)))))))
```

```
. . |      ⇒
. . |      s(i;t+1).x
. . |      =
. . |      2of(1of(2of(2of(2of(2of((with ds: ds
. . |               init: init
. . |              action a:T
. . |               precondition a(v) is
. . |               P)))))))
. . |      (<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>;...)
. . |      ⇒
. . |      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(1of(2of(2of(2of(2of(2of(
. . |                                  (with ds: ds
. . |                                   init: init
. . |                                  action a:T
. . |                                   precondition a(v) is
. . |                                   P)))))))
. . |                           (<kind(a(i;t)),l>)))
. . |      else nil fi)
. . |   & (∀x:Id.
. . |      ¬(deq-member(IdDeq;x;1of(1of(2of(2of(2of(2of(2of(2of(
. . |                                  (with ds: ds
. . |                                   init: init
. . |                                  action a:T
. . |                                   precondition a(v) is
. . |                                   P)))))))))
. . |        ⇒
. . |        deq-member(KindDeq;kind(a(i;t));2of(
. . |                                      1of(2of(2of(2of(2of(2of(
. . |                                          2of((with ds: ds
. . |                                           init: init
. . |                                          action a:T
. . |                                           precondition a(v) is
. . |                                           P)))))))))
. . |                                      (x)))
. . |      ⇒
. . |      s(i;t).x = s(i;t+1).x)
. . |   & (∀l:IdLnk, tg:Id.
. . |      ¬(deq-member(product-deq(IdLnk;Id;IdLnkDeq;IdDeq);...;...)
. . |        ⇒
. . |        deq-member(KindDeq;kind(a(i;t));2of(
. . |                                      1of(2of(2of(2of(2of(2of(
. . |                                          2of(2of((with ds: ds
. . |                                           init: init
```

```
. . |                                                action a:T
. . |                                                 precondition a(v) is
. . |                                                 P)))))))))))
. . |                                              (<l,tg>)))
. . |      ⇒
. . |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . 17. ∀x:Id.
. . |   deq-member(IdDeq;x;1of(1of(2of(2of((with ds: ds
. . |                                  init: init
. . |                                 action a:T
. . |                                  precondition a(v) is
. . |                                  P))))))
. . |   ⇒
. . |   s(i;0).x
. . |   =
. . |   2of(1of(2of(2of((with ds: ds
. . |            init: init
. . |           action a:T
. . |            precondition a(v) is
. . |            P)))))
. . |   (x)
. . 18. ∀a@0:Action(i).
. . |   ¬isnull(a@0)
. . |   ⇒
. . |   (valtype(i;a@0) ⊆r 1of(2of((with ds: ds
. . |                             init: init
. . |                            action a:T
. . |                             precondition a(v) is
. . |                             P)))(kind(a@0))?Top)
. . 19. ∀x:Id.
. . |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(1of((with ds: ds
. . |                                               init: init
. . |                                              action a:T
. . |                                               precondition a(v) is
. . |                                               P))))→
. . |                        2of(1of((with ds: ds
. . |                             init: init
. . |                            action a:T
. . |                             precondition a(v) is
. . |                             P)))
. . |                       (x)
. . |                    else Top fi
. . 20. (λx.init(x)?•) ∈ State(ds)
. . ⊢  ∃e:E. loc(e) = i
. . | by AllHyps (λh.InstHyp [a;0] h THENA (Auto THEN PWTrivial))
. . |    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. init : x:Id fp-> ds(x)?Void
. . | 7. ∀x:Id. x ∈ dom(ds) ⇒ x ∈ dom(init)
. . | 8. v : T
. . | 9. P((λx.init(x)?•),v)
. . | 10. w : World
. . | 11. FairFifo
. . | 12. FairFifo
. . | 13. ∀l:IdLnk, tg:Id.
. . | |   (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . | |                    (with ds: ds
. . | |                     init: init
. . | |                    action a:T
. . | |                     precondition a(v) is
. . | |                     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(1of(2of((with ds: ds
. . | |                              init: init
. . | |                             action a:T
. . | |                              precondition a(v) is
. . | |                              P))))
. . | |     ∨ P@0 != 1of(2of(2of(2of((with ds: ds
. . | |                    init: init
. . | |                   action a:T
. . | |                    precondition a(v) is
. . | |                    P)))))(a@0) ==> ∀v:1of(2of((with ds: ds
. . | |                                                init: init
. . | |                                               action a:T
. . | |                                                precondition a(v) is
. . | |                                                P)))(locl(a@0))?Top.
. . | |       ¬P@0((λx.s(i;t').x),v)
. . | 16. ∀t:ℕ.
. . | |   ¬isnull(a(i;t))
. . | |   ⇒
. . | |   (islocal(kind(a(i;t)))
. . | |    ⇒
. . | |    deq-member(IdDeq;act(kind(a(i;t)));1of(1of(
. . | |                                        2of(2of(2of((with ds: ds
. . | |                                         init: init
. . | |                                        action a:T
. . | |                                         precondition a(v) is
. . | |                                         P)))))))
. . | |    ⇒
. . | |    2of(1of(2of(2of(2of((with ds: ds
. . | |              init: init
. . | |             action a:T
. . | |              precondition a(v) is
. . | |              P))))))
. . | |    (act(kind(a(i;t)))
. . | |    ,λx.s(i;t).x
```

```
. . | |    ,val(a(i;t))))
. . | |   & (∀x:Id.
. . | |      deq-member(product-deq(Knd;Id;KindDeq;IdDeq);<kind(...)
. . | |                                                    ,x>;...)
. . | |      ⇒
. . | |      s(i;t+1).x
. . | |      =
. . | |      2of(1of(2of(2of(2of(2of((with ds: ds
. . | |               init: init
. . | |              action a:T
. . | |               precondition a(v) is
. . | |               P)))))))
. . | |      (<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>;...)
. . | |      ⇒
. . | |      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(1of(2of(2of(2of(2of(2of(
. . | |                                  (with ds: ds
. . | |                                   init: init
. . | |                                  action a:T
. . | |                                   precondition a(v) is
. . | |                                   P)))))))
. . | |                            (<kind(a(i;t)),l>)))
. . | |      else nil fi)
. . | |   & (∀x:Id.
. . | |      ¬(deq-member(IdDeq;x;1of(1of(2of(2of(2of(2of(2of(2of(
. . | |                                  (with ds: ds
. . | |                                   init: init
. . | |                                  action a:T
. . | |                                   precondition a(v) is
. . | |                                   P)))))))))
. . | |        ⇒
. . | |        deq-member(KindDeq;kind(a(i;t));2of(
. . | |                                      1of(
. . | |                                      2of(2of(2of(2of(2of(
. . | |                                      2of((with ds: ds
. . | |                                       init: init
. . | |                                      action a:T
. . | |                                       precondition a(v) is
. . | |                                       P)))))))))
. . | |                                      (x)))
. . | |      ⇒
. . | |      s(i;t).x = s(i;t+1).x)
. . | |   & (∀l:IdLnk, tg:Id.
. . | |      ¬(deq-member(product-deq(IdLnk;Id;IdLnkDeq;...);...;...)
```

```
. . | |        ⇒
. . | |        deq-member(KindDeq;kind(a(i;t));2of(
. . | |                                          1of(
. . | |                                          2of(2of(2of(2of(2of(
. . | |                                          2of(2of((with ds: ds
. . | |                                           init: init
. . | |                                          action a:T
. . | |                                           precondition a(v) is
. . | |                                           P))))))))))
. . | |                                          (<l,tg>)))
. . | |      ⇒
. . | |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . | 17. ∀x:Id.
. . | |   deq-member(IdDeq;x;1of(1of(2of(2of((with ds: ds
. . | |                                 init: init
. . | |                                action a:T
. . | |                                 precondition a(v) is
. . | |                                 P))))))
. . | |   ⇒
. . | |   s(i;0).x
. . | |   =
. . | |   2of(1of(2of(2of((with ds: ds
. . | |            init: init
. . | |           action a:T
. . | |            precondition a(v) is
. . | |            P)))))
. . | |   (x)
. . | 18. ∀a@0:Action(i).
. . | |   ¬isnull(a@0)
. . | |   ⇒
. . | |   (valtype(i;a@0) ⊆r 1of(2of((with ds: ds
. . | |                             init: init
. . | |                            action a:T
. . | |                             precondition a(v) is
. . | |                             P)))(kind(a@0))?Top)
. . | 19. ∀x:Id.
. . | |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(1of((with ds: ds
. . | |                                              init: init
. . | |                                             action a:T
. . | |                                              precondition a(v) is
. . | |                                              P))))→
. . | |                       2of(1of((with ds: ds
. . | |                            init: init
. . | |                           action a:T
. . | |                            precondition a(v) is
. . | |                            P)))
. . | |                       (x)
. . | |                   else Top fi
. . | 20. (λx.init(x)?•) ∈ State(ds)
. . | 21. t' : ℕ
. . | 22. 0≤t'
. . | 23. ¬isnull(a(i;t')) & kind(a(i;t')) = locl(a)
. . | ⊢  ∃e:E. loc(e) = i  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. init : x:Id fp-> ds(x)?Void
. . | | 7. ∀x:Id. x ∈ dom(ds) ⇒ x ∈ dom(init)
. . | | 8. v : T
. . | | 9. P((λx.init(x)?•),v)
. . | | 10. w : World
. . | | 11. FairFifo
. . | | 12. FairFifo
. . | | 13. ∀l:IdLnk, tg:Id.
. . | |     (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . | |                        (with ds: ds
. . | |                         init: init
. . | |                        action a:T
. . | |                         precondition a(v) is
. . | |                         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(1of(2of((with ds: ds
. . | |                                  init: init
. . | |                                 action a:T
. . | |                                  precondition a(v) is
. . | |                                  P))))
. . | |       ∨ P@0 != 1of(
. . | |                 2of(2of(2of((with ds: ds
. . | |                  init: init
. . | |                 action a:T
. . | |                  precondition a(v) is
. . | |                  P)))))(a@0) ==> ∀v:1of(2of((with ds: ds
. . | |                                              init: init
. . | |                                             action a:T
. . | |                                              precondition a(v) is
. . | |                                              P)))(locl(a@0))?Top.
. . | |         ¬P@0((λx.s(i;t').x),v)
. . | | 16. ∀t:ℕ.
. . | |     ¬isnull(a(i;t))
. . | |     ⇒
. . | |     (islocal(kind(a(i;t)))
. . | |      ⇒
. . | |      deq-member(IdDeq;act(kind(a(i;t)));1of(1of(
. . | |                                              2of(2of(2of(
. . | |                                              (with ds: ds
. . | |                                               init: init
. . | |                                              action a:T
. . | |                                               precondition a(v) is
. . | |                                               P)))))))
. . | |      ⇒
```

```
. . | |      2of(1of(2of(2of(2of((with ds: ds
. . | |               init: init
. . | |              action a:T
. . | |               precondition a(v) is
. . | |               P))))))
. . | |      (act(kind(a(i;t)))
. . | |      ,λx.s(i;t).x
. . | |      ,val(a(i;t))))
. . | |     & (∀x:Id.
. . | |        deq-member(product-deq(Knd;Id;KindDeq;IdDeq);<kind(...)
. . | |                                                    ,x>;...)
. . | |        ⇒
. . | |        s(i;t+1).x
. . | |        =
. . | |        2of(1of(2of(2of(2of(2of((with ds: ds
. . | |                 init: init
. . | |                action a:T
. . | |                 precondition a(v) is
. . | |                 P)))))))
. . | |        (<kind(a(i;t)),x>
. . | |        ,λx.s(i;t).x
. . | |        ,val(a(i;t))))
. . | |     & (∀l:IdLnk.
. . | |        deq-member(product-deq(Knd;IdLnk;KindDeq;...);<...
. . | |                                                     ,l>;...)
. . | |        ⇒
. . | |        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(1of(2of(2of(2of(2of(2of(
. . | |                                    (with ds: ds
. . | |                                     init: init
. . | |                                    action a:T
. . | |                                     precondition a(v) is
. . | |                                     P)))))))
. . | |                                (<kind(a(i;t)),l>)))
. . | |        else nil fi)
. . | |     & (∀x:Id.
. . | |        ¬(deq-member(IdDeq;x;1of(1of(2of(2of(2of(2of(2of(2of(
. . | |                                    (with ds: ds
. . | |                                     init: init
. . | |                                    action a:T
. . | |                                     precondition a(v) is
. . | |                                     P)))))))))))
. . | |          ⇒
. . | |          deq-member(KindDeq;kind(a(i;t));2of(
. . | |                                        1of(
. . | |                                        2of(2of(2of(2of(2of(
. . | |                                        2of((with ds: ds
. . | |                                         init: init
. . | |                                        action a:T
```

```
. . | |                                          precondition a(v) is
. . | |                                          P)))))))))
. . | |                                         (x)))
. . | |       ⇒
. . | |       s(i;t).x = s(i;t+1).x)
. . | |    & (∀l:IdLnk, tg:Id.
. . | |       ¬(deq-member(product-deq(IdLnk;Id;...;IdDeq);...;...)
. . | |         ⇒
. . | |         deq-member(KindDeq;kind(a(i;t));2of(
. . | |                                         1of(
. . | |                                         2of(2of(2of(2of(2of(
. . | |                                         2of(2of((with ds: ds
. . | |                                          init: init
. . | |                                         action a:T
. . | |                                          precondition a(v) is
. . | |                                          P)))))))))
. . | |                                         (<l,tg>)))
. . | |       ⇒
. . | |       w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . | | 17. ∀x:Id.
. . | |     deq-member(IdDeq;x;1of(1of(2of(2of((with ds: ds
. . | |                                 init: init
. . | |                                action a:T
. . | |                                 precondition a(v) is
. . | |                                 P))))))
. . | |     ⇒
. . | |     s(i;0).x
. . | |     =
. . | |     2of(1of(2of(2of((with ds: ds
. . | |              init: init
. . | |             action a:T
. . | |              precondition a(v) is
. . | |              P)))))
. . | |     (x)
. . | | 18. ∀a@0:Action(i).
. . | |     ¬isnull(a@0)
. . | |     ⇒
. . | |     (valtype(i;a@0) ⊆r 1of(2of((with ds: ds
. . | |                              init: init
. . | |                             action a:T
. . | |                              precondition a(v) is
. . | |                              P)))(kind(a@0))?Top)
. . | | 19. ∀x:Id.
. . | |     vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(1of(...)))→
. . | |                          2of(1of((with ds: ds
. . | |                               init: init
. . | |                              action a:T
. . | |                               precondition a(v) is
. . | |                               P)))
. . | |                         (x)
. . | |                       else Top fi
. . | | 20. (λx.init(x)?•) ∈ State(ds)
. . | | 21. t' : ℕ
. . | | 22. 0≤t'
. . | | 23. ¬isnull(a(i;t'))
```

```
. . | | 24. 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. init : x:Id fp-> ds(x)?Void
. . | | 7. ∀x:Id. x ∈ dom(ds) ⇒ x ∈ dom(init)
. . | | 8. v : T
. . | | 9. P((λx.init(x)?•),v)
. . | | 10. w : World
. . | | 11. FairFifo
. . | | 12. FairFifo
. . | | 13. ∀l:IdLnk, tg:Id.
. . | |     (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . | |                        (with ds: ds
. . | |                         init: init
. . | |                        action a:T
. . | |                         precondition a(v) is
. . | |                         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(1of(2of((with ds: ds
. . | |                                  init: init
. . | |                                 action a:T
. . | |                                  precondition a(v) is
. . | |                                  P))))
. . | |       ∨ P@0 != 1of(
. . | |                2of(2of(2of((with ds: ds
. . | |                 init: init
. . | |                action a:T
. . | |                 precondition a(v) is
. . | |                 P)))))(a@0) ==> ∀v:1of(2of((with ds: ds
. . | |                                             init: init
. . | |                                            action a:T
. . | |                                             precondition a(v) is
. . | |                                             P)))(locl(a@0))?Top.
. . | |         ¬P@0((λx.s(i;t').x),v)
. . | | 16. ∀t:ℕ.
. . | |     ¬isnull(a(i;t))
. . | |     ⇒
. . | |     (islocal(kind(a(i;t)))
. . | |      ⇒
```

```
. . | |      deq-member(IdDeq;act(kind(a(i;t)));1of(1of(
. . | |                                          2of(2of(2of(
. . | |                                          (with ds: ds
. . | |                                           init: init
. . | |                                          action a:T
. . | |                                           precondition a(v) is
. . | |                                           P)))))))
. . | |      ⇒
. . | |      2of(1of(2of(2of(2of((with ds: ds
. . | |               init: init
. . | |              action a:T
. . | |               precondition a(v) is
. . | |               P))))))
. . | |      (act(kind(a(i;t)))
. . | |      ,λx.s(i;t).x
. . | |      ,val(a(i;t))))
. . | |     & (∀x:Id.
. . | |        deq-member(product-deq(Knd;Id;KindDeq;IdDeq);<kind(...)
. . | |                                                     ,x>;...)
. . | |        ⇒
. . | |        s(i;t+1).x
. . | |        =
. . | |        2of(1of(2of(2of(2of(2of((with ds: ds
. . | |                 init: init
. . | |                action a:T
. . | |                 precondition a(v) is
. . | |                 P)))))))
. . | |        (<kind(a(i;t)),x>
. . | |        ,λx.s(i;t).x
. . | |        ,val(a(i;t))))
. . | |     & (∀l:IdLnk.
. . | |        deq-member(product-deq(Knd;IdLnk;KindDeq;...);<...
. . | |                                                      ,l>;...)
. . | |        ⇒
. . | |        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(1of(2of(2of(2of(2of(2of(
. . | |                                      (with ds: ds
. . | |                                       init: init
. . | |                                      action a:T
. . | |                                       precondition a(v) is
. . | |                                       P))))))))
. . | |                              (<kind(a(i;t)),l>)))
. . | |        else nil fi)
. . | |     & (∀x:Id.
. . | |        ¬(deq-member(IdDeq;x;1of(1of(2of(2of(2of(2of(2of(2of(
. . | |                                     (with ds: ds
. . | |                                      init: init
. . | |                                     action a:T
. . | |                                      precondition a(v) is
```

```
. . | |                                        P)))))))))))
. . | |          ⇒
. . | |          deq-member(KindDeq;kind(a(i;t));2of(
. . | |                                         1of(
. . | |                                         2of(2of(2of(2of(2of(
. . | |                                         2of((with ds: ds
. . | |                                          init: init
. . | |                                         action a:T
. . | |                                          precondition a(v) is
. . | |                                          P)))))))))
. . | |                                         (x)))
. . | |        ⇒
. . | |        s(i;t).x = s(i;t+1).x)
. . | |     & (∀l:IdLnk, tg:Id.
. . | |        ¬(deq-member(product-deq(IdLnk;Id;...;IdDeq);...;...)
. . | |          ⇒
. . | |          deq-member(KindDeq;kind(a(i;t));2of(
. . | |                                         1of(
. . | |                                         2of(2of(2of(2of(2of(
. . | |                                         2of(2of((with ds: ds
. . | |                                          init: init
. . | |                                         action a:T
. . | |                                          precondition a(v) is
. . | |                                          P)))))))))
. . | |                                         (<l,tg>)))
. . | |        ⇒
. . | |        w-tagged(tg; onlnk(l;m(i;t))) = nil)

. . | | 17. ∀x:Id.
. . | |     deq-member(IdDeq;x;1of(1of(2of(2of((with ds: ds
. . | |                                 init: init
. . | |                                action a:T
. . | |                                 precondition a(v) is
. . | |                                 P))))))
. . | |     ⇒
. . | |     s(i;0).x
. . | |     =
. . | |     2of(1of(2of(2of((with ds: ds
. . | |              init: init
. . | |             action a:T
. . | |              precondition a(v) is
. . | |              P)))))
. . | |     (x)
. . | | 18. ∀a@0:Action(i).
. . | |     ¬isnull(a@0)
. . | |     ⇒
. . | |     (valtype(i;a@0) ⊆r 1of(2of((with ds: ds
. . | |                             init: init
. . | |                            action a:T
. . | |                             precondition a(v) is
. . | |                             P)))(kind(a@0))?Top)
. . | | 19. ∀x:Id.
. . | |     vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(1of(...)))→
. . | |                         2of(1of((with ds: ds
. . | |                              init: init
. . | |                             action a:T
```

```
. . | |                              precondition a(v) is
. . | |                              P)))
. . | |                         (x)
. . | |                       else Top fi
. . | | 20. (λx.init(x)?·) ∈ State(ds)
. . | | 21. t' : ℕ
. . | | 22. 0≤t'
. . | | 23. ¬isnull(a(i;t'))
. . | | 24. kind(a(i;t')) = locl(a)
. . | | ⊢  loc(<i,t'>) = i
. . | |   by Unfold `w-loc` 0 THEN Reduce 0 THEN Fold `member` 0
. . | |      THEN
. . | |      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. init : x:Id fp-> ds(x)?Void
. . | . 7. ∀x:Id. x ∈ dom(ds) ⇒ x ∈ dom(init)
. . | . 8. v : T
. . | . 9. P((λx.init(x)?·),v)
. . | . 10. w : World
. . | . 11. FairFifo
. . | . 12. FairFifo
. . | . 13. ∀l:IdLnk, tg:Id.
. . | .     (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . | .                       (with ds: ds
. . | .                        init: init
. . | .                       action a:T
. . | .                        precondition a(v) is
. . | .                        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(1of(2of((with ds: ds
. . | .                                   init: init
. . | .                                  action a:T
. . | .                                   precondition a(v) is
. . | .                                   P))))
. . | .       ∨ P@0 != 1of(
. . | .                 2of(2of(2of((with ds: ds
. . | .                  init: init
. . | .                 action a:T
. . | .                  precondition a(v) is
. . | .                  P)))))(a@0) ==> ∀v:1of(2of((with ds: ds
. . | .                                             init: init
. . | .                                            action a:T
. . | .                                             precondition a(v) is
```

```
. . | .                                          P)))(locl(a@0))?Top.
. . | .         ¬P@0((λx.s(i;t').x),v)
. . | . 16. ∀t:ℕ.
. . | .     ¬isnull(a(i;t))
. . | .     ⇒
. . | .     (islocal(kind(a(i;t)))
. . | .      ⇒
. . | .      deq-member(IdDeq;act(kind(a(i;t)));1of(1of(
. . | .                                          2of(2of(2of(
. . | .                                          (with ds: ds
. . | .                                           init: init
. . | .                                          action a:T
. . | .                                           precondition a(v) is
. . | .                                           P)))))))
. . | .      ⇒
. . | .      2of(1of(2of(2of(2of((with ds: ds
. . | .                 init: init
. . | .                action a:T
. . | .                 precondition a(v) is
. . | .                 P))))))
. . | .      (act(kind(a(i;t)))
. . | .      ,λx.s(i;t).x
. . | .      ,val(a(i;t))))
. . | .     & (∀x:Id.
. . | .        deq-member(product-deq(Knd;Id;KindDeq;IdDeq);<kind(...)
. . | .                                                    ,x>;...)
. . | .        ⇒
. . | .        s(i;t+1).x
. . | .        =
. . | .        2of(1of(2of(2of(2of(2of((with ds: ds
. . | .                  init: init
. . | .                 action a:T
. . | .                  precondition a(v) is
. . | .                  P)))))))
. . | .        (<kind(a(i;t)),x>
. . | .        ,λx.s(i;t).x
. . | .        ,val(a(i;t))))
. . | .     & (∀l:IdLnk.
. . | .        deq-member(product-deq(Knd;IdLnk;KindDeq;...);<...
. . | .                                                     ,l>;...)
. . | .        ⇒
. . | .        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(1of(2of(2of(2of(2of(2of(
. . | .                                     (with ds: ds
. . | .                                      init: init
. . | .                                     action a:T
. . | .                                      precondition a(v) is
. . | .                                      P)))))))
. . | .                              (<kind(a(i;t)),l>)))
```

```
. . | .        else nil fi)
. . | .     & (∀x:Id.
. . | .        ¬(deq-member(IdDeq;x;1of(1of(2of(2of(2of(2of(2of(2of(
. . | .                                    (with ds: ds
. . | .                                     init: init
. . | .                                    action a:T
. . | .                                     precondition a(v) is
. . | .                                     P))))))))))
. . | .          ⇒
. . | .          deq-member(KindDeq;kind(a(i;t));2of(
. . | .                                          1of(
. . | .                                          2of(2of(2of(2of(2of(
. . | .                                          2of((with ds: ds
. . | .                                           init: init
. . | .                                          action a:T
. . | .                                           precondition a(v) is
. . | .                                           P)))))))))
. . | .                                          (x)))
. . | .        ⇒
. . | .        s(i;t).x = s(i;t+1).x)
. . | .     & (∀l:IdLnk, tg:Id.
. . | .        ¬(deq-member(product-deq(IdLnk;Id;...;IdDeq);...;...)
. . | .          ⇒
. . | .          deq-member(KindDeq;kind(a(i;t));2of(
. . | .                                          1of(
. . | .                                          2of(2of(2of(2of(2of(
. . | .                                          2of(2of((with ds: ds
. . | .                                           init: init
. . | .                                          action a:T
. . | .                                           precondition a(v) is
. . | .                                           P))))))))))
. . | .                                          (<l,tg>)))
. . | .        ⇒
. . | .        w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . | . 17. ∀x:Id.
. . | .     deq-member(IdDeq;x;1of(1of(2of(2of((with ds: ds
. . | .                                 init: init
. . | .                                action a:T
. . | .                                 precondition a(v) is
. . | .                                 P))))))
. . | .     ⇒
. . | .     s(i;0).x
. . | .     =
. . | .     2of(1of(2of(2of((with ds: ds
. . | .              init: init
. . | .             action a:T
. . | .              precondition a(v) is
. . | .              P)))))
. . | .     (x)
. . | . 18. ∀a@0:Action(i).
. . | .     ¬isnull(a@0)
. . | .     ⇒
. . | .     (valtype(i;a@0) ⊆r 1of(2of((with ds: ds
. . | .                              init: init
. . | .                             action a:T
```

```
. . | .                              precondition a(v) is
. . | .                              P)))(kind(a@0))?Top)
. . | . 19. ∀x:Id.
. . | .     vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(1of(...)))→
. . | .                          2of(1of((with ds: ds
. . | .                               init: init
. . | .                              action a:T

. . | .                               precondition a(v) is
. . | .                               P)))
. . | .                          (x)
. . | .                        else Top fi
. . | . 20. (λx.init(x)?•) ∈ State(ds)
. . | . 21. t' : ℕ
. . | . 22. 0≤t'
. . | . 23. ¬isnull(a(i;t'))
. . | . 24. kind(a(i;t')) = locl(a)
. . | . 25. e : E
. . | . ⊢  (loc(e) = i) ∈ Prop  by 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. init : x:Id fp-> ds(x)?Void
. . | 7. ∀x:Id. x ∈ dom(ds) ⇒ x ∈ dom(init)
. . | 8. v : T
. . | 9. P((λx.init(x)?•),v)
. . | 10. w : World
. . | 11. FairFifo
. . | 12. FairFifo
. . | 13. ∀l:IdLnk, tg:Id.
. . | |   (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . | |                     (with ds: ds
. . | |                      init: init
. . | |                     action a:T
. . | |                      precondition a(v) is
. . | |                      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(1of(2of((with ds: ds
. . | |                               init: init
. . | |                              action a:T
. . | |                               precondition a(v) is
. . | |                               P))))
. . | |     ∨ P@0 != 1of(2of(2of(2of((with ds: ds
. . | |                    init: init
. . | |                   action a:T
. . | |                    precondition a(v) is
. . | |                    P)))))(a@0) ==> ∀v:1of(2of((with ds: ds
```

```
. . | |                                          init: init
. . | |                                         action a:T
. . | |                                          precondition a(v) is
. . | |                                          P)))(locl(a@0))?Top.
. . | |       ¬P@0((λx.s(i;t').x),v)
. . | 16. ∀t:ℕ.
. . | |   ¬isnull(a(i;t))
. . | |   ⇒
. . | |   (islocal(kind(a(i;t)))
. . | |    ⇒
. . | |    deq-member(IdDeq;act(kind(a(i;t)));1of(1of(1of(
. . | |                                       2of(2of(2of((with ds: ds
. . | |                                        init: init
. . | |                                       action a:T
. . | |                                        precondition a(v) is
. . | |                                        P)))))))
. . | |    ⇒
. . | |    2of(1of(2of(2of(2of((with ds: ds
. . | |             init: init
. . | |            action a:T
. . | |             precondition a(v) is
. . | |             P))))))
. . | |    (act(kind(a(i;t)))
. . | |    ,λx.s(i;t).x
. . | |    ,val(a(i;t))))
. . | |   & (∀x:Id.
. . | |      deq-member(product-deq(Knd;Id;KindDeq;IdDeq);<kind(...)
. . | |                                                    ,x>;...)
. . | |      ⇒
. . | |      s(i;t+1).x
. . | |      =
. . | |      2of(1of(2of(2of(2of(2of((with ds: ds
. . | |               init: init
. . | |              action a:T
. . | |               precondition a(v) is
. . | |               P)))))))
. . | |      (<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>;...)
. . | |      ⇒
. . | |      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(1of(2of(2of(2of(2of(2of(
. . | |                                    (with ds: ds
. . | |                                     init: init
. . | |                                    action a:T
. . | |                                     precondition a(v) is
```

```
. . | |                                      P)))))))))
. . | |                                (<kind(a(i;t)),l>)))
. . | |      else nil fi)
. . | |   & (∀x:Id.
. . | |      ¬(deq-member(IdDeq;x;1of(1of(2of(2of(2of(2of(2of(2of(
. . | |                                    (with ds: ds
. . | |                                     init: init
. . | |                                    action a:T
. . | |                                     precondition a(v) is
. . | |                                     P)))))))))
. . | |        ⇒
. . | |        deq-member(KindDeq;kind(a(i;t));2of(
. . | |                                        1of(
. . | |                                        2of(2of(2of(2of(2of(
. . | |                                        2of((with ds: ds
. . | |                                         init: init
. . | |                                        action a:T
. . | |                                         precondition a(v) is
. . | |                                         P)))))))))
. . | |                                        (x)))
. . | |      ⇒
. . | |      s(i;t).x = s(i;t+1).x)
. . | |   & (∀l:IdLnk, tg:Id.
. . | |      ¬(deq-member(product-deq(IdLnk;Id;IdLnkDeq;...);...;...)
. . | |        ⇒
. . | |        deq-member(KindDeq;kind(a(i;t));2of(
. . | |                                        1of(
. . | |                                        2of(2of(2of(2of(2of(
. . | |                                        2of(2of((with ds: ds
. . | |                                         init: init
. . | |                                        action a:T
. . | |                                         precondition a(v) is
. . | |                                         P)))))))))))
. . | |                                        (<l,tg>)))
. . | |      ⇒
. . | |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . | 17. ∀x:Id.
. . | |   deq-member(IdDeq;x;1of(1of(2of(2of((with ds: ds
. . | |                                  init: init
. . | |                                 action a:T
. . | |                                  precondition a(v) is
. . | |                                  P))))))
. . | |   ⇒
. . | |   s(i;0).x
. . | |   =
. . | |   2of(1of(2of(2of((with ds: ds
. . | |            init: init
. . | |           action a:T
. . | |            precondition a(v) is
. . | |            P)))))
. . | |   (x)
. . | 18. ∀a@0:Action(i).
. . | |   ¬isnull(a@0)
. . | |   ⇒
. . | |   (valtype(i;a@0) ⊆r 1of(2of((with ds: ds
```

```
. . | |                          init: init
. . | |                         action a:T
. . | |                          precondition a(v) is
. . | |                          P)))(kind(a@0))?Top)
. . | 19. ∀x:Id.
. . | |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(1of((with ds: ds
. . | |                                          init: init
. . | |                                         action a:T
. . | |                                          precondition a(v) is
. . | |                                          P))))→
. . | |                      2of(1of((with ds: ds
. . | |                           init: init
. . | |                          action a:T
. . | |                           precondition a(v) is
. . | |                           P)))
. . | |                      (x)
. . | |                    else Top fi
. . | 20. (λx.init(x)?⋅) ∈ State(ds)
. . | 21. t' : ℕ
. . | 22. 0≤t'
. . | 23. ¬locl(a) ∈ dom(1of(2of((with ds: ds
. . | |                        init: init
. . | |                       action a:T
. . | |                        precondition a(v) is
. . | |                        P))))
. . | ⊢  ∃e:E. loc(e) = i
. . | | by Repeat
. . | |    (Unfolds
. . | |     [‘fpf-single‘;‘fpf-dom‘;‘ma-single-pre-init‘;‘mk-ma‘]
. . | |     -1
. . | |     THEN
. . | |     Reduce -1)
. . | |    THEN
. . | |    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. init : x:Id fp-> ds(x)?Void
. . | | 7. ∀x:Id. x ∈ dom(ds) ⇒ x ∈ dom(init)
. . | | 8. v : T
. . | | 9. P((λx.init(x)?⋅),v)
. . | | 10. w : World
. . | | 11. FairFifo
. . | | 12. FairFifo
. . | | 13. ∀l:IdLnk, tg:Id.
. . | |     (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . | |                        (with ds: ds
. . | |                         init: init
. . | |                        action a:T
. . | |                         precondition a(v) is
```

```
. . | |                        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(1of(2of((with ds: ds
. . | |                                 init: init
. . | |                                action a:T
. . | |                                 precondition a(v) is
. . | |                                 P))))
. . | |       ∨ P@0 != 1of(
. . | |                 2of(2of(2of((with ds: ds
. . | |                  init: init
. . | |                 action a:T
. . | |                  precondition a(v) is
. . | |                  P)))))(a@0) ==> ∀v:1of(2of((with ds: ds
. . | |                                          init: init
. . | |                                         action a:T
. . | |                                          precondition a(v) is
. . | |                                          P)))(locl(a@0))?Top.
. . | |         ¬P@0((λx.s(i;t').x),v)
. . | | 16. ∀t:ℕ.
. . | |     ¬isnull(a(i;t))
. . | |     ⇒
. . | |     (islocal(kind(a(i;t)))
. . | |      ⇒
. . | |      deq-member(IdDeq;act(kind(a(i;t)));1of(1of(
. . | |                                          2of(2of(2of(
. . | |                                          (with ds: ds
. . | |                                           init: init
. . | |                                          action a:T
. . | |                                           precondition a(v) is
. . | |                                           P)))))))
. . | |      ⇒
. . | |      2of(1of(2of(2of(2of((with ds: ds
. . | |                 init: init
. . | |                action a:T
. . | |                 precondition a(v) is
. . | |                 P))))))
. . | |      (act(kind(a(i;t)))
. . | |      ,λx.s(i;t).x
. . | |      ,val(a(i;t))))
. . | |     & (∀x:Id.
. . | |        deq-member(product-deq(Knd;Id;KindDeq;IdDeq);<kind(...)
. . | |                                                     ,x>;...)
. . | |        ⇒
. . | |        s(i;t+1).x
. . | |        =
. . | |        2of(1of(2of(2of(2of(2of((with ds: ds
. . | |                  init: init
. . | |                 action a:T
. . | |                  precondition a(v) is
. . | |                  P)))))))
```

```
. . | |        (<kind(a(i;t)),x>
. . | |        ,λx.s(i;t).x
. . | |        ,val(a(i;t))))
. . | |     & (∀l:IdLnk.
. . | |        deq-member(product-deq(Knd;IdLnk;KindDeq;...);<...
. . | |                                                    ,l>;...)
. . | |        ⇒
. . | |        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(1of(2of(2of(2of(2of(2of(
. . | |                                    (with ds: ds
. . | |                                     init: init
. . | |                                    action a:T
. . | |                                     precondition a(v) is
. . | |                                     P)))))))))
. . | |                               (<kind(a(i;t)),l>)))
. . | |        else nil fi)
. . | |     & (∀x:Id.
. . | |        ¬(deq-member(IdDeq;x;1of(1of(2of(2of(2of(2of(2of(2of(
. . | |                                    (with ds: ds
. . | |                                     init: init
. . | |                                    action a:T
. . | |                                     precondition a(v) is
. . | |                                     P)))))))))))
. . | |          ⇒
. . | |          deq-member(KindDeq;kind(a(i;t));2of(
. . | |                                         1of(
. . | |                                         2of(2of(2of(2of(2of(
. . | |                                         2of((with ds: ds
. . | |                                          init: init
. . | |                                         action a:T
. . | |                                          precondition a(v) is
. . | |                                          P)))))))))
. . | |                                         (x)))
. . | |        ⇒
. . | |        s(i;t).x = s(i;t+1).x)
. . | |     & (∀l:IdLnk, tg:Id.
. . | |        ¬(deq-member(product-deq(IdLnk;Id;...;IdDeq);...;...)
. . | |          ⇒
. . | |          deq-member(KindDeq;kind(a(i;t));2of(
. . | |                                         1of(
. . | |                                         2of(2of(2of(2of(2of(
. . | |                                         2of(2of((with ds: ds
. . | |                                          init: init
. . | |                                         action a:T
. . | |                                          precondition a(v) is
. . | |                                          P)))))))))))
. . | |                                         (<l,tg>)))
. . | |        ⇒
. . | |        w-tagged(tg; onlnk(l;m(i;t))) = nil)
```

```
. . | | 17. ∀x:Id.
. . | |     deq-member(IdDeq;x;1of(1of(2of(2of((with ds: ds
. . | |                                  init: init
. . | |                                 action a:T
. . | |                                  precondition a(v) is
. . | |                                  P))))))
. . | |     ⇒
. . | |     s(i;0).x
. . | |     =
. . | |     2of(1of(2of(2of((with ds: ds
. . | |              init: init
. . | |             action a:T
. . | |              precondition a(v) is
. . | |              P)))))
. . | |     (x)
. . | | 18. ∀a@0:Action(i).
. . | |     ¬isnull(a@0)
. . | |     ⇒
. . | |     (valtype(i;a@0) ⊆r 1of(2of((with ds: ds
. . | |                               init: init
. . | |                              action a:T
. . | |                               precondition a(v) is
. . | |                               P)))(kind(a@0))?Top)
. . | | 19. ∀x:Id.
. . | |     vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(1of(...)))→
. . | |                         2of(1of((with ds: ds
. . | |                              init: init
. . | |                             action a:T
. . | |                              precondition a(v) is
. . | |                              P)))
. . | |                        (x)
. . | |                       else Top fi
. . | | 20. (λx.init(x)?•) ∈ State(ds)
. . | | 21. t' : ℕ
. . | | 22. 0≤t'
. . | | 23. ¬(eqof(KindDeq)(locl(a),locl(a)) ∨₂ false₂)
. . | | ⊢  IdDeq ∈ EqDecider(Id)
. . | |   by SubsumeC EqDecider(Id)
. . | |      THEN
. . | |      Try
. . | |      (BackThru
. . | |       Thm* strong-subtype(A;B)
. . | |            ⇒
. . | |            (EqDecider(B) ⊆r EqDecider(A))
. . | |       {strong_DASH_subtype_DASH_deq_DASH_subtype}
. . | |       THEN
. . | |       All (Unfold `dstype`)
. . | |       THEN
. . | |       All Reduce
. . | |       THEN
. . | |       Trivial)
. . | |      THEN
. . | |      AllHyps
. . | |      (λi.Unfold_Wld i THEN Reduce 0 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. init : x:Id fp-> ds(x)?Void
. . | . 7. ∀x:Id. x ∈ dom(ds) ⇒ x ∈ dom(init)
. . | . 8. v : T
. . | . 9. P((λx.init(x)?•),v)
. . | . 10. w : World
. . | . 11. FairFifo
. . | . 12. FairFifo
. . | . 13. ∀l:IdLnk, tg:Id.
. . | .     (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . | .                       (with ds: ds
. . | .                        init: init
. . | .                       action a:T
. . | .                        precondition a(v) is
. . | .                        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(1of(2of((with ds: ds
. . | .                                   init: init
. . | .                                  action a:T
. . | .                                   precondition a(v) is
. . | .                                   P))))
. . | .       ∨ P@0 != 1of(
. . | .                 2of(2of(2of((with ds: ds
. . | .                  init: init
. . | .                 action a:T
. . | .                  precondition a(v) is
. . | .                  P)))))(a@0) ==> ∀v:1of(2of((with ds: ds
. . | .                                             init: init
. . | .                                            action a:T
. . | .                                             precondition a(v) is
. . | .                                             P)))(locl(a@0))?Top.
. . | .         ¬P@0((λx.s(i;t').x),v)
. . | . 16. ∀t:ℕ.
. . | .     ¬isnull(a(i;t))
. . | .     ⇒
. . | .     (islocal(kind(a(i;t)))
. . | .      ⇒
. . | .      deq-member(IdDeq;act(kind(a(i;t)));1of(1of(
. . | .                                             2of(2of(2of(
. . | .                                             (with ds: ds
. . | .                                              init: init
. . | .                                             action a:T
. . | .                                              precondition a(v) is
. . | .                                              P)))))))
. . | .      ⇒
```

```
. . | .      2of(1of(2of(2of(2of((with ds: ds
. . | .               init: init
. . | .              action a:T
. . | .               precondition a(v) is
. . | .               P))))))
. . | .      (act(kind(a(i;t)))
. . | .      ,λx.s(i;t).x
. . | .      ,val(a(i;t))))
. . | .     & (∀x:Id.
. . | .        deq-member(product-deq(Knd;Id;KindDeq;IdDeq);<kind(...)
. . | .                                                    ,x>;...)
. . | .        ⇒
. . | .        s(i;t+1).x
. . | .        =
. . | .        2of(1of(2of(2of(2of(2of((with ds: ds
. . | .                 init: init
. . | .                action a:T
. . | .                 precondition a(v) is
. . | .                 P)))))))
. . | .        (<kind(a(i;t)),x>
. . | .        ,λx.s(i;t).x
. . | .        ,val(a(i;t))))
. . | .     & (∀l:IdLnk.
. . | .        deq-member(product-deq(Knd;IdLnk;KindDeq;...);<...
. . | .                                                     ,l>;...)
. . | .        ⇒
. . | .        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(1of(2of(2of(2of(2of(2of(
. . | .                                    (with ds: ds
. . | .                                     init: init
. . | .                                    action a:T
. . | .                                     precondition a(v) is
. . | .                                     P)))))))
. . | .                               (<kind(a(i;t)),l>)))
. . | .        else nil fi)
. . | .     & (∀x:Id.
. . | .        ¬(deq-member(IdDeq;x;1of(1of(2of(2of(2of(2of(2of(2of(
. . | .                                       (with ds: ds
. . | .                                        init: init
. . | .                                       action a:T
. . | .                                        precondition a(v) is
. . | .                                        P)))))))))
. . | .          ⇒
. . | .          deq-member(KindDeq;kind(a(i;t));2of(
. . | .                                            1of(
. . | .                                            2of(2of(2of(2of(2of(
. . | .                                            2of((with ds: ds
. . | .                                             init: init
. . | .                                            action a:T
```

```
. . | .                                          precondition a(v) is
. . | .                                          P)))))))))
. . | .                                         (x)))
. . | .        ⇒
. . | .        s(i;t).x = s(i;t+1).x)
. . | .     & (∀l:IdLnk, tg:Id.
. . | .        ¬(deq-member(product-deq(IdLnk;Id;...;IdDeq);...;...)
. . | .          ⇒
. . | .          deq-member(KindDeq;kind(a(i;t));2of(
. . | .                                          1of(
. . | .                                          2of(2of(2of(2of(2of(
. . | .                                          2of(2of((with ds: ds
. . | .                                           init: init
. . | .                                          action a:T
. . | .                                           precondition a(v) is
. . | .                                           P))))))))))
. . | .                                          (<l,tg>)))
. . | .        ⇒
. . | .        w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . | . 17. ∀x:Id.
. . | .     deq-member(IdDeq;x;1of(1of(2of(2of((with ds: ds
. . | .                                  init: init
. . | .                                 action a:T
. . | .                                  precondition a(v) is
. . | .                                  P))))))
. . | .     ⇒
. . | .     s(i;0).x
. . | .     =
. . | .     2of(1of(2of(2of((with ds: ds
. . | .              init: init
. . | .             action a:T
. . | .              precondition a(v) is
. . | .              P)))))
. . | .     (x)
. . | . 18. ∀a@0:Action(i).
. . | .     ¬isnull(a@0)
. . | .     ⇒
. . | .     (valtype(i;a@0) ⊆r 1of(2of((with ds: ds
. . | .                               init: init
. . | .                              action a:T
. . | .                               precondition a(v) is
. . | .                               P)))(kind(a@0))?Top)
. . | . 19. ∀x:Id.
. . | .     vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(1of(...)))→
. . | .                          2of(1of((with ds: ds
. . | .                               init: init
. . | .                              action a:T
. . | .                               precondition a(v) is
. . | .                               P)))
. . | .                         (x)
. . | .                       else Top fi
. . | . 20. (λx.init(x)?•) ∈ State(ds)
. . | . 21. t' : ℕ
. . | . 22. 0≤t'
. . | . 23. ¬(eqof(KindDeq)(locl(a),locl(a)) ∨₂ false₂)
```

```
. . | . 24. IdDeq ∈ EqDecider(Id)
. . | . ⊢  ∃e:E. loc(e) = i
. . | .   by RWO
. . | .      Thm* ∀d:EqDecider(A), i:A. (eqof(d)(i,i)) ∼ true₂
. . | .      {eqof_eq_btrue}
. . | .      -2
. . | .      THEN
. . | .      Reduce -2
. . | .      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. init : x:Id fp-> ds(x)?Void
. . . 7. ∀x:Id. x ∈ dom(ds) ⇒ x ∈ dom(init)
. . . 8. v : T
. . . 9. P((λx.init(x)?•),v)
. . . 10. w : World
. . . 11. FairFifo
. . . 12. FairFifo
. . . 13. ∀l:IdLnk, tg:Id.
. . . |   (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . |                     (with ds: ds
. . . |                      init: init
. . . |                     action a:T
. . . |                      precondition a(v) is
. . . |                      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(1of(2of((with ds: ds
. . . |                              init: init
. . . |                             action a:T
. . . |                              precondition a(v) is
. . . |                              P))))
. . . |     ∨ P@0 != 1of(2of(2of(2of((with ds: ds
. . . |                    init: init
. . . |                   action a:T
. . . |                    precondition a(v) is
. . . |                    P)))))(a@0) ==> ∀v:1of(2of((with ds: ds
. . . |                                             init: init
. . . |                                            action a:T
. . . |                                             precondition a(v) is
. . . |                                             P)))(locl(a@0))?Top.
. . . |       ¬P@0((λx.s(i;t').x),v)
. . . 16. ∀t:ℕ.
. . . |   ¬isnull(a(i;t))
. . . |   ⇒
```

```
. . . |   (islocal(kind(a(i;t)))
. . . |    ⇒
. . . |    deq-member(IdDeq;act(kind(a(i;t)));1of(1of(
. . . |                                      2of(2of(2of((with ds: ds
. . . |                                       init: init
. . . |                                      action a:T
. . . |                                       precondition a(v) is
. . . |                                       P)))))))
. . . |    ⇒
. . . |    2of(1of(2of(2of(2of((with ds: ds
. . . |             init: init
. . . |            action a:T
. . . |             precondition a(v) is
. . . |             P))))))
. . . |    (act(kind(a(i;t)))
. . . |    ,λx.s(i;t).x
. . . |    ,val(a(i;t))))
. . . |   & (∀x:Id.
. . . |      deq-member(product-deq(Knd;Id;KindDeq;IdDeq);<kind(...)
. . . |                                                    ,x>;...)
. . . |      ⇒
. . . |      s(i;t+1).x
. . . |      =
. . . |      2of(1of(2of(2of(2of(2of((with ds: ds
. . . |               init: init
. . . |              action a:T
. . . |               precondition a(v) is
. . . |               P)))))))
. . . |      (<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>;...)
. . . |      ⇒
. . . |      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(1of(2of(2of(2of(2of(2of(
. . . |                                    (with ds: ds
. . . |                                     init: init
. . . |                                    action a:T
. . . |                                     precondition a(v) is
. . . |                                     P)))))))
. . . |                              (<kind(a(i;t)),l>)))
. . . |      else nil fi)
. . . |   & (∀x:Id.
. . . |      ¬(deq-member(IdDeq;x;1of(1of(2of(2of(2of(2of(2of(2of(
. . . |                                    (with ds: ds
. . . |                                     init: init
. . . |                                    action a:T
```

```
. . . |                                    precondition a(v) is
. . . |                                    P))))))))))
. . . |        ⇒
. . . |        deq-member(KindDeq;kind(a(i;t));2of(
. . . |                                     1of(
. . . |                                     2of(2of(2of(2of(2of(
. . . |                                     2of((with ds: ds
. . . |                                      init: init
. . . |                                     action a:T
. . . |                                      precondition a(v) is
. . . |                                      P)))))))))
. . . |                                     (x)))
. . . |      ⇒
. . . |      s(i;t).x = s(i;t+1).x)
. . . |   & (∀l:IdLnk, tg:Id.
. . . |      ¬(deq-member(product-deq(IdLnk;Id;IdLnkDeq;...);...;...)
. . . |        ⇒
. . . |        deq-member(KindDeq;kind(a(i;t));2of(
. . . |                                     1of(
. . . |                                     2of(2of(2of(2of(2of(
. . . |                                     2of(2of((with ds: ds
. . . |                                      init: init
. . . |                                     action a:T
. . . |                                      precondition a(v) is
. . . |                                      P))))))))))
. . . |                                     (<l,tg>)))
. . . |      ⇒
. . . |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . 17. ∀x:Id.
. . . |   deq-member(IdDeq;x;1of(1of(2of(2of((with ds: ds
. . . |                              init: init
. . . |                             action a:T
. . . |                              precondition a(v) is
. . . |                              P))))))
. . . |   ⇒
. . . |   s(i;0).x
. . . |   =
. . . |   2of(1of(2of(2of((with ds: ds
. . . |            init: init
. . . |           action a:T
. . . |            precondition a(v) is
. . . |            P)))))
. . . |   (x)
. . . 18. ∀a@0:Action(i).
. . . |   ¬isnull(a@0)
. . . |   ⇒
. . . |   (valtype(i;a@0) ⊆r 1of(2of((with ds: ds
. . . |                           init: init
. . . |                          action a:T
. . . |                           precondition a(v) is
. . . |                           P)))(kind(a@0))?Top)
. . . 19. ∀x:Id.
. . . |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(1of((with ds: ds
. . . |                                              init: init
. . . |                                             action a:T
```

```
. . . |                                          precondition a(v) is
. . . |                                          P))))→
. . . |                     2of(1of((with ds: ds
. . . |                          init: init
. . . |                         action a:T
. . . |                          precondition a(v) is
. . . |                          P)))
. . . |                     (x)
. . . |                   else Top fi
. . . 20. (λx.init(x)?•) ∈ State(ds)
. . . 21. t' : ℕ
. . . 22. 0≤t'
. . . 23. P@0 != 1of(2of(2of(2of((with ds: ds
. . . |              init: init
. . . |             action a:T
. . . |              precondition a(v) is
. . . |              P)))))(a) ==> ∀v:1of(2of((with ds: ds
. . . |                                    init: init
. . . |                                   action a:T
. . . |                                    precondition a(v) is
. . . |                                    P)))(locl(a@0))?Top.
. . . |   ¬P@0((λx.s(i;t').x),v)
. . . ⊢  ∃e:E. loc(e) = i
. . . | by Repeat
. . . |    (Unfolds [‘ma-single-pre-init‘;‘mk-ma‘;‘fpf-single‘] -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. init : x:Id fp-> ds(x)?Void
. . . 7. ∀x:Id. x ∈ dom(ds) ⇒ x ∈ dom(init)
. . . 8. v : T
. . . 9. P((λx.init(x)?•),v)
. . . 10. w : World
. . . 11. FairFifo
. . . 12. FairFifo
. . . 13. ∀l:IdLnk, tg:Id.
. . . |   (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . |                     (with ds: ds
. . . |                      init: init
. . . |                     action a:T
. . . |                      precondition a(v) is
. . . |                      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(1of(2of((with ds: ds
. . . |                              init: init
```

```
. . . |                            action a:T
. . . |                             precondition a(v) is
. . . |                             P))))
. . . |     ∨ P@0 != 1of(2of(2of(2of((with ds: ds
. . . |                    init: init
. . . |                   action a:T
. . . |                    precondition a(v) is
. . . |                    P)))))(a@0) ==> ∀v:1of(2of((with ds: ds
. . . |                                             init: init
. . . |                                            action a:T
. . . |                                             precondition a(v) is
. . . |                                             P)))(locl(a@0))?Top.
. . . |       ¬P@0((λx.s(i;t').x),v)
. . . 16. ∀t:ℕ.
. . . |   ¬isnull(a(i;t))
. . . |   ⇒
. . . |   (islocal(kind(a(i;t)))
. . . |    ⇒
. . . |    deq-member(IdDeq;act(kind(a(i;t)));1of(1of(
. . . |                                         2of(2of(2of((with ds: ds
. . . |                                          init: init
. . . |                                         action a:T
. . . |                                          precondition a(v) is
. . . |                                          P)))))))
. . . |    ⇒
. . . |    2of(1of(2of(2of(2of((with ds: ds
. . . |              init: init
. . . |             action a:T
. . . |              precondition a(v) is
. . . |              P))))))
. . . |    (act(kind(a(i;t)))
. . . |    ,λx.s(i;t).x
. . . |    ,val(a(i;t))))
. . . |   & (∀x:Id.
. . . |      deq-member(product-deq(Knd;Id;KindDeq;IdDeq);<kind(...)
. . . |                                                    ,x>;...)
. . . |      ⇒
. . . |      s(i;t+1).x
. . . |      =
. . . |      2of(1of(2of(2of(2of(2of((with ds: ds
. . . |                 init: init
. . . |                action a:T
. . . |                 precondition a(v) is
. . . |                 P)))))))
. . . |      (<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>;...)
. . . |      ⇒
. . . |      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(1of(2of(2of(2of(2of(2of(
. . . |                                    (with ds: ds
. . . |                                     init: init
. . . |                                    action a:T
. . . |                                     precondition a(v) is
. . . |                                     P)))))))
. . . |                               (<kind(a(i;t)),1>)))
. . . |       else nil fi)
. . . |    & (∀x:Id.
. . . |       ¬(deq-member(IdDeq;x;1of(1of(2of(2of(2of(2of(2of(2of(
. . . |                                    (with ds: ds
. . . |                                     init: init
. . . |                                    action a:T
. . . |                                     precondition a(v) is
. . . |                                     P)))))))))
. . . |         ⇒
. . . |         deq-member(KindDeq;kind(a(i;t));2of(
. . . |                                        1of(
. . . |                                        2of(2of(2of(2of(2of(
. . . |                                        2of((with ds: ds
. . . |                                         init: init
. . . |                                        action a:T
. . . |                                         precondition a(v) is
. . . |                                         P)))))))))
. . . |                                        (x)))
. . . |       ⇒
. . . |       s(i;t).x = s(i;t+1).x)
. . . |    & (∀l:IdLnk, tg:Id.
. . . |       ¬(deq-member(product-deq(IdLnk;Id;IdLnkDeq;...);...;...)
. . . |         ⇒
. . . |         deq-member(KindDeq;kind(a(i;t));2of(
. . . |                                        1of(
. . . |                                        2of(2of(2of(2of(2of(
. . . |                                        2of(2of((with ds: ds
. . . |                                         init: init
. . . |                                        action a:T
. . . |                                         precondition a(v) is
. . . |                                         P)))))))))
. . . |                                        (<l,tg>)))
. . . |       ⇒
. . . |       w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . 17. ∀x:Id.
. . . |    deq-member(IdDeq;x;1of(1of(2of(2of((with ds: ds
. . . |                                 init: init
. . . |                                action a:T
. . . |                                 precondition a(v) is
. . . |                                 P))))))
. . . |    ⇒
. . . |    s(i;0).x
. . . |    =
. . . |    2of(1of(2of(2of((with ds: ds
. . . |              init: init
```

```
. . . |           action a:T
. . . |            precondition a(v) is
. . . |            P)))))
. . . |   (x)
. . . 18. ∀a@0:Action(i).
. . . |   ¬isnull(a@0)
. . . |   ⇒
. . . |   (valtype(i;a@0) ⊆r 1of(2of((with ds: ds
. . . |                              init: init
. . . |                             action a:T
. . . |                              precondition a(v) is
. . . |                              P)))(kind(a@0))?Top)
. . . 19. ∀x:Id.
. . . |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(1of((with ds: ds
. . . |                                                 init: init
. . . |                                                action a:T
. . . |                                                 precondition a(v) is
. . . |                                                 P))))→
. . . |                      2of(1of((with ds: ds
. . . |                           init: init
. . . |                          action a:T
. . . |                           precondition a(v) is
. . . |                           P)))
. . . |                     (x)
. . . |                  else Top fi
. . . 20. (λx.init(x)?•) ∈ State(ds)
. . . 21. t' : ℕ
. . . 22. 0≤t'
. . . 23. 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. loc(e) = i
. . . | by Decide (∃t:ℕt'. ¬isnull(a(i;t)))
. . . |    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. init : x:Id fp-> ds(x)?Void
. . . | 7. ∀x:Id. x ∈ dom(ds) ⇒ x ∈ dom(init)
. . . | 8. v : T
. . . | 9. P((λx.init(x)?•),v)
. . . | 10. w : World
. . . | 11. FairFifo
. . . | 12. FairFifo
. . . | 13. ∀l:IdLnk, tg:Id.
. . . | |   (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . | |                     (with ds: ds
. . . | |                      init: init
. . . | |                     action a:T
. . . | |                      precondition a(v) is
. . . | |                      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(1of(2of((with ds: ds
. . . | |                               init: init
. . . | |                              action a:T
. . . | |                               precondition a(v) is
. . . | |                               P))))
. . . | |     ∨ P@0 != 1of(
. . . | |              2of(2of(2of((with ds: ds
. . . | |               init: init
. . . | |              action a:T
. . . | |               precondition a(v) is
. . . | |               P)))))(a@0) ==> ∀v:1of(2of((with ds: ds
. . . | |                                        init: init
. . . | |                                       action a:T
. . . | |                                        precondition a(v) is
. . . | |                                        P)))(locl(a@0))?Top.
. . . | |       ¬P@0((λx.s(i;t').x),v)
. . . | 16. ∀t:ℕ.
. . . | |   ¬isnull(a(i;t))
. . . | |   ⇒
. . . | |   (islocal(kind(a(i;t)))
. . . | |    ⇒
. . . | |    deq-member(IdDeq;act(kind(a(i;t)));1of(1of(
. . . | |                                        2of(2of(2of(
. . . | |                                        (with ds: ds
. . . | |                                         init: init
. . . | |                                        action a:T
. . . | |                                         precondition a(v) is
. . . | |                                         P)))))))
. . . | |    ⇒
. . . | |    2of(1of(2of(2of(2of((with ds: ds
. . . | |              init: init
. . . | |             action a:T
. . . | |              precondition a(v) is
. . . | |              P))))))
. . . | |    (act(kind(a(i;t)))
. . . | |    ,λx.s(i;t).x
. . . | |    ,val(a(i;t))))
. . . | |   & (∀x:Id.
. . . | |      deq-member(product-deq(Knd;Id;KindDeq;IdDeq);<kind(...)
. . . | |                                                   ,x>;...)
. . . | |      ⇒
. . . | |      s(i;t+1).x
. . . | |      =
. . . | |      2of(1of(2of(2of(2of(2of((with ds: ds
. . . | |               init: init
. . . | |              action a:T
. . . | |               precondition a(v) is
. . . | |               P)))))))
. . . | |      (<kind(a(i;t)),x>
```

```
. . . | |      ,λx.s(i;t).x
. . . | |      ,val(a(i;t))))
. . . | |   & (∀l:IdLnk.
. . . | |      deq-member(product-deq(Knd;IdLnk;KindDeq;...);<...
. . . | |                                                    ,l>;...)
. . . | |      ⇒
. . . | |      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(1of(2of(2of(2of(2of(2of(
. . . | |                                  (with ds: ds
. . . | |                                   init: init
. . . | |                                  action a:T
. . . | |                                   precondition a(v) is
. . . | |                                   P)))))))
. . . | |                            (<kind(a(i;t)),l>)))
. . . | |      else nil fi)
. . . | |   & (∀x:Id.
. . . | |      ¬(deq-member(IdDeq;x;1of(1of(2of(2of(2of(2of(2of(2of(
. . . | |                                  (with ds: ds
. . . | |                                   init: init
. . . | |                                  action a:T
. . . | |                                   precondition a(v) is
. . . | |                                   P)))))))))
. . . | |        ⇒
. . . | |        deq-member(KindDeq;kind(a(i;t));2of(
. . . | |                                      1of(
. . . | |                                      2of(2of(2of(2of(2of(
. . . | |                                      2of((with ds: ds
. . . | |                                       init: init
. . . | |                                      action a:T
. . . | |                                       precondition a(v) is
. . . | |                                       P)))))))))
. . . | |                                      (x)))
. . . | |      ⇒
. . . | |      s(i;t).x = s(i;t+1).x)
. . . | |   & (∀l:IdLnk, tg:Id.
. . . | |      ¬(deq-member(product-deq(IdLnk;Id;...;IdDeq);...;...)
. . . | |        ⇒
. . . | |        deq-member(KindDeq;kind(a(i;t));2of(
. . . | |                                      1of(
. . . | |                                      2of(2of(2of(2of(2of(
. . . | |                                      2of(2of((with ds: ds
. . . | |                                       init: init
. . . | |                                      action a:T
. . . | |                                       precondition a(v) is
. . . | |                                       P)))))))))
. . . | |                                      (<l,tg>)))
. . . | |      ⇒
. . . | |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . | 17. ∀x:Id.
```

```
. . . | |   deq-member(IdDeq;x;1of(1of(2of(2of((with ds: ds
. . . | |                                 init: init
. . . | |                                action a:T
. . . | |                                 precondition a(v) is
. . . | |                                 P))))))
. . . | |   ⇒
. . . | |   s(i;0).x
. . . | |   =
. . . | |   2of(1of(2of(2of((with ds: ds
. . . | |            init: init
. . . | |           action a:T
. . . | |            precondition a(v) is
. . . | |            P)))))
. . . | |   (x)
. . . | 18. ∀a@0:Action(i).
. . . | |   ¬isnull(a@0)
. . . | |   ⇒
. . . | |   (valtype(i;a@0) ⊆r 1of(2of((with ds: ds
. . . | |                            init: init
. . . | |                           action a:T
. . . | |                            precondition a(v) is
. . . | |                            P)))(kind(a@0))?Top)
. . . | 19. ∀x:Id.
. . . | |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(1of(...)))→
. . . | |                       2of(1of((with ds: ds
. . . | |                            init: init
. . . | |                           action a:T
. . . | |                            precondition a(v) is
. . . | |                            P)))
. . . | |                      (x)
. . . | |                  else Top fi
. . . | 20. (λx.init(x)?•) ∈ State(ds)
. . . | 21. t' : ℕ
. . . | 22. 0≤t'
. . . | 23. P@0 != <[a],λx.P>(a) ==> ∀v:<[locl(a)]
. . . | |                                ,λx.T>(locl(a@0))?Top.
. . . | |   ¬P@0((λx.s(i;t').x),v)
. . . | 24. ∃t:ℕt'. ¬isnull(a(i;t))
. . . | ⊢  ∃e:E. loc(e) = i  by ExRepD
. . . | |
. . . | 1. i : Id
. . . | 2. a : Id
. . . | 3. T : Type
. . . | 4. ds : x:Id fp-> Type
. . . | 5. P : State(ds)→T→Prop
. . . | 6. init : x:Id fp-> ds(x)?Void
. . . | 7. ∀x:Id. x ∈ dom(ds) ⇒ x ∈ dom(init)
. . . | 8. v : T
. . . | 9. P((λx.init(x)?•),v)
. . . | 10. w : World
. . . | 11. FairFifo
. . . | 12. FairFifo
. . . | 13. ∀l:IdLnk, tg:Id.
. . . | |   (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . | |                     (with ds: ds
```

```
. . . | |                      init: init
. . . | |                     action a:T
. . . | |                      precondition a(v) is
. . . | |                      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(1of(2of((with ds: ds
. . . | |                              init: init
. . . | |                             action a:T
. . . | |                              precondition a(v) is
. . . | |                              P))))
. . . | |     ∨ P@0 != 1of(
. . . | |              2of(2of(2of((with ds: ds
. . . | |               init: init
. . . | |              action a:T
. . . | |               precondition a(v) is
. . . | |               P)))))(a@0) ==> ∀v:1of(2of((with ds: ds
. . . | |                                        init: init
. . . | |                                       action a:T
. . . | |                                        precondition a(v) is
. . . | |                                        P)))(locl(a@0))?Top.
. . . | |       ¬P@0((λx.s(i;t').x),v)
. . . | 16. ∀t:ℕ.
. . . | |   ¬isnull(a(i;t))
. . . | |   ⇒
. . . | |   (islocal(kind(a(i;t)))
. . . | |    ⇒
. . . | |    deq-member(IdDeq;act(kind(a(i;t)));1of(1of(
. . . | |                                        2of(2of(2of(
. . . | |                                        (with ds: ds
. . . | |                                         init: init
. . . | |                                        action a:T
. . . | |                                         precondition a(v) is
. . . | |                                         P)))))))
. . . | |    ⇒
. . . | |    2of(1of(2of(2of(2of((with ds: ds
. . . | |              init: init
. . . | |             action a:T
. . . | |              precondition a(v) is
. . . | |              P))))))
. . . | |    (act(kind(a(i;t)))
. . . | |    ,λx.s(i;t).x
. . . | |    ,val(a(i;t))))
. . . | |   & (∀x:Id.
. . . | |      deq-member(product-deq(Knd;Id;KindDeq;IdDeq);<kind(...)
. . . | |                                                   ,x>;...)
. . . | |      ⇒
. . . | |      s(i;t+1).x
. . . | |      =
. . . | |      2of(1of(2of(2of(2of(2of((with ds: ds
. . . | |               init: init
```

```
. . . | |              action a:T
. . . | |               precondition a(v) is
. . . | |               P)))))))
. . . | |      (<kind(a(i;t)),x>
. . . | |      ,λx.s(i;t).x
. . . | |      ,val(a(i;t))))
. . . | |   & (∀l:IdLnk.
. . . | |      deq-member(product-deq(Knd;IdLnk;KindDeq;...);<...
. . . | |                                                  ,l>;...)
. . . | |      ⇒
. . . | |      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(1of(2of(2of(2of(2of(2of(
. . . | |                                  (with ds: ds
. . . | |                                   init: init
. . . | |                                  action a:T
. . . | |                                   precondition a(v) is
. . . | |                                   P)))))))))
. . . | |                            (<kind(a(i;t)),l>)))
. . . | |      else nil fi)
. . . | |   & (∀x:Id.
. . . | |      ¬(deq-member(IdDeq;x;1of(1of(2of(2of(2of(2of(2of(2of(
. . . | |                                  (with ds: ds
. . . | |                                   init: init
. . . | |                                  action a:T
. . . | |                                   precondition a(v) is
. . . | |                                   P)))))))))))
. . . | |        ⇒
. . . | |        deq-member(KindDeq;kind(a(i;t));2of(
. . . | |                                     1of(
. . . | |                                     2of(2of(2of(2of(2of(
. . . | |                                     2of((with ds: ds
. . . | |                                      init: init
. . . | |                                     action a:T
. . . | |                                      precondition a(v) is
. . . | |                                      P)))))))))
. . . | |                                     (x)))
. . . | |      ⇒
. . . | |      s(i;t).x = s(i;t+1).x)
. . . | |   & (∀l:IdLnk, tg:Id.
. . . | |      ¬(deq-member(product-deq(IdLnk;Id;...;IdDeq);...;...)
. . . | |        ⇒
. . . | |        deq-member(KindDeq;kind(a(i;t));2of(
. . . | |                                     1of(
. . . | |                                     2of(2of(2of(2of(2of(
. . . | |                                     2of(2of((with ds: ds
. . . | |                                      init: init
. . . | |                                     action a:T
. . . | |                                      precondition a(v) is
. . . | |                                      P)))))))))))
```

```
. . . | |                                          (<l,tg>)))
. . . | |      ⇒
. . . | |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . | 17. ∀x:Id.
. . . | |   deq-member(IdDeq;x;1of(1of(2of(2of((with ds: ds
. . . | |                                 init: init
. . . | |                                action a:T
. . . | |                                 precondition a(v) is
. . . | |                                 P))))))
. . . | |   ⇒
. . . | |   s(i;0).x
. . . | |   =
. . . | |   2of(1of(2of(2of((with ds: ds
. . . | |            init: init
. . . | |           action a:T
. . . | |            precondition a(v) is
. . . | |            P)))))
. . . | |   (x)
. . . | 18. ∀a@0:Action(i).
. . . | |   ¬isnull(a@0)
. . . | |   ⇒
. . . | |   (valtype(i;a@0) ⊆r 1of(2of((with ds: ds
. . . | |                            init: init
. . . | |                           action a:T
. . . | |                            precondition a(v) is
. . . | |                            P)))(kind(a@0))?Top)
. . . | 19. ∀x:Id.
. . . | |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(1of(...)))→
. . . | |                       2of(1of((with ds: ds
. . . | |                            init: init
. . . | |                           action a:T
. . . | |                            precondition a(v) is
. . . | |                            P)))
. . . | |                      (x)
. . . | |                   else Top fi
. . . | 20. (λx.init(x)?⋅) ∈ State(ds)
. . . | 21. t' : ℕ
. . . | 22. 0≤t'
. . . | 23. P@0 != <[a],λx.P>(a) ==> ∀v:<[locl(a)]
. . . | |                                  ,λx.T>(locl(a@0))?Top.
. . . | |   ¬P@0((λx.s(i;t').x),v)
. . . | 24. t : ℕt'
. . . | 25. ¬isnull(a(i;t))
. . . | ⊢  ∃e:E. loc(e) = i  by 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. init : x:Id fp-> ds(x)?Void
. . . | | 7. ∀x:Id. x ∈ dom(ds) ⇒ x ∈ dom(init)
. . . | | 8. v : T
```

```
. . . | | 9. P((λx.init(x)?•),v)
. . . | | 10. w : World
. . . | | 11. FairFifo
. . . | | 12. FairFifo
. . . | | 13. ∀l:IdLnk, tg:Id.
. . . | |     (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . | |                        (with ds: ds
. . . | |                         init: init
. . . | |                        action a:T
. . . | |                         precondition a(v) is
. . . | |                         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(1of(2of((with ds: ds
. . . | |                                 init: init
. . . | |                                action a:T
. . . | |                                 precondition a(v) is
. . . | |                                 P))))
. . . | |       ∨ P@0 != 1of(
. . . | |                2of(2of(2of((with ds: ds
. . . | |                 init: init
. . . | |                action a:T
. . . | |                 precondition a(v) is
. . . | |                 P)))))(a@0) ==> ∀v:1of(2of((with ds: ds
. . . | |                                             init: init
. . . | |                                            action a:T
. . . | |                                             precondition a(v) is
. . . | |                                             P)))(locl(a@0))?Top.
. . . | |         ¬P@0((λx.s(i;t').x),v)
. . . | | 16. ∀t:ℕ.
. . . | |     ¬isnull(a(i;t))
. . . | |     ⇒
. . . | |     (islocal(kind(a(i;t)))
. . . | |      ⇒
. . . | |      deq-member(IdDeq;act(kind(a(i;t)));1of(1of(
. . . | |                                             2of(2of(2of(
. . . | |                                             ...))))))
. . . | |      ⇒
. . . | |      2of(1of(2of(2of(2of((with ds: ds
. . . | |               init: init
. . . | |              action a:T
. . . | |               precondition a(v) is
. . . | |               P))))))
. . . | |      (act(kind(a(i;t)))
. . . | |      ,λx.s(i;t).x
. . . | |      ,val(a(i;t))))
. . . | |     & (∀x:Id.
. . . | |        deq-member(product-deq(Knd;Id;KindDeq;IdDeq);<...
. . . | |                                                    ,x>;...)
. . . | |        ⇒
. . . | |        s(i;t+1).x
```

```
. . . | |        =
. . . | |        2of(1of(2of(2of(2of(2of((with ds: ds
. . . | |                 init: init
. . . | |                action a:T
. . . | |                 precondition a(v) is
. . . | |                 P)))))))
. . . | |        (<kind(a(i;t)),x>
. . . | |        ,λx.s(i;t).x
. . . | |        ,val(a(i;t))))
. . . | |     & (∀l:IdLnk.
. . . | |        deq-member(product-deq(Knd;IdLnk;...;...);<kind(...)
. . . | |                                                  ,l>;...)
. . . | |        ⇒
. . . | |        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(1of(2of(2of(2of(2of(2of(
. . . | |                                    (with ds: ds
. . . | |                                     init: init
. . . | |                                    action a:T
. . . | |                                     precondition a(v) is
. . . | |                                     P)))))))
. . . | |                               (<kind(a(i;t)),l>)))
. . . | |        else nil fi)
. . . | |     & (∀x:Id.
. . . | |        ¬(deq-member(IdDeq;x;1of(1of(2of(2of(2of(2of(2of(2of(
. . . | |                                    (with ds: ds
. . . | |                                     init: init
. . . | |                                    action a:T
. . . | |                                     precondition a(v) is
. . . | |                                     P)))))))))
. . . | |          ⇒
. . . | |          deq-member(KindDeq;kind(a(i;t));2of(
. . . | |                                        1of(
. . . | |                                        2of(2of(2of(2of(
. . . | |                                        2of(2of(
. . . | |                                        ...)))))))))
. . . | |                                        (x)))
. . . | |        ⇒
. . . | |        s(i;t).x = s(i;t+1).x)
. . . | |     & (∀l:IdLnk, tg:Id.
. . . | |        ¬(deq-member(product-deq(IdLnk;Id;...;IdDeq);...;...)
. . . | |          ⇒
. . . | |          deq-member(KindDeq;kind(a(i;t));2of(
. . . | |                                        1of(
. . . | |                                        2of(2of(2of(2of(
. . . | |                                        2of(2of(2of(
. . . | |                                        ...)))))))))
. . . | |                                        (<l,tg>)))
. . . | |        ⇒
. . . | |        w-tagged(tg; onlnk(l;m(i;t))) = nil)
```

```
. . . | | 17. ∀x:Id.
. . . | |     deq-member(IdDeq;x;1of(1of(2of(2of((with ds: ds
. . . | |                                  init: init
. . . | |                                 action a:T
. . . | |                                  precondition a(v) is
. . . | |                                  P))))))
. . . | |     ⇒
. . . | |     s(i;0).x
. . . | |     =
. . . | |     2of(1of(2of(2of((with ds: ds
. . . | |              init: init
. . . | |             action a:T
. . . | |              precondition a(v) is
. . . | |              P)))))
. . . | |     (x)
. . . | | 18. ∀a@0:Action(i).
. . . | |     ¬isnull(a@0)
. . . | |     ⇒
. . . | |     (valtype(i;a@0) ⊆r 1of(2of((with ds: ds
. . . | |                               init: init
. . . | |                              action a:T
. . . | |                               precondition a(v) is
. . . | |                               P)))(kind(a@0))?Top)
. . . | | 19. ∀x:Id.
. . . | |     vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(1of(
. . . | |                                              ...)))→
. . . | |                         2of(1of((with ds: ds
. . . | |                              init: init
. . . | |                             action a:T
. . . | |                              precondition a(v) is
. . . | |                              P)))
. . . | |                         (x)
. . . | |                       else Top fi
. . . | | 20. (λx.init(x)?•) ∈ State(ds)
. . . | | 21. t' : ℕ
. . . | | 22. 0≤t'
. . . | | 23. P@0 != <[a],λx.P>(a) ==> ∀v:<[locl(a)]
. . . | |                                    ,λx.T>(locl(a@0))?Top.
. . . | |     ¬P@0((λx.s(i;t').x),v)
. . . | | 24. t : ℕt'
. . . | | 25. ¬isnull(a(i;t))
. . . | | ⊢  <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. init : x:Id fp-> ds(x)?Void
```

```
. . . | | 7. ∀x:Id. x ∈ dom(ds) ⇒ x ∈ dom(init)
. . . | | 8. v : T
. . . | | 9. P((λx.init(x)?•),v)
. . . | | 10. w : World
. . . | | 11. FairFifo
. . . | | 12. FairFifo
. . . | | 13. ∀l:IdLnk, tg:Id.
. . . | |     (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . | |                        (with ds: ds
. . . | |                         init: init
. . . | |                        action a:T
. . . | |                         precondition a(v) is
. . . | |                         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(1of(2of((with ds: ds
. . . | |                                  init: init
. . . | |                                 action a:T
. . . | |                                  precondition a(v) is
. . . | |                                  P))))
. . . | |       ∨ P@0 != 1of(
. . . | |                 2of(2of(2of((with ds: ds
. . . | |                  init: init
. . . | |                 action a:T
. . . | |                  precondition a(v) is
. . . | |                  P)))))(a@0) ==> ∀v:1of(2of((with ds: ds
. . . | |                                              init: init
. . . | |                                             action a:T
. . . | |                                              precondition a(v) is
. . . | |                                              P)))(locl(a@0))?Top.
. . . | |         ¬P@0((λx.s(i;t').x),v)
. . . | | 16. ∀t:ℕ.
. . . | |     ¬isnull(a(i;t))
. . . | |     ⇒
. . . | |     (islocal(kind(a(i;t)))
. . . | |      ⇒
. . . | |      deq-member(IdDeq;act(kind(a(i;t)));1of(1of(
. . . | |                                           2of(2of(2of(
. . . | |                                           ...))))))
. . . | |      ⇒
. . . | |      2of(1of(2of(2of(2of((with ds: ds
. . . | |               init: init
. . . | |              action a:T
. . . | |               precondition a(v) is
. . . | |               P))))))
. . . | |      (act(kind(a(i;t)))
. . . | |      ,λx.s(i;t).x
. . . | |      ,val(a(i;t))))
. . . | |     & (∀x:Id.
. . . | |        deq-member(product-deq(Knd;Id;KindDeq;IdDeq);<...
. . . | |                                                    ,x>;...)
```

```
. . . | |       ⇒
. . . | |       s(i;t+1).x
. . . | |       =
. . . | |       2of(1of(2of(2of(2of(2of((with ds: ds
. . . | |                 init: init
. . . | |                action a:T
. . . | |                 precondition a(v) is
. . . | |                 P)))))))
. . . | |       (<kind(a(i;t)),x>
. . . | |       ,λx.s(i;t).x
. . . | |       ,val(a(i;t))))
. . . | |    & (∀l:IdLnk.
. . . | |       deq-member(product-deq(Knd;IdLnk;...;...);<kind(...)
. . . | |                                                 ,l>;...)
. . . | |       ⇒
. . . | |       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(1of(2of(2of(2of(2of(2of(
. . . | |                                  (with ds: ds
. . . | |                                   init: init
. . . | |                                  action a:T
. . . | |                                   precondition a(v) is
. . . | |                                   P)))))))
. . . | |                              (<kind(a(i;t)),l>)))
. . . | |       else nil fi)
. . . | |    & (∀x:Id.
. . . | |       ¬(deq-member(IdDeq;x;1of(1of(2of(2of(2of(2of(2of(2of(
. . . | |                                  (with ds: ds
. . . | |                                   init: init
. . . | |                                  action a:T
. . . | |                                   precondition a(v) is
. . . | |                                   P)))))))))
. . . | |         ⇒
. . . | |         deq-member(KindDeq;kind(a(i;t));2of(
. . . | |                                      1of(
. . . | |                                      2of(2of(2of(2of(
. . . | |                                      2of(2of(
. . . | |                                      ...)))))))))
. . . | |                                      (x)))
. . . | |       ⇒
. . . | |       s(i;t).x = s(i;t+1).x)
. . . | |    & (∀l:IdLnk, tg:Id.
. . . | |       ¬(deq-member(product-deq(IdLnk;Id;...;IdDeq);...;...)
. . . | |         ⇒
. . . | |         deq-member(KindDeq;kind(a(i;t));2of(
. . . | |                                      1of(
. . . | |                                      2of(2of(2of(2of(
. . . | |                                      2of(2of(2of(
. . . | |                                      ...)))))))))
. . . | |                                      (<l,tg>)))
```

```
. . . | |        ⇒
. . . | |        w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . | | 17. ∀x:Id.
. . . | |     deq-member(IdDeq;x;1of(1of(2of(2of((with ds: ds
. . . | |                                  init: init
. . . | |                                action a:T
. . . | |                                 precondition a(v) is
. . . | |                                 P))))))
. . . | |     ⇒
. . . | |     s(i;0).x
. . . | |     =
. . . | |     2of(1of(2of(2of((with ds: ds
. . . | |              init: init
. . . | |             action a:T
. . . | |              precondition a(v) is
. . . | |              P)))))
. . . | |     (x)
. . . | | 18. ∀a@0:Action(i).
. . . | |     ¬isnull(a@0)
. . . | |     ⇒
. . . | |     (valtype(i;a@0) ⊆r 1of(2of((with ds: ds
. . . | |                              init: init
. . . | |                             action a:T
. . . | |                              precondition a(v) is
. . . | |                              P)))(kind(a@0))?Top)
. . . | | 19. ∀x:Id.
. . . | |     vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(1of(
. . . | |                                                ...)))→
. . . | |                         2of(1of((with ds: ds
. . . | |                              init: init
. . . | |                             action a:T
. . . | |                              precondition a(v) is
. . . | |                              P)))
. . . | |                        (x)
. . . | |                      else Top fi
. . . | | 20. (λx.init(x)?·) ∈ State(ds)
. . . | | 21. t' : ℕ
. . . | | 22. 0≤t'
. . . | | 23. P@0 != <[a],λx.P>(a) ==> ∀v:<[locl(a)]
. . . | |                                  ,λx.T>(locl(a@0))?Top.
. . . | |     ¬P@0((λx.s(i;t').x),v)
. . . | | 24. t : ℕt'
. . . | | 25. ¬isnull(a(i;t))
. . . | | ⊢  loc(<i,t>) = i
. . . | |   by Unfold `w-loc` 0 THEN Reduce 0 THEN Fold `member` 0
. . . | |      THEN
. . . | |      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. init : x:Id fp-> ds(x)?Void
. . . | . 7. ∀x:Id. x ∈ dom(ds) ⇒ x ∈ dom(init)
. . . | . 8. v : T
. . . | . 9. P((λx.init(x)?•),v)
. . . | . 10. w : World
. . . | . 11. FairFifo
. . . | . 12. FairFifo
. . . | . 13. ∀l:IdLnk, tg:Id.
. . . | .     (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . | .                         (with ds: ds
. . . | .                          init: init
. . . | .                         action a:T
. . . | .                          precondition a(v) is
. . . | .                          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(1of(2of((with ds: ds
. . . | .                                  init: init
. . . | .                                 action a:T
. . . | .                                  precondition a(v) is
. . . | .                                  P))))
. . . | .       ∨ P@0 != 1of(
. . . | .                2of(2of(2of((with ds: ds
. . . | .                 init: init
. . . | .                action a:T
. . . | .                 precondition a(v) is
. . . | .                 P)))))(a@0) ==> ∀v:1of(2of((with ds: ds
. . . | .                                           init: init
. . . | .                                          action a:T
. . . | .                                           precondition a(v) is
. . . | .                                           P)))(locl(a@0))?Top.
. . . | .         ¬P@0((λx.s(i;t').x),v)
. . . | . 16. ∀t:ℕ.
. . . | .     ¬isnull(a(i;t))
. . . | .     ⇒
. . . | .     (islocal(kind(a(i;t)))
. . . | .      ⇒
. . . | .      deq-member(IdDeq;act(kind(a(i;t)));1of(1of(
. . . | .                                           2of(2of(2of(
. . . | .                                           ...))))))
. . . | .      ⇒
. . . | .      2of(1of(2of(2of(2of((with ds: ds
. . . | .                 init: init
. . . | .                action a:T
. . . | .                 precondition a(v) is
. . . | .                 P))))))
. . . | .      (act(kind(a(i;t)))
. . . | .      ,λx.s(i;t).x
. . . | .      ,val(a(i;t))))
. . . | .     & (∀x:Id.
. . . | .        deq-member(product-deq(Knd;Id;KindDeq;IdDeq);<...
```

```
. . . | .                                                    ,x>;...)
. . . | .       ⇒
. . . | .       s(i;t+1).x
. . . | .       =
. . . | .       2of(1of(2of(2of(2of(2of((with ds: ds
. . . | .                init: init
. . . | .               action a:T
. . . | .                precondition a(v) is
. . . | .                P)))))))
. . . | .       (<kind(a(i;t)),x>
. . . | .       ,λx.s(i;t).x
. . . | .       ,val(a(i;t))))
. . . | .    & (∀l:IdLnk.
. . . | .       deq-member(product-deq(Knd;IdLnk;...;...);<kind(...)
. . . | .                                                 ,l>;...)
. . . | .       ⇒
. . . | .       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(1of(2of(2of(2of(2of(2of(
. . . | .                                  (with ds: ds
. . . | .                                   init: init
. . . | .                                  action a:T
. . . | .                                   precondition a(v) is
. . . | .                                   P)))))))
. . . | .                           (<kind(a(i;t)),l>)))
. . . | .       else nil fi)
. . . | .    & (∀x:Id.
. . . | .       ¬(deq-member(IdDeq;x;1of(1of(2of(2of(2of(2of(2of(2of(
. . . | .                                  (with ds: ds
. . . | .                                   init: init
. . . | .                                  action a:T
. . . | .                                   precondition a(v) is
. . . | .                                   P)))))))))
. . . | .         ⇒
. . . | .         deq-member(KindDeq;kind(a(i;t));2of(
. . . | .                                      1of(
. . . | .                                      2of(2of(2of(2of(
. . . | .                                      2of(2of(
. . . | .                                      ...)))))))))
. . . | .                                      (x)))
. . . | .       ⇒
. . . | .       s(i;t).x = s(i;t+1).x)
. . . | .    & (∀l:IdLnk, tg:Id.
. . . | .       ¬(deq-member(product-deq(IdLnk;Id;...;IdDeq);...;...)
. . . | .         ⇒
. . . | .         deq-member(KindDeq;kind(a(i;t));2of(
. . . | .                                      1of(
. . . | .                                      2of(2of(2of(2of(
. . . | .                                      2of(2of(2of(
. . . | .                                      ...)))))))))
```

```
. . . | .                                              (<l,tg>)))
. . . | .        ⇒
. . . | .        w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . | . 17. ∀x:Id.
. . . | .     deq-member(IdDeq;x;1of(1of(2of(2of((with ds: ds
. . . | .                                      init: init
. . . | .                                     action a:T
. . . | .                                      precondition a(v) is
. . . | .                                      P))))))
. . . | .     ⇒
. . . | .     s(i;0).x
. . . | .     =
. . . | .     2of(1of(2of(2of((with ds: ds
. . . | .                      init: init
. . . | .                     action a:T
. . . | .                      precondition a(v) is
. . . | .                      P)))))
. . . | .     (x)
. . . | . 18. ∀a@0:Action(i).
. . . | .     ¬isnull(a@0)
. . . | .     ⇒
. . . | .     (valtype(i;a@0) ⊆r 1of(2of((with ds: ds
. . . | .                                  init: init
. . . | .                                 action a:T
. . . | .                                  precondition a(v) is
. . . | .                                  P)))(kind(a@0))?Top)
. . . | . 19. ∀x:Id.
. . . | .     vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(1of(
. . . | .                                                ...)))→
. . . | .                           2of(1of((with ds: ds
. . . | .                                init: init
. . . | .                               action a:T
. . . | .                                precondition a(v) is
. . . | .                                P)))
. . . | .                           (x)
. . . | .                      else Top fi
. . . | . 20. (λx.init(x)?•) ∈ State(ds)
. . . | . 21. t' : ℕ
. . . | . 22. 0≤t'
. . . | . 23. P@0 != <[a],λx.P>(a) ==> ∀v:<[locl(a)]
. . . | .                                    ,λx.T>(locl(a@0))?Top.
. . . | .     ¬P@0((λx.s(i;t').x),v)
. . . | . 24. t : ℕt'
. . . | . 25. ¬isnull(a(i;t))
. . . | . 26. e : E
. . . | . ⊢  (loc(e) = i) ∈ Prop  by 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. init : x:Id fp-> ds(x)?Void
. . . . 7. ∀x:Id. x ∈ dom(ds) ⇒ x ∈ dom(init)
```

```
. . . . 8. v : T
. . . . 9. P((λx.init(x)?•),v)
. . . . 10. w : World
. . . . 11. FairFifo
. . . . 12. FairFifo
. . . . 13. ∀l:IdLnk, tg:Id.
. . . . |   (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . |                     (with ds: ds
. . . . |                      init: init
. . . . |                     action a:T
. . . . |                      precondition a(v) is
. . . . |                      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(1of(2of((with ds: ds
. . . . |                              init: init
. . . . |                             action a:T
. . . . |                              precondition a(v) is
. . . . |                              P))))
. . . . |     ∨ P@0 != 1of(
. . . . |              2of(2of(2of((with ds: ds
. . . . |               init: init
. . . . |              action a:T
. . . . |               precondition a(v) is
. . . . |               P)))))(a@0) ==> ∀v:1of(2of((with ds: ds
. . . . |                                        init: init
. . . . |                                       action a:T
. . . . |                                        precondition a(v) is
. . . . |                                        P)))(1ocl(a@0))?Top.
. . . . |       ¬P@0((λx.s(i;t').x),v)
. . . . 16. ∀t:ℕ.
. . . . |   ¬isnull(a(i;t))
. . . . |   ⇒
. . . . |   (islocal(kind(a(i;t)))
. . . . |    ⇒
. . . . |    deq-member(IdDeq;act(kind(a(i;t)));1of(1of(
. . . . |                                        2of(2of(2of(
. . . . |                                        (with ds: ds
. . . . |                                         init: init
. . . . |                                        action a:T
. . . . |                                         precondition a(v) is
. . . . |                                         P)))))))
. . . . |    ⇒
. . . . |    2of(1of(2of(2of(2of((with ds: ds
. . . . |              init: init
. . . . |             action a:T
. . . . |              precondition a(v) is
. . . . |              P))))))
. . . . |    (act(kind(a(i;t)))
. . . . |    ,λx.s(i;t).x
. . . . |    ,val(a(i;t))))
```

```
. . . . |   & (∀x:Id.
. . . . |      deq-member(product-deq(Knd;Id;KindDeq;IdDeq);<kind(...)
. . . . |                                                    ,x>;...)
. . . . |      ⇒
. . . . |      s(i;t+1).x
. . . . |      =
. . . . |      2of(1of(2of(2of(2of(2of((with ds: ds
. . . . |               init: init
. . . . |              action a:T
. . . . |               precondition a(v) is
. . . . |               P)))))))
. . . . |      (<kind(a(i;t)),x>
. . . . |      ,λx.s(i;t).x
. . . . |      ,val(a(i;t))))
. . . . |   & (∀l:IdLnk.
. . . . |      deq-member(product-deq(Knd;IdLnk;KindDeq;...);<...
. . . . |                                                     ,l>;...)
. . . . |      ⇒
. . . . |      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(1of(2of(2of(2of(2of(2of(
. . . . |                                    (with ds: ds
. . . . |                                     init: init
. . . . |                                    action a:T
. . . . |                                     precondition a(v) is
. . . . |                                     P)))))))
. . . . |                              (<kind(a(i;t)),l>)))
. . . . |      else nil fi)
. . . . |   & (∀x:Id.
. . . . |      ¬(deq-member(IdDeq;x;1of(1of(2of(2of(2of(2of(2of(2of(
. . . . |                                   (with ds: ds
. . . . |                                    init: init
. . . . |                                   action a:T
. . . . |                                    precondition a(v) is
. . . . |                                    P)))))))))
. . . . |        ⇒
. . . . |        deq-member(KindDeq;kind(a(i;t));2of(
. . . . |                                        1of(
. . . . |                                        2of(2of(2of(2of(2of(
. . . . |                                        2of((with ds: ds
. . . . |                                         init: init
. . . . |                                        action a:T
. . . . |                                         precondition a(v) is
. . . . |                                         P)))))))))
. . . . |                                        (x)))
. . . . |      ⇒
. . . . |      s(i;t).x = s(i;t+1).x)
. . . . |   & (∀l:IdLnk, tg:Id.
. . . . |      ¬(deq-member(product-deq(IdLnk;Id;...;IdDeq);...;...)
. . . . |        ⇒
```

```
. . . . |        deq-member(KindDeq;kind(a(i;t));2of(
. . . . |                                          1of(
. . . . |                                          2of(2of(2of(2of(2of(
. . . . |                                          2of(2of((with ds: ds
. . . . |                                           init: init
. . . . |                                          action a:T
. . . . |                                           precondition a(v) is
. . . . |                                           P))))))))))
. . . . |                                          (<l,tg>)))
. . . . |      ⇒
. . . . |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . 17. ∀x:Id.
. . . . |   deq-member(IdDeq;x;1of(1of(2of(2of((with ds: ds
. . . . |                                 init: init
. . . . |                                action a:T
. . . . |                                 precondition a(v) is
. . . . |                                 P))))))
. . . . |   ⇒
. . . . |   s(i;0).x
. . . . |   =
. . . . |   2of(1of(2of(2of((with ds: ds
. . . . |            init: init
. . . . |           action a:T
. . . . |            precondition a(v) is
. . . . |            P)))))
. . . . |   (x)
. . . . 18. ∀a@0:Action(i).
. . . . |   ¬isnull(a@0)
. . . . |   ⇒
. . . . |   (valtype(i;a@0) ⊆r 1of(2of((with ds: ds
. . . . |                            init: init
. . . . |                           action a:T
. . . . |                            precondition a(v) is
. . . . |                            P)))(kind(a@0))?Top)
. . . . 19. ∀x:Id.
. . . . |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(1of(...)))→
. . . . |                      2of(1of((with ds: ds
. . . . |                           init: init
. . . . |                          action a:T
. . . . |                           precondition a(v) is
. . . . |                           P)))
. . . . |                     (x)
. . . . |                  else Top fi
. . . . 20. (λx.init(x)?•) ∈ State(ds)
. . . . 21. t' : ℕ
. . . . 22. 0≤t'
. . . . 23. P@0 != <[a],λx.P>(a) ==> ∀v:<[locl(a)]
. . . . |                                ,λx.T>(locl(a@0))?Top.
. . . . |   ¬P@0((λx.s(i;t').x),v)
. . . . 24. ¬(∃t:ℕt'. ¬isnull(a(i;t)))
. . . . ⊢  ∃e:E. loc(e) = i  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. init : x:Id fp-> ds(x)?Void
. . . . | 7. ∀x:Id. x ∈ dom(ds) ⇒ x ∈ dom(init)
. . . . | 8. v : T
. . . . | 9. P((λx.init(x)?•),v)
. . . . | 10. w : World
. . . . | 11. FairFifo
. . . . | 12. FairFifo
. . . . | 13. ∀l:IdLnk, tg:Id.
. . . . |     (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . |                        (with ds: ds
. . . . |                         init: init
. . . . |                        action a:T
. . . . |                         precondition a(v) is
. . . . |                         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(1of(2of((with ds: ds
. . . . |                                  init: init
. . . . |                                 action a:T
. . . . |                                  precondition a(v) is
. . . . |                                  P))))
. . . . |       ∨ P@0 != 1of(
. . . . |                 2of(2of(2of((with ds: ds
. . . . |                  init: init
. . . . |                 action a:T
. . . . |                  precondition a(v) is
. . . . |                  P)))))(a@0) ==> ∀v:1of(2of((with ds: ds
. . . . |                                              init: init
. . . . |                                             action a:T
. . . . |                                              precondition a(v) is
. . . . |                                              P)))(locl(a@0))?Top.
. . . . |         ¬P@0((λx.s(i;t').x),v)
. . . . | 16. ∀t:ℕ.
. . . . |     ¬isnull(a(i;t))
. . . . |     ⇒
. . . . |     (islocal(kind(a(i;t)))
. . . . |      ⇒
. . . . |      deq-member(IdDeq;act(kind(a(i;t)));1of(1of(
. . . . |                                             2of(2of(2of(
. . . . |                                             ...))))))
. . . . |      ⇒
. . . . |      2of(1of(2of(2of(2of((with ds: ds
. . . . |               init: init
. . . . |              action a:T
. . . . |               precondition a(v) is
. . . . |               P))))))
. . . . |      (act(kind(a(i;t)))
```

```
. . . . |      ,λx.s(i;t).x
. . . . |      ,val(a(i;t))))
. . . . |    & (∀x:Id.
. . . . |       deq-member(product-deq(Knd;Id;KindDeq;IdDeq);<...
. . . . |                                                    ,x>;...)
. . . . |       ⇒
. . . . |       s(i;t+1).x
. . . . |       =
. . . . |       2of(1of(2of(2of(2of(2of((with ds: ds
. . . . |                 init: init
. . . . |                action a:T
. . . . |                 precondition a(v) is
. . . . |                 P)))))))
. . . . |       (<kind(a(i;t)),x>
. . . . |       ,λx.s(i;t).x
. . . . |       ,val(a(i;t))))
. . . . |    & (∀l:IdLnk.
. . . . |       deq-member(product-deq(Knd;IdLnk;...;...);<kind(...)
. . . . |                                                 ,l>;...)
. . . . |       ⇒
. . . . |       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(1of(2of(2of(2of(2of(2of(
. . . . |                                  (with ds: ds
. . . . |                                   init: init
. . . . |                                  action a:T
. . . . |                                   precondition a(v) is
. . . . |                                   P)))))))))
. . . . |                             (<kind(a(i;t)),l>)))
. . . . |       else nil fi)
. . . . |    & (∀x:Id.
. . . . |       ¬(deq-member(IdDeq;x;1of(1of(2of(2of(2of(2of(2of(2of(
. . . . |                                  (with ds: ds
. . . . |                                   init: init
. . . . |                                  action a:T
. . . . |                                   precondition a(v) is
. . . . |                                   P)))))))))))
. . . . |         ⇒
. . . . |         deq-member(KindDeq;kind(a(i;t));2of(
. . . . |                                      1of(
. . . . |                                      2of(2of(2of(2of(
. . . . |                                      2of(2of(
. . . . |                                      ...)))))))))
. . . . |                                      (x)))
. . . . |       ⇒
. . . . |       s(i;t).x = s(i;t+1).x)
. . . . |    & (∀l:IdLnk, tg:Id.
. . . . |       ¬(deq-member(product-deq(IdLnk;Id;...;IdDeq);...;...)
. . . . |         ⇒
. . . . |         deq-member(KindDeq;kind(a(i;t));2of(
```

```
. . . . |                                          1of(
. . . . |                                          2of(2of(2of(2of(
. . . . |                                          2of(2of(2of(
. . . . |                                          ...)))))))))
. . . . |                                          (<l,tg>)))
. . . . |       ⇒
. . . . |       w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . | 17. ∀x:Id.
. . . . |     deq-member(IdDeq;x;1of(1of(2of(2of((with ds: ds
. . . . |                                 init: init
. . . . |                                action a:T
. . . . |                                 precondition a(v) is
. . . . |                                 P))))))
. . . . |     ⇒
. . . . |     s(i;0).x
. . . . |     =
. . . . |     2of(1of(2of(2of((with ds: ds
. . . . |              init: init
. . . . |             action a:T
. . . . |              precondition a(v) is
. . . . |              P)))))
. . . . |     (x)
. . . . | 18. ∀a@0:Action(i).
. . . . |     ¬isnull(a@0)
. . . . |     ⇒
. . . . |     (valtype(i;a@0) ⊆r 1of(2of((with ds: ds
. . . . |                              init: init
. . . . |                             action a:T
. . . . |                              precondition a(v) is
. . . . |                              P)))(kind(a@0))?Top)
. . . . | 19. ∀x:Id.
. . . . |     vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(1of(
. . . . |                                          ...)))→
. . . . |                         2of(1of((with ds: ds
. . . . |                              init: init
. . . . |                             action a:T
. . . . |                              precondition a(v) is
. . . . |                              P)))
. . . . |                        (x)
. . . . |                      else Top fi
. . . . | 20. (λx.init(x)?•) ∈ State(ds)
. . . . | 21. t' : ℕ
. . . . | 22. 0≤t'
. . . . | 23. P@0 != <[a],λx.P>(a) ==> ∀v:<[locl(a)]
. . . . |                                  ,λx.T>(locl(a@0))?Top.
. . . . |     ¬P@0((λx.s(i;t').x),v)
. . . . | 24. ¬(∃t:ℕt'. ¬isnull(a(i;t)))
. . . . | ⊢  IdDeq ∈ EqDecider(Id)
. . . . |   by SubsumeC EqDecider(Id)
. . . . |      THEN
. . . . |      Try
. . . . |      (BackThru
. . . . |       Thm* strong-subtype(A;B)
. . . . |            ⇒
. . . . |            (EqDecider(B) ⊆r EqDecider(A))
```

```
. . . . |       {strong_DASH_subtype_DASH_deq_DASH_subtype}
. . . . |       THEN
. . . . |       All (Unfold ‘dstype‘)
. . . . |       THEN
. . . . |       All Reduce
. . . . |       THEN
. . . . |       Trivial)
. . . . |      THEN
. . . . |      AllHyps
. . . . |      (λi.Unfold_Wld i THEN Reduce 0 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. init : x:Id fp-> ds(x)?Void
. . . . . 7. ∀x:Id. x ∈ dom(ds) ⇒ x ∈ dom(init)
. . . . . 8. v : T
. . . . . 9. P((λx.init(x)?•),v)
. . . . . 10. w : World
. . . . . 11. FairFifo
. . . . . 12. FairFifo
. . . . . 13. ∀l:IdLnk, tg:Id.
. . . . . |   (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . |                    (with ds: ds
. . . . . |                     init: init
. . . . . |                    action a:T
. . . . . |                     precondition a(v) is
. . . . . |                     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(1of(2of((with ds: ds
. . . . . |                              init: init
. . . . . |                             action a:T
. . . . . |                              precondition a(v) is
. . . . . |                              P))))
. . . . . |     ∨ P@0 != 1of(
. . . . . |              2of(2of(2of((with ds: ds
. . . . . |               init: init
. . . . . |              action a:T
. . . . . |               precondition a(v) is
. . . . . |               P)))))(a@0) ==> ∀v:1of(2of((with ds: ds
. . . . . |                                    init: init
. . . . . |                                   action a:T
. . . . . |                                    precondition a(v) is
. . . . . |                                    P)))(locl(a@0))?Top.
. . . . . |       ¬P@0((λx.s(i;t').x),v)
. . . . . 16. ∀t:ℕ.
. . . . . |   ¬isnull(a(i;t))
```

```
. . . . . |   ⇒
. . . . . |   (islocal(kind(a(i;t)))
. . . . . |    ⇒
. . . . . |    deq-member(IdDeq;act(kind(a(i;t)));1of(1of(
. . . . . |                                       2of(2of(2of(
. . . . . |                                       ...)))))))
. . . . . |    ⇒
. . . . . |    2of(1of(2of(2of(2of((with ds: ds
. . . . . |             init: init
. . . . . |            action a:T
. . . . . |             precondition a(v) is
. . . . . |             P))))))
. . . . . |    (act(kind(a(i;t)))
. . . . . |    ,λx.s(i;t).x
. . . . . |    ,val(a(i;t))))
. . . . . |   & (∀x:Id.
. . . . . |      deq-member(product-deq(Knd;Id;KindDeq;IdDeq);<...
. . . . . |                                                  ,x>;...)
. . . . . |      ⇒
. . . . . |      s(i;t+1).x
. . . . . |      =
. . . . . |      2of(1of(2of(2of(2of(2of((with ds: ds
. . . . . |               init: init
. . . . . |              action a:T
. . . . . |               precondition a(v) is
. . . . . |               P)))))))
. . . . . |      (<kind(a(i;t)),x>
. . . . . |      ,λx.s(i;t).x
. . . . . |      ,val(a(i;t))))
. . . . . |   & (∀l:IdLnk.
. . . . . |      deq-member(product-deq(Knd;IdLnk;...;...);<kind(...)
. . . . . |                                               ,l>;...)
. . . . . |      ⇒
. . . . . |      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(1of(2of(2of(2of(2of(2of(
. . . . . |                                    (with ds: ds
. . . . . |                                     init: init
. . . . . |                                    action a:T
. . . . . |                                     precondition a(v) is
. . . . . |                                     P)))))))
. . . . . |                              (<kind(a(i;t)),l>)))
. . . . . |      else nil fi)
. . . . . |   & (∀x:Id.
. . . . . |      ¬(deq-member(IdDeq;x;1of(1of(2of(2of(2of(2of(2of(2of(
. . . . . |                                   (with ds: ds
. . . . . |                                    init: init
. . . . . |                                   action a:T
. . . . . |                                    precondition a(v) is
. . . . . |                                    P)))))))))
```

```
. . . . . |        ⇒
. . . . . |        deq-member(KindDeq;kind(a(i;t));2of(
. . . . . |                                          1of(
. . . . . |                                          2of(2of(2of(2of(
. . . . . |                                          2of(2of(
. . . . . |                                          ...)))))))))
. . . . . |                                          (x)))

. . . . . |      ⇒
. . . . . |      s(i;t).x = s(i;t+1).x)
. . . . . |    & (∀l:IdLnk, tg:Id.
. . . . . |      ¬(deq-member(product-deq(IdLnk;Id;...;IdDeq);...;...)
. . . . . |        ⇒
. . . . . |        deq-member(KindDeq;kind(a(i;t));2of(
. . . . . |                                          1of(
. . . . . |                                          2of(2of(2of(2of(
. . . . . |                                          2of(2of(2of(
. . . . . |                                          ...)))))))))
. . . . . |                                          (<l,tg>)))
. . . . . |      ⇒
. . . . . |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . 17. ∀x:Id.
. . . . . |    deq-member(IdDeq;x;1of(1of(2of(2of((with ds: ds
. . . . . |                                 init: init
. . . . . |                                action a:T
. . . . . |                                 precondition a(v) is
. . . . . |                                 P))))))
. . . . . |    ⇒
. . . . . |    s(i;0).x
. . . . . |    =
. . . . . |    2of(1of(2of(2of((with ds: ds
. . . . . |              init: init
. . . . . |             action a:T
. . . . . |              precondition a(v) is
. . . . . |              P)))))
. . . . . |    (x)
. . . . . 18. ∀a@0:Action(i).
. . . . . |    ¬isnull(a@0)
. . . . . |    ⇒
. . . . . |    (valtype(i;a@0) ⊆r 1of(2of((with ds: ds
. . . . . |                              init: init
. . . . . |                             action a:T
. . . . . |                              precondition a(v) is
. . . . . |                              P)))(kind(a@0))?Top)
. . . . . 19. ∀x:Id.
. . . . . |    vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(1of(
. . . . . |                                            ...)))→
. . . . . |                        2of(1of((with ds: ds
. . . . . |                             init: init
. . . . . |                            action a:T
. . . . . |                             precondition a(v) is
. . . . . |                             P)))
. . . . . |                       (x)
. . . . . |                    else Top fi
. . . . . 20. (λx.init(x)?•) ∈ State(ds)
. . . . . 21. t' : ℕ
```

```
. . . . . 22. 0≤t'
. . . . . 23. P@0 != <[a],λx.P>(a) ==> ∀v:<[locl(a)]
. . . . . |                              ,λx.T>(locl(a@0))?Top.
. . . . . |   ¬P@0((λx.s(i;t').x),v)
. . . . . 24. ¬(∃t:ℕt'. ¬isnull(a(i;t)))
. . . . . 25. IdDeq ∈ EqDecider(Id)
. . . . . ⊢  ∃e:E. loc(e) = i  by MoveToHyp 20 -1
. . . . . |
. . . . . 1. i : Id
. . . . . 2. a : Id
. . . . . 3. T : Type
. . . . . 4. ds : x:Id fp-> Type
. . . . . 5. P : State(ds)→T→Prop
. . . . . 6. init : x:Id fp-> ds(x)?Void
. . . . . 7. ∀x:Id. x ∈ dom(ds) ⇒ x ∈ dom(init)
. . . . . 8. v : T
. . . . . 9. P((λx.init(x)?•),v)
. . . . . 10. w : World
. . . . . 11. FairFifo
. . . . . 12. FairFifo
. . . . . 13. ∀l:IdLnk, tg:Id.
. . . . . |   (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . |                    (with ds: ds
. . . . . |                     init: init
. . . . . |                    action a:T
. . . . . |                     precondition a(v) is
. . . . . |                     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(1of(2of((with ds: ds
. . . . . |                              init: init
. . . . . |                             action a:T
. . . . . |                              precondition a(v) is
. . . . . |                              P))))
. . . . . |     ∨ P@0 != 1of(
. . . . . |              2of(2of(2of((with ds: ds
. . . . . |               init: init
. . . . . |              action a:T
. . . . . |               precondition a(v) is
. . . . . |               P)))))(a@0) ==> ∀v:1of(2of((with ds: ds
. . . . . |                                        init: init
. . . . . |                                       action a:T
. . . . . |                                        precondition a(v) is
. . . . . |                                        P)))(locl(a@0))?Top.
. . . . . |       ¬P@0((λx.s(i;t').x),v)
. . . . . 16. ∀t:ℕ.
. . . . . |   ¬isnull(a(i;t))
. . . . . |   ⇒
. . . . . |   (islocal(kind(a(i;t)))
. . . . . |    ⇒
. . . . . |    deq-member(IdDeq;act(kind(a(i;t)));1of(1of(
```

```
. . . . . |                                        2of(2of(2of(
. . . . . |                                        ...))))))
. . . . . |    ⇒
. . . . . |    2of(1of(2of(2of(2of((with ds: ds
. . . . . |             init: init
. . . . . |            action a:T
. . . . . |             precondition a(v) is
. . . . . |             P))))))
. . . . . |    (act(kind(a(i;t)))
. . . . . |    ,λx.s(i;t).x
. . . . . |    ,val(a(i;t))))
. . . . . |   & (∀x:Id.
. . . . . |      deq-member(product-deq(Knd;Id;KindDeq;IdDeq);<...
. . . . . |                                                  ,x>;...)
. . . . . |      ⇒
. . . . . |      s(i;t+1).x
. . . . . |      =
. . . . . |      2of(1of(2of(2of(2of(2of((with ds: ds
. . . . . |               init: init
. . . . . |              action a:T
. . . . . |               precondition a(v) is
. . . . . |               P)))))))
. . . . . |      (<kind(a(i;t)),x>
. . . . . |      ,λx.s(i;t).x
. . . . . |      ,val(a(i;t))))
. . . . . |   & (∀l:IdLnk.
. . . . . |      deq-member(product-deq(Knd;IdLnk;...;...);<kind(...)
. . . . . |                                               ,l>;...)
. . . . . |      ⇒
. . . . . |      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(1of(2of(2of(2of(2of(2of(
. . . . . |                                    (with ds: ds
. . . . . |                                     init: init
. . . . . |                                    action a:T
. . . . . |                                     precondition a(v) is
. . . . . |                                     P)))))))))
. . . . . |                              (<kind(a(i;t)),l>)))
. . . . . |      else nil fi)
. . . . . |   & (∀x:Id.
. . . . . |      ¬(deq-member(IdDeq;x;1of(1of(2of(2of(2of(2of(2of(2of(2of(
. . . . . |                                   (with ds: ds
. . . . . |                                    init: init
. . . . . |                                   action a:T
. . . . . |                                    precondition a(v) is
. . . . . |                                    P)))))))))))
. . . . . |        ⇒
. . . . . |        deq-member(KindDeq;kind(a(i;t));2of(
. . . . . |                                        1of(
. . . . . |                                        2of(2of(2of(2of(
```

```
. . . . . |                                        2of(2of(
. . . . . |                                        ...)))))))))
. . . . . |                                        (x)))
. . . . . |      ⇒
. . . . . |      s(i;t).x = s(i;t+1).x)
. . . . . |   & (∀l:IdLnk, tg:Id.
. . . . . |      ¬(deq-member(product-deq(IdLnk;Id;...;IdDeq);...;...)
. . . . . |        ⇒
. . . . . |        deq-member(KindDeq;kind(a(i;t));2of(
. . . . . |                                        1of(
. . . . . |                                        2of(2of(2of(2of(
. . . . . |                                        2of(2of(2of(
. . . . . |                                        ...)))))))))
. . . . . |                                        (<l,tg>)))
. . . . . |      ⇒
. . . . . |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . 17. ∀x:Id.
. . . . . |   deq-member(IdDeq;x;1of(1of(2of(2of((with ds: ds
. . . . . |                                 init: init
. . . . . |                                action a:T
. . . . . |                                 precondition a(v) is
. . . . . |                                 P))))))
. . . . . |   ⇒
. . . . . |   s(i;0).x
. . . . . |   =
. . . . . |   2of(1of(2of(2of((with ds: ds
. . . . . |            init: init
. . . . . |           action a:T
. . . . . |            precondition a(v) is
. . . . . |            P)))))
. . . . . |   (x)
. . . . . 18. ∀a@0:Action(i).
. . . . . |   ¬isnull(a@0)
. . . . . |   ⇒
. . . . . |   (valtype(i;a@0) ⊆r 1of(2of((with ds: ds
. . . . . |                            init: init
. . . . . |                           action a:T
. . . . . |                            precondition a(v) is
. . . . . |                            P)))(kind(a@0))?Top)
. . . . . 19. ∀x:Id.
. . . . . |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(1of(
. . . . . |                                          ...)))→
. . . . . |                       2of(1of((with ds: ds
. . . . . |                            init: init
. . . . . |                           action a:T
. . . . . |                            precondition a(v) is
. . . . . |                            P)))
. . . . . |                      (x)
. . . . . |                  else Top fi
. . . . . 20. IdDeq ∈ EqDecider(Id)
. . . . . 21. (λx.init(x)?•) ∈ State(ds)
. . . . . 22. t' : ℕ
. . . . . 23. 0≤t'
. . . . . 24. P@0 != <[a],λx.P>(a) ==> ∀v:<[locl(a)]
. . . . . |                               ,λx.T>(locl(a@0))?Top.
```

```
. . . . . |   ¬P@0((λx.s(i;t').x),v)
. . . . . 25. ¬(∃t:ℕt'. ¬isnull(a(i;t)))
. . . . . ⊢  ∃e:E. loc(e) = i
. . . . . | by Fold `fpf-single` -2 THEN Reduce -2
. . . . . |    THENA
. . . . . |    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. init : x:Id fp-> ds(x)?Void
. . . . . 7. ∀x:Id. x ∈ dom(ds) ⇒ x ∈ dom(init)
. . . . . 8. v : T
. . . . . 9. P((λx.init(x)?•),v)
. . . . . 10. w : World
. . . . . 11. FairFifo
. . . . . 12. FairFifo
. . . . . 13. ∀l:IdLnk, tg:Id.
. . . . . |   (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . |                    (with ds: ds
. . . . . |                     init: init
. . . . . |                    action a:T
. . . . . |                     precondition a(v) is
. . . . . |                     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(1of(2of((with ds: ds
. . . . . |                              init: init
. . . . . |                             action a:T
. . . . . |                              precondition a(v) is
. . . . . |                              P))))
. . . . . |     ∨ P@0 != 1of(
. . . . . |              2of(2of(2of((with ds: ds
. . . . . |               init: init
. . . . . |              action a:T
. . . . . |               precondition a(v) is
. . . . . |               P)))))(a@0) ==> ∀v:1of(2of((with ds: ds
. . . . . |                                        init: init
. . . . . |                                       action a:T
. . . . . |                                        precondition a(v) is
. . . . . |                                        P)))(locl(a@0))?Top.
. . . . . |       ¬P@0((λx.s(i;t').x),v)
. . . . . 16. ∀t:ℕ.
. . . . . |   ¬isnull(a(i;t))
. . . . . |   ⇒
. . . . . |   (islocal(kind(a(i;t)))
. . . . . |    ⇒
. . . . . |    deq-member(IdDeq;act(kind(a(i;t)));1of(1of(
. . . . . |                                        2of(2of(2of(
```

```
. . . . . |                                          ...))))))
. . . . . |    ⇒
. . . . . |    2of(1of(2of(2of(2of((with ds: ds
. . . . . |             init: init
. . . . . |            action a:T
. . . . . |             precondition a(v) is
. . . . . |             P))))))
. . . . . |    (act(kind(a(i;t)))
. . . . . |    ,λx.s(i;t).x
. . . . . |    ,val(a(i;t))))
. . . . . |   & (∀x:Id.
. . . . . |      deq-member(product-deq(Knd;Id;KindDeq;IdDeq);<...
. . . . . |                                                  ,x>;...)
. . . . . |      ⇒
. . . . . |      s(i;t+1).x
. . . . . |      =
. . . . . |      2of(1of(2of(2of(2of(2of((with ds: ds
. . . . . |               init: init
. . . . . |              action a:T
. . . . . |               precondition a(v) is
. . . . . |               P)))))))
. . . . . |      (<kind(a(i;t)),x>
. . . . . |      ,λx.s(i;t).x
. . . . . |      ,val(a(i;t))))
. . . . . |   & (∀l:IdLnk.
. . . . . |      deq-member(product-deq(Knd;IdLnk;...;...);<kind(...)
. . . . . |                                                ,l>;...)
. . . . . |      ⇒
. . . . . |      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(1of(2of(2of(2of(2of(2of(
. . . . . |                                    (with ds: ds
. . . . . |                                     init: init
. . . . . |                                    action a:T
. . . . . |                                     precondition a(v) is
. . . . . |                                     P)))))))))
. . . . . |                               (<kind(a(i;t)),l>)))
. . . . . |      else nil fi)
. . . . . |   & (∀x:Id.
. . . . . |      ¬(deq-member(IdDeq;x;1of(1of(2of(2of(2of(2of(2of(2of(
. . . . . |                                   (with ds: ds
. . . . . |                                    init: init
. . . . . |                                   action a:T
. . . . . |                                    precondition a(v) is
. . . . . |                                    P)))))))))
. . . . . |        ⇒
. . . . . |        deq-member(KindDeq;kind(a(i;t));2of(
. . . . . |                                       1of(
. . . . . |                                       2of(2of(2of(2of(
. . . . . |                                       2of(2of(
```

```
. . . . . |                                        ...)))))))))
. . . . . |                                        (x)))
. . . . . |      ⇒
. . . . . |      s(i;t).x = s(i;t+1).x)
. . . . . |   & (∀l:IdLnk, tg:Id.
. . . . . |      ¬(deq-member(product-deq(IdLnk;Id;...;IdDeq);...;...)
. . . . . |        ⇒
. . . . . |        deq-member(KindDeq;kind(a(i;t));2of(
. . . . . |                                        1of(
. . . . . |                                        2of(2of(2of(2of(2of(
. . . . . |                                        2of(2of(2of(
. . . . . |                                        ...)))))))))
. . . . . |                                        (<l,tg>)))
. . . . . |      ⇒
. . . . . |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . 17. ∀x:Id.
. . . . . |   deq-member(IdDeq;x;1of(1of(2of(2of((with ds: ds
. . . . . |                                 init: init
. . . . . |                                action a:T
. . . . . |                                 precondition a(v) is
. . . . . |                                 P))))))
. . . . . |   ⇒
. . . . . |   s(i;0).x
. . . . . |   =
. . . . . |   2of(1of(2of(2of((with ds: ds
. . . . . |            init: init
. . . . . |           action a:T
. . . . . |            precondition a(v) is
. . . . . |            P)))))
. . . . . |   (x)
. . . . . 18. ∀a@0:Action(i).
. . . . . |   ¬isnull(a@0)
. . . . . |   ⇒
. . . . . |   (valtype(i;a@0) ⊆r 1of(2of((with ds: ds
. . . . . |                            init: init
. . . . . |                           action a:T
. . . . . |                            precondition a(v) is
. . . . . |                            P)))(kind(a@0))?Top)
. . . . . 19. ∀x:Id.
. . . . . |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(1of(
. . . . . |                                          ...)))→
. . . . . |                       2of(1of((with ds: ds
. . . . . |                            init: init
. . . . . |                           action a:T
. . . . . |                            precondition a(v) is
. . . . . |                            P)))
. . . . . |                      (x)
. . . . . |                  else Top fi
. . . . . 20. IdDeq ∈ EqDecider(Id)
. . . . . 21. (λx.init(x)?•) ∈ State(ds)
. . . . . 22. t' : ℕ
. . . . . 23. 0≤t'
. . . . . 24. True ⇒ (∀v:T. ¬P((λx.s(i;t').x),v))
. . . . . 25. ¬(∃t:ℕt'. ¬isnull(a(i;t)))
. . . . . ⊢  ∃e:E. loc(e) = i  by InstHyp [v] -2
```

```
. . . . . |
. . . . . 1. i : Id
. . . . . 2. a : Id
. . . . . 3. T : Type
. . . . . 4. ds : x:Id fp-> Type
. . . . . 5. P : State(ds)→T→Prop
. . . . . 6. init : x:Id fp-> ds(x)?Void
. . . . . 7. ∀x:Id. x ∈ dom(ds) ⇒ x ∈ dom(init)
. . . . . 8. v : T
. . . . . 9. P((λx.init(x)?•),v)
. . . . . 10. w : World
. . . . . 11. FairFifo
. . . . . 12. FairFifo
. . . . . 13. ∀l:IdLnk, tg:Id.
. . . . . |   (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . |                     (with ds: ds
. . . . . |                      init: init
. . . . . |                     action a:T
. . . . . |                      precondition a(v) is
. . . . . |                      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(1of(2of((with ds: ds
. . . . . |                              init: init
. . . . . |                             action a:T
. . . . . |                              precondition a(v) is
. . . . . |                              P))))
. . . . . |     ∨ P@0 != 1of(
. . . . . |              2of(2of(2of((with ds: ds
. . . . . |               init: init
. . . . . |              action a:T
. . . . . |               precondition a(v) is
. . . . . |               P)))))(a@0) ==> ∀v:1of(2of((with ds: ds
. . . . . |                                        init: init
. . . . . |                                       action a:T
. . . . . |                                        precondition a(v) is
. . . . . |                                        P)))(locl(a@0))?Top.
. . . . . |       ¬P@0((λx.s(i;t').x),v)
. . . . . 16. ∀t:ℕ.
. . . . . |   ¬isnull(a(i;t))
. . . . . |   ⇒
. . . . . |   (islocal(kind(a(i;t)))
. . . . . |    ⇒
. . . . . |    deq-member(IdDeq;act(kind(a(i;t)));1of(1of(
. . . . . |                                        2of(2of(2of(
. . . . . |                                        ...))))))
. . . . . |    ⇒
. . . . . |    2of(1of(2of(2of(2of((with ds: ds
. . . . . |              init: init
. . . . . |             action a:T
. . . . . |              precondition a(v) is
```

```
. . . . . |            P))))))
. . . . . |    (act(kind(a(i;t)))
. . . . . |    ,λx.s(i;t).x
. . . . . |    ,val(a(i;t))))
. . . . . |   & (∀x:Id.
. . . . . |      deq-member(product-deq(Knd;Id;KindDeq;IdDeq);<...
. . . . . |                                                  ,x>;...)
. . . . . |      ⇒
. . . . . |      s(i;t+1).x
. . . . . |      =
. . . . . |      2of(1of(2of(2of(2of(2of((with ds: ds
. . . . . |               init: init
. . . . . |              action a:T
. . . . . |               precondition a(v) is
. . . . . |               P)))))))
. . . . . |      (<kind(a(i;t)),x>
. . . . . |      ,λx.s(i;t).x
. . . . . |      ,val(a(i;t))))
. . . . . |   & (∀l:IdLnk.
. . . . . |      deq-member(product-deq(Knd;IdLnk;...;...);<kind(...)
. . . . . |                                               ,l>;...)
. . . . . |      ⇒
. . . . . |      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(1of(2of(2of(2of(2of(2of(
. . . . . |                                  (with ds: ds
. . . . . |                                   init: init
. . . . . |                                  action a:T
. . . . . |                                   precondition a(v) is
. . . . . |                                   P)))))))))
. . . . . |                            (<kind(a(i;t)),l>)))
. . . . . |      else nil fi)
. . . . . |   & (∀x:Id.
. . . . . |      ¬(deq-member(IdDeq;x;1of(1of(2of(2of(2of(2of(2of(2of(2of(
. . . . . |                                   (with ds: ds
. . . . . |                                    init: init
. . . . . |                                   action a:T
. . . . . |                                    precondition a(v) is
. . . . . |                                    P)))))))))))
. . . . . |        ⇒
. . . . . |        deq-member(KindDeq;kind(a(i;t));2of(
. . . . . |                                      1of(
. . . . . |                                      2of(2of(2of(2of(
. . . . . |                                      2of(2of(
. . . . . |                                      ...)))))))))
. . . . . |                                      (x)))
. . . . . |      ⇒
. . . . . |      s(i;t).x = s(i;t+1).x)
. . . . . |   & (∀l:IdLnk, tg:Id.
. . . . . |      ¬(deq-member(product-deq(IdLnk;Id;...;IdDeq);...;...)
```

```
. . . . . |        ⇒
. . . . . |        deq-member(KindDeq;kind(a(i;t));2of(
. . . . . |                                          1of(
. . . . . |                                          2of(2of(2of(2of(
. . . . . |                                          2of(2of(2of(
. . . . . |                                          ...)))))))))
. . . . . |                                          (<1,tg>)))
. . . . . |      ⇒
. . . . . |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . 17. ∀x:Id.
. . . . . |   deq-member(IdDeq;x;1of(1of(2of(2of((with ds: ds
. . . . . |                                  init: init
. . . . . |                                 action a:T
. . . . . |                                  precondition a(v) is
. . . . . |                                  P))))))
. . . . . |   ⇒
. . . . . |   s(i;0).x
. . . . . |   =
. . . . . |   2of(1of(2of(2of((with ds: ds
. . . . . |            init: init
. . . . . |           action a:T
. . . . . |            precondition a(v) is
. . . . . |            P)))))
. . . . . |   (x)
. . . . . 18. ∀a@0:Action(i).
. . . . . |   ¬isnull(a@0)
. . . . . |   ⇒
. . . . . |   (valtype(i;a@0) ⊆r 1of(2of((with ds: ds
. . . . . |                             init: init
. . . . . |                            action a:T
. . . . . |                             precondition a(v) is
. . . . . |                             P)))(kind(a@0))?Top)
. . . . . 19. ∀x:Id.
. . . . . |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(1of(
. . . . . |                                          ...)))→
. . . . . |                       2of(1of((with ds: ds
. . . . . |                            init: init
. . . . . |                           action a:T
. . . . . |                            precondition a(v) is
. . . . . |                            P)))
. . . . . |                      (x)
. . . . . |                  else Top fi
. . . . . 20. IdDeq ∈ EqDecider(Id)
. . . . . 21. (λx.init(x)?•) ∈ State(ds)
. . . . . 22. t' : ℕ
. . . . . 23. 0≤t'
. . . . . 24. True ⇒ (∀v:T. ¬P((λx.s(i;t').x),v))
. . . . . 25. ¬(∃t:ℕt'. ¬isnull(a(i;t)))
. . . . . 26. ¬P((λx.s(i;t').x),v)
. . . . . ⊢  ∃e:E. loc(e) = i  by Analyze -1
. . . . . |
. . . . . 1. i : Id
. . . . . 2. a : Id
. . . . . 3. T : Type
. . . . . 4. ds : x:Id fp-> Type
```

```
. . . . . 5. P : State(ds)→T→Prop
. . . . . 6. init : x:Id fp-> ds(x)?Void
. . . . . 7. ∀x:Id. x ∈ dom(ds) ⇒ x ∈ dom(init)
. . . . . 8. v : T
. . . . . 9. P((λx.init(x)?•),v)
. . . . . 10. w : World
. . . . . 11. FairFifo
. . . . . 12. FairFifo
. . . . . 13. ∀l:IdLnk, tg:Id.
. . . . . |   (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . |                     (with ds: ds
. . . . . |                      init: init
. . . . . |                     action a:T
. . . . . |                      precondition a(v) is
. . . . . |                      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(1of(2of((with ds: ds
. . . . . |                              init: init
. . . . . |                             action a:T
. . . . . |                              precondition a(v) is
. . . . . |                              P))))
. . . . . |     ∨ P@0 != 1of(
. . . . . |              2of(2of(2of((with ds: ds
. . . . . |               init: init
. . . . . |              action a:T
. . . . . |               precondition a(v) is
. . . . . |               P)))))(a@0) ==> ∀v:1of(2of((with ds: ds
. . . . . |                                        init: init
. . . . . |                                       action a:T
. . . . . |                                        precondition a(v) is
. . . . . |                                        P)))(locl(a@0))?Top.
. . . . . |       ¬P@0((λx.s(i;t').x),v)
. . . . . 16. ∀t:ℕ.
. . . . . |   ¬isnull(a(i;t))
. . . . . |   ⇒
. . . . . |   (islocal(kind(a(i;t)))
. . . . . |    ⇒
. . . . . |    deq-member(IdDeq;act(kind(a(i;t)));1of(1of(
. . . . . |                                        2of(2of(2of(
. . . . . |                                        ...))))))
. . . . . |    ⇒
. . . . . |    2of(1of(2of(2of(2of((with ds: ds
. . . . . |              init: init
. . . . . |             action a:T
. . . . . |              precondition a(v) is
. . . . . |              P))))))
. . . . . |    (act(kind(a(i;t)))
. . . . . |    ,λx.s(i;t).x
. . . . . |    ,val(a(i;t))))
. . . . . |   & (∀x:Id.
```

```
. . . . . |      deq-member(product-deq(Knd;Id;KindDeq;IdDeq);<...
. . . . . |                                                  ,x>;...)
. . . . . |      ⇒
. . . . . |      s(i;t+1).x
. . . . . |      =
. . . . . |      2of(1of(2of(2of(2of(2of((with ds: ds
. . . . . |               init: init
. . . . . |              action a:T
. . . . . |               precondition a(v) is
. . . . . |               P)))))))
. . . . . |      (<kind(a(i;t)),x>
. . . . . |      ,λx.s(i;t).x
. . . . . |      ,val(a(i;t))))
. . . . . |   & (∀l:IdLnk.
. . . . . |      deq-member(product-deq(Knd;IdLnk;...;...);<kind(...)
. . . . . |                                               ,l>;...)
. . . . . |      ⇒
. . . . . |      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(1of(2of(2of(2of(2of(2of(
. . . . . |                                    (with ds: ds
. . . . . |                                     init: init
. . . . . |                                    action a:T
. . . . . |                                     precondition a(v) is
. . . . . |                                     P)))))))))
. . . . . |                              (<kind(a(i;t)),l>)))
. . . . . |      else nil fi)
. . . . . |   & (∀x:Id.
. . . . . |      ¬(deq-member(IdDeq;x;1of(1of(2of(2of(2of(2of(2of(2of(
. . . . . |                                    (with ds: ds
. . . . . |                                     init: init
. . . . . |                                    action a:T
. . . . . |                                     precondition a(v) is
. . . . . |                                     P)))))))))))
. . . . . |        ⇒
. . . . . |        deq-member(KindDeq;kind(a(i;t));2of(
. . . . . |                                        1of(
. . . . . |                                        2of(2of(2of(2of(
. . . . . |                                        2of(2of(
. . . . . |                                        ...)))))))))
. . . . . |                                        (x)))
. . . . . |      ⇒
. . . . . |      s(i;t).x = s(i;t+1).x)
. . . . . |   & (∀l:IdLnk, tg:Id.
. . . . . |      ¬(deq-member(product-deq(IdLnk;Id;...;IdDeq);...;...)
. . . . . |        ⇒
. . . . . |        deq-member(KindDeq;kind(a(i;t));2of(
. . . . . |                                        1of(
. . . . . |                                        2of(2of(2of(2of(
. . . . . |                                        2of(2of(2of(
```

```
. . . . . |                                          ...))))))))))
. . . . . |                                          (<l,tg>)))
. . . . . |      ⇒
. . . . . |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . 17. ∀x:Id.
. . . . . |   deq-member(IdDeq;x;1of(1of(2of(2of((with ds: ds
. . . . . |                                  init: init
. . . . . |                                action a:T
. . . . . |                                 precondition a(v) is
. . . . . |                                 P))))))
. . . . . |   ⇒
. . . . . |   s(i;0).x
. . . . . |   =
. . . . . |   2of(1of(2of(2of((with ds: ds
. . . . . |            init: init
. . . . . |           action a:T
. . . . . |            precondition a(v) is
. . . . . |            P)))))
. . . . . |   (x)
. . . . . 18. ∀a@0:Action(i).
. . . . . |   ¬isnull(a@0)
. . . . . |   ⇒
. . . . . |   (valtype(i;a@0) ⊆r 1of(2of((with ds: ds
. . . . . |                            init: init
. . . . . |                           action a:T
. . . . . |                            precondition a(v) is
. . . . . |                            P)))(kind(a@0))?Top)
. . . . . 19. ∀x:Id.
. . . . . |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(1of(
. . . . . |                                              ...)))→
. . . . . |                       2of(1of((with ds: ds
. . . . . |                            init: init
. . . . . |                           action a:T
. . . . . |                            precondition a(v) is
. . . . . |                            P)))
. . . . . |                       (x)
. . . . . |                    else Top fi
. . . . . 20. IdDeq ∈ EqDecider(Id)
. . . . . 21. (λx.init(x)?•) ∈ State(ds)
. . . . . 22. t' : ℕ
. . . . . 23. 0≤t'
. . . . . 24. True ⇒ (∀v:T. ¬P((λx.s(i;t').x),v))
. . . . . 25. ¬(∃t:ℕt'. ¬isnull(a(i;t)))
. . . . . ⊢  P((λx.s(i;t').x),v)  by NthHypEq 9
. . . . . |
. . . . . .....assertion .....
. . . . . 1. i : Id
. . . . . 2. a : Id
. . . . . 3. T : Type
. . . . . 4. ds : x:Id fp-> Type
. . . . . 5. P : State(ds)→T→Prop
. . . . . 6. init : x:Id fp-> ds(x)?Void
. . . . . 7. ∀x:Id. x ∈ dom(ds) ⇒ x ∈ dom(init)
. . . . . 8. v : T
. . . . . 9. P((λx.init(x)?•),v)
```

```
. . . . . 10. w : World
. . . . . 11. FairFifo
. . . . . 12. FairFifo
. . . . . 13. ∀l:IdLnk, tg:Id.
. . . . . |   (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . |                     (with ds: ds
. . . . . |                      init: init
. . . . . |                     action a:T
. . . . . |                      precondition a(v) is
. . . . . |                      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(1of(2of((with ds: ds
. . . . . |                               init: init
. . . . . |                              action a:T
. . . . . |                               precondition a(v) is
. . . . . |                               P))))
. . . . . |     ∨ P@0 != 1of(
. . . . . |              2of(2of(2of((with ds: ds
. . . . . |               init: init
. . . . . |              action a:T
. . . . . |               precondition a(v) is
. . . . . |               P)))))(a@0) ==> ∀v:1of(2of((with ds: ds
. . . . . |                                        init: init
. . . . . |                                       action a:T
. . . . . |                                        precondition a(v) is
. . . . . |                                        P)))(locl(a@0))?Top.
. . . . . |       ¬P@0((λx.s(i;t').x),v)
. . . . . 16. ∀t:ℕ.
. . . . . |   ¬isnull(a(i;t))
. . . . . |   ⇒
. . . . . |   (islocal(kind(a(i;t)))
. . . . . |    ⇒
. . . . . |    deq-member(IdDeq;act(kind(a(i;t)));1of(1of(
. . . . . |                                        2of(2of(2of(
. . . . . |                                        ...))))))
. . . . . |    ⇒
. . . . . |    2of(1of(2of(2of(2of((with ds: ds
. . . . . |              init: init
. . . . . |             action a:T
. . . . . |              precondition a(v) is
. . . . . |              P))))))
. . . . . |    (act(kind(a(i;t)))
. . . . . |    ,λx.s(i;t).x
. . . . . |    ,val(a(i;t))))
. . . . . |   & (∀x:Id.
. . . . . |      deq-member(product-deq(Knd;Id;KindDeq;IdDeq);<...
. . . . . |                                                   ,x>;...)
. . . . . |      ⇒
. . . . . |      s(i;t+1).x
. . . . . |      =
```

```
. . . . . |      2of(1of(2of(2of(2of(2of(2of((with ds: ds
. . . . . |               init: init
. . . . . |              action a:T
. . . . . |               precondition a(v) is
. . . . . |               P)))))))
. . . . . |      (<kind(a(i;t)),x>
. . . . . |      ,λx.s(i;t).x
. . . . . |      ,val(a(i;t))))
. . . . . |   & (∀l:IdLnk.
. . . . . |      deq-member(product-deq(Knd;IdLnk;...;...);<kind(...)
. . . . . |                                                ,l>;...)
. . . . . |      ⇒
. . . . . |      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(1of(2of(2of(2of(2of(2of(
. . . . . |                                  (with ds: ds
. . . . . |                                   init: init
. . . . . |                                  action a:T
. . . . . |                                   precondition a(v) is
. . . . . |                                   P)))))))))
. . . . . |                             (<kind(a(i;t)),l>)))
. . . . . |      else nil fi)
. . . . . |   & (∀x:Id.
. . . . . |      ¬(deq-member(IdDeq;x;1of(1of(2of(2of(2of(2of(2of(2of(2of(
. . . . . |                                   (with ds: ds
. . . . . |                                    init: init
. . . . . |                                   action a:T
. . . . . |                                    precondition a(v) is
. . . . . |                                    P)))))))))))
. . . . . |        ⇒
. . . . . |        deq-member(KindDeq;kind(a(i;t));2of(
. . . . . |                                      1of(
. . . . . |                                      2of(2of(2of(2of(
. . . . . |                                      2of(2of(
. . . . . |                                      ...)))))))))
. . . . . |                                      (x)))
. . . . . |      ⇒
. . . . . |      s(i;t).x = s(i;t+1).x)
. . . . . |   & (∀l:IdLnk, tg:Id.
. . . . . |      ¬(deq-member(product-deq(IdLnk;Id;...;IdDeq);...;...)
. . . . . |        ⇒
. . . . . |        deq-member(KindDeq;kind(a(i;t));2of(
. . . . . |                                      1of(
. . . . . |                                      2of(2of(2of(2of(
. . . . . |                                      2of(2of(2of(
. . . . . |                                      ...)))))))))
. . . . . |                                      (<l,tg>)))
. . . . . |      ⇒
. . . . . |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . 17. ∀x:Id.
```

```
. . . . . |   deq-member(IdDeq;x;1of(1of(2of(2of((with ds: ds
. . . . . |                                  init: init
. . . . . |                                 action a:T
. . . . . |                                  precondition a(v) is
. . . . . |                                  P))))))
. . . . . |   ⇒
. . . . . |   s(i;0).x
. . . . . |   =
. . . . . |   2of(1of(2of(2of((with ds: ds
. . . . . |            init: init
. . . . . |           action a:T
. . . . . |            precondition a(v) is
. . . . . |            P)))))
. . . . . |   (x)
. . . . . 18. ∀a@0:Action(i).
. . . . . |   ¬isnull(a@0)
. . . . . |   ⇒
. . . . . |   (valtype(i;a@0) ⊆r 1of(2of((with ds: ds
. . . . . |                             init: init
. . . . . |                            action a:T
. . . . . |                             precondition a(v) is
. . . . . |                             P)))(kind(a@0))?Top)
. . . . . 19. ∀x:Id.
. . . . . |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(1of(
. . . . . |                                                ...)))→
. . . . . |                       2of(1of((with ds: ds
. . . . . |                            init: init
. . . . . |                           action a:T
. . . . . |                            precondition a(v) is
. . . . . |                            P)))
. . . . . |                      (x)
. . . . . |                    else Top fi
. . . . . 20. IdDeq ∈ EqDecider(Id)
. . . . . 21. (λx.init(x)?•) ∈ State(ds)
. . . . . 22. t' : ℕ
. . . . . 23. 0≤t'
. . . . . 24. True ⇒ (∀v:T. ¬P((λx.s(i;t').x),v))
. . . . . 25. ¬(∃t:ℕt'. ¬isnull(a(i;t)))
. . . . . ⊢  P((λx.s(i;t').x),v) = P((λx.init(x)?•),v)
. . . . . | by RepeatFor 2 Analyze
. . . . . |
. . . . . .....subterm .....
. . . . . 1. i : Id
. . . . . 2. a : Id
. . . . . 3. T : Type
. . . . . 4. ds : x:Id fp-> Type
. . . . . 5. P : State(ds)→T→Prop
. . . . . 6. init : x:Id fp-> ds(x)?Void
. . . . . 7. ∀x:Id. x ∈ dom(ds) ⇒ x ∈ dom(init)
. . . . . 8. v : T
. . . . . 9. P((λx.init(x)?•),v)
. . . . . 10. w : World
. . . . . 11. FairFifo
. . . . . 12. FairFifo
. . . . . 13. ∀l:IdLnk, tg:Id.
```

```
. . . . . |   (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . |                     (with ds: ds
. . . . . |                      init: init
. . . . . |                     action a:T
. . . . . |                      precondition a(v) is
. . . . . |                      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(1of(2of((with ds: ds
. . . . . |                               init: init
. . . . . |                              action a:T
. . . . . |                               precondition a(v) is
. . . . . |                               P))))
. . . . . |     ∨ P@0 != 1of(
. . . . . |              2of(2of(2of((with ds: ds
. . . . . |               init: init
. . . . . |              action a:T
. . . . . |               precondition a(v) is
. . . . . |               P)))))(a@0) ==> ∀v:1of(2of((with ds: ds
. . . . . |                                        init: init
. . . . . |                                       action a:T
. . . . . |                                        precondition a(v) is
. . . . . |                                        P)))(locl(a@0))?Top.

. . . . . |       ¬P@0((λx.s(i;t').x),v)
. . . . . 16. ∀t:ℕ.
. . . . . |   ¬isnull(a(i;t))
. . . . . |   ⇒
. . . . . |   (islocal(kind(a(i;t)))
. . . . . |    ⇒
. . . . . |    deq-member(IdDeq;act(kind(a(i;t)));1of(1of(
. . . . . |                                        2of(2of(2of(
. . . . . |                                        ...))))))
. . . . . |    ⇒
. . . . . |    2of(1of(2of(2of(2of((with ds: ds
. . . . . |              init: init
. . . . . |             action a:T
. . . . . |              precondition a(v) is
. . . . . |              P))))))
. . . . . |    (act(kind(a(i;t)))
. . . . . |    ,λx.s(i;t).x
. . . . . |    ,val(a(i;t))))
. . . . . |   & (∀x:Id.
. . . . . |      deq-member(product-deq(Knd;Id;KindDeq;IdDeq);<...
. . . . . |                                                  ,x>;...)
. . . . . |      ⇒
. . . . . |      s(i;t+1).x
. . . . . |      =
. . . . . |      2of(1of(2of(2of(2of(2of((with ds: ds
. . . . . |               init: init
. . . . . |              action a:T
. . . . . |               precondition a(v) is
```

```
. . . . . |               P)))))))
. . . . . |      (<kind(a(i;t)),x>
. . . . . |      ,λx.s(i;t).x
. . . . . |      ,val(a(i;t))))
. . . . . |   & (∀l:IdLnk.
. . . . . |      deq-member(product-deq(Knd;IdLnk;...;...);<kind(...)
. . . . . |                                                ,l>;...)
. . . . . |      ⇒
. . . . . |      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(1of(2of(2of(2of(2of(2of(
. . . . . |                                  (with ds: ds
. . . . . |                                   init: init
. . . . . |                                  action a:T
. . . . . |                                   precondition a(v) is
. . . . . |                                   P)))))))))
. . . . . |                           (<kind(a(i;t)),l>)))
. . . . . |      else nil fi)
. . . . . |   & (∀x:Id.
. . . . . |      ¬(deq-member(IdDeq;x;1of(1of(2of(2of(2of(2of(2of(2of(2of(
. . . . . |                                  (with ds: ds
. . . . . |                                   init: init
. . . . . |                                  action a:T
. . . . . |                                   precondition a(v) is
. . . . . |                                   P)))))))))))
. . . . . |        ⇒
. . . . . |        deq-member(KindDeq;kind(a(i;t));2of(
. . . . . |                                      1of(
. . . . . |                                      2of(2of(2of(2of(
. . . . . |                                      2of(2of(
. . . . . |                                      ...)))))))))
. . . . . |                                      (x)))
. . . . . |      ⇒
. . . . . |      s(i;t).x = s(i;t+1).x)
. . . . . |   & (∀l:IdLnk, tg:Id.
. . . . . |      ¬(deq-member(product-deq(IdLnk;Id;...;IdDeq);...;...)
. . . . . |        ⇒
. . . . . |        deq-member(KindDeq;kind(a(i;t));2of(
. . . . . |                                      1of(
. . . . . |                                      2of(2of(2of(2of(
. . . . . |                                      2of(2of(2of(
. . . . . |                                      ...)))))))))
. . . . . |                                      (<l,tg>)))
. . . . . |      ⇒
. . . . . |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . 17. ∀x:Id.
. . . . . |   deq-member(IdDeq;x;1of(1of(2of(2of((with ds: ds
. . . . . |                                  init: init
. . . . . |                                 action a:T
. . . . . |                                  precondition a(v) is
```

```
. . . . . |                                P)))))))
. . . . . |   ⇒
. . . . . |   s(i;0).x
. . . . . |   =
. . . . . |   2of(1of(2of(2of((with ds: ds
. . . . . |            init: init
. . . . . |           action a:T
. . . . . |            precondition a(v) is
. . . . . |            P)))))
. . . . . |   (x)
. . . . . 18. ∀a@0:Action(i).
. . . . . |   ¬isnull(a@0)
. . . . . |   ⇒
. . . . . |   (valtype(i;a@0) ⊆r 1of(2of((with ds: ds
. . . . . |                            init: init
. . . . . |                           action a:T
. . . . . |                            precondition a(v) is
. . . . . |                            P)))(kind(a@0))?Top)
. . . . . 19. ∀x:Id.
. . . . . |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(1of(
. . . . . |                                          ...)))→
. . . . . |                       2of(1of((with ds: ds
. . . . . |                            init: init
. . . . . |                           action a:T
. . . . . |                            precondition a(v) is
. . . . . |                            P)))
. . . . . |                      (x)
. . . . . |                    else Top fi
. . . . . 20. IdDeq ∈ EqDecider(Id)
. . . . . 21. (λx.init(x)?•) ∈ State(ds)
. . . . . 22. t' : ℕ
. . . . . 23. 0≤t'
. . . . . 24. True ⇒ (∀v:T. ¬P((λx.s(i;t').x),v))
. . . . . 25. ¬(∃t:ℕt'. ¬isnull(a(i;t)))
. . . . . ⊢  (λx.s(i;t').x) = (λx.init(x)?•)
. . . . . | by Subst ((λx.s(i;t').x) = (λx.s(i;0).x)) 0
. . . . . |
. . . . . |\
. . . . . | .....equality .....
. . . . . | 1. i : Id
. . . . . | 2. a : Id
. . . . . | 3. T : Type
. . . . . | 4. ds : x:Id fp-> Type
. . . . . | 5. P : State(ds)→T→Prop
. . . . . | 6. init : x:Id fp-> ds(x)?Void
. . . . . | 7. ∀x:Id. x ∈ dom(ds) ⇒ x ∈ dom(init)
. . . . . | 8. v : T
. . . . . | 9. P((λx.init(x)?•),v)
. . . . . | 10. w : World
. . . . . | 11. FairFifo
. . . . . | 12. FairFifo
. . . . . | 13. ∀l:IdLnk, tg:Id.
. . . . . | |   (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | |                    (with ds: ds
. . . . . | |                     init: init
```

```
. . . . . | |                    action a:T
. . . . . | |                     precondition a(v) is
. . . . . | |                     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(1of(2of((with ds: ds
. . . . . | |                              init: init
. . . . . | |                             action a:T
. . . . . | |                              precondition a(v) is
. . . . . | |                              P))))
. . . . . | |     ∨ P@0 != 1of(
. . . . . | |              2of(2of(2of((with ds: ds
. . . . . | |               init: init
. . . . . | |              action a:T
. . . . . | |               precondition a(v) is
. . . . . | |               P)))))(a@0) ==> ∀v:1of(
. . . . . | |                                  2of((with ds: ds
. . . . . | |                                   init: init
. . . . . | |                                  action a:T
. . . . . | |                                   precondition a(v) is
. . . . . | |                                   P)))(locl(a@0))?Top.
. . . . . | |       ¬P@0((λx.s(i;t').x),v)
. . . . . | 16. ∀t:ℕ.
. . . . . | |   ¬isnull(a(i;t))
. . . . . | |   ⇒
. . . . . | |   (islocal(kind(a(i;t)))
. . . . . | |    ⇒
. . . . . | |    deq-member(IdDeq;act(kind(a(i;t)));1of(1of(
. . . . . | |                                       2of(2of(2of(
. . . . . | |                                       ...))))))
. . . . . | |    ⇒
. . . . . | |    2of(1of(2of(2of(2of((with ds: ds
. . . . . | |             init: init
. . . . . | |            action a:T
. . . . . | |             precondition a(v) is
. . . . . | |             P))))))
. . . . . | |    (act(kind(a(i;t)))
. . . . . | |    ,λx.s(i;t).x
. . . . . | |    ,val(a(i;t))))
. . . . . | |   & (∀x:Id.
. . . . . | |      deq-member(product-deq(Knd;Id;KindDeq;...);<...
. . . . . | |                                                 ,x>;...)
. . . . . | |      ⇒
. . . . . | |      s(i;t+1).x
. . . . . | |      =
. . . . . | |      2of(1of(2of(2of(2of(2of((with ds: ds
. . . . . | |               init: init
. . . . . | |              action a:T
. . . . . | |               precondition a(v) is
. . . . . | |               P)))))))
. . . . . | |      (<kind(a(i;t)),x>
```

```
. . . . . | |      ,λx.s(i;t).x
. . . . . | |      ,val(a(i;t))))
. . . . . | |   & (∀l:IdLnk.
. . . . . | |      deq-member(product-deq(Knd;IdLnk;...;...);<...
. . . . . | |                                                ,l>;...)
. . . . . | |      ⇒
. . . . . | |      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(1of(2of(2of(2of(2of(2of(
. . . . . | |                                  (with ds: ds
. . . . . | |                                   init: init
. . . . . | |                                  action a:T
. . . . . | |                                   precondition a(v) is
. . . . . | |                                   P)))))))
. . . . . | |                            (<kind(a(i;t)),l>)))
. . . . . | |      else nil fi)
. . . . . | |   & (∀x:Id.
. . . . . | |      ¬(deq-member(IdDeq;x;1of(1of(2of(2of(2of(2of(2of(
. . . . . | |                                  2of((with ds: ds
. . . . . | |                                   init: init
. . . . . | |                                  action a:T
. . . . . | |                                   precondition a(v) is
. . . . . | |                                   P)))))))))
. . . . . | |        ⇒
. . . . . | |        deq-member(KindDeq;kind(a(i;t));2of(
. . . . . | |                                      1of(
. . . . . | |                                      2of(2of(2of(2of(
. . . . . | |                                      2of(2of(
. . . . . | |                                      ...)))))))
. . . . . | |                                      (x)))
. . . . . | |      ⇒
. . . . . | |      s(i;t).x = s(i;t+1).x)
. . . . . | |   & (∀l:IdLnk, tg:Id.
. . . . . | |      ¬(deq-member(product-deq(IdLnk;Id;...;...);...;...)
. . . . . | |        ⇒
. . . . . | |        deq-member(KindDeq;kind(a(i;t));2of(
. . . . . | |                                      1of(
. . . . . | |                                      2of(2of(2of(2of(
. . . . . | |                                      2of(2of(2of(
. . . . . | |                                      ...)))))))))
. . . . . | |                                      (<l,tg>)))
. . . . . | |      ⇒
. . . . . | |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . | 17. ∀x:Id.
. . . . . | |   deq-member(IdDeq;x;1of(1of(2of(2of((with ds: ds
. . . . . | |                                  init: init
. . . . . | |                                 action a:T
. . . . . | |                                  precondition a(v) is
. . . . . | |                                  P))))))
. . . . . | |   ⇒
```

```
. . . . . | |   s(i;0).x
. . . . . | |   =
. . . . . | |   2of(1of(2of(2of((with ds: ds
. . . . . | |            init: init
. . . . . | |           action a:T
. . . . . | |            precondition a(v) is
. . . . . | |            P)))))
. . . . . | |   (x)
. . . . . | 18. ∀a@0:Action(i).
. . . . . | |   ¬isnull(a@0)
. . . . . | |   ⇒
. . . . . | |   (valtype(i;a@0) ⊆r 1of(2of((with ds: ds
. . . . . | |                           init: init
. . . . . | |                          action a:T
. . . . . | |                           precondition a(v) is
. . . . . | |                           P)))(kind(a@0))?Top)
. . . . . | 19. ∀x:Id.
. . . . . | |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(1of(
. . . . . | |                                          ...)))→
. . . . . | |                      2of(1of((with ds: ds
. . . . . | |                           init: init
. . . . . | |                          action a:T
. . . . . | |                           precondition a(v) is
. . . . . | |                           P)))
. . . . . | |                     (x)
. . . . . | |                  else Top fi
. . . . . | 20. IdDeq ∈ EqDecider(Id)
. . . . . | 21. (λx.init(x)?•) ∈ State(ds)
. . . . . | 22. t' : ℕ
. . . . . | 23. 0≤t'
. . . . . | 24. True ⇒ (∀v:T. ¬P((λx.s(i;t').x),v))
. . . . . | 25. ¬(∃t:ℕt'. ¬isnull(a(i;t)))
. . . . . | ⊢  (λx.s(i;t').x) = (λx.s(i;0).x)
. . . . . | | by 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. init : x:Id fp-> ds(x)?Void
. . . . . | 7. ∀x:Id. x ∈ dom(ds) ⇒ x ∈ dom(init)
. . . . . | 8. v : T
. . . . . | 9. P((λx.init(x)?•),v)
. . . . . | 10. w : World
. . . . . | 11. FairFifo
. . . . . | 12. FairFifo
. . . . . | 13. ∀l:IdLnk, tg:Id.
. . . . . | |   (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | |                    (with ds: ds
. . . . . | |                     init: init
. . . . . | |                    action a:T
. . . . . | |                     precondition a(v) is
. . . . . | |                     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(1of(2of((with ds: ds
. . . . . | |                                 init: init
. . . . . | |                                action a:T
. . . . . | |                                 precondition a(v) is
. . . . . | |                                 P))))
. . . . . | |     ∨ P@0 != 1of(
. . . . . | |               2of(2of(2of((with ds: ds
. . . . . | |                init: init
. . . . . | |               action a:T
. . . . . | |                precondition a(v) is
. . . . . | |                P)))))(a@0) ==> ∀v:1of(
. . . . . | |                                      2of((with ds: ds
. . . . . | |                                       init: init
. . . . . | |                                      action a:T
. . . . . | |                                       precondition a(v) is
. . . . . | |                                       P)))(locl(a@0))?Top.
. . . . . | |       ¬P@0((λx.s(i;t').x),v)
. . . . . | 16. ∀t:ℕ.
. . . . . | |   ¬isnull(a(i;t))
. . . . . | |   ⇒
. . . . . | |   (islocal(kind(a(i;t)))
. . . . . | |    ⇒
. . . . . | |    deq-member(IdDeq;act(kind(a(i;t)));1of(1of(
. . . . . | |                                         2of(2of(2of(
. . . . . | |                                         ...))))))
. . . . . | |    ⇒
. . . . . | |    2of(1of(2of(2of(2of((with ds: ds
. . . . . | |              init: init
. . . . . | |             action a:T
. . . . . | |              precondition a(v) is
. . . . . | |              P))))))
. . . . . | |    (act(kind(a(i;t)))
. . . . . | |    ,λx.s(i;t).x
. . . . . | |    ,val(a(i;t))))
. . . . . | |   & (∀x:Id.
. . . . . | |      deq-member(product-deq(Knd;Id;KindDeq;...);<...
. . . . . | |                                                 ,x>;...)
. . . . . | |      ⇒
. . . . . | |      s(i;t+1).x
. . . . . | |      =
. . . . . | |      2of(1of(2of(2of(2of(2of((with ds: ds
. . . . . | |                init: init
. . . . . | |               action a:T
. . . . . | |                precondition a(v) is
. . . . . | |                P)))))))
. . . . . | |      (<kind(a(i;t)),x>
. . . . . | |      ,λx.s(i;t).x
. . . . . | |      ,val(a(i;t))))
. . . . . | |   & (∀l:IdLnk.
```

```
. . . . . | |      deq-member(product-deq(Knd;IdLnk;...;...);<...
. . . . . | |                                                ,l>;...)
. . . . . | |      ⇒
. . . . . | |      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(1of(2of(2of(2of(2of(2of(
. . . . . | |                                  (with ds: ds
. . . . . | |                                   init: init
. . . . . | |                                  action a:T
. . . . . | |                                   precondition a(v) is
. . . . . | |                                   P)))))))))
. . . . . | |                              (<kind(a(i;t)),l>)))
. . . . . | |      else nil fi)
. . . . . | |   & (∀x:Id.
. . . . . | |      ¬(deq-member(IdDeq;x;1of(1of(2of(2of(2of(2of(2of(
. . . . . | |                                  2of((with ds: ds
. . . . . | |                                   init: init
. . . . . | |                                  action a:T
. . . . . | |                                   precondition a(v) is
. . . . . | |                                   P)))))))))))
. . . . . | |        ⇒
. . . . . | |        deq-member(KindDeq;kind(a(i;t));2of(
. . . . . | |                                      1of(
. . . . . | |                                      2of(2of(2of(2of(
. . . . . | |                                      2of(2of(
. . . . . | |                                      ...)))))))))
. . . . . | |                                      (x)))
. . . . . | |      ⇒
. . . . . | |      s(i;t).x = s(i;t+1).x)
. . . . . | |   & (∀l:IdLnk, tg:Id.
. . . . . | |      ¬(deq-member(product-deq(IdLnk;Id;...;...);...;...)
. . . . . | |        ⇒
. . . . . | |        deq-member(KindDeq;kind(a(i;t));2of(
. . . . . | |                                      1of(
. . . . . | |                                      2of(2of(2of(2of(
. . . . . | |                                      2of(2of(2of(
. . . . . | |                                      ...)))))))))
. . . . . | |                                      (<l,tg>)))
. . . . . | |      ⇒
. . . . . | |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . | 17. ∀x:Id.
. . . . . | |   deq-member(IdDeq;x;1of(1of(2of(2of((with ds: ds
. . . . . | |                               init: init
. . . . . | |                              action a:T
. . . . . | |                               precondition a(v) is
. . . . . | |                               P))))))
. . . . . | |   ⇒
. . . . . | |   s(i;0).x
. . . . . | |   =
. . . . . | |   2of(1of(2of(2of((with ds: ds
```

```
. . . . . | |            init: init
. . . . . | |           action a:T
. . . . . | |            precondition a(v) is
. . . . . | |            P)))))
. . . . . | |   (x)
. . . . . | 18. ∀a@0:Action(i).
. . . . . | |   ¬isnull(a@0)
. . . . . | |   ⇒
. . . . . | |   (valtype(i;a@0) ⊆r 1of(2of((with ds: ds
. . . . . | |                              init: init
. . . . . | |                             action a:T
. . . . . | |                              precondition a(v) is
. . . . . | |                              P)))(kind(a@0))?Top)
. . . . . | 19. ∀x:Id.
. . . . . | |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(1of(
. . . . . | |                                              ...)))→
. . . . . | |                        2of(1of((with ds: ds
. . . . . | |                             init: init
. . . . . | |                            action a:T
. . . . . | |                             precondition a(v) is
. . . . . | |                             P)))
. . . . . | |                       (x)
. . . . . | |                    else Top fi
. . . . . | 20. IdDeq ∈ EqDecider(Id)
. . . . . | 21. (λx.init(x)?•) ∈ State(ds)
. . . . . | 22. t' : ℕ
. . . . . | 23. 0≤t'
. . . . . | 24. True ⇒ (∀v:T. ¬P((λx.s(i;t').x),v))
. . . . . | 25. ¬(∃t:ℕt'. ¬isnull(a(i;t)))
. . . . . | 26. x : Id
. . . . . | ⊢  s(i;t').x = s(i;0).x  by RenameTo 'z' 'x'
. . . . . | |
. . . . . | 1. i : Id
. . . . . | 2. a : Id
. . . . . | 3. T : Type
. . . . . | 4. ds : x:Id fp-> Type
. . . . . | 5. P : State(ds)→T→Prop
. . . . . | 6. init : x:Id fp-> ds(x)?Void
. . . . . | 7. ∀x:Id. x ∈ dom(ds) ⇒ x ∈ dom(init)
. . . . . | 8. v : T
. . . . . | 9. P((λx.init(x)?•),v)
. . . . . | 10. w : World
. . . . . | 11. FairFifo
. . . . . | 12. FairFifo
. . . . . | 13. ∀l:IdLnk, tg:Id.
. . . . . | |   (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | |                    (with ds: ds
. . . . . | |                     init: init
. . . . . | |                    action a:T
. . . . . | |                     precondition a(v) is
. . . . . | |                     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(1of(2of((with ds: ds
. . . . . | |                              init: init
. . . . . | |                             action a:T
. . . . . | |                              precondition a(v) is
. . . . . | |                              P))))
. . . . . | |     ∨ P@0 != 1of(
. . . . . | |              2of(2of(2of((with ds: ds
. . . . . | |               init: init
. . . . . | |              action a:T
. . . . . | |               precondition a(v) is
. . . . . | |               P)))))(a@0) ==> ∀v:1of(
. . . . . | |                                  2of((with ds: ds
. . . . . | |                                   init: init
. . . . . | |                                  action a:T
. . . . . | |                                   precondition a(v) is
. . . . . | |                                   P)))(locl(a@0))?Top.
. . . . . | |       ¬P@0((λx.s(i;t').x),v)
. . . . . | 16. ∀t:ℕ.
. . . . . | |   ¬isnull(a(i;t))
. . . . . | |   ⇒
. . . . . | |   (islocal(kind(a(i;t)))
. . . . . | |    ⇒
. . . . . | |    deq-member(IdDeq;act(kind(a(i;t)));1of(1of(
. . . . . | |                                       2of(2of(2of(
. . . . . | |                                       ...))))))
. . . . . | |    ⇒
. . . . . | |    2of(1of(2of(2of(2of((with ds: ds
. . . . . | |             init: init
. . . . . | |            action a:T
. . . . . | |             precondition a(v) is
. . . . . | |             P))))))
. . . . . | |    (act(kind(a(i;t)))
. . . . . | |    ,λx.s(i;t).x
. . . . . | |    ,val(a(i;t))))
. . . . . | |   & (∀x:Id.
. . . . . | |      deq-member(product-deq(Knd;Id;KindDeq;...);<...
. . . . . | |                                                ,x>;...)
. . . . . | |      ⇒
. . . . . | |      s(i;t+1).x
. . . . . | |      =
. . . . . | |      2of(1of(2of(2of(2of(2of((with ds: ds
. . . . . | |               init: init
. . . . . | |              action a:T
. . . . . | |               precondition a(v) is
. . . . . | |               P)))))))
. . . . . | |      (<kind(a(i;t)),x>
. . . . . | |      ,λx.s(i;t).x
. . . . . | |      ,val(a(i;t))))
. . . . . | |   & (∀l:IdLnk.
. . . . . | |      deq-member(product-deq(Knd;IdLnk;...;...);<...
. . . . . | |                                              ,l>;...)
. . . . . | |      ⇒
. . . . . | |      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(1of(2of(2of(2of(2of(2of(
. . . . . | |                                    (with ds: ds
. . . . . | |                                     init: init
. . . . . | |                                    action a:T
. . . . . | |                                     precondition a(v) is
. . . . . | |                                     P)))))))
. . . . . | |                               (<kind(a(i;t)),l>)))
. . . . . | |      else nil fi)
. . . . . | |   & (∀x:Id.
. . . . . | |      ¬(deq-member(IdDeq;x;1of(1of(2of(2of(2of(2of(2of(
. . . . . | |                                    2of((with ds: ds
. . . . . | |                                     init: init
. . . . . | |                                    action a:T
. . . . . | |                                     precondition a(v) is
. . . . . | |                                     P)))))))))
. . . . . | |        ⇒
. . . . . | |        deq-member(KindDeq;kind(a(i;t));2of(
. . . . . | |                                        1of(
. . . . . | |                                        2of(2of(2of(2of(
. . . . . | |                                        2of(2of(
. . . . . | |                                        ...))))))))
. . . . . | |                                        (x)))
. . . . . | |      ⇒
. . . . . | |      s(i;t).x = s(i;t+1).x)
. . . . . | |   & (∀l:IdLnk, tg:Id.
. . . . . | |      ¬(deq-member(product-deq(IdLnk;Id;...;...);...;...)
. . . . . | |        ⇒
. . . . . | |        deq-member(KindDeq;kind(a(i;t));2of(
. . . . . | |                                        1of(
. . . . . | |                                        2of(2of(2of(2of(
. . . . . | |                                        2of(2of(2of(
. . . . . | |                                        ...)))))))))
. . . . . | |                                        (<l,tg>)))
. . . . . | |      ⇒
. . . . . | |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . | 17. ∀x:Id.
. . . . . | |   deq-member(IdDeq;x;1of(1of(2of(2of((with ds: ds
. . . . . | |                                 init: init
. . . . . | |                                action a:T
. . . . . | |                                 precondition a(v) is
. . . . . | |                                 P))))))
. . . . . | |   ⇒
. . . . . | |   s(i;0).x
. . . . . | |   =
. . . . . | |   2of(1of(2of(2of((with ds: ds
. . . . . | |            init: init
. . . . . | |           action a:T
. . . . . | |            precondition a(v) is
. . . . . | |            P)))))
```

```
. . . . . | |   (x)
. . . . . | 18. ∀a@0:Action(i).
. . . . . | |   ¬isnull(a@0)
. . . . . | |   ⇒
. . . . . | |   (valtype(i;a@0) ⊆r 1of(2of((with ds: ds
. . . . . | |                              init: init
. . . . . | |                             action a:T
. . . . . | |                              precondition a(v) is
. . . . . | |                              P)))(kind(a@0))?Top)
. . . . . | 19. ∀x:Id.
. . . . . | |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(1of(
. . . . . | |                                              ...)))→
. . . . . | |                       2of(1of((with ds: ds
. . . . . | |                            init: init
. . . . . | |                           action a:T
. . . . . | |                            precondition a(v) is
. . . . . | |                            P)))
. . . . . | |                      (x)
. . . . . | |                   else Top fi
. . . . . | 20. IdDeq ∈ EqDecider(Id)
. . . . . | 21. (λx.init(x)?•) ∈ State(ds)
. . . . . | 22. t' : ℕ
. . . . . | 23. 0≤t'
. . . . . | 24. True ⇒ (∀v:T. ¬P((λx.s(i;t').x),v))
. . . . . | 25. ¬(∃t:ℕt'. ¬isnull(a(i;t)))
. . . . . | 26. z : Id
. . . . . | ⊢  s(i;t').z = s(i;0).z
. . . . . | | by Assert (∀t:ℕ. t≤t' ⇒ s(i;0).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. init : x:Id fp-> ds(x)?Void
. . . . . | 7. ∀x:Id. x ∈ dom(ds) ⇒ x ∈ dom(init)
. . . . . | 8. v : T
. . . . . | 9. P((λx.init(x)?•),v)
. . . . . | 10. w : World
. . . . . | 11. FairFifo
. . . . . | 12. FairFifo
. . . . . | 13. ∀l:IdLnk, tg:Id.
. . . . . | |   (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | |                     (with ds: ds
. . . . . | |                      init: init
. . . . . | |                     action a:T
. . . . . | |                      precondition a(v) is
. . . . . | |                      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(1of(2of((with ds: ds
. . . . . | |                              init: init
. . . . . | |                             action a:T
. . . . . | |                              precondition a(v) is
. . . . . | |                              P))))
. . . . . | |     ∨ P@0 != 1of(
. . . . . | |              2of(2of(2of((with ds: ds
. . . . . | |               init: init
. . . . . | |              action a:T
. . . . . | |               precondition a(v) is
. . . . . | |               P)))))(a@0) ==> ∀v:1of(
. . . . . | |                                  2of((with ds: ds
. . . . . | |                                   init: init
. . . . . | |                                  action a:T
. . . . . | |                                   precondition a(v) is
. . . . . | |                                   P)))(locl(a@0))?Top.
. . . . . | |       ¬P@0((λx.s(i;t').x),v)
. . . . . | 16. ∀t:ℕ.
. . . . . | |   ¬isnull(a(i;t))
. . . . . | |   ⇒
. . . . . | |   (islocal(kind(a(i;t)))
. . . . . | |    ⇒
. . . . . | |    deq-member(IdDeq;act(kind(a(i;t)));1of(1of(
. . . . . | |                                       2of(2of(2of(
. . . . . | |                                       ...))))))
. . . . . | |    ⇒
. . . . . | |    2of(1of(2of(2of(2of((with ds: ds
. . . . . | |             init: init
. . . . . | |            action a:T
. . . . . | |             precondition a(v) is
. . . . . | |             P))))))
. . . . . | |    (act(kind(a(i;t)))
. . . . . | |    ,λx.s(i;t).x
. . . . . | |    ,val(a(i;t))))
. . . . . | |   & (∀x:Id.
. . . . . | |      deq-member(product-deq(Knd;Id;KindDeq;...);<...
. . . . . | |                                                ,x>;...)
. . . . . | |      ⇒
. . . . . | |      s(i;t+1).x
. . . . . | |      =
. . . . . | |      2of(1of(2of(2of(2of(2of((with ds: ds
. . . . . | |               init: init
. . . . . | |              action a:T
. . . . . | |               precondition a(v) is
. . . . . | |               P)))))))
. . . . . | |      (<kind(a(i;t)),x>
. . . . . | |      ,λx.s(i;t).x
. . . . . | |      ,val(a(i;t))))
. . . . . | |   & (∀l:IdLnk.
. . . . . | |      deq-member(product-deq(Knd;IdLnk;...;...);<...
. . . . . | |                                              ,l>;...)
. . . . . | |      ⇒
. . . . . | |      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(1of(2of(2of(2of(2of(2of(
. . . . . | |                                    (with ds: ds
. . . . . | |                                     init: init
. . . . . | |                                    action a:T
. . . . . | |                                     precondition a(v) is
. . . . . | |                                     P)))))))
. . . . . | |                               (<kind(a(i;t)),l>)))
. . . . . | |      else nil fi)
. . . . . | |   & (∀x:Id.
. . . . . | |      ¬(deq-member(IdDeq;x;1of(1of(2of(2of(2of(2of(2of(
. . . . . | |                                    2of((with ds: ds
. . . . . | |                                     init: init
. . . . . | |                                    action a:T
. . . . . | |                                     precondition a(v) is
. . . . . | |                                     P)))))))))
. . . . . | |        ⇒
. . . . . | |        deq-member(KindDeq;kind(a(i;t));2of(
. . . . . | |                                        1of(
. . . . . | |                                        2of(2of(2of(2of(
. . . . . | |                                        2of(2of(
. . . . . | |                                        ...)))))))
. . . . . | |                                        (x)))
. . . . . | |      ⇒
. . . . . | |      s(i;t).x = s(i;t+1).x)
. . . . . | |   & (∀l:IdLnk, tg:Id.
. . . . . | |      ¬(deq-member(product-deq(IdLnk;Id;...;...);...;...)
. . . . . | |        ⇒
. . . . . | |        deq-member(KindDeq;kind(a(i;t));2of(
. . . . . | |                                        1of(
. . . . . | |                                        2of(2of(2of(2of(
. . . . . | |                                        2of(2of(2of(
. . . . . | |                                        ...)))))))))
. . . . . | |                                        (<l,tg>)))
. . . . . | |      ⇒
. . . . . | |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . | 17. ∀x:Id.
. . . . . | |   deq-member(IdDeq;x;1of(1of(2of(2of((with ds: ds
. . . . . | |                                  init: init
. . . . . | |                                 action a:T
. . . . . | |                                  precondition a(v) is
. . . . . | |                                  P))))))
. . . . . | |   ⇒
. . . . . | |   s(i;0).x
. . . . . | |   =
. . . . . | |   2of(1of(2of(2of((with ds: ds
. . . . . | |            init: init
. . . . . | |           action a:T
. . . . . | |            precondition a(v) is
. . . . . | |            P)))))
```

```
. . . . . | |   (x)
. . . . . | 18. ∀a@0:Action(i).
. . . . . | |   ¬isnull(a@0)
. . . . . | |   ⇒
. . . . . | |   (valtype(i;a@0) ⊆r 1of(2of((with ds: ds
. . . . . | |                            init: init
. . . . . | |                           action a:T
. . . . . | |                            precondition a(v) is
. . . . . | |                            P)))(kind(a@0))?Top)
. . . . . | 19. ∀x:Id.
. . . . . | |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(1of(
. . . . . | |                                          ...)))→
. . . . . | |                       2of(1of((with ds: ds
. . . . . | |                            init: init
. . . . . | |                           action a:T
. . . . . | |                            precondition a(v) is
. . . . . | |                            P)))
. . . . . | |                       (x)
. . . . . | |                   else Top fi
. . . . . | 20. IdDeq ∈ EqDecider(Id)
. . . . . | 21. (λx.init(x)?•) ∈ State(ds)
. . . . . | 22. t' : ℕ
. . . . . | 23. 0≤t'
. . . . . | 24. True ⇒ (∀v:T. ¬P((λx.s(i;t').x),v))
. . . . . | 25. ¬(∃t:ℕt'. ¬isnull(a(i;t)))
. . . . . | 26. z : Id
. . . . . | ⊢  ∀t:ℕ. t≤t' ⇒ s(i;0).z = s(i;t).z  by InductionOnNat
. . . . . | |
. . . . . | |\
. . . . . | | .....basecase .....
. . . . . | | 1. i : Id
. . . . . | | 2. a : Id
. . . . . | | 3. T : Type
. . . . . | | 4. ds : x:Id fp-> Type
. . . . . | | 5. P : State(ds)→T→Prop
. . . . . | | 6. init : x:Id fp-> ds(x)?Void
. . . . . | | 7. ∀x:Id. x ∈ dom(ds) ⇒ x ∈ dom(init)
. . . . . | | 8. v : T
. . . . . | | 9. P((λx.init(x)?•),v)
. . . . . | | 10. w : World
. . . . . | | 11. FairFifo
. . . . . | | 12. FairFifo
. . . . . | | 13. ∀l:IdLnk, tg:Id.
. . . . . | | |   (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | | |                    (with ds: ds
. . . . . | | |                     init: init
. . . . . | | |                    action a:T
. . . . . | | |                     precondition a(v) is
. . . . . | | |                     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(1of(2of((with ds: ds
. . . . . | | |                              init: init

. . . . . | | |                             action a:T
. . . . . | | |                              precondition a(v) is
. . . . . | | |                              P))))
. . . . . | | |     ∨ P@0 != 1of(
. . . . . | | |               2of(2of(2of((with ds: ds
. . . . . | | |                init: init
. . . . . | | |               action a:T
. . . . . | | |                precondition a(v) is
. . . . . | | |                P)))))(a@0) ==> ∀v:1of(
. . . . . | | |                                    2of((with ds: ds
. . . . . | | |                                     init: init
. . . . . | | |                                    action a:T
. . . . . | | |                                     precondition a(v) is
. . . . . | | |                                     P)))(locl(a@0))?Top.
. . . . . | | |       ¬P@0((λx.s(i;t').x),v)
. . . . . | | 16. ∀t:ℕ.
. . . . . | | |   ¬isnull(a(i;t))
. . . . . | | |   ⇒
. . . . . | | |   (islocal(kind(a(i;t)))
. . . . . | | |    ⇒
. . . . . | | |    deq-member(IdDeq;act(kind(a(i;t)));1of(1of(
. . . . . | | |                                        2of(2of(2of(
. . . . . | | |                                        ...))))))
. . . . . | | |    ⇒
. . . . . | | |    2of(1of(2of(2of(2of((with ds: ds
. . . . . | | |              init: init
. . . . . | | |             action a:T
. . . . . | | |              precondition a(v) is
. . . . . | | |              P))))))
. . . . . | | |    (act(kind(a(i;t)))
. . . . . | | |    ,λx.s(i;t).x
. . . . . | | |    ,val(a(i;t))))
. . . . . | | |   & (∀x:Id.
. . . . . | | |      deq-member(product-deq(Knd;Id;...;IdDeq);<...
. . . . . | | |                                                ,x>;...)
. . . . . | | |      ⇒
. . . . . | | |      s(i;t+1).x
. . . . . | | |      =
. . . . . | | |      2of(1of(2of(2of(2of(2of((with ds: ds
. . . . . | | |                init: init
. . . . . | | |               action a:T
. . . . . | | |                precondition a(v) is
. . . . . | | |                P)))))))
. . . . . | | |      (<kind(a(i;t)),x>
. . . . . | | |      ,λx.s(i;t).x
. . . . . | | |      ,val(a(i;t))))
. . . . . | | |   & (∀l:IdLnk.
. . . . . | | |      deq-member(product-deq(Knd;...;...;...);<...
. . . . . | | |                                              ,l>;...)
. . . . . | | |      ⇒
. . . . . | | |      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(
. . . . . | | |                              1of(2of(2of(2of(2of(2of(
. . . . . | | |                                  (with ds: ds
. . . . . | | |                                   init: init
. . . . . | | |                                  action a:T
. . . . . | | |                                   precondition a(v) is
. . . . . | | |                                   P)))))))
. . . . . | | |                              (<kind(a(i;t)),1>)))
. . . . . | | |       else nil fi)
. . . . . | | |    & (∀x:Id.
. . . . . | | |       ¬(deq-member(IdDeq;x;1of(1of(
. . . . . | | |                              2of(2of(2of(2of(2of(2of(
. . . . . | | |                              (with ds: ds
. . . . . | | |                               init: init
. . . . . | | |                              action a:T
. . . . . | | |                               precondition a(v) is
. . . . . | | |                               P)))))))))
. . . . . | | |         ⇒
. . . . . | | |         deq-member(KindDeq;kind(a(i;t));2of(
. . . . . | | |                                         1of(
. . . . . | | |                                         2of(2of(2of(
. . . . . | | |                                         2of(2of(2of(
. . . . . | | |                                         ...))))))))
. . . . . | | |                                         (x)))
. . . . . | | |       ⇒
. . . . . | | |       s(i;t).x = s(i;t+1).x)
. . . . . | | |    & (∀l:IdLnk, tg:Id.
. . . . . | | |       ¬(deq-member(product-deq(...;Id;...;...);...;...)
. . . . . | | |         ⇒
. . . . . | | |         deq-member(KindDeq;kind(a(i;t));2of(
. . . . . | | |                                         1of(
. . . . . | | |                                         2of(2of(2of(
. . . . . | | |                                         2of(2of(2of(
. . . . . | | |                                         2of(
. . . . . | | |                                         ...)))))))))
. . . . . | | |                                         (<l,tg>)))
. . . . . | | |       ⇒
. . . . . | | |       w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . | | 17. ∀x:Id.
. . . . . | | |    deq-member(IdDeq;x;1of(1of(2of(2of((with ds: ds
. . . . . | | |                                 init: init
. . . . . | | |                                action a:T
. . . . . | | |                                 precondition a(v) is
. . . . . | | |                                 P))))))
. . . . . | | |    ⇒
. . . . . | | |    s(i;0).x
. . . . . | | |    =
. . . . . | | |    2of(1of(2of(2of((with ds: ds
. . . . . | | |              init: init
. . . . . | | |             action a:T
. . . . . | | |              precondition a(v) is
```

```
. . . . . | | |            P)))))
. . . . . | | |   (x)
. . . . . | | 18. ∀a@0:Action(i).
. . . . . | | |   ¬isnull(a@0)
. . . . . | | |   ⇒
. . . . . | | |   (valtype(i;a@0) ⊆r 1of(2of((with ds: ds
. . . . . | | |                           init: init
. . . . . | | |                          action a:T
. . . . . | | |                           precondition a(v) is
. . . . . | | |                           P)))(kind(a@0))?Top)
. . . . . | | 19. ∀x:Id.
. . . . . | | |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(1of(
. . . . . | | |                                          ...)))→
. . . . . | | |                     2of(1of((with ds: ds
. . . . . | | |                          init: init
. . . . . | | |                         action a:T
. . . . . | | |                          precondition a(v) is
. . . . . | | |                          P)))
. . . . . | | |                     (x)
. . . . . | | |                   else Top fi
. . . . . | | 20. IdDeq ∈ EqDecider(Id)
. . . . . | | 21. (λx.init(x)?•) ∈ State(ds)
. . . . . | | 22. t' : ℕ
. . . . . | | 23. 0≤t'
. . . . . | | 24. True ⇒ (∀v:T. ¬P((λx.s(i;t').x),v))
. . . . . | | 25. ¬(∃t:ℕt'. ¬isnull(a(i;t)))
. . . . . | | 26. z : Id
. . . . . | | ⊢  0≤t' ⇒ s(i;0).z = s(i;0).z
. . . . . | | | by AllHyps
. . . . . | | |    (λh.
. . . . . | | |     Repeat
. . . . . | | |     (Unfolds [‘ma-single-pre-init‘;‘mk-ma‘] h
. . . . . | | |      THEN
. . . . . | | |      Reduce h))
. . . . . | | |    THEN
. . . . . | | |    Fold ‘member‘ 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. init : x:Id fp-> ds(x)?Void
. . . . . | | 7. ∀x:Id. x ∈ dom(ds) ⇒ x ∈ dom(init)
. . . . . | | 8. v : T
. . . . . | | 9. P((λx.init(x)?•),v)
. . . . . | | 10. w : World
. . . . . | | 11. FairFifo
. . . . . | | 12. FairFifo
. . . . . | | 13. ∀l:IdLnk, tg:Id.
. . . . . | |     (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | |                      <ds,locl(a) : T,init,a : 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) : T)
. . . . . | |       ∨ P@0 != a : P(a@0) ==> ∀v:locl(a) : T(...)?Top.
. . . . . | |         ¬P@0((λx.s(i;t').x),v)
. . . . . | | 16. ∀t:ℕ.
. . . . . | |     ¬isnull(a(i;t))
. . . . . | |     ⇒
. . . . . | |     (islocal(kind(a(i;t)))
. . . . . | |      ⇒
. . . . . | |      deq-member(IdDeq;act(kind(a(i;t)));1of(a : P))
. . . . . | |      ⇒
. . . . . | |      2of(a : P)
. . . . . | |      (act(kind(a(i;t)))
. . . . . | |      ,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)
```

```
. . . . . | | 17. ∀x:Id.
. . . . . | |     deq-member(IdDeq;x;1of(init))
. . . . . | |     ⇒
. . . . . | |     s(i;0).x = 2of(init)(x)
. . . . . | | 18. ∀a@0:Action(i).
. . . . . | |     ¬isnull(a@0)
. . . . . | |     ⇒
. . . . . | |     (valtype(i;a@0) ⊆r locl(a) : 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. (λx.init(x)?•) ∈ State(ds)
. . . . . | | 22. t' : ℕ
. . . . . | | 23. 0≤t'
. . . . . | | 24. True ⇒ (∀v:T. ¬P((λx.s(i;t').x),v))
. . . . . | | 25. ¬(∃t:ℕt'. ¬isnull(a(i;t)))
. . . . . | | 26. z : Id
. . . . . | | 27. 0≤t'
. . . . . | | ⊢  vartype(i;z) ⊆r ds(z)?Top
. . . . . | |   by Repeat (Unfolds [‘fpf-cap‘;‘fpf-ap‘;‘fpf-dom‘] 0)
. . . . . | |      THEN
. . . . . | |      BackThruSomeHyp
. . . . . | |
. . . . . | .\
. . . . . | . .....upcase .....
. . . . . | . 1. i : Id
. . . . . | . 2. a : Id
. . . . . | . 3. T : Type
. . . . . | . 4. ds : x:Id fp-> Type
. . . . . | . 5. P : State(ds)→T→Prop
. . . . . | . 6. init : x:Id fp-> ds(x)?Void
. . . . . | . 7. ∀x:Id. x ∈ dom(ds) ⇒ x ∈ dom(init)
. . . . . | . 8. v : T
. . . . . | . 9. P((λx.init(x)?•),v)
. . . . . | . 10. w : World
. . . . . | . 11. FairFifo
. . . . . | . 12. FairFifo
. . . . . | . 13. ∀l:IdLnk, tg:Id.
. . . . . | . |   (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | . |                    (with ds: ds
. . . . . | . |                     init: init
. . . . . | . |                    action a:T
. . . . . | . |                     precondition a(v) is
. . . . . | . |                     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(1of(2of((with ds: ds
. . . . . | . |                              init: init
. . . . . | . |                             action a:T
```

```
. . . . . | . |                              precondition a(v) is
. . . . . | . |                              P))))
. . . . . | . |     ∨ P@0 != 1of(
. . . . . | . |              2of(2of(2of((with ds: ds
. . . . . | . |               init: init
. . . . . | . |              action a:T
. . . . . | . |               precondition a(v) is
. . . . . | . |               P)))))(a@0) ==> ∀v:1of(
. . . . . | . |                                  2of((with ds: ds
. . . . . | . |                                   init: init
. . . . . | . |                                  action a:T
. . . . . | . |                                   precondition a(v) is
. . . . . | . |                                   P)))(locl(a@0))?Top.
. . . . . | . |       ¬P@0((λx.s(i;t').x),v)
. . . . . | . 16. ∀t:ℕ.
. . . . . | . |   ¬isnull(a(i;t))
. . . . . | . |   ⇒
. . . . . | . |   (islocal(kind(a(i;t)))
. . . . . | . |    ⇒
. . . . . | . |    deq-member(IdDeq;act(kind(a(i;t)));1of(1of(
. . . . . | . |                                        2of(2of(2of(
. . . . . | . |                                        ...))))))
. . . . . | . |    ⇒
. . . . . | . |    2of(1of(2of(2of(2of((with ds: ds
. . . . . | . |              init: init
. . . . . | . |             action a:T
. . . . . | . |              precondition a(v) is
. . . . . | . |              P))))))
. . . . . | . |    (act(kind(a(i;t)))
. . . . . | . |    ,λx.s(i;t).x
. . . . . | . |    ,val(a(i;t))))
. . . . . | . |   & (∀x:Id.
. . . . . | . |      deq-member(product-deq(Knd;Id;...;IdDeq);<...
. . . . . | . |                                              ,x>;...)
. . . . . | . |      ⇒
. . . . . | . |      s(i;t+1).x
. . . . . | . |      =
. . . . . | . |      2of(1of(2of(2of(2of(2of((with ds: ds
. . . . . | . |               init: init
. . . . . | . |              action a:T
. . . . . | . |               precondition a(v) is
. . . . . | . |               P)))))))
. . . . . | . |      (<kind(a(i;t)),x>
. . . . . | . |      ,λx.s(i;t).x
. . . . . | . |      ,val(a(i;t))))
. . . . . | . |   & (∀l:IdLnk.
. . . . . | . |      deq-member(product-deq(Knd;...;...;...);<...
. . . . . | . |                                            ,l>;...)
. . . . . | . |      ⇒
. . . . . | . |      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(
. . . . . | . |                              1of(2of(2of(2of(2of(2of(
. . . . . | . |                                  (with ds: ds
. . . . . | . |                                   init: init
. . . . . | . |                                  action a:T
. . . . . | . |                                   precondition a(v) is
. . . . . | . |                                   P)))))))
. . . . . | . |                              (<kind(a(i;t)),l>)))
. . . . . | . |      else nil fi)
. . . . . | . |   & (∀x:Id.
. . . . . | . |      ¬(deq-member(IdDeq;x;1of(1of(
. . . . . | . |                             2of(2of(2of(2of(2of(2of(
. . . . . | . |                             (with ds: ds
. . . . . | . |                              init: init
. . . . . | . |                             action a:T
. . . . . | . |                              precondition a(v) is
. . . . . | . |                              P)))))))))
. . . . . | . |        ⇒
. . . . . | . |        deq-member(KindDeq;kind(a(i;t));2of(
. . . . . | . |                                        1of(
. . . . . | . |                                        2of(2of(2of(
. . . . . | . |                                        2of(2of(2of(
. . . . . | . |                                        ...)))))))
. . . . . | . |                                        (x)))
. . . . . | . |      ⇒
. . . . . | . |      s(i;t).x = s(i;t+1).x)
. . . . . | . |   & (∀l:IdLnk, tg:Id.
. . . . . | . |      ¬(deq-member(product-deq(...;Id;...;...);...;...)
. . . . . | . |        ⇒
. . . . . | . |        deq-member(KindDeq;kind(a(i;t));2of(
. . . . . | . |                                        1of(
. . . . . | . |                                        2of(2of(2of(
. . . . . | . |                                        2of(2of(2of(
. . . . . | . |                                        2of(
. . . . . | . |                                        ...)))))))))
. . . . . | . |                                        (<l,tg>)))
. . . . . | . |      ⇒
. . . . . | . |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . | . 17. ∀x:Id.
. . . . . | . |   deq-member(IdDeq;x;1of(1of(2of(2of((with ds: ds
. . . . . | . |                                  init: init
. . . . . | . |                                 action a:T
. . . . . | . |                                  precondition a(v) is
. . . . . | . |                                  P))))))
. . . . . | . |   ⇒
. . . . . | . |   s(i;0).x
. . . . . | . |   =
. . . . . | . |   2of(1of(2of(2of((with ds: ds
. . . . . | . |             init: init
. . . . . | . |            action a:T
. . . . . | . |             precondition a(v) is
. . . . . | . |             P)))))
. . . . . | . |   (x)
. . . . . | . 18. ∀a@0:Action(i).
```

```
. . . . . | . |   ¬isnull(a@0)
. . . . . | . |   ⇒
. . . . . | . |   (valtype(i;a@0) ⊆r 1of(2of((with ds: ds
. . . . . | . |                           init: init
. . . . . | . |                          action a:T
. . . . . | . |                           precondition a(v) is
. . . . . | . |                           P)))(kind(a@0))?Top)
. . . . . | . 19. ∀x:Id.
. . . . . | . |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(1of(
. . . . . | . |                                          ...)))→
. . . . . | . |                     2of(1of((with ds: ds
. . . . . | . |                          init: init
. . . . . | . |                         action a:T
. . . . . | . |                          precondition a(v) is
. . . . . | . |                          P)))
. . . . . | . |                     (x)
. . . . . | . |                  else Top fi
. . . . . | . 20. IdDeq ∈ EqDecider(Id)
. . . . . | . 21. (λx.init(x)?•) ∈ State(ds)
. . . . . | . 22. t' : ℕ
. . . . . | . 23. 0≤t'
. . . . . | . 24. True ⇒ (∀v:T. ¬P((λx.s(i;t').x),v))
. . . . . | . 25. ¬(∃t:ℕt'. ¬isnull(a(i;t)))
. . . . . | . 26. z : Id
. . . . . | . 27. t : ℤ
. . . . . | . 28. 0<t
. . . . . | . 29. t-1≤t' ⇒ s(i;0).z = s(i;t-1).z
. . . . . | . ⊢  t≤t' ⇒ s(i;0).z = s(i;t).z  by Auto THEN Analyze -2
. . . . . | . |
. . . . . | . 1. i : Id
. . . . . | . 2. a : Id
. . . . . | . 3. T : Type
. . . . . | . 4. ds : x:Id fp-> Type
. . . . . | . 5. P : State(ds)→T→Prop
. . . . . | . 6. init : x:Id fp-> ds(x)?Void
. . . . . | . 7. ∀x:Id. x ∈ dom(ds) ⇒ x ∈ dom(init)
. . . . . | . 8. v : T
. . . . . | . 9. P((λx.init(x)?•),v)
. . . . . | . 10. w : World
. . . . . | . 11. FairFifo
. . . . . | . 12. FairFifo
. . . . . | . 13. ∀l:IdLnk, tg:Id.
. . . . . | . |   (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | . |                    (with ds: ds
. . . . . | . |                     init: init
. . . . . | . |                    action a:T
. . . . . | . |                     precondition a(v) is
. . . . . | . |                     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(1of(2of((with ds: ds
```

```
. . . . . | . |                              init: init
. . . . . | . |                             action a:T
. . . . . | . |                              precondition a(v) is
. . . . . | . |                              P))))
. . . . . | . |     ∨ P@0 != 1of(
. . . . . | . |              2of(2of(2of((with ds: ds
. . . . . | . |               init: init
. . . . . | . |              action a:T
. . . . . | . |               precondition a(v) is
. . . . . | . |               P)))))(a@0) ==> ∀v:1of(
. . . . . | . |                                    2of((with ds: ds
. . . . . | . |                                     init: init
. . . . . | . |                                    action a:T
. . . . . | . |                                     precondition a(v) is
. . . . . | . |                                     P)))(1ocl(a@0))?Top.
. . . . . | . |       ¬P@0((λx.s(i;t').x),v)
. . . . . | . 16. ∀t:ℕ.
. . . . . | . |    ¬isnull(a(i;t))
. . . . . | . |    ⇒
. . . . . | . |    (islocal(kind(a(i;t)))
. . . . . | . |     ⇒
. . . . . | . |     deq-member(IdDeq;act(kind(a(i;t)));1of(1of(
. . . . . | . |                                          2of(2of(2of(
. . . . . | . |                                          ...)))))))
. . . . . | . |     ⇒
. . . . . | . |     2of(1of(2of(2of(2of((with ds: ds
. . . . . | . |              init: init
. . . . . | . |             action a:T
. . . . . | . |              precondition a(v) is
. . . . . | . |              P))))))
. . . . . | . |     (act(kind(a(i;t)))
. . . . . | . |     ,λx.s(i;t).x
. . . . . | . |     ,val(a(i;t))))
. . . . . | . |    & (∀x:Id.
. . . . . | . |       deq-member(product-deq(Knd;Id;...;IdDeq);<...
. . . . . | . |                                                ,x>;...)
. . . . . | . |       ⇒
. . . . . | . |       s(i;t+1).x
. . . . . | . |       =
. . . . . | . |       2of(1of(2of(2of(2of(2of((with ds: ds
. . . . . | . |                init: init
. . . . . | . |               action a:T
. . . . . | . |                precondition a(v) is
. . . . . | . |                P)))))))
. . . . . | . |       (<kind(a(i;t)),x>
. . . . . | . |       ,λx.s(i;t).x
. . . . . | . |       ,val(a(i;t))))
. . . . . | . |    & (∀l:IdLnk.
. . . . . | . |       deq-member(product-deq(Knd;...;...;...);<...
. . . . . | . |                                              ,l>;...)
. . . . . | . |       ⇒
. . . . . | . |       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(
. . . . . | . |                              1of(2of(2of(2of(2of(2of(
. . . . . | . |                                  (with ds: ds
. . . . . | . |                                   init: init

. . . . . | . |                                  action a:T
. . . . . | . |                                   precondition a(v) is
. . . . . | . |                                   P)))))))
. . . . . | . |                              (<kind(a(i;t)),1>)))
. . . . . | . |      else nil fi)
. . . . . | . |   & (∀x:Id.
. . . . . | . |      ¬(deq-member(IdDeq;x;1of(1of(
. . . . . | . |                             2of(2of(2of(2of(2of(2of(
. . . . . | . |                             (with ds: ds
. . . . . | . |                              init: init
. . . . . | . |                             action a:T
. . . . . | . |                              precondition a(v) is
. . . . . | . |                              P)))))))))
. . . . . | . |        ⇒
. . . . . | . |        deq-member(KindDeq;kind(a(i;t));2of(
. . . . . | . |                                         1of(
. . . . . | . |                                         2of(2of(2of(
. . . . . | . |                                         2of(2of(2of(
. . . . . | . |                                         ...)))))))
. . . . . | . |                                         (x)))
. . . . . | . |      ⇒
. . . . . | . |      s(i;t).x = s(i;t+1).x)
. . . . . | . |   & (∀l:IdLnk, tg:Id.
. . . . . | . |      ¬(deq-member(product-deq(...;Id;...;...);...;...)
. . . . . | . |        ⇒
. . . . . | . |        deq-member(KindDeq;kind(a(i;t));2of(
. . . . . | . |                                         1of(
. . . . . | . |                                         2of(2of(2of(
. . . . . | . |                                         2of(2of(2of(
. . . . . | . |                                         2of(
. . . . . | . |                                         ...)))))))))
. . . . . | . |                                         (<l,tg>)))
. . . . . | . |      ⇒
. . . . . | . |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . | . 17. ∀x:Id.
. . . . . | . |   deq-member(IdDeq;x;1of(1of(2of(2of((with ds: ds
. . . . . | . |                                  init: init
. . . . . | . |                                 action a:T
. . . . . | . |                                  precondition a(v) is
. . . . . | . |                                  P))))))
. . . . . | . |   ⇒
. . . . . | . |   s(i;0).x
. . . . . | . |   =
. . . . . | . |   2of(1of(2of(2of((with ds: ds
. . . . . | . |            init: init
. . . . . | . |           action a:T
. . . . . | . |            precondition a(v) is
. . . . . | . |            P)))))
```

```
. . . . . | . |   (x)
. . . . . | . 18. ∀a@0:Action(i).
. . . . . | . |   ¬isnull(a@0)
. . . . . | . |   ⇒
. . . . . | . |   (valtype(i;a@0) ⊆r 1of(2of((with ds: ds
. . . . . | . |                           init: init
. . . . . | . |                          action a:T
. . . . . | . |                           precondition a(v) is
. . . . . | . |                           P)))(kind(a@0))?Top)
. . . . . | . 19. ∀x:Id.
. . . . . | . |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(1of(
. . . . . | . |                                          ...)))→
. . . . . | . |                     2of(1of((with ds: ds
. . . . . | . |                          init: init
. . . . . | . |                         action a:T
. . . . . | . |                          precondition a(v) is
. . . . . | . |                          P)))
. . . . . | . |                      (x)
. . . . . | . |                  else Top fi
. . . . . | . 20. IdDeq ∈ EqDecider(Id)
. . . . . | . 21. (λx.init(x)?•) ∈ State(ds)
. . . . . | . 22. t' : ℕ
. . . . . | . 23. 0≤t'
. . . . . | . 24. True ⇒ (∀v:T. ¬P((λx.s(i;t').x),v))
. . . . . | . 25. ¬(∃t:ℕt'. ¬isnull(a(i;t)))
. . . . . | . 26. z : Id
. . . . . | . 27. t : ℤ
. . . . . | . 28. 0<t
. . . . . | . 29. t≤t'
. . . . . | . 30. s(i;0).z = s(i;t-1).z
. . . . . | . ⊢  s(i;0).z = s(i;t).z
. . . . . | . | by Assert (s(i;t-1).z = s(i;t).z)
. . . . . | . |
. . . . . | . .....assertion .....
. . . . . | . 1. i : Id
. . . . . | . 2. a : Id
. . . . . | . 3. T : Type
. . . . . | . 4. ds : x:Id fp-> Type
. . . . . | . 5. P : State(ds)→T→Prop
. . . . . | . 6. init : x:Id fp-> ds(x)?Void
. . . . . | . 7. ∀x:Id. x ∈ dom(ds) ⇒ x ∈ dom(init)
. . . . . | . 8. v : T
. . . . . | . 9. P((λx.init(x)?•),v)
. . . . . | . 10. w : World
. . . . . | . 11. FairFifo
. . . . . | . 12. FairFifo
. . . . . | . 13. ∀l:IdLnk, tg:Id.
. . . . . | . |   (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | . |                    (with ds: ds
. . . . . | . |                     init: init
. . . . . | . |                    action a:T
. . . . . | . |                     precondition a(v) is
. . . . . | . |                     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(1of(2of((with ds: ds
. . . . . | . |                              init: init
. . . . . | . |                             action a:T
. . . . . | . |                              precondition a(v) is
. . . . . | . |                              P))))
. . . . . | . |     ∨ P@0 != 1of(
. . . . . | . |              2of(2of(2of((with ds: ds
. . . . . | . |               init: init
. . . . . | . |              action a:T
. . . . . | . |               precondition a(v) is
. . . . . | . |               P)))))(a@0) ==> ∀v:1of(
. . . . . | . |                                  2of((with ds: ds
. . . . . | . |                                   init: init
. . . . . | . |                                  action a:T
. . . . . | . |                                   precondition a(v) is
. . . . . | . |                                   P)))(locl(a@0))?Top.
. . . . . | . |       ¬P@0((λx.s(i;t').x),v)
. . . . . | . 16. ∀t:ℕ.
. . . . . | . |   ¬isnull(a(i;t))
. . . . . | . |   ⇒
. . . . . | . |   (islocal(kind(a(i;t)))
. . . . . | . |    ⇒
. . . . . | . |    deq-member(IdDeq;act(kind(a(i;t)));1of(1of(
. . . . . | . |                                        2of(2of(2of(
. . . . . | . |                                        ...))))))
. . . . . | . |    ⇒
. . . . . | . |    2of(1of(2of(2of(2of((with ds: ds
. . . . . | . |              init: init
. . . . . | . |             action a:T
. . . . . | . |              precondition a(v) is
. . . . . | . |              P))))))
. . . . . | . |    (act(kind(a(i;t)))
. . . . . | . |    ,λx.s(i;t).x
. . . . . | . |    ,val(a(i;t))))
. . . . . | . |   & (∀x:Id.
. . . . . | . |      deq-member(product-deq(Knd;Id;...;IdDeq);<...
. . . . . | . |                                              ,x>;...)
. . . . . | . |      ⇒
. . . . . | . |      s(i;t+1).x
. . . . . | . |      =
. . . . . | . |      2of(1of(2of(2of(2of(2of((with ds: ds
. . . . . | . |                init: init
. . . . . | . |               action a:T
. . . . . | . |                precondition a(v) is
. . . . . | . |                P)))))))
. . . . . | . |      (<kind(a(i;t)),x>
. . . . . | . |      ,λx.s(i;t).x
. . . . . | . |      ,val(a(i;t))))
. . . . . | . |   & (∀l:IdLnk.
. . . . . | . |      deq-member(product-deq(Knd;...;...;...);<...
. . . . . | . |                                            ,l>;...)
```

```
. . . . . | . |      ⇒
. . . . . | . |      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(
. . . . . | . |                              1of(2of(2of(2of(2of(2of(
. . . . . | . |                                  (with ds: ds
. . . . . | . |                                   init: init
. . . . . | . |                                  action a:T
. . . . . | . |                                   precondition a(v) is
. . . . . | . |                                   P)))))))
. . . . . | . |                              (<kind(a(i;t)),l>)))
. . . . . | . |      else nil fi)
. . . . . | . |   & (∀x:Id.
. . . . . | . |      ¬(deq-member(IdDeq;x;1of(1of(
. . . . . | . |                             2of(2of(2of(2of(2of(2of(
. . . . . | . |                             (with ds: ds
. . . . . | . |                              init: init
. . . . . | . |                             action a:T
. . . . . | . |                              precondition a(v) is
. . . . . | . |                              P)))))))))
. . . . . | . |        ⇒
. . . . . | . |        deq-member(KindDeq;kind(a(i;t));2of(
. . . . . | . |                                         1of(
. . . . . | . |                                         2of(2of(2of(
. . . . . | . |                                         2of(2of(2of(
. . . . . | . |                                         ...)))))))
. . . . . | . |                                         (x)))
. . . . . | . |      ⇒
. . . . . | . |      s(i;t).x = s(i;t+1).x)
. . . . . | . |   & (∀l:IdLnk, tg:Id.
. . . . . | . |      ¬(deq-member(product-deq(...;Id;...;...);...;...)
. . . . . | . |        ⇒
. . . . . | . |        deq-member(KindDeq;kind(a(i;t));2of(
. . . . . | . |                                         1of(
. . . . . | . |                                         2of(2of(2of(
. . . . . | . |                                         2of(2of(2of(
. . . . . | . |                                         2of(
. . . . . | . |                                         ...)))))))))
. . . . . | . |                                         (<l,tg>)))
. . . . . | . |      ⇒
. . . . . | . |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . | . 17. ∀x:Id.
. . . . . | . |   deq-member(IdDeq;x;1of(1of(2of(2of((with ds: ds
. . . . . | . |                                 init: init
. . . . . | . |                                action a:T
. . . . . | . |                                 precondition a(v) is
. . . . . | . |                                 P))))))
. . . . . | . |   ⇒
. . . . . | . |   s(i;0).x
. . . . . | . |   =
```

```
. . . . . | . |   2of(1of(2of(2of((with ds: ds
. . . . . | . |            init: init
. . . . . | . |           action a:T
. . . . . | . |            precondition a(v) is
. . . . . | . |            P)))))
. . . . . | . |   (x)
. . . . . | . 18. ∀a@0:Action(i).
. . . . . | . |   ¬isnull(a@0)
. . . . . | . |   ⇒
. . . . . | . |   (valtype(i;a@0) ⊆r 1of(2of((with ds: ds
. . . . . | . |                           init: init
. . . . . | . |                          action a:T
. . . . . | . |                           precondition a(v) is
. . . . . | . |                           P)))(kind(a@0))?Top)
. . . . . | . 19. ∀x:Id.
. . . . . | . |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(1of(
. . . . . | . |                                          ...)))→
. . . . . | . |                      2of(1of((with ds: ds
. . . . . | . |                           init: init
. . . . . | . |                          action a:T
. . . . . | . |                           precondition a(v) is
. . . . . | . |                           P)))
. . . . . | . |                     (x)
. . . . . | . |                  else Top fi
. . . . . | . 20. IdDeq ∈ EqDecider(Id)
. . . . . | . 21. (λx.init(x)?•) ∈ State(ds)
. . . . . | . 22. t' : ℕ
. . . . . | . 23. 0≤t'
. . . . . | . 24. True ⇒ (∀v:T. ¬P((λx.s(i;t').x),v))
. . . . . | . 25. ¬(∃t:ℕt'. ¬isnull(a(i;t)))
. . . . . | . 26. z : Id
. . . . . | . 27. t : ℤ
. . . . . | . 28. 0<t
. . . . . | . 29. t≤t'
. . . . . | . 30. s(i;0).z = s(i;t-1).z
. . . . . | . ⊢  s(i;t-1).z = s(i;t).z
. . . . . | . | by AssertBY
. . . . . | . |    (∀i:Id, t:ℕ.
. . . . . | . |     isnull(a(i;t))
. . . . . | . |     ⇒
. . . . . | . |     (∀x:Id. s(i;t+1).x = s(i;t).x) & m(i;t) = nil)
. . . . . | . |    (AllHyps
. . . . . | . |     (λh.
. . . . . | . |      Unfold `fair-fifo` h THEN Analyze h
. . . . . | . |      THEN
. . . . . | . |      Analyze h+1
. . . . . | . |      THEN
. . . . . | . |      Trivial))
. . . . . | . |
. . . . . | . 1. i : Id
. . . . . | . 2. a : Id
. . . . . | . 3. T : Type
. . . . . | . 4. ds : x:Id fp-> Type
. . . . . | . 5. P : State(ds)→T→Prop
. . . . . | . 6. init : x:Id fp-> ds(x)?Void
```

```
. . . . . | . 7. ∀x:Id. x ∈ dom(ds) ⇒ x ∈ dom(init)
. . . . . | . 8. v : T
. . . . . | . 9. P((λx.init(x)?•),v)
. . . . . | . 10. w : World
. . . . . | . 11. FairFifo
. . . . . | . 12. FairFifo
. . . . . | . 13. ∀l:IdLnk, tg:Id.
. . . . . | . |   (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | . |                    (with ds: ds
. . . . . | . |                     init: init
. . . . . | . |                    action a:T
. . . . . | . |                     precondition a(v) is
. . . . . | . |                     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(1of(2of((with ds: ds
. . . . . | . |                              init: init
. . . . . | . |                             action a:T
. . . . . | . |                              precondition a(v) is
. . . . . | . |                              P))))
. . . . . | . |     ∨ P@0 != 1of(
. . . . . | . |              2of(2of(2of((with ds: ds
. . . . . | . |               init: init
. . . . . | . |              action a:T
. . . . . | . |               precondition a(v) is
. . . . . | . |               P)))))(a@0) ==> ∀v:1of(
. . . . . | . |                                  2of((with ds: ds
. . . . . | . |                                   init: init
. . . . . | . |                                  action a:T
. . . . . | . |                                   precondition a(v) is
. . . . . | . |                                   P)))(locl(a@0))?Top.
. . . . . | . |       ¬P@0((λx.s(i;t').x),v)
. . . . . | . 16. ∀t:ℕ.
. . . . . | . |   ¬isnull(a(i;t))
. . . . . | . |   ⇒
. . . . . | . |   (islocal(kind(a(i;t)))
. . . . . | . |    ⇒
. . . . . | . |    deq-member(IdDeq;act(kind(a(i;t)));1of(1of(
. . . . . | . |                                        2of(2of(2of(
. . . . . | . |                                        ...)))))
. . . . . | . |    ⇒
. . . . . | . |    2of(1of(2of(2of(2of((with ds: ds
. . . . . | . |             init: init
. . . . . | . |            action a:T
. . . . . | . |             precondition a(v) is
. . . . . | . |             P))))))
. . . . . | . |    (act(kind(a(i;t)))
. . . . . | . |    ,λx.s(i;t).x
. . . . . | . |    ,val(a(i;t))))
. . . . . | . |   & (∀x:Id.
. . . . . | . |      deq-member(product-deq(Knd;Id;...;IdDeq);<...
```

```
. . . . . | . |                                                ,x>;...)
. . . . . | . |      ⇒
. . . . . | . |      s(i;t+1).x
. . . . . | . |      =
. . . . . | . |      2of(1of(2of(2of(2of(2of((with ds: ds
. . . . . | . |               init: init
. . . . . | . |              action a:T
. . . . . | . |               precondition a(v) is
. . . . . | . |               P)))))))
. . . . . | . |      (<kind(a(i;t)),x>
. . . . . | . |      ,λx.s(i;t).x
. . . . . | . |      ,val(a(i;t))))
. . . . . | . |   & (∀l:IdLnk.
. . . . . | . |      deq-member(product-deq(Knd;...;...;...);<...
. . . . . | . |                                                ,l>;...)
. . . . . | . |      ⇒
. . . . . | . |      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(
. . . . . | . |                              1of(2of(2of(2of(2of(2of(
. . . . . | . |                                  (with ds: ds
. . . . . | . |                                   init: init
. . . . . | . |                                  action a:T
. . . . . | . |                                   precondition a(v) is
. . . . . | . |                                   P)))))))))
. . . . . | . |                              (<kind(a(i;t)),l>)))
. . . . . | . |      else nil fi)
. . . . . | . |   & (∀x:Id.
. . . . . | . |      ¬(deq-member(IdDeq;x;1of(1of(
. . . . . | . |                             2of(2of(2of(2of(2of(2of(
. . . . . | . |                             (with ds: ds
. . . . . | . |                              init: init
. . . . . | . |                             action a:T
. . . . . | . |                              precondition a(v) is
. . . . . | . |                              P)))))))))))
. . . . . | . |        ⇒
. . . . . | . |        deq-member(KindDeq;kind(a(i;t));2of(
. . . . . | . |                                         1of(
. . . . . | . |                                         2of(2of(2of(
. . . . . | . |                                         2of(2of(2of(
. . . . . | . |                                         ...)))))))))
. . . . . | . |                                         (x)))
. . . . . | . |      ⇒
. . . . . | . |      s(i;t).x = s(i;t+1).x)
. . . . . | . |   & (∀l:IdLnk, tg:Id.
. . . . . | . |      ¬(deq-member(product-deq(...;Id;...;...);...;...)
. . . . . | . |        ⇒
. . . . . | . |        deq-member(KindDeq;kind(a(i;t));2of(
. . . . . | . |                                         1of(
. . . . . | . |                                         2of(2of(2of(
```

```
. . . . . | . |                                        2of(2of(2of(
. . . . . | . |                                        2of(
. . . . . | . |                                        ...)))))))))
. . . . . | . |                                        (<l,tg>)))
. . . . . | . |      ⇒
. . . . . | . |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . | . 17. ∀x:Id.
. . . . . | . |   deq-member(IdDeq;x;1of(1of(2of(2of((with ds: ds
. . . . . | . |                                 init: init
. . . . . | . |                                action a:T
. . . . . | . |                                 precondition a(v) is
. . . . . | . |                                 P)))))
. . . . . | . |   ⇒
. . . . . | . |   s(i;0).x
. . . . . | . |   =
. . . . . | . |   2of(1of(2of(2of((with ds: ds
. . . . . | . |            init: init
. . . . . | . |           action a:T
. . . . . | . |            precondition a(v) is
. . . . . | . |            P)))))
. . . . . | . |   (x)
. . . . . | . 18. ∀a@0:Action(i).
. . . . . | . |   ¬isnull(a@0)
. . . . . | . |   ⇒
. . . . . | . |   (valtype(i;a@0) ⊆r 1of(2of((with ds: ds
. . . . . | . |                            init: init
. . . . . | . |                           action a:T
. . . . . | . |                            precondition a(v) is
. . . . . | . |                            P)))(kind(a@0))?Top)
. . . . . | . 19. ∀x:Id.
. . . . . | . |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(1of(
. . . . . | . |                                          ...)))→
. . . . . | . |                       2of(1of((with ds: ds
. . . . . | . |                            init: init
. . . . . | . |                           action a:T
. . . . . | . |                            precondition a(v) is
. . . . . | . |                            P)))
. . . . . | . |                       (x)
. . . . . | . |                    else Top fi
. . . . . | . 20. IdDeq ∈ EqDecider(Id)
. . . . . | . 21. (λx.init(x)?•) ∈ State(ds)
. . . . . | . 22. t' : ℕ
. . . . . | . 23. 0≤t'
. . . . . | . 24. True ⇒ (∀v:T. ¬P((λx.s(i;t').x),v))
. . . . . | . 25. ¬(∃t:ℕt'. ¬isnull(a(i;t)))
. . . . . | . 26. z : Id
. . . . . | . 27. t : ℤ
. . . . . | . 28. 0<t
. . . . . | . 29. t≤t'
. . . . . | . 30. s(i;0).z = s(i;t-1).z
. . . . . | . 31. ∀i:Id, t:ℕ.
. . . . . | . |   isnull(a(i;t))
. . . . . | . |   ⇒
. . . . . | . |   (∀x:Id. s(i;t+1).x = s(i;t).x) & m(i;t) = nil
. . . . . | . ⊢  s(i;t-1).z = s(i;t).z
```

```
. . . . . | . | by InstHyp [i;t-1] -1
. . . . . | . |    THENA
. . . . . | . |    (Auto THEN Try D_ES_Subtype)
. . . . . | . |
. . . . . | . |\
. . . . . | . | .....antecedent .....
. . . . . | . | 1. i : Id
. . . . . | . | 2. a : Id
. . . . . | . | 3. T : Type
. . . . . | . | 4. ds : x:Id fp-> Type
. . . . . | . | 5. P : State(ds)→T→Prop
. . . . . | . | 6. init : x:Id fp-> ds(x)?Void
. . . . . | . | 7. ∀x:Id. x ∈ dom(ds) ⇒ x ∈ dom(init)
. . . . . | . | 8. v : T
. . . . . | . | 9. P((λx.init(x)?•),v)
. . . . . | . | 10. w : World
. . . . . | . | 11. FairFifo
. . . . . | . | 12. FairFifo
. . . . . | . | 13. ∀l:IdLnk, tg:Id.
. . . . . | . | |   (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | . | |                    (with ds: ds
. . . . . | . | |                     init: init
. . . . . | . | |                    action a:T
. . . . . | . | |                     precondition a(v) is
. . . . . | . | |                     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(1of(2of((with ds: ds
. . . . . | . | |                              init: init
. . . . . | . | |                             action a:T
. . . . . | . | |                              precondition a(v) is
. . . . . | . | |                              P))))
. . . . . | . | |     ∨ P@0 != 1of(
. . . . . | . | |              2of(2of(2of((with ds: ds
. . . . . | . | |               init: init
. . . . . | . | |              action a:T
. . . . . | . | |               precondition a(v) is
. . . . . | . | |               P)))))(a@0) ==> ∀v:1of(
. . . . . | . | |                                  2of(
. . . . . | . | |                                  ...))(...)?Top.
. . . . . | . | |       ¬P@0((λx.s(i;t').x),v)
. . . . . | . | 16. ∀t:ℕ.
. . . . . | . | |   ¬isnull(a(i;t))
. . . . . | . | |   ⇒
. . . . . | . | |   (islocal(kind(a(i;t)))
. . . . . | . | |    ⇒
. . . . . | . | |    deq-member(IdDeq;act(kind(a(i;t)));1of(1of(
. . . . . | . | |                                       2of(2of(2of(
. . . . . | . | |                                       ...))))))
. . . . . | . | |    ⇒
. . . . . | . | |    2of(1of(2of(2of(2of((with ds: ds
```

```
. . . . . | . | |             init: init
. . . . . | . | |            action a:T
. . . . . | . | |             precondition a(v) is
. . . . . | . | |             P))))))
. . . . . | . | |    (act(kind(a(i;t)))
. . . . . | . | |    ,λx.s(i;t).x
. . . . . | . | |    ,val(a(i;t))))
. . . . . | . | |   & (∀x:Id.
. . . . . | . | |      deq-member(product-deq(Knd;Id;...;...);<...
. . . . . | . | |                                            ,x>;...)
. . . . . | . | |      ⇒
. . . . . | . | |      s(i;t+1).x
. . . . . | . | |      =
. . . . . | . | |      2of(1of(2of(2of(2of(2of((with ds: ds
. . . . . | . | |               init: init
. . . . . | . | |              action a:T
. . . . . | . | |               precondition a(v) is
. . . . . | . | |               P)))))))
. . . . . | . | |      (<kind(a(i;t)),x>
. . . . . | . | |      ,λx.s(i;t).x
. . . . . | . | |      ,val(a(i;t))))
. . . . . | . | |   & (∀l:IdLnk.
. . . . . | . | |      deq-member(...;<kind(a(i;t))
. . . . . | . | |                     ,l>;1of(1of(
. . . . . | . | |                         2of(2of(2of(2of(2of(
. . . . . | . | |                         (with ds: ds
. . . . . | . | |                          init: init
. . . . . | . | |                         action a:T
. . . . . | . | |                          precondition a(v) is
. . . . . | . | |                          P)))))))))
. . . . . | . | |      ⇒
. . . . . | . | |      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(
. . . . . | . | |                              1of(2of(2of(2of(2of(2of(
. . . . . | . | |                                  (with ds: ds
. . . . . | . | |                                   init: init
. . . . . | . | |                                  action a:T
. . . . . | . | |                                   precondition a(v) is
. . . . . | . | |                                   P)))))))
. . . . . | . | |                              (<kind(a(i;t)),l>)))
. . . . . | . | |      else nil fi)
. . . . . | . | |   & (∀x:Id.
. . . . . | . | |      ¬(deq-member(IdDeq;x;1of(1of(
. . . . . | . | |                             2of(2of(2of(2of(2of(2of(
. . . . . | . | |                             (with ds: ds
. . . . . | . | |                              init: init
. . . . . | . | |                             action a:T
. . . . . | . | |                              precondition a(v) is
. . . . . | . | |                              P)))))))))
```

```
. . . . . | . | |        ⇒
. . . . . | . | |        deq-member(KindDeq;kind(a(i;t));2of(
. . . . . | . | |                                         1of(
. . . . . | . | |                                         2of(2of(2of(
. . . . . | . | |                                         2of(2of(2of(
. . . . . | . | |                                         ...)))))))))
. . . . . | . | |                                         (x)))
. . . . . | . | |      ⇒
. . . . . | . | |      s(i;t).x = s(i;t+1).x)
. . . . . | . | |   & (∀l:IdLnk, tg:Id.
. . . . . | . | |      ¬(deq-member(...;<l,tg>;1of(1of(
. . . . . | . | |                                2of(2of(2of(2of(2of(
. . . . . | . | |                                2of(2of((with ds: ds
. . . . . | . | |                                 init: init
. . . . . | . | |                                action a:T
. . . . . | . | |                                 precondition a(v) is
. . . . . | . | |                                 P)))))))))))
. . . . . | . | |        ⇒
. . . . . | . | |        deq-member(KindDeq;kind(a(i;t));2of(
. . . . . | . | |                                         1of(
. . . . . | . | |                                         2of(2of(2of(
. . . . . | . | |                                         2of(2of(2of(
. . . . . | . | |                                         2of(
. . . . . | . | |                                         ...)))))))))
. . . . . | . | |                                         (<l,tg>)))
. . . . . | . | |      ⇒
. . . . . | . | |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . | . | 17. ∀x:Id.
. . . . . | . | |   deq-member(IdDeq;x;1of(1of(2of(2of((with ds: ds
. . . . . | . | |                                 init: init
. . . . . | . | |                                action a:T
. . . . . | . | |                                 precondition a(v) is
. . . . . | . | |                                 P))))))
. . . . . | . | |   ⇒
. . . . . | . | |   s(i;0).x
. . . . . | . | |   =
. . . . . | . | |   2of(1of(2of(2of((with ds: ds
. . . . . | . | |            init: init
. . . . . | . | |           action a:T
. . . . . | . | |            precondition a(v) is
. . . . . | . | |            P)))))
. . . . . | . | |   (x)
. . . . . | . | 18. ∀a@0:Action(i).
. . . . . | . | |   ¬isnull(a@0)
. . . . . | . | |   ⇒
. . . . . | . | |   (valtype(i;a@0) ⊆r 1of(2of((with ds: ds
. . . . . | . | |                            init: init
. . . . . | . | |                           action a:T
. . . . . | . | |                            precondition a(v) is
. . . . . | . | |                            P)))(kind(a@0))?Top)
. . . . . | . | 19. ∀x:Id.
. . . . . | . | |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(1of(
. . . . . | . | |                                          ...)))→
. . . . . | . | |                       2of(1of((with ds: ds
. . . . . | . | |                            init: init
```

```
. . . . . | . | |                          action a:T
. . . . . | . | |                           precondition a(v) is
. . . . . | . | |                           P)))
. . . . . | . | |                      (x)
. . . . . | . | |                  else Top fi
. . . . . | . | 20. IdDeq ∈ EqDecider(Id)
. . . . . | . | 21. (λx.init(x)?•) ∈ State(ds)
. . . . . | . | 22. t' : ℕ
. . . . . | . | 23. 0≤t'
. . . . . | . | 24. True ⇒ (∀v:T. ¬P((λx.s(i;t').x),v))
. . . . . | . | 25. ¬(∃t:ℕt'. ¬isnull(a(i;t)))
. . . . . | . | 26. z : Id
. . . . . | . | 27. t : ℤ
. . . . . | . | 28. 0<t
. . . . . | . | 29. t≤t'
. . . . . | . | 30. s(i;0).z = s(i;t-1).z
. . . . . | . | 31. ∀i:Id, t:ℕ.
. . . . . | . | |   isnull(a(i;t))
. . . . . | . | |   ⇒
. . . . . | . | |   (∀x:Id. s(i;t+1).x = s(i;t).x) & m(i;t) = nil
. . . . . | . | ⊢  isnull(a(i;t-1))
. . . . . | . | | by SupposeNot 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. init : x:Id fp-> ds(x)?Void
. . . . . | . | 7. ∀x:Id. x ∈ dom(ds) ⇒ x ∈ dom(init)
. . . . . | . | 8. v : T
. . . . . | . | 9. P((λx.init(x)?•),v)
. . . . . | . | 10. w : World
. . . . . | . | 11. FairFifo
. . . . . | . | 12. FairFifo
. . . . . | . | 13. ∀l:IdLnk, tg:Id.
. . . . . | . |     (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | . |                        (with ds: ds
. . . . . | . |                         init: init
. . . . . | . |                        action a:T
. . . . . | . |                         precondition a(v) is
. . . . . | . |                         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(1of(2of((with ds: ds
. . . . . | . |                                  init: init
. . . . . | . |                                 action a:T
. . . . . | . |                                  precondition a(v) is
. . . . . | . |                                  P))))
. . . . . | . |       ∨ P@0 != 1of(
. . . . . | . |               2of(2of(2of((with ds: ds
```

```
. . . . . | . |                 init: init
. . . . . | . |                action a:T
. . . . . | . |                 precondition a(v) is
. . . . . | . |                 P)))))(a@0) ==> ∀v:1of(
. . . . . | . |                                    2of(
. . . . . | . |                                    ...))(...)?Top.
. . . . . | . |         ¬P@0((λx.s(i;t').x),v)
. . . . . | . | 16. ∀t:ℕ.
. . . . . | . |     ¬isnull(a(i;t))
. . . . . | . |     ⇒
. . . . . | . |     (islocal(kind(a(i;t)))
. . . . . | . |      ⇒
. . . . . | . |      deq-member(IdDeq;act(kind(a(i;t)));1of(1of(
. . . . . | . |                                          2of(2of(2of(
. . . . . | . |                                          ...))))))
. . . . . | . |      ⇒
. . . . . | . |      2of(1of(2of(2of(2of((with ds: ds
. . . . . | . |               init: init
. . . . . | . |              action a:T
. . . . . | . |               precondition a(v) is
. . . . . | . |               P))))))
. . . . . | . |      (act(kind(a(i;t)))
. . . . . | . |      ,λx.s(i;t).x
. . . . . | . |      ,val(a(i;t))))
. . . . . | . |     & (∀x:Id.
. . . . . | . |        deq-member(product-deq(Knd;Id;...;...);<...
. . . . . | . |                                              ,x>;...)
. . . . . | . |        ⇒
. . . . . | . |        s(i;t+1).x
. . . . . | . |        =
. . . . . | . |        2of(1of(2of(2of(2of(2of((with ds: ds
. . . . . | . |                 init: init
. . . . . | . |                action a:T
. . . . . | . |                 precondition a(v) is
. . . . . | . |                 P)))))))
. . . . . | . |        (<kind(a(i;t)),x>
. . . . . | . |        ,λx.s(i;t).x
. . . . . | . |        ,val(a(i;t))))
. . . . . | . |     & (∀l:IdLnk.
. . . . . | . |        deq-member(...;<kind(a(i;t))
. . . . . | . |                        ,l>;1of(1of(
. . . . . | . |                            2of(2of(2of(2of(2of(
. . . . . | . |                            (with ds: ds
. . . . . | . |                             init: init
. . . . . | . |                            action a:T
. . . . . | . |                             precondition a(v) is
. . . . . | . |                             P)))))))))

. . . . . | . |        ⇒
. . . . . | . |        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(
. . . . . | . |                              1of(2of(2of(2of(2of(2of(
. . . . . | . |                                  (with ds: ds
. . . . . | . |                                   init: init
. . . . . | . |                                  action a:T
. . . . . | . |                                   precondition a(v) is
. . . . . | . |                                   P)))))))
. . . . . | . |                              (<kind(a(i;t)),1>)))
. . . . . | . |       else nil fi)
. . . . . | . |     & (∀x:Id.
. . . . . | . |       ¬(deq-member(IdDeq;x;1of(1of(
. . . . . | . |                           2of(2of(2of(2of(2of(2of(
. . . . . | . |                           (with ds: ds
. . . . . | . |                            init: init
. . . . . | . |                           action a:T
. . . . . | . |                            precondition a(v) is
. . . . . | . |                            P)))))))))
. . . . . | . |         ⇒
. . . . . | . |         deq-member(KindDeq;kind(a(i;t));2of(
. . . . . | . |                                         1of(
. . . . . | . |                                         2of(2of(2of(
. . . . . | . |                                         2of(2of(2of(
. . . . . | . |                                         ...)))))))))
. . . . . | . |                                         (x)))
. . . . . | . |       ⇒
. . . . . | . |       s(i;t).x = s(i;t+1).x)
. . . . . | . |     & (∀l:IdLnk, tg:Id.
. . . . . | . |       ¬(deq-member(...;<l,tg>;1of(1of(
. . . . . | . |                              2of(2of(2of(2of(2of(2of(
. . . . . | . |                              2of(2of((with ds: ds
. . . . . | . |                               init: init
. . . . . | . |                              action a:T
. . . . . | . |                               precondition a(v) is
. . . . . | . |                               P)))))))))))
. . . . . | . |         ⇒
. . . . . | . |         deq-member(KindDeq;kind(a(i;t));2of(
. . . . . | . |                                         1of(
. . . . . | . |                                         2of(2of(2of(
. . . . . | . |                                         2of(2of(2of(
. . . . . | . |                                         2of(
. . . . . | . |                                         ...)))))))))
. . . . . | . |                                         (<l,tg>)))
. . . . . | . |       ⇒
. . . . . | . |       w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . | . | 17. ∀x:Id.
. . . . . | . |     deq-member(IdDeq;x;1of(1of(2of(2of((with ds: ds
. . . . . | . |                                 init: init
. . . . . | . |                                action a:T
. . . . . | . |                                 precondition a(v) is
. . . . . | . |                                 P))))))
. . . . . | . |     ⇒
. . . . . | . |     s(i;0).x
. . . . . | . |     =
. . . . . | . |     2of(1of(2of(2of((with ds: ds
. . . . . | . |              init: init
```

```
. . . . . | . |             action a:T
. . . . . | . |              precondition a(v) is
. . . . . | . |              P)))))
. . . . . | . |     (x)
. . . . . | . | 18. ∀a@0:Action(i).
. . . . . | . |     ¬isnull(a@0)
. . . . . | . |     ⇒
. . . . . | . |     (valtype(i;a@0) ⊆r 1of(2of((with ds: ds
. . . . . | . |                               init: init
. . . . . | . |                              action a:T
. . . . . | . |                               precondition a(v) is
. . . . . | . |                               P)))(kind(a@0))?Top)
. . . . . | . | 19. ∀x:Id.
. . . . . | . |     vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(1of(
. . . . . | . |                                              ...)))→
. . . . . | . |                          2of(1of((with ds: ds
. . . . . | . |                               init: init
. . . . . | . |                              action a:T
. . . . . | . |                               precondition a(v) is
. . . . . | . |                               P)))
. . . . . | . |                          (x)
. . . . . | . |                        else Top fi
. . . . . | . | 20. IdDeq ∈ EqDecider(Id)
. . . . . | . | 21. (λx.init(x)?•) ∈ State(ds)
. . . . . | . | 22. t' : ℕ
. . . . . | . | 23. 0≤t'
. . . . . | . | 24. True ⇒ (∀v:T. ¬P((λx.s(i;t').x),v))
. . . . . | . | 25. ¬(∃t:ℕt'. ¬isnull(a(i;t)))
. . . . . | . | 26. z : Id
. . . . . | . | 27. t : ℤ
. . . . . | . | 28. 0<t
. . . . . | . | 29. t≤t'
. . . . . | . | 30. s(i;0).z = s(i;t-1).z
. . . . . | . | 31. ∀i:Id, t:ℕ.
. . . . . | . |     isnull(a(i;t))
. . . . . | . |     ⇒
. . . . . | . |     (∀x:Id. s(i;t+1).x = s(i;t).x) & m(i;t) = nil

. . . . . | . | 32. ¬isnull(a(i;t-1))
. . . . . | . | ⊢  isnull(a(i;t-1))
. . . . . | . |   by AllHyps
. . . . . | . |      (λh.
. . . . . | . |       Analyze h THEN InstConcl [t-1]
. . . . . | . |       THEN
. . . . . | . |       Complete 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. init : x:Id fp-> ds(x)?Void
. . . . . | . . 7. ∀x:Id. x ∈ dom(ds) ⇒ x ∈ dom(init)
. . . . . | . . 8. v : T
. . . . . | . . 9. P((λx.init(x)?•),v)
```

```
. . . . . | . . 10. w : World
. . . . . | . . 11. FairFifo
. . . . . | . . 12. FairFifo
. . . . . | . . 13. ∀l:IdLnk, tg:Id.
. . . . . | . . |   (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | . . |                    (with ds: ds
. . . . . | . . |                     init: init
. . . . . | . . |                    action a:T
. . . . . | . . |                     precondition a(v) is
. . . . . | . . |                     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(1of(2of((with ds: ds
. . . . . | . . |                             init: init
. . . . . | . . |                            action a:T
. . . . . | . . |                             precondition a(v) is
. . . . . | . . |                             P))))
. . . . . | . . |     ∨ P@0 != 1of(
. . . . . | . . |              2of(2of(2of((with ds: ds
. . . . . | . . |               init: init
. . . . . | . . |              action a:T
. . . . . | . . |               precondition a(v) is
. . . . . | . . |               P)))))(a@0) ==> ∀v:1of(
. . . . . | . . |                                  2of(
. . . . . | . . |                                  ...))(...)?Top.
. . . . . | . . |       ¬P@0((λx.s(i;t').x),v)
. . . . . | . . 16. ∀t:ℕ.
. . . . . | . . |   ¬isnull(a(i;t))
. . . . . | . . |   ⇒
. . . . . | . . |   (islocal(kind(a(i;t)))
. . . . . | . . |    ⇒
. . . . . | . . |    deq-member(IdDeq;act(kind(a(i;t)));1of(1of(
. . . . . | . . |                                       2of(2of(2of(
. . . . . | . . |                                       ...))))))
. . . . . | . . |    ⇒
. . . . . | . . |    2of(1of(2of(2of(2of((with ds: ds
. . . . . | . . |             init: init
. . . . . | . . |            action a:T
. . . . . | . . |             precondition a(v) is
. . . . . | . . |             P))))))
. . . . . | . . |    (act(kind(a(i;t)))
. . . . . | . . |    ,λx.s(i;t).x
. . . . . | . . |    ,val(a(i;t))))
. . . . . | . . |   & (∀x:Id.
. . . . . | . . |      deq-member(product-deq(Knd;Id;...;...);<...
. . . . . | . . |                                           ,x>;...)
. . . . . | . . |      ⇒
. . . . . | . . |      s(i;t+1).x
. . . . . | . . |      =
. . . . . | . . |      2of(1of(2of(2of(2of(2of((with ds: ds
. . . . . | . . |               init: init
```

```
. . . . . | . . |              action a:T
. . . . . | . . |               precondition a(v) is
. . . . . | . . |               P)))))))
. . . . . | . . |      (<kind(a(i;t)),x>
. . . . . | . . |      ,λx.s(i;t).x
. . . . . | . . |      ,val(a(i;t))))
. . . . . | . . |   & (∀l:IdLnk.
. . . . . | . . |      deq-member(...;<kind(a(i;t))
. . . . . | . . |                     ,l>;1of(1of(
. . . . . | . . |                         2of(2of(2of(2of(2of(
. . . . . | . . |                         (with ds: ds
. . . . . | . . |                          init: init
. . . . . | . . |                         action a:T
. . . . . | . . |                          precondition a(v) is
. . . . . | . . |                          P)))))))))
. . . . . | . . |      ⇒
. . . . . | . . |      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(
. . . . . | . . |                              1of(2of(2of(2of(2of(2of(
. . . . . | . . |                                  (with ds: ds
. . . . . | . . |                                   init: init
. . . . . | . . |                                  action a:T
. . . . . | . . |                                   precondition a(v) is
. . . . . | . . |                                   P)))))))
. . . . . | . . |                               (<kind(a(i;t)),l>)))
. . . . . | . . |      else nil fi)
. . . . . | . . |   & (∀x:Id.
. . . . . | . . |      ¬(deq-member(IdDeq;x;1of(1of(
. . . . . | . . |                              2of(2of(2of(2of(2of(2of(
. . . . . | . . |                              (with ds: ds
. . . . . | . . |                               init: init
. . . . . | . . |                              action a:T
. . . . . | . . |                               precondition a(v) is
. . . . . | . . |                               P)))))))))
. . . . . | . . |        ⇒
. . . . . | . . |        deq-member(KindDeq;kind(a(i;t));2of(
. . . . . | . . |                                        1of(
. . . . . | . . |                                        2of(2of(2of(
. . . . . | . . |                                        2of(2of(2of(
. . . . . | . . |                                        ...)))))))))
. . . . . | . . |                                        (x)))
. . . . . | . . |      ⇒
. . . . . | . . |      s(i;t).x = s(i;t+1).x)
. . . . . | . . |   & (∀l:IdLnk, tg:Id.
. . . . . | . . |      ¬(deq-member(...;<l,tg>;1of(1of(
. . . . . | . . |                                 2of(2of(2of(2of(2of(
. . . . . | . . |                                 2of(2of((with ds: ds
. . . . . | . . |                                  init: init
. . . . . | . . |                                 action a:T
```

```
. . . . . | . . |                                precondition a(v) is
. . . . . | . . |                                P)))))))))))
. . . . . | . . |        ⇒
. . . . . | . . |        deq-member(KindDeq;kind(a(i;t));2of(
. . . . . | . . |                                         1of(
. . . . . | . . |                                         2of(2of(2of(
. . . . . | . . |                                         2of(2of(2of(
. . . . . | . . |                                         2of(
. . . . . | . . |                                         ...)))))))))
. . . . . | . . |                                         (<1,tg>)))
. . . . . | . . |      ⇒
. . . . . | . . |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . | . . 17. ∀x:Id.
. . . . . | . . |   deq-member(IdDeq;x;1of(1of(2of(2of((with ds: ds
. . . . . | . . |                                 init: init
. . . . . | . . |                                action a:T
. . . . . | . . |                                 precondition a(v) is
. . . . . | . . |                                 P))))))
. . . . . | . . |   ⇒
. . . . . | . . |   s(i;0).x
. . . . . | . . |   =
. . . . . | . . |   2of(1of(2of(2of((with ds: ds
. . . . . | . . |            init: init
. . . . . | . . |           action a:T
. . . . . | . . |            precondition a(v) is
. . . . . | . . |            P)))))
. . . . . | . . |   (x)
. . . . . | . . 18. ∀a@0:Action(i).
. . . . . | . . |   ¬isnull(a@0)
. . . . . | . . |   ⇒
. . . . . | . . |   (valtype(i;a@0) ⊆r 1of(2of((with ds: ds
. . . . . | . . |                              init: init
. . . . . | . . |                             action a:T
. . . . . | . . |                              precondition a(v) is
. . . . . | . . |                              P)))(kind(a@0))?Top)
. . . . . | . . 19. ∀x:Id.
. . . . . | . . |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(1of(
. . . . . | . . |                                          ...)))→
. . . . . | . . |                       2of(1of((with ds: ds
. . . . . | . . |                            init: init
. . . . . | . . |                           action a:T
. . . . . | . . |                            precondition a(v) is
. . . . . | . . |                            P)))
. . . . . | . . |                      (x)
. . . . . | . . |                  else Top fi
. . . . . | . . 20. IdDeq ∈ EqDecider(Id)
. . . . . | . . 21. (λx.init(x)?•) ∈ State(ds)
. . . . . | . . 22. t' : ℕ
. . . . . | . . 23. 0≤t'
. . . . . | . . 24. True ⇒ (∀v:T. ¬P((λx.s(i;t').x),v))
. . . . . | . . 25. ¬(∃t:ℕt'. ¬isnull(a(i;t)))
. . . . . | . . 26. z : Id
. . . . . | . . 27. t : ℤ
. . . . . | . . 28. 0<t
. . . . . | . . 29. t≤t'
```

```
. . . . . | . . 30. s(i;0).z = s(i;t-1).z
. . . . . | . . 31. ∀i:Id, t:ℕ.
. . . . . | . . |   isnull(a(i;t))
. . . . . | . . |   ⇒
. . . . . | . . |   (∀x:Id. s(i;t+1).x = s(i;t).x) & m(i;t) = nil
. . . . . | . . 32. (∀x:Id. s(i;t-1+1).x = s(i;t-1).x)
. . . . . | . . |   & m(i;t-1) = nil
. . . . . | . . ⊢  s(i;t-1).z = s(i;t).z
. . . . . | . . | by 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. init : x:Id fp-> ds(x)?Void
. . . . . | . . 7. ∀x:Id. x ∈ dom(ds) ⇒ x ∈ dom(init)
. . . . . | . . 8. v : T
. . . . . | . . 9. P((λx.init(x)?•),v)
. . . . . | . . 10. w : World
. . . . . | . . 11. FairFifo
. . . . . | . . 12. FairFifo
. . . . . | . . 13. ∀l:IdLnk, tg:Id.
. . . . . | . . |   (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | . . |                    (with ds: ds
. . . . . | . . |                     init: init
. . . . . | . . |                    action a:T
. . . . . | . . |                     precondition a(v) is
. . . . . | . . |                     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(1of(2of((with ds: ds
. . . . . | . . |                              init: init
. . . . . | . . |                             action a:T
. . . . . | . . |                              precondition a(v) is
. . . . . | . . |                              P))))
. . . . . | . . |     ∨ P@0 != 1of(
. . . . . | . . |              2of(2of(2of((with ds: ds
. . . . . | . . |               init: init
. . . . . | . . |              action a:T
. . . . . | . . |               precondition a(v) is
. . . . . | . . |               P)))))(a@0) ==> ∀v:1of(
. . . . . | . . |                                  2of(
. . . . . | . . |                                  ...))(...)?Top.
. . . . . | . . |       ¬P@0((λx.s(i;t').x),v)
. . . . . | . . 16. ∀t:ℕ.
. . . . . | . . |   ¬isnull(a(i;t))
. . . . . | . . |   ⇒
. . . . . | . . |   (islocal(kind(a(i;t)))
```

```
. . . . . | . . |    ⇒
. . . . . | . . |    deq-member(IdDeq;act(kind(a(i;t)));1of(1of(
. . . . . | . . |                                       2of(2of(2of(
. . . . . | . . |                                       ...))))))
. . . . . | . . |    ⇒
. . . . . | . . |    2of(1of(2of(2of(2of((with ds: ds
. . . . . | . . |             init: init
. . . . . | . . |            action a:T
. . . . . | . . |             precondition a(v) is
. . . . . | . . |             P))))))
. . . . . | . . |    (act(kind(a(i;t)))
. . . . . | . . |    ,λx.s(i;t).x
. . . . . | . . |    ,val(a(i;t))))
. . . . . | . . |   & (∀x:Id.
. . . . . | . . |      deq-member(product-deq(Knd;Id;...;...);<...
. . . . . | . . |                                           ,x>;...)
. . . . . | . . |      ⇒
. . . . . | . . |      s(i;t+1).x
. . . . . | . . |      =
. . . . . | . . |      2of(1of(2of(2of(2of(2of((with ds: ds
. . . . . | . . |               init: init
. . . . . | . . |              action a:T
. . . . . | . . |               precondition a(v) is
. . . . . | . . |               P)))))))
. . . . . | . . |      (<kind(a(i;t)),x>
. . . . . | . . |      ,λx.s(i;t).x
. . . . . | . . |      ,val(a(i;t))))
. . . . . | . . |   & (∀l:IdLnk.
. . . . . | . . |      deq-member(...;<kind(a(i;t))
. . . . . | . . |                     ,l>;1of(1of(
. . . . . | . . |                         2of(2of(2of(2of(2of(
. . . . . | . . |                         (with ds: ds
. . . . . | . . |                          init: init
. . . . . | . . |                         action a:T
. . . . . | . . |                          precondition a(v) is
. . . . . | . . |                          P)))))))))
. . . . . | . . |      ⇒
. . . . . | . . |      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(
. . . . . | . . |                              1of(2of(2of(2of(2of(2of(
. . . . . | . . |                                  (with ds: ds
. . . . . | . . |                                   init: init
. . . . . | . . |                                  action a:T
. . . . . | . . |                                   precondition a(v) is
. . . . . | . . |                                   P)))))))
. . . . . | . . |                              (<kind(a(i;t)),l>)))
. . . . . | . . |      else nil fi)
. . . . . | . . |   & (∀x:Id.
. . . . . | . . |      ¬(deq-member(IdDeq;x;1of(1of(
```

```
. . . . . | . . |                          2of(2of(2of(2of(2of(2of(
. . . . . | . . |                          (with ds: ds
. . . . . | . . |                           init: init
. . . . . | . . |                          action a:T
. . . . . | . . |                           precondition a(v) is
. . . . . | . . |                           P))))))))))
. . . . . | . . |        ⇒
. . . . . | . . |        deq-member(KindDeq;kind(a(i;t));2of(
. . . . . | . . |                                         1of(
. . . . . | . . |                                         2of(2of(2of(
. . . . . | . . |                                         2of(2of(2of(
. . . . . | . . |                                         ...)))))))))
. . . . . | . . |                                         (x)))
. . . . . | . . |      ⇒
. . . . . | . . |      s(i;t).x = s(i;t+1).x)
. . . . . | . . |   & (∀l:IdLnk, tg:Id.
. . . . . | . . |      ¬(deq-member(...;<l,tg>;1of(1of(
. . . . . | . . |                              2of(2of(2of(2of(2of(
. . . . . | . . |                              2of(2of((with ds: ds
. . . . . | . . |                               init: init
. . . . . | . . |                              action a:T
. . . . . | . . |                               precondition a(v) is
. . . . . | . . |                               P))))))))))))
. . . . . | . . |        ⇒
. . . . . | . . |        deq-member(KindDeq;kind(a(i;t));2of(
. . . . . | . . |                                         1of(
. . . . . | . . |                                         2of(2of(2of(
. . . . . | . . |                                         2of(2of(2of(
. . . . . | . . |                                         2of(
. . . . . | . . |                                         ...)))))))))
. . . . . | . . |                                         (<l,tg>)))
. . . . . | . . |      ⇒
. . . . . | . . |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . | . . 17. ∀x:Id.
. . . . . | . . |   deq-member(IdDeq;x;1of(1of(2of(2of((with ds: ds
. . . . . | . . |                               init: init
. . . . . | . . |                              action a:T
. . . . . | . . |                               precondition a(v) is
. . . . . | . . |                               P))))))
. . . . . | . . |   ⇒
. . . . . | . . |   s(i;0).x
. . . . . | . . |   =
. . . . . | . . |   2of(1of(2of(2of((with ds: ds
. . . . . | . . |            init: init
. . . . . | . . |           action a:T
. . . . . | . . |            precondition a(v) is
. . . . . | . . |            P)))))
. . . . . | . . |   (x)
. . . . . | . . 18. ∀a@0:Action(i).
. . . . . | . . |   ¬isnull(a@0)
. . . . . | . . |   ⇒
. . . . . | . . |   (valtype(i;a@0) ⊆r 1of(2of((with ds: ds
. . . . . | . . |                           init: init
. . . . . | . . |                          action a:T
. . . . . | . . |                           precondition a(v) is
```

```
. . . . . | . . |                              P)))(kind(a@0))?Top)
. . . . . | . . 19. ∀x:Id.
. . . . . | . . |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(1of(
. . . . . | . . |                                              ...)))→
. . . . . | . . |                       2of(1of((with ds: ds
. . . . . | . . |                            init: init
. . . . . | . . |                           action a:T
. . . . . | . . |                            precondition a(v) is
. . . . . | . . |                            P)))
. . . . . | . . |                       (x)
. . . . . | . . |                     else Top fi
. . . . . | . . 20. IdDeq ∈ EqDecider(Id)
. . . . . | . . 21. (λx.init(x)?•) ∈ State(ds)
. . . . . | . . 22. t' : ℕ
. . . . . | . . 23. 0≤t'
. . . . . | . . 24. True ⇒ (∀v:T. ¬P((λx.s(i;t').x),v))
. . . . . | . . 25. ¬(∃t:ℕt'. ¬isnull(a(i;t)))
. . . . . | . . 26. z : Id
. . . . . | . . 27. t : ℤ
. . . . . | . . 28. 0<t
. . . . . | . . 29. t≤t'
. . . . . | . . 30. s(i;0).z = s(i;t-1).z
. . . . . | . . 31. ∀i:Id, t:ℕ.
. . . . . | . . |   isnull(a(i;t))
. . . . . | . . |   ⇒
. . . . . | . . |   (∀x:Id. s(i;t+1).x = s(i;t).x) & m(i;t) = nil
. . . . . | . . 32. ∀x:Id. s(i;t-1+1).x = s(i;t-1).x
. . . . . | . . 33. m(i;t-1) = nil
. . . . . | . . 34. s(i;t-1+1).z = s(i;t-1).z
. . . . . | . . ⊢  s(i;t-1).z = s(i;t).z  by Subst ((t-1+1) ∼ 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. init : x:Id fp-> ds(x)?Void
. . . . . | . . | 7. ∀x:Id. x ∈ dom(ds) ⇒ x ∈ dom(init)
. . . . . | . . | 8. v : T
. . . . . | . . | 9. P((λx.init(x)?•),v)
. . . . . | . . | 10. w : World
. . . . . | . . | 11. FairFifo
. . . . . | . . | 12. FairFifo
. . . . . | . . | 13. ∀l:IdLnk, tg:Id.
. . . . . | . . |     (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | . . |                       (with ds: ds
. . . . . | . . |                        init: init
. . . . . | . . |                       action a:T
. . . . . | . . |                        precondition a(v) is
. . . . . | . . |                        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(1of(2of((with ds: ds
. . . . . | . . |                                  init: init
. . . . . | . . |                                 action a:T
. . . . . | . . |                                  precondition a(v) is
. . . . . | . . |                                  P))))
. . . . . | . . |       ∨ P@0 != 1of(
. . . . . | . . |                 2of(2of(2of((with ds: ds
. . . . . | . . |                  init: init
. . . . . | . . |                 action a:T
. . . . . | . . |                  precondition a(v) is
. . . . . | . . |                  P)))))(a@0) ==> ∀v:1of(
. . . . . | . . |                                      2of(
. . . . . | . . |                                      ...))(...)?Top.
. . . . . | . . |          ¬P@0((λx.s(i;t').x),v)
. . . . . | . . | 16. ∀t:ℕ.
. . . . . | . . |     ¬isnull(a(i;t))
. . . . . | . . |     ⇒
. . . . . | . . |     (islocal(kind(a(i;t)))
. . . . . | . . |      ⇒
. . . . . | . . |      deq-member(IdDeq;act(kind(a(i;t)));1of(1of(
. . . . . | . . |                                          2of(2of(2of(
. . . . . | . . |                                          ...))))))
. . . . . | . . |      ⇒
. . . . . | . . |      2of(1of(2of(2of(2of((with ds: ds
. . . . . | . . |                 init: init
. . . . . | . . |                action a:T
. . . . . | . . |                 precondition a(v) is
. . . . . | . . |                 P))))))
. . . . . | . . |      (act(kind(a(i;t)))
. . . . . | . . |      ,λx.s(i;t).x
. . . . . | . . |      ,val(a(i;t))))
. . . . . | . . |     & (∀x:Id.
. . . . . | . . |        deq-member(...;<kind(a(i;t))
. . . . . | . . |                       ,x>;1of(1of(
. . . . . | . . |                           2of(2of(2of(2of(
. . . . . | . . |                           (with ds: ds
. . . . . | . . |                            init: init
. . . . . | . . |                           action a:T
. . . . . | . . |                            precondition a(v) is
. . . . . | . . |                            P))))))))
. . . . . | . . |        ⇒
. . . . . | . . |        s(i;t+1).x
. . . . . | . . |        =
. . . . . | . . |        2of(1of(2of(2of(2of(2of((with ds: ds
. . . . . | . . |                 init: init
. . . . . | . . |                action a:T
. . . . . | . . |                 precondition a(v) is
. . . . . | . . |                 P)))))))
. . . . . | . . |        (<kind(a(i;t)),x>
. . . . . | . . |        ,λx.s(i;t).x
. . . . . | . . |        ,val(a(i;t))))
. . . . . | . . |     & (∀l:IdLnk.
```

```
. . . . . | . . |        deq-member(...;<kind(a(i;t))
. . . . . | . . |                       ,l>;1of(1of(
. . . . . | . . |                           2of(2of(2of(2of(2of(
. . . . . | . . |                           (with ds: ds
. . . . . | . . |                            init: init
. . . . . | . . |                           action a:T
. . . . . | . . |                            precondition a(v) is
. . . . . | . . |                            P)))))))))
. . . . . | . . |        ⇒
. . . . . | . . |        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(
. . . . . | . . |                               1of(
. . . . . | . . |                               2of(2of(2of(2of(2of(
. . . . . | . . |                               (with ds: ds
. . . . . | . . |                                init: init
. . . . . | . . |                               action a:T
. . . . . | . . |                                precondition a(v) is
. . . . . | . . |                                P)))))))
. . . . . | . . |                               (<kind(a(i;t)),l>)))
. . . . . | . . |        else nil fi)
. . . . . | . . |     & (∀x:Id.
. . . . . | . . |           ¬(deq-member(IdDeq;x;1of(1of(
. . . . . | . . |                               2of(2of(2of(2of(2of(2of(2of(
. . . . . | . . |                               (with ds: ds
. . . . . | . . |                                init: init
. . . . . | . . |                               action a:T
. . . . . | . . |                                precondition a(v) is
. . . . . | . . |                                P)))))))))))
. . . . . | . . |             ⇒
. . . . . | . . |             deq-member(KindDeq;kind(a(i;t));2of(
. . . . . | . . |                                           1of(
. . . . . | . . |                                           2of(2of(
. . . . . | . . |                                           2of(2of(
. . . . . | . . |                                           2of(2of(
. . . . . | . . |                                           ...)))))))))
. . . . . | . . |                                           (x)))
. . . . . | . . |           ⇒
. . . . . | . . |           s(i;t).x = s(i;t+1).x)
. . . . . | . . |     & (∀l:IdLnk, tg:Id.
. . . . . | . . |           ¬(deq-member(...;<l,tg>;1of(1of(
. . . . . | . . |                                 2of(2of(2of(2of(2of(2of(
. . . . . | . . |                                 2of(2of((with ds: ds
. . . . . | . . |                                  init: init
. . . . . | . . |                                 action a:T
. . . . . | . . |                                  precondition a(v) is
. . . . . | . . |                                  P)))))))))))
. . . . . | . . |             ⇒
. . . . . | . . |             deq-member(KindDeq;kind(a(i;t));2of(
. . . . . | . . |                                           1of(
```

```
. . . . . | . . |                                          2of(2of(
. . . . . | . . |                                          2of(2of(
. . . . . | . . |                                          2of(2of(
. . . . . | . . |                                          ...)))))))))
. . . . . | . . |                                          (<l,tg>)))
. . . . . | . . |        ⇒
. . . . . | . . |        w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . | . . | 17. ∀x:Id.
. . . . . | . . |     deq-member(IdDeq;x;1of(1of(2of(2of((with ds: ds
. . . . . | . . |                                  init: init
. . . . . | . . |                                 action a:T
. . . . . | . . |                                  precondition a(v) is
. . . . . | . . |                                  P))))))
. . . . . | . . |     ⇒
. . . . . | . . |     s(i;0).x
. . . . . | . . |     =
. . . . . | . . |     2of(1of(2of(2of((with ds: ds
. . . . . | . . |              init: init
. . . . . | . . |             action a:T
. . . . . | . . |              precondition a(v) is
. . . . . | . . |              P)))))
. . . . . | . . |     (x)
. . . . . | . . | 18. ∀a@0:Action(i).
. . . . . | . . |     ¬isnull(a@0)
. . . . . | . . |     ⇒
. . . . . | . . |     (valtype(i;a@0) ⊆r 1of(2of((with ds: ds
. . . . . | . . |                               init: init
. . . . . | . . |                              action a:T
. . . . . | . . |                               precondition a(v) is
. . . . . | . . |                               P)))(kind(a@0))?Top)
. . . . . | . . | 19. ∀x:Id.
. . . . . | . . |     vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(1of(
. . . . . | . . |                                                ...)))→
. . . . . | . . |                          2of(1of((with ds: ds
. . . . . | . . |                               init: init
. . . . . | . . |                              action a:T
. . . . . | . . |                               precondition a(v) is
. . . . . | . . |                               P)))
. . . . . | . . |                           (x)
. . . . . | . . |                       else Top fi
. . . . . | . . | 20. IdDeq ∈ EqDecider(Id)
. . . . . | . . | 21. (λx.init(x)?•) ∈ State(ds)
. . . . . | . . | 22. t' : ℕ
. . . . . | . . | 23. 0≤t'
. . . . . | . . | 24. True ⇒ (∀v:T. ¬P((λx.s(i;t').x),v))
. . . . . | . . | 25. ¬(∃t:ℕt'. ¬isnull(a(i;t)))
. . . . . | . . | 26. z : Id
. . . . . | . . | 27. t : ℤ
. . . . . | . . | 28. 0<t
. . . . . | . . | 29. t≤t'
. . . . . | . . | 30. s(i;0).z = s(i;t-1).z
. . . . . | . . | 31. ∀i:Id, t:ℕ.
. . . . . | . . |     isnull(a(i;t))
. . . . . | . . |     ⇒
. . . . . | . . |     (∀x:Id. s(i;t+1).x = s(i;t).x) & m(i;t) = nil
```

```
. . . . . | . . | 32. ∀x:Id. s(i;t-1+1).x = s(i;t-1).x
. . . . . | . . | 33. m(i;t-1) = nil
. . . . . | . . | 34. s(i;t-1+1).z = s(i;t-1).z
. . . . . | . . | ⊢  (t-1+1) ∼ 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. init : x:Id fp-> ds(x)?Void
. . . . . | . . . 7. ∀x:Id. x ∈ dom(ds) ⇒ x ∈ dom(init)
. . . . . | . . . 8. v : T
. . . . . | . . . 9. P((λx.init(x)?•),v)
. . . . . | . . . 10. w : World
. . . . . | . . . 11. FairFifo
. . . . . | . . . 12. FairFifo
. . . . . | . . . 13. ∀l:IdLnk, tg:Id.
. . . . . | . . . |   (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | . . . |                    (with ds: ds
. . . . . | . . . |                     init: init
. . . . . | . . . |                    action a:T
. . . . . | . . . |                     precondition a(v) is
. . . . . | . . . |                     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(1of(2of((with ds: ds
. . . . . | . . . |                             init: init
. . . . . | . . . |                            action a:T
. . . . . | . . . |                             precondition a(v) is
. . . . . | . . . |                             P))))
. . . . . | . . . |     ∨ P@0 != 1of(
. . . . . | . . . |              2of(2of(2of((with ds: ds
. . . . . | . . . |               init: init
. . . . . | . . . |              action a:T
. . . . . | . . . |               precondition a(v) is
. . . . . | . . . |               P)))))(a@0) ==> ∀v:1of(
. . . . . | . . . |                                  2of(
. . . . . | . . . |                                  ...))(...)?Top.
. . . . . | . . . |       ¬P@0((λx.s(i;t').x),v)
. . . . . | . . . 16. ∀t:ℕ.
. . . . . | . . . |   ¬isnull(a(i;t))
. . . . . | . . . |   ⇒
. . . . . | . . . |   (islocal(kind(a(i;t)))
. . . . . | . . . |    ⇒
. . . . . | . . . |    deq-member(IdDeq;act(kind(a(i;t)));1of(1of(
. . . . . | . . . |                                        2of(2of(2of(
. . . . . | . . . |                                        ...))))))
. . . . . | . . . |    ⇒
. . . . . | . . . |    2of(1of(2of(2of(2of((with ds: ds
```

```
. . . . . | . . . |             init: init
. . . . . | . . . |            action a:T
. . . . . | . . . |             precondition a(v) is
. . . . . | . . . |             P))))))
. . . . . | . . . |    (act(kind(a(i;t)))
. . . . . | . . . |    ,λx.s(i;t).x
. . . . . | . . . |    ,val(a(i;t))))
. . . . . | . . . |   & (∀x:Id.
. . . . . | . . . |      deq-member(...;<kind(a(i;t))
. . . . . | . . . |                     ,x>;1of(1of(
. . . . . | . . . |                         2of(2of(2of(2of(
. . . . . | . . . |                         (with ds: ds
. . . . . | . . . |                          init: init
. . . . . | . . . |                         action a:T
. . . . . | . . . |                          precondition a(v) is
. . . . . | . . . |                          P)))))))
. . . . . | . . . |      ⇒
. . . . . | . . . |      s(i;t+1).x
. . . . . | . . . |      =
. . . . . | . . . |      2of(1of(2of(2of(2of(2of((with ds: ds
. . . . . | . . . |               init: init
. . . . . | . . . |              action a:T
. . . . . | . . . |               precondition a(v) is
. . . . . | . . . |               P)))))))
. . . . . | . . . |      (<kind(a(i;t)),x>
. . . . . | . . . |      ,λx.s(i;t).x
. . . . . | . . . |      ,val(a(i;t))))
. . . . . | . . . |   & (∀l:IdLnk.
. . . . . | . . . |      deq-member(...;<kind(a(i;t))
. . . . . | . . . |                     ,l>;1of(1of(
. . . . . | . . . |                         2of(2of(2of(2of(2of(
. . . . . | . . . |                         (with ds: ds
. . . . . | . . . |                          init: init
. . . . . | . . . |                         action a:T
. . . . . | . . . |                          precondition a(v) is
. . . . . | . . . |                          P)))))))))
. . . . . | . . . |      ⇒
. . . . . | . . . |      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(
. . . . . | . . . |                              1of(
. . . . . | . . . |                              2of(2of(2of(2of(2of(
. . . . . | . . . |                              (with ds: ds
. . . . . | . . . |                               init: init
. . . . . | . . . |                              action a:T
. . . . . | . . . |                               precondition a(v) is
. . . . . | . . . |                               P)))))))
. . . . . | . . . |                              (<kind(a(i;t)),l>)))
. . . . . | . . . |      else nil fi)
. . . . . | . . . |   & (∀x:Id.
```

```
. . . . . | . . . |      ¬(deq-member(IdDeq;x;1of(1of(
. . . . . | . . . |                          2of(2of(2of(2of(2of(2of(
. . . . . | . . . |                          (with ds: ds
. . . . . | . . . |                           init: init
. . . . . | . . . |                          action a:T
. . . . . | . . . |                           precondition a(v) is
. . . . . | . . . |                           P))))))))))
. . . . . | . . . |        ⇒
. . . . . | . . . |        deq-member(KindDeq;kind(a(i;t));2of(
. . . . . | . . . |                                          1of(
. . . . . | . . . |                                          2of(2of(
. . . . . | . . . |                                          2of(2of(
. . . . . | . . . |                                          2of(2of(
. . . . . | . . . |                                          ...)))))))))
. . . . . | . . . |                                          (x)))
. . . . . | . . . |      ⇒
. . . . . | . . . |      s(i;t).x = s(i;t+1).x)
. . . . . | . . . |    & (∀l:IdLnk, tg:Id.
. . . . . | . . . |      ¬(deq-member(...;<l,tg>;1of(1of(
. . . . . | . . . |                               2of(2of(2of(2of(2of(
. . . . . | . . . |                               2of(2of((with ds: ds
. . . . . | . . . |                                init: init
. . . . . | . . . |                               action a:T
. . . . . | . . . |                                precondition a(v) is
. . . . . | . . . |                                P))))))))))
. . . . . | . . . |        ⇒
. . . . . | . . . |        deq-member(KindDeq;kind(a(i;t));2of(
. . . . . | . . . |                                          1of(
. . . . . | . . . |                                          2of(2of(
. . . . . | . . . |                                          2of(2of(
. . . . . | . . . |                                          2of(2of(
. . . . . | . . . |                                          ...)))))))))
. . . . . | . . . |                                          (<l,tg>)))
. . . . . | . . . |      ⇒
. . . . . | . . . |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . | . . . 17. ∀x:Id.
. . . . . | . . . |    deq-member(IdDeq;x;1of(1of(2of(2of((with ds: ds
. . . . . | . . . |                                init: init
. . . . . | . . . |                               action a:T
. . . . . | . . . |                                precondition a(v) is
. . . . . | . . . |                                P))))))
. . . . . | . . . |    ⇒
. . . . . | . . . |    s(i;0).x
. . . . . | . . . |    =
. . . . . | . . . |    2of(1of(2of(2of((with ds: ds
. . . . . | . . . |             init: init
. . . . . | . . . |            action a:T
. . . . . | . . . |             precondition a(v) is
. . . . . | . . . |             P)))))
. . . . . | . . . |    (x)
. . . . . | . . . 18. ∀a@0:Action(i).
. . . . . | . . . |    ¬isnull(a@0)
. . . . . | . . . |    ⇒
. . . . . | . . . |    (valtype(i;a@0) ⊆r 1of(2of((with ds: ds
. . . . . | . . . |                               init: init
```

```
. . . . . | . . . |                          action a:T
. . . . . | . . . |                           precondition a(v) is
. . . . . | . . . |                           P)))(kind(a@0))?Top)
. . . . . | . . . 19. ∀x:Id.
. . . . . | . . . |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(1of(
. . . . . | . . . |                                                ...)))→
. . . . . | . . . |                      2of(1of((with ds: ds
. . . . . | . . . |                           init: init
. . . . . | . . . |                          action a:T
. . . . . | . . . |                           precondition a(v) is
. . . . . | . . . |                           P)))
. . . . . | . . . |                       (x)
. . . . . | . . . |                    else Top fi
. . . . . | . . . 20. IdDeq ∈ EqDecider(Id)
. . . . . | . . . 21. (λx.init(x)?•) ∈ State(ds)
. . . . . | . . . 22. t' : ℕ
. . . . . | . . . 23. 0≤t'
. . . . . | . . . 24. True ⇒ (∀v:T. ¬P((λx.s(i;t').x),v))
. . . . . | . . . 25. ¬(∃t:ℕt'. ¬isnull(a(i;t)))
. . . . . | . . . 26. z : Id
. . . . . | . . . 27. t : ℤ
. . . . . | . . . 28. 0<t
. . . . . | . . . 29. t≤t'
. . . . . | . . . 30. s(i;0).z = s(i;t-1).z
. . . . . | . . . 31. ∀i:Id, t:ℕ.
. . . . . | . . . |   isnull(a(i;t))
. . . . . | . . . |   ⇒
. . . . . | . . . |   (∀x:Id. s(i;t+1).x = s(i;t).x) & m(i;t) = nil
. . . . . | . . . 32. ∀x:Id. s(i;t-1+1).x = s(i;t-1).x
. . . . . | . . . 33. m(i;t-1) = nil
. . . . . | . . . 34. s(i;t).z = s(i;t-1).z
. . . . . | . . . ⊢  s(i;t-1).z = s(i;t).z
. . . . . | . . . | by HypSubst -1 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. init : x:Id fp-> ds(x)?Void
. . . . . | . . . 7. ∀x:Id. x ∈ dom(ds) ⇒ x ∈ dom(init)
. . . . . | . . . 8. v : T
. . . . . | . . . 9. P((λx.init(x)?•),v)
. . . . . | . . . 10. w : World
. . . . . | . . . 11. FairFifo
. . . . . | . . . 12. FairFifo
. . . . . | . . . 13. ∀l:IdLnk, tg:Id.
. . . . . | . . .     (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | . . .                       (with ds: ds
. . . . . | . . .                        init: init
. . . . . | . . .                       action a:T
. . . . . | . . .                        precondition a(v) is
. . . . . | . . .                        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(1of(2of((with ds: ds
. . . . . | . . .                                  init: init
. . . . . | . . .                                 action a:T
. . . . . | . . .                                  precondition a(v) is
. . . . . | . . .                                  P))))
. . . . . | . . .       ∨ P@0 != 1of(
. . . . . | . . .                 2of(2of(2of(2of((with ds: ds
. . . . . | . . .                  init: init
. . . . . | . . .                 action a:T
. . . . . | . . .                  precondition a(v) is
. . . . . | . . .                  P))))))(a@0) ==> ∀v:1of(
. . . . . | . . .                                      2of(
. . . . . | . . .                                      ...))(...)?Top.
. . . . . | . . .          ¬P@0((λx.s(i;t').x),v)
. . . . . | . . . 16. ∀t:ℕ.
. . . . . | . . .     ¬isnull(a(i;t))
. . . . . | . . .     ⇒
. . . . . | . . .     (islocal(kind(a(i;t)))
. . . . . | . . .      ⇒
. . . . . | . . .      deq-member(IdDeq;act(kind(a(i;t)));1of(1of(
. . . . . | . . .                                          2of(2of(2of(
. . . . . | . . .                                          ...))))))
. . . . . | . . .      ⇒
. . . . . | . . .      2of(1of(2of(2of(2of((with ds: ds
. . . . . | . . .                 init: init
. . . . . | . . .                action a:T
. . . . . | . . .                 precondition a(v) is
. . . . . | . . .                 P))))))
. . . . . | . . .      (act(kind(a(i;t)))
. . . . . | . . .      ,λx.s(i;t).x
. . . . . | . . .      ,val(a(i;t))))
. . . . . | . . .     & (∀x:Id.
. . . . . | . . .        deq-member(...;<kind(a(i;t))
. . . . . | . . .                       ,x>;1of(1of(
. . . . . | . . .                           2of(2of(2of(2of(
. . . . . | . . .                           (with ds: ds
. . . . . | . . .                            init: init
. . . . . | . . .                           action a:T
. . . . . | . . .                            precondition a(v) is
. . . . . | . . .                            P))))))))
. . . . . | . . .          ⇒
. . . . . | . . .          s(i;t+1).x
. . . . . | . . .          =
. . . . . | . . .          2of(1of(2of(2of(2of(2of((with ds: ds
. . . . . | . . .                   init: init
. . . . . | . . .                  action a:T
. . . . . | . . .                   precondition a(v) is
. . . . . | . . .                   P)))))))
. . . . . | . . .          (<kind(a(i;t)),x>
. . . . . | . . .          ,λx.s(i;t).x
```

```
. . . . . | . . .        ,val(a(i;t))))
. . . . . | . . .     & (∀l:IdLnk.
. . . . . | . . .        deq-member(...;<kind(a(i;t))
. . . . . | . . .                      ,l>;1of(1of(
. . . . . | . . .                          2of(2of(2of(2of(2of(
. . . . . | . . .                          (with ds: ds
. . . . . | . . .                           init: init
. . . . . | . . .                          action a:T
. . . . . | . . .                           precondition a(v) is
. . . . . | . . .                           P)))))))))
. . . . . | . . .        ⇒
. . . . . | . . .        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(
. . . . . | . . .                            1of(
. . . . . | . . .                            2of(2of(2of(2of(2of(
. . . . . | . . .                            (with ds: ds
. . . . . | . . .                             init: init
. . . . . | . . .                            action a:T
. . . . . | . . .                             precondition a(v) is
. . . . . | . . .                             P)))))))))
. . . . . | . . .                            (<kind(a(i;t)),l>)))
. . . . . | . . .        else nil fi)
. . . . . | . . .     & (∀x:Id.
. . . . . | . . .        ¬(deq-member(IdDeq;x;1of(1of(
. . . . . | . . .                           2of(2of(2of(2of(2of(2of(2of(
. . . . . | . . .                           (with ds: ds
. . . . . | . . .                            init: init
. . . . . | . . .                           action a:T
. . . . . | . . .                            precondition a(v) is
. . . . . | . . .                            P)))))))))))
. . . . . | . . .          ⇒
. . . . . | . . .          deq-member(KindDeq;kind(a(i;t));2of(
. . . . . | . . .                                          1of(
. . . . . | . . .                                          2of(2of(
. . . . . | . . .                                          2of(2of(
. . . . . | . . .                                          2of(2of(
. . . . . | . . .                                          ...)))))))))
. . . . . | . . .                                          (x)))
. . . . . | . . .        ⇒
. . . . . | . . .        s(i;t).x = s(i;t+1).x)
. . . . . | . . .     & (∀l:IdLnk, tg:Id.
. . . . . | . . .        ¬(deq-member(...;<l,tg>;1of(1of(
. . . . . | . . .                              2of(2of(2of(2of(2of(2of(
. . . . . | . . .                              2of(2of((with ds: ds
. . . . . | . . .                               init: init
. . . . . | . . .                              action a:T
. . . . . | . . .                               precondition a(v) is
. . . . . | . . .                               P)))))))))))
. . . . . | . . .          ⇒
```

```
. . . . . | . . .          deq-member(KindDeq;kind(a(i;t));2of(
. . . . . | . . .                                          1of(
. . . . . | . . .                                          2of(2of(
. . . . . | . . .                                          2of(2of(
. . . . . | . . .                                          2of(2of(
. . . . . | . . .                                          ...)))))))))
. . . . . | . . .                                          (<1,tg>)))
. . . . . | . . .        ⇒
. . . . . | . . .        w-tagged(tg; onlnk(1;m(i;t))) = nil)
. . . . . | . . . 17. ∀x:Id.
. . . . . | . . .     deq-member(IdDeq;x;1of(1of(2of(2of((with ds: ds
. . . . . | . . .                                  init: init
. . . . . | . . .                                 action a:T
. . . . . | . . .                                  precondition a(v) is
. . . . . | . . .                                  P))))))
. . . . . | . . .     ⇒
. . . . . | . . .     s(i;0).x
. . . . . | . . .     =
. . . . . | . . .     2of(1of(2of(2of((with ds: ds
. . . . . | . . .              init: init
. . . . . | . . .             action a:T
. . . . . | . . .              precondition a(v) is
. . . . . | . . .              P)))))
. . . . . | . . .     (x)
. . . . . | . . . 18. ∀a@0:Action(i).
. . . . . | . . .     ¬isnull(a@0)
. . . . . | . . .     ⇒
. . . . . | . . .     (valtype(i;a@0) ⊆r 1of(2of((with ds: ds
. . . . . | . . .                               init: init
. . . . . | . . .                              action a:T
. . . . . | . . .                               precondition a(v) is
. . . . . | . . .                               P)))(kind(a@0))?Top)
. . . . . | . . . 19. ∀x:Id.
. . . . . | . . .     vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(1of(
. . . . . | . . .                                              ...)))→
. . . . . | . . .                         2of(1of((with ds: ds
. . . . . | . . .                              init: init
. . . . . | . . .                             action a:T
. . . . . | . . .                              precondition a(v) is
. . . . . | . . .                              P)))
. . . . . | . . .                          (x)
. . . . . | . . .                       else Top fi
. . . . . | . . . 20. IdDeq ∈ EqDecider(Id)
. . . . . | . . . 21. (λx.init(x)?•) ∈ State(ds)
. . . . . | . . . 22. t' : ℕ
. . . . . | . . . 23. 0≤t'
. . . . . | . . . 24. True ⇒ (∀v:T. ¬P((λx.s(i;t').x),v))
. . . . . | . . . 25. ¬(∃t:ℕt'. ¬isnull(a(i;t)))
. . . . . | . . . 26. z : Id
. . . . . | . . . 27. t : ℤ
. . . . . | . . . 28. 0<t
. . . . . | . . . 29. t≤t'
. . . . . | . . . 30. s(i;0).z = s(i;t-1).z
. . . . . | . . . 31. ∀i:Id, t:ℕ.
. . . . . | . . .     isnull(a(i;t))
```

```
. . . . . | . . .     ⇒
. . . . . | . . .     (∀x:Id. s(i;t+1).x = s(i;t).x) & m(i;t) = nil
. . . . . | . . . 32. ∀x:Id. s(i;t-1+1).x = s(i;t-1).x
. . . . . | . . . 33. m(i;t-1) = nil
. . . . . | . . . 34. s(i;t).z = s(i;t-1).z
. . . . . | . . . 35. vartype(i;z)
. . . . . | . . . ⊢  vartype(i;z) ⊆r ds(z)?Top
. . . . . | . . .   by AllHyps
. . . . . | . . .      (λh.
. . . . . | . . .       Repeat
. . . . . | . . .       (Unfolds [‘ma-single-pre-init‘;‘mk-ma‘] h
. . . . . | . . .        THEN
. . . . . | . . .        Reduce h))
. . . . . | . . .      THEN
. . . . . | . . .      Repeat
. . . . . | . . .      (Unfolds [‘fpf-cap‘;‘fpf-ap‘;‘fpf-dom‘] 0)
. . . . . | . . .      THEN
. . . . . | . . .      BackThruSomeHyp
. . . . . |
. . . . . .\
. . . . . . 1. i : Id
. . . . . . 2. a : Id
. . . . . . 3. T : Type
. . . . . . 4. ds : x:Id fp-> Type
. . . . . . 5. P : State(ds)→T→Prop
. . . . . . 6. init : x:Id fp-> ds(x)?Void
. . . . . . 7. ∀x:Id. x ∈ dom(ds) ⇒ x ∈ dom(init)
. . . . . . 8. v : T
. . . . . . 9. P((λx.init(x)?•),v)
. . . . . . 10. w : World
. . . . . . 11. FairFifo
. . . . . . 12. FairFifo
. . . . . . 13. ∀l:IdLnk, tg:Id.
. . . . . . |   (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . . |                    (with ds: ds
. . . . . . |                     init: init
. . . . . . |                    action a:T
. . . . . . |                     precondition a(v) is
. . . . . . |                     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(1of(2of((with ds: ds
. . . . . . |                              init: init
. . . . . . |                             action a:T
. . . . . . |                              precondition a(v) is
. . . . . . |                              P))))
. . . . . . |     ∨ P@0 != 1of(
. . . . . . |              2of(2of(2of((with ds: ds
. . . . . . |               init: init
. . . . . . |              action a:T
. . . . . . |               precondition a(v) is
```

```
. . . . . |              P)))))(a@0) ==> ∀v:1of(
. . . . . |                                  2of((with ds: ds
. . . . . |                                   init: init
. . . . . |                                  action a:T
. . . . . |                                   precondition a(v) is
. . . . . |                                   P)))(locl(a@0))?Top.
. . . . . |      ¬P@0((λx.s(i;t').x),v)
. . . . . 16. ∀t:ℕ.
. . . . . |   ¬isnull(a(i;t))
. . . . . |   ⇒
. . . . . |   (islocal(kind(a(i;t)))
. . . . . |    ⇒
. . . . . |    deq-member(IdDeq;act(kind(a(i;t)));1of(1of(
. . . . . |                                       2of(2of(2of(
. . . . . |                                       ...))))))
. . . . . |    ⇒
. . . . . |    2of(1of(2of(2of(2of((with ds: ds
. . . . . |             init: init
. . . . . |            action a:T
. . . . . |             precondition a(v) is
. . . . . |             P))))))
. . . . . |    (act(kind(a(i;t)))
. . . . . |    ,λx.s(i;t).x
. . . . . |    ,val(a(i;t))))
. . . . . |   & (∀x:Id.
. . . . . |      deq-member(product-deq(Knd;Id;KindDeq;...);<...
. . . . . |                                                 ,x>;...)
. . . . . |      ⇒
. . . . . |      s(i;t+1).x
. . . . . |      =
. . . . . |      2of(1of(2of(2of(2of(2of((with ds: ds
. . . . . |               init: init
. . . . . |              action a:T
. . . . . |               precondition a(v) is
. . . . . |               P)))))))
. . . . . |      (<kind(a(i;t)),x>
. . . . . |      ,λx.s(i;t).x
. . . . . |      ,val(a(i;t))))
. . . . . |   & (∀l:IdLnk.
. . . . . |      deq-member(product-deq(Knd;IdLnk;...;...);<...
. . . . . |                                               ,l>;...)
. . . . . |      ⇒
. . . . . |      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(1of(2of(2of(2of(2of(2of(
. . . . . |                                    (with ds: ds
. . . . . |                                     init: init
. . . . . |                                    action a:T
. . . . . |                                     precondition a(v) is
. . . . . |                                     P))))))))
```

```
. . . . . |                              (<kind(a(i;t)),1>)))
. . . . . |      else nil fi)
. . . . . |   & (∀x:Id.
. . . . . |      ¬(deq-member(IdDeq;x;1of(1of(2of(2of(2of(2of(2of(
. . . . . |                                  2of((with ds: ds
. . . . . |                                   init: init
. . . . . |                                  action a:T
. . . . . |                                   precondition a(v) is
. . . . . |                                   P))))))))))
. . . . . |        ⇒
. . . . . |        deq-member(KindDeq;kind(a(i;t));2of(
. . . . . |                                        1of(
. . . . . |                                        2of(2of(2of(2of(
. . . . . |                                        2of(2of(
. . . . . |                                        ...)))))))))
. . . . . |                                        (x)))
. . . . . |      ⇒
. . . . . |      s(i;t).x = s(i;t+1).x)
. . . . . |   & (∀l:IdLnk, tg:Id.
. . . . . |      ¬(deq-member(product-deq(IdLnk;Id;...;...);...;...)
. . . . . |        ⇒
. . . . . |        deq-member(KindDeq;kind(a(i;t));2of(
. . . . . |                                        1of(
. . . . . |                                        2of(2of(2of(2of(
. . . . . |                                        2of(2of(2of(
. . . . . |                                        ...)))))))))
. . . . . |                                        (<l,tg>)))
. . . . . |      ⇒
. . . . . |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . 17. ∀x:Id.
. . . . . |   deq-member(IdDeq;x;1of(1of(2of(2of((with ds: ds
. . . . . |                                  init: init
. . . . . |                                 action a:T
. . . . . |                                  precondition a(v) is
. . . . . |                                  P))))))
. . . . . |   ⇒
. . . . . |   s(i;0).x
. . . . . |   =
. . . . . |   2of(1of(2of(2of((with ds: ds
. . . . . |            init: init
. . . . . |           action a:T
. . . . . |            precondition a(v) is
. . . . . |            P)))))
. . . . . |   (x)
. . . . . 18. ∀a@0:Action(i).
. . . . . |   ¬isnull(a@0)
. . . . . |   ⇒
. . . . . |   (valtype(i;a@0) ⊆r 1of(2of((with ds: ds
. . . . . |                             init: init
. . . . . |                            action a:T
. . . . . |                             precondition a(v) is
. . . . . |                             P)))(kind(a@0))?Top)
. . . . . 19. ∀x:Id.
. . . . . |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(1of(
. . . . . |                                          ...)))→
```

```
. . . . . |                      2of(1of((with ds: ds
. . . . . |                           init: init
. . . . . |                          action a:T
. . . . . |                           precondition a(v) is
. . . . . |                           P)))
. . . . . |                     (x)
. . . . . |                  else Top fi
. . . . . 20. IdDeq ∈ EqDecider(Id)
. . . . . 21. (λx.init(x)?•) ∈ State(ds)
. . . . . 22. t' : ℕ
. . . . . 23. 0≤t'
. . . . . 24. True ⇒ (∀v:T. ¬P((λx.s(i;t').x),v))
. . . . . 25. ¬(∃t:ℕt'. ¬isnull(a(i;t)))
. . . . . ⊢  (λx.s(i;0).x) = (λx.init(x)?•)
. . . . . | by 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. init : x:Id fp-> ds(x)?Void
. . . . . | 7. ∀x:Id. x ∈ dom(ds) ⇒ x ∈ dom(init)
. . . . . | 8. v : T
. . . . . | 9. P((λx.init(x)?•),v)
. . . . . | 10. w : World
. . . . . | 11. FairFifo
. . . . . | 12. FairFifo
. . . . . | 13. ∀l:IdLnk, tg:Id.
. . . . . | |   (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | |                     (with ds: ds
. . . . . | |                      init: init
. . . . . | |                     action a:T
. . . . . | |                      precondition a(v) is
. . . . . | |                      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(1of(2of((with ds: ds
. . . . . | |                              init: init
. . . . . | |                             action a:T
. . . . . | |                              precondition a(v) is
. . . . . | |                              P))))
. . . . . | |     ∨ P@0 != 1of(
. . . . . | |              2of(2of(2of((with ds: ds
. . . . . | |               init: init
. . . . . | |              action a:T
. . . . . | |               precondition a(v) is
. . . . . | |               P)))))(a@0) ==> ∀v:1of(
. . . . . | |                                  2of((with ds: ds
```

```
. . . . . | |                                  init: init
. . . . . | |                                 action a:T
. . . . . | |                                  precondition a(v) is
. . . . . | |                                  P)))(locl(a@0))?Top.
. . . . . | |       ¬P@0((λx.s(i;t').x),v)
. . . . . | 16. ∀t:ℕ.
. . . . . | |   ¬isnull(a(i;t))
. . . . . | |   ⇒
. . . . . | |   (islocal(kind(a(i;t)))
. . . . . | |    ⇒
. . . . . | |    deq-member(IdDeq;act(kind(a(i;t)));1of(1of(
. . . . . | |                                       2of(2of(2of(
. . . . . | |                                       ...)))))))
. . . . . | |    ⇒
. . . . . | |    2of(1of(2of(2of(2of((with ds: ds
. . . . . | |             init: init
. . . . . | |            action a:T
. . . . . | |             precondition a(v) is
. . . . . | |             P))))))
. . . . . | |    (act(kind(a(i;t)))
. . . . . | |    ,λx.s(i;t).x
. . . . . | |    ,val(a(i;t))))
. . . . . | |   & (∀x:Id.
. . . . . | |      deq-member(product-deq(Knd;Id;...;IdDeq);<...
. . . . . | |                                                ,x>;...)
. . . . . | |      ⇒
. . . . . | |      s(i;t+1).x
. . . . . | |      =
. . . . . | |      2of(1of(2of(2of(2of(2of((with ds: ds
. . . . . | |               init: init
. . . . . | |              action a:T
. . . . . | |               precondition a(v) is
. . . . . | |               P)))))))
. . . . . | |      (<kind(a(i;t)),x>
. . . . . | |      ,λx.s(i;t).x
. . . . . | |      ,val(a(i;t))))
. . . . . | |   & (∀l:IdLnk.
. . . . . | |      deq-member(product-deq(Knd;...;...;...);<...
. . . . . | |                                              ,l>;...)
. . . . . | |      ⇒
. . . . . | |      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(
. . . . . | |                              1of(2of(2of(2of(2of(2of(
. . . . . | |                                  (with ds: ds
. . . . . | |                                   init: init
. . . . . | |                                  action a:T
. . . . . | |                                   precondition a(v) is
. . . . . | |                                   P)))))))
. . . . . | |                              (<kind(a(i;t)),l>)))
```

```
. . . . . | |      else nil fi)
. . . . . | |   & (∀x:Id.
. . . . . | |      ¬(deq-member(IdDeq;x;1of(1of(
. . . . . | |                          2of(2of(2of(2of(2of(2of(
. . . . . | |                          (with ds: ds
. . . . . | |                           init: init
. . . . . | |                          action a:T
. . . . . | |                           precondition a(v) is
. . . . . | |                           P))))))))))
. . . . . | |        ⇒
. . . . . | |        deq-member(KindDeq;kind(a(i;t));2of(
. . . . . | |                                        1of(
. . . . . | |                                        2of(2of(2of(
. . . . . | |                                        2of(2of(2of(
. . . . . | |                                        ...)))))))))
. . . . . | |                                        (x)))
. . . . . | |      ⇒
. . . . . | |      s(i;t).x = s(i;t+1).x)
. . . . . | |   & (∀l:IdLnk, tg:Id.
. . . . . | |      ¬(deq-member(product-deq(...;Id;...;...);...;...)
. . . . . | |        ⇒
. . . . . | |        deq-member(KindDeq;kind(a(i;t));2of(
. . . . . | |                                        1of(
. . . . . | |                                        2of(2of(2of(
. . . . . | |                                        2of(2of(2of(
. . . . . | |                                        2of(
. . . . . | |                                        ...)))))))))
. . . . . | |                                        (<l,tg>)))
. . . . . | |      ⇒
. . . . . | |      w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . | 17. ∀x:Id.
. . . . . | |   deq-member(IdDeq;x;1of(1of(2of(2of((with ds: ds
. . . . . | |                                 init: init
. . . . . | |                                action a:T
. . . . . | |                                 precondition a(v) is
. . . . . | |                                 P))))))
. . . . . | |   ⇒
. . . . . | |   s(i;0).x
. . . . . | |   =
. . . . . | |   2of(1of(2of(2of((with ds: ds
. . . . . | |            init: init
. . . . . | |           action a:T
. . . . . | |            precondition a(v) is
. . . . . | |            P)))))
. . . . . | |   (x)
. . . . . | 18. ∀a@0:Action(i).
. . . . . | |   ¬isnull(a@0)
. . . . . | |   ⇒
. . . . . | |   (valtype(i;a@0) ⊆r 1of(2of((with ds: ds
. . . . . | |                             init: init
. . . . . | |                            action a:T
. . . . . | |                             precondition a(v) is
. . . . . | |                             P)))(kind(a@0))?Top)
. . . . . | 19. ∀x:Id.
. . . . . | |   vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(1of(
```

```
. . . . . | |                                          ...)))→
. . . . . | |                     2of(1of((with ds: ds
. . . . . | |                              init: init
. . . . . | |                             action a:T
. . . . . | |                              precondition a(v) is
. . . . . | |                              P)))
. . . . . | |                     (x)
. . . . . | |                   else Top fi
. . . . . | 20. IdDeq ∈ EqDecider(Id)
. . . . . | 21. (λx.init(x)?•) ∈ State(ds)
. . . . . | 22. t' : ℕ
. . . . . | 23. 0≤t'
. . . . . | 24. True ⇒ (∀v:T. ¬P((λx.s(i;t').x),v))
. . . . . | 25. ¬(∃t:ℕt'. ¬isnull(a(i;t)))
. . . . . | 26. x : Id
. . . . . | ⊢  s(i;0).x = init(x)?•
. . . . . | | by AllHyps

. . . . . | |    (λi.
. . . . . | |     Repeat
. . . . . | |     (Unfolds [‘ma-single-pre-init‘;‘mk-ma‘] i
. . . . . | |      THEN
. . . . . | |      Reduce i))
. . . . . | |
. . . . . | 1. i : Id
. . . . . | 2. a : Id
. . . . . | 3. T : Type
. . . . . | 4. ds : x:Id fp-> Type
. . . . . | 5. P : State(ds)→T→Prop
. . . . . | 6. init : x:Id fp-> ds(x)?Void
. . . . . | 7. ∀x:Id. x ∈ dom(ds) ⇒ x ∈ dom(init)
. . . . . | 8. v : T
. . . . . | 9. P((λx.init(x)?•),v)
. . . . . | 10. w : World
. . . . . | 11. FairFifo
. . . . . | 12. FairFifo
. . . . . | 13. ∀l:IdLnk, tg:Id.
. . . . . | |   (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | |                    <ds,locl(a) : T,init,a : 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) : T)
. . . . . | |     ∨ P@0 != a : P(a@0) ==> ∀v:locl(a) : T(...)?Top.
. . . . . | |       ¬P@0((λx.s(i;t').x),v)
. . . . . | 16. ∀t:ℕ.
. . . . . | |   ¬isnull(a(i;t))
. . . . . | |   ⇒
. . . . . | |   (islocal(kind(a(i;t)))
. . . . . | |    ⇒
. . . . . | |    deq-member(IdDeq;act(kind(a(i;t)));1of(a : P))
. . . . . | |    ⇒
. . . . . | |    2of(a : P)
```

```
. . . . . | |    (act(kind(a(i;t)))
. . . . . | |    ,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)
. . . . . | 17. ∀x:Id.
. . . . . | |   deq-member(IdDeq;x;1of(init))
. . . . . | |   ⇒
. . . . . | |   s(i;0).x = 2of(init)(x)
. . . . . | 18. ∀a@0:Action(i).
. . . . . | |   ¬isnull(a@0)
. . . . . | |   ⇒
. . . . . | |   (valtype(i;a@0) ⊆r locl(a) : 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. (λx.init(x)?•) ∈ State(ds)
. . . . . | 22. t' : ℕ
. . . . . | 23. 0≤t'
. . . . . | 24. True ⇒ (∀v:T. ¬P((λx.s(i;t').x),v))
```

```
. . . . . | 25. ¬(∃t:ℕt'. ¬isnull(a(i;t)))
. . . . . | 26. x : Id
. . . . . | ⊢  s(i;0).x = init(x)?•
. . . . . | | by RW (AddrC [3] (UnfoldC `fpf-cap`)) 0
. . . . . | |    THEN
. . . . . | |    SplitOnConclITE
. . . . . | |
. . . . . | |\
. . . . . | | .....truecase .....
. . . . . | | 1. i : Id
. . . . . | | 2. a : Id
. . . . . | | 3. T : Type
. . . . . | | 4. ds : x:Id fp-> Type
. . . . . | | 5. P : State(ds)→T→Prop
. . . . . | | 6. init : x:Id fp-> ds(x)?Void
. . . . . | | 7. ∀x:Id. x ∈ dom(ds) ⇒ x ∈ dom(init)
. . . . . | | 8. v : T
. . . . . | | 9. P((λx.init(x)?•),v)
. . . . . | | 10. w : World
. . . . . | | 11. FairFifo
. . . . . | | 12. FairFifo
. . . . . | | 13. ∀l:IdLnk, tg:Id.
. . . . . | | |   (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | | |                    <ds
. . . . . | | |                    ,locl(a) : T
. . . . . | | |                    ,init
. . . . . | | |                    ,a : 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) : T)
. . . . . | | |     ∨ P@0 != a : P(a@0) ==> ∀v:locl(a) : T(...)?Top.
. . . . . | | |       ¬P@0((λx.s(i;t').x),v)
. . . . . | | 16. ∀t:ℕ.
. . . . . | | |   ¬isnull(a(i;t))
. . . . . | | |   ⇒
. . . . . | | |   (islocal(kind(a(i;t)))
. . . . . | | |    ⇒
. . . . . | | |    deq-member(IdDeq;act(kind(a(i;t)));1of(a : P))
. . . . . | | |    ⇒
. . . . . | | |    2of(a : P)
. . . . . | | |    (act(kind(a(i;t)))
. . . . . | | |    ,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)
. . . . . | | 17. ∀x:Id.
. . . . . | | |   deq-member(IdDeq;x;1of(init))
. . . . . | | |   ⇒
. . . . . | | |   s(i;0).x = 2of(init)(x)
. . . . . | | 18. ∀a@0:Action(i).
. . . . . | | |   ¬isnull(a@0)
. . . . . | | |   ⇒
. . . . . | | |   (valtype(i;a@0) ⊆r locl(a) : 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. (λx.init(x)?•) ∈ State(ds)
. . . . . | | 22. t' : ℕ
. . . . . | | 23. 0≤t'
. . . . . | | 24. True ⇒ (∀v:T. ¬P((λx.s(i;t').x),v))
. . . . . | | 25. ¬(∃t:ℕt'. ¬isnull(a(i;t)))

. . . . . | | 26. x : Id
. . . . . | | 27. x ∈ dom(init)
. . . . . | | ⊢  s(i;0).x = init(x)  by InstHyp [x] 17
```

```
. . . . . | | |
. . . . . | | |\
. . . . . | | | .....antecedent .....
. . . . . | | | 1. i : Id
. . . . . | | | 2. a : Id
. . . . . | | | 3. T : Type
. . . . . | | | 4. ds : x:Id fp-> Type
. . . . . | | | 5. P : State(ds)→T→Prop
. . . . . | | | 6. init : x:Id fp-> ds(x)?Void
. . . . . | | | 7. ∀x:Id. x ∈ dom(ds) ⇒ x ∈ dom(init)
. . . . . | | | 8. v : T
. . . . . | | | 9. P((λx.init(x)?•),v)
. . . . . | | | 10. w : World
. . . . . | | | 11. FairFifo
. . . . . | | | 12. FairFifo
. . . . . | | | 13. ∀l:IdLnk, tg:Id.
. . . . . | | |     (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | | |                        <ds
. . . . . | | |                        ,locl(a) : T
. . . . . | | |                        ,init
. . . . . | | |                        ,a : 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) : T)
. . . . . | | |       ∨ P@0 != a : P(a@0) ==> ∀v:... : T(...)?Top.
. . . . . | | |         ¬P@0((λx.s(i;t').x),v)
. . . . . | | | 16. ∀t:ℕ.
. . . . . | | |     ¬isnull(a(i;t))
. . . . . | | |     ⇒
. . . . . | | |     (islocal(kind(a(i;t)))
. . . . . | | |      ⇒
. . . . . | | |      deq-member(IdDeq;act(kind(a(i;t)));1of(a : P))
. . . . . | | |      ⇒
. . . . . | | |      2of(a : P)
. . . . . | | |      (act(kind(a(i;t)))
. . . . . | | |      ,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)
. . . . . | | | 17. ∀x:Id.
. . . . . | | |     deq-member(IdDeq;x;1of(init))
. . . . . | | |     ⇒
. . . . . | | |     s(i;0).x = 2of(init)(x)
. . . . . | | | 18. ∀a@0:Action(i).
. . . . . | | |     ¬isnull(a@0)
. . . . . | | |     ⇒
. . . . . | | |     (valtype(i;a@0) ⊆r locl(a) : 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. (λx.init(x)?·) ∈ State(ds)
. . . . . | | | 22. t' : ℕ
. . . . . | | | 23. 0≤t'
. . . . . | | | 24. True ⇒ (∀v:T. ¬P((λx.s(i;t').x),v))
. . . . . | | | 25. ¬(∃t:ℕt'. ¬isnull(a(i;t)))
. . . . . | | | 26. x : Id
. . . . . | | | 27. x ∈ dom(init)
. . . . . | | | ⊢  deq-member(IdDeq;x;1of(init))
. . . . . | | |   by Fold ‘fpf-dom‘ 0
. . . . . | | |
. . . . . | | .\
. . . . . | | . 1. i : Id
. . . . . | | . 2. a : Id
. . . . . | | . 3. T : Type
. . . . . | | . 4. ds : x:Id fp-> Type
. . . . . | | . 5. P : State(ds)→T→Prop
```

```
. . . . . | | . 6. init : x:Id fp-> ds(x)?Void
. . . . . | | . 7. ∀x:Id. x ∈ dom(ds) ⇒ x ∈ dom(init)
. . . . . | | . 8. v : T
. . . . . | | . 9. P((λx.init(x)?•),v)
. . . . . | | . 10. w : World
. . . . . | | . 11. FairFifo
. . . . . | | . 12. FairFifo
. . . . . | | . 13. ∀l:IdLnk, tg:Id.
. . . . . | | . |   (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | | . |                    <ds
. . . . . | | . |                    ,locl(a) : T
. . . . . | | . |                    ,init
. . . . . | | . |                    ,a : 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) : T)
. . . . . | | . |     ∨ P@0 != a : P(a@0) ==> ∀v:... : T(...)?Top.
. . . . . | | . |       ¬P@0((λx.s(i;t').x),v)
. . . . . | | . 16. ∀t:ℕ.
. . . . . | | . |   ¬isnull(a(i;t))
. . . . . | | . |   ⇒
. . . . . | | . |   (islocal(kind(a(i;t)))
. . . . . | | . |    ⇒
. . . . . | | . |    deq-member(IdDeq;act(kind(a(i;t)));1of(a : P))
. . . . . | | . |    ⇒
. . . . . | | . |    2of(a : P)
. . . . . | | . |    (act(kind(a(i;t)))
. . . . . | | . |    ,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))
. . . . . | | . |                                     ,1>)))
. . . . . | | . |     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)
. . . . . | | . 17. ∀x:Id.
. . . . . | | . |   deq-member(IdDeq;x;1of(init))
. . . . . | | . |   ⇒
. . . . . | | . |   s(i;0).x = 2of(init)(x)
. . . . . | | . 18. ∀a@0:Action(i).
. . . . . | | . |   ¬isnull(a@0)
. . . . . | | . |   ⇒
. . . . . | | . |   (valtype(i;a@0) ⊆r locl(a) : 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. (λx.init(x)?•) ∈ State(ds)

. . . . . | | . 22. t' : ℕ
. . . . . | | . 23. 0≤t'
. . . . . | | . 24. True ⇒ (∀v:T. ¬P((λx.s(i;t').x),v))
. . . . . | | . 25. ¬(∃t:ℕt'. ¬isnull(a(i;t)))
. . . . . | | . 26. x : Id
. . . . . | | . 27. x ∈ dom(init)
. . . . . | | . 28. s(i;0).x = 2of(init)(x)
. . . . . | | . ⊢  s(i;0).x = init(x)
. . . . . | | . | by Repeat
. . . . . | | . |    (Unfolds [‘fpf-cap‘;‘fpf-dom‘;‘fpf-ap‘] 0)
. . . . . | | . |    THEN
. . . . . | | . |    SplitOnHypITE -1
. . . . . | | . |    THENA
. . . . . | | . |    (Auto THEN DVar ‘ds’)
. . . . . | | . |
. . . . . | | . |\
. . . . . | | . | .....truecase .....
. . . . . | | . | 1. i : Id
. . . . . | | . | 2. a : Id
. . . . . | | . | 3. T : Type
. . . . . | | . | 4. ds : x:Id fp-> Type
. . . . . | | . | 5. P : State(ds)→T→Prop
. . . . . | | . | 6. init : x:Id fp-> ds(x)?Void
```

```
. . . . . | | . | 7. ∀x:Id. x ∈ dom(ds) ⇒ x ∈ dom(init)
. . . . . | | . | 8. v : T
. . . . . | | . | 9. P((λx.init(x)?•),v)
. . . . . | | . | 10. w : World
. . . . . | | . | 11. FairFifo
. . . . . | | . | 12. FairFifo
. . . . . | | . | 13. ∀l:IdLnk, tg:Id.
. . . . . | | . |     (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | | . |                        <ds
. . . . . | | . |                        ,locl(a) : T
. . . . . | | . |                        ,init
. . . . . | | . |                        ,a : 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) : T)
. . . . . | | . |       ∨ P@0 != a : P(a@0) ==> ∀v:... : T(...)?Top.
. . . . . | | . |         ¬P@0((λx.s(i;t').x),v)
. . . . . | | . | 16. ∀t:ℕ.
. . . . . | | . |     ¬isnull(a(i;t))
. . . . . | | . |     ⇒
. . . . . | | . |     (islocal(kind(a(i;t)))
. . . . . | | . |      ⇒
. . . . . | | . |      deq-member(IdDeq;act(kind(a(i;t)));1of(
. . . . . | | . |                                        a : P))
. . . . . | | . |      ⇒
. . . . . | | . |      2of(a : P)
. . . . . | | . |      (act(kind(a(i;t)))
. . . . . | | . |      ,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)
. . . . . | | . | 17. ∀x:Id.
. . . . . | | . |     deq-member(IdDeq;x;1of(init))
. . . . . | | . |     ⇒
. . . . . | | . |     s(i;0).x = 2of(init)(x)
. . . . . | | . | 18. ∀a@0:Action(i).
. . . . . | | . |     ¬isnull(a@0)

. . . . . | | . |     ⇒
. . . . . | | . |     (valtype(i;a@0) ⊆r locl(a) : 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. (λx.init(x)?•) ∈ State(ds)
. . . . . | | . | 22. t' : ℕ
. . . . . | | . | 23. 0≤t'
. . . . . | | . | 24. True ⇒ (∀v:T. ¬P((λx.s(i;t').x),v))
. . . . . | | . | 25. ¬(∃t:ℕt'. ¬isnull(a(i;t)))
. . . . . | | . | 26. x : Id
. . . . . | | . | 27. x ∈ dom(init)
. . . . . | | . | 28. s(i;0).x = 2of(init)(x)
. . . . . | | . | 29. deq-member(IdDeq;x;1of(ds))
. . . . . | | . | ⊢  s(i;0).x = 2of(init)(x)
. . . . . | | . |   by SplitOnConclITE THEN DVar 'ds'
. . . . . | | . |
. . . . . | | . .\
. . . . . | | . . .....falsecase .....
. . . . . | | . . 1. i : Id
. . . . . | | . . 2. a : Id
. . . . . | | . . 3. T : Type
. . . . . | | . . 4. ds : x:Id fp-> Type
. . . . . | | . . 5. P : State(ds)→T→Prop
. . . . . | | . . 6. init : x:Id fp-> ds(x)?Void
. . . . . | | . . 7. ∀x:Id. x ∈ dom(ds) ⇒ x ∈ dom(init)
. . . . . | | . . 8. v : T
. . . . . | | . . 9. P((λx.init(x)?•),v)
. . . . . | | . . 10. w : World
. . . . . | | . . 11. FairFifo
```

```
. . . . . | | . . 12. FairFifo
. . . . . | | . . 13. ∀l:IdLnk, tg:Id.
. . . . . | | . . |   (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | | . . |                    <ds
. . . . . | | . . |                    ,locl(a) : T
. . . . . | | . . |                    ,init
. . . . . | | . . |                    ,a : 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) : T)
. . . . . | | . . |     ∨ P@0 != a : P(a@0) ==> ∀v:... : T(...)?Top.
. . . . . | | . . |       ¬P@0((λx.s(i;t').x),v)
. . . . . | | . . 16. ∀t:ℕ.
. . . . . | | . . |   ¬isnull(a(i;t))
. . . . . | | . . |   ⇒
. . . . . | | . . |   (islocal(kind(a(i;t)))
. . . . . | | . . |    ⇒
. . . . . | | . . |    deq-member(IdDeq;act(kind(a(i;t)));1of(
. . . . . | | . . |                                        a : P))
. . . . . | | . . |    ⇒
. . . . . | | . . |    2of(a : P)
. . . . . | | . . |    (act(kind(a(i;t)))
. . . . . | | . . |    ,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)
. . . . . | | . . 17. ∀x:Id.
. . . . . | | . . |   deq-member(IdDeq;x;1of(init))
. . . . . | | . . |   ⇒
. . . . . | | . . |   s(i;0).x = 2of(init)(x)
. . . . . | | . . 18. ∀a@0:Action(i).
. . . . . | | . . |   ¬isnull(a@0)
. . . . . | | . . |   ⇒
. . . . . | | . . |   (valtype(i;a@0) ⊆r locl(a) : 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. (λx.init(x)?•) ∈ State(ds)
. . . . . | | . . 22. t' : ℕ
. . . . . | | . . 23. 0≤t'
. . . . . | | . . 24. True ⇒ (∀v:T. ¬P((λx.s(i;t').x),v))
. . . . . | | . . 25. ¬(∃t:ℕt'. ¬isnull(a(i;t)))
. . . . . | | . . 26. x : Id
. . . . . | | . . 27. x ∈ dom(init)
. . . . . | | . . 28. s(i;0).x = 2of(init)(x)
. . . . . | | . . 29. ¬deq-member(IdDeq;x;1of(ds))
. . . . . | | . . ⊢  s(i;0).x = 2of(init)(x)
. . . . . | | . . | by DupHyp -2 THEN RevHypSubst -3 -1
. . . . . | | . . |    THEN
. . . . . | | . . |    Fold `member` -1
. . . . . | | . . |
. . . . . | | . . 1. i : Id
. . . . . | | . . 2. a : Id
. . . . . | | . . 3. T : Type
. . . . . | | . . 4. ds : x:Id fp-> Type
. . . . . | | . . 5. P : State(ds)→T→Prop
. . . . . | | . . 6. init : x:Id fp-> ds(x)?Void
. . . . . | | . . 7. ∀x:Id. x ∈ dom(ds) ⇒ x ∈ dom(init)
. . . . . | | . . 8. v : T
. . . . . | | . . 9. P((λx.init(x)?•),v)
. . . . . | | . . 10. w : World
. . . . . | | . . 11. FairFifo
. . . . . | | . . 12. FairFifo
. . . . . | | . . 13. ∀l:IdLnk, tg:Id.
. . . . . | | . .     (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | | . .                      <ds
. . . . . | | . .                      ,locl(a) : T
```

```
. . . . . | | . .                      ,init
. . . . . | | . .                      ,a : 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) : T)
. . . . . | | . .       ∨ P@0 != a : P(a@0) ==> ∀v:... : T(...)?Top.
. . . . . | | . .         ¬P@0((λx.s(i;t').x),v)
. . . . . | | . . 16. ∀t:ℕ.
. . . . . | | . .     ¬isnull(a(i;t))
. . . . . | | . .     ⇒
. . . . . | | . .     (islocal(kind(a(i;t)))
. . . . . | | . .      ⇒
. . . . . | | . .      deq-member(IdDeq;act(kind(a(i;t)));1of(
. . . . . | | . .                                          a : P))
. . . . . | | . .      ⇒
. . . . . | | . .      2of(a : P)
. . . . . | | . .      (act(kind(a(i;t)))
. . . . . | | . .      ,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)
. . . . . | | . . 17. ∀x:Id.
. . . . . | | . .     deq-member(IdDeq;x;1of(init))
. . . . . | | . .     ⇒
. . . . . | | . .     s(i;0).x = 2of(init)(x)
. . . . . | | . . 18. ∀a@0:Action(i).
. . . . . | | . .     ¬isnull(a@0)
. . . . . | | . .     ⇒
. . . . . | | . .     (valtype(i;a@0) ⊆r locl(a) : 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. (λx.init(x)?•) ∈ State(ds)
. . . . . | | . . 22. t' : ℕ
. . . . . | | . . 23. 0≤t'
. . . . . | | . . 24. True ⇒ (∀v:T. ¬P((λx.s(i;t').x),v))
. . . . . | | . . 25. ¬(∃t:ℕt'. ¬isnull(a(i;t)))
. . . . . | | . . 26. x : Id
. . . . . | | . . 27. x ∈ dom(init)
. . . . . | | . . 28. s(i;0).x = 2of(init)(x)
. . . . . | | . . 29. ¬deq-member(IdDeq;x;1of(ds))
. . . . . | | . . 30. s(i;0).x ∈ Void
. . . . . | | . . ⊢  s(i;0).x = 2of(init)(x)  by GenConclAtAddr [2]
. . . . . | |
. . . . . | .\
. . . . . | . .....falsecase .....
. . . . . | . 1. i : Id
. . . . . | . 2. a : Id
. . . . . | . 3. T : Type
. . . . . | . 4. ds : x:Id fp-> Type
. . . . . | . 5. P : State(ds)→T→Prop
. . . . . | . 6. init : x:Id fp-> ds(x)?Void
. . . . . | . 7. ∀x:Id. x ∈ dom(ds) ⇒ x ∈ dom(init)
. . . . . | . 8. v : T
. . . . . | . 9. P((λx.init(x)?•),v)
. . . . . | . 10. w : World
. . . . . | . 11. FairFifo
. . . . . | . 12. FairFifo
. . . . . | . 13. ∀l:IdLnk, tg:Id.
. . . . . | . |   (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | . |                    <ds
. . . . . | . |                    ,locl(a) : T
. . . . . | . |                    ,init
. . . . . | . |                    ,a : 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) : T)
. . . . . | . |     ∨ P@0 != a : P(a@0) ==> ∀v:locl(a) : T(...)?Top.
. . . . . | . |       ¬P@0((λx.s(i;t').x),v)
. . . . . | . 16. ∀t:ℕ.
. . . . . | . |   ¬isnull(a(i;t))
. . . . . | . |   ⇒
. . . . . | . |   (islocal(kind(a(i;t)))
. . . . . | . |    ⇒
. . . . . | . |    deq-member(IdDeq;act(kind(a(i;t)));1of(a : P))
. . . . . | . |    ⇒
. . . . . | . |    2of(a : P)
. . . . . | . |    (act(kind(a(i;t)))
. . . . . | . |    ,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)
. . . . . | . 17. ∀x:Id.
. . . . . | . |   deq-member(IdDeq;x;1of(init))
. . . . . | . |   ⇒
. . . . . | . |   s(i;0).x = 2of(init)(x)
. . . . . | . 18. ∀a@0:Action(i).
. . . . . | . |   ¬isnull(a@0)
. . . . . | . |   ⇒
. . . . . | . |   (valtype(i;a@0) ⊆r locl(a) : 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. (λx.init(x)?•) ∈ State(ds)
. . . . . | . 22. t' : ℕ
. . . . . | . 23. 0≤t'
. . . . . | . 24. True ⇒ (∀v:T. ¬P((λx.s(i;t').x),v))
. . . . . | . 25. ¬(∃t:ℕt'. ¬isnull(a(i;t)))
. . . . . | . 26. x : Id
. . . . . | . 27. ¬x ∈ dom(init)
. . . . . | . ⊢  s(i;0).x = •
. . . . . | . | by Unfold `fpf-cap` 0 THEN SplitOnConclITE
. . . . . | . |
. . . . . | . |\
. . . . . | . | .....truecase .....
. . . . . | . | 1. i : Id
. . . . . | . | 2. a : Id
. . . . . | . | 3. T : Type
. . . . . | . | 4. ds : x:Id fp-> Type
. . . . . | . | 5. P : State(ds)→T→Prop
. . . . . | . | 6. init : x:Id fp-> ds(x)?Void
. . . . . | . | 7. ∀x:Id. x ∈ dom(ds) ⇒ x ∈ dom(init)
. . . . . | . | 8. v : T
. . . . . | . | 9. P((λx.init(x)?•),v)
. . . . . | . | 10. w : World
. . . . . | . | 11. FairFifo
. . . . . | . | 12. FairFifo
. . . . . | . | 13. ∀l:IdLnk, tg:Id.
. . . . . | . |     (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | . |                       <ds
. . . . . | . |                       ,locl(a) : T
. . . . . | . |                       ,init
. . . . . | . |                       ,a : 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) : T)
. . . . . | . |       ∨ P@0 != a : P(a@0) ==> ∀v:... : T(...)?Top.
. . . . . | . |         ¬P@0((λx.s(i;t').x),v)
. . . . . | . | 16. ∀t:ℕ.
. . . . . | . |     ¬isnull(a(i;t))
. . . . . | . |     ⇒
. . . . . | . |     (islocal(kind(a(i;t)))
. . . . . | . |      ⇒
. . . . . | . |      deq-member(IdDeq;act(kind(a(i;t)));1of(a : P))
. . . . . | . |      ⇒
. . . . . | . |      2of(a : P)
. . . . . | . |      (act(kind(a(i;t)))
. . . . . | . |      ,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)
. . . . . | . | 17. ∀x:Id.
. . . . . | . |     deq-member(IdDeq;x;1of(init))
. . . . . | . |     ⇒
```

```
. . . . . | . |     s(i;0).x = 2of(init)(x)
. . . . . | . | 18. ∀a@0:Action(i).
. . . . . | . |     ¬isnull(a@0)
. . . . . | . |     ⇒
. . . . . | . |     (valtype(i;a@0) ⊆r locl(a) : 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. (λx.init(x)?•) ∈ State(ds)
. . . . . | . | 22. t' : ℕ
. . . . . | . | 23. 0≤t'
. . . . . | . | 24. True ⇒ (∀v:T. ¬P((λx.s(i;t').x),v))
. . . . . | . | 25. ¬(∃t:ℕt'. ¬isnull(a(i;t)))
. . . . . | . | 26. x : Id
. . . . . | . | 27. ¬x ∈ dom(init)
. . . . . | . | 28. x ∈ dom(ds)
. . . . . | . | ⊢  s(i;0).x = •  by Analyze -2 THEN BackThruSomeHyp
. . . . . | . |
. . . . . | . .\
. . . . . | . . .....falsecase .....
. . . . . | . . 1. i : Id
. . . . . | . . 2. a : Id
. . . . . | . . 3. T : Type
. . . . . | . . 4. ds : x:Id fp-> Type
. . . . . | . . 5. P : State(ds)→T→Prop
. . . . . | . . 6. init : x:Id fp-> ds(x)?Void
. . . . . | . . 7. ∀x:Id. x ∈ dom(ds) ⇒ x ∈ dom(init)
. . . . . | . . 8. v : T
. . . . . | . . 9. P((λx.init(x)?•),v)
. . . . . | . . 10. w : World
. . . . . | . . 11. FairFifo
. . . . . | . . 12. FairFifo
. . . . . | . . 13. ∀l:IdLnk, tg:Id.
. . . . . | . .     (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . | . .                      <ds
. . . . . | . .                      ,locl(a) : T
. . . . . | . .                      ,init
. . . . . | . .                      ,a : 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) : T)
. . . . . | . .       ∨ P@0 != a : P(a@0) ==> ∀v:... : T(...)?Top.
. . . . . | . .         ¬P@0((λx.s(i;t').x),v)
. . . . . | . . 16. ∀t:ℕ.
```

```
. . . . . | . .     ¬isnull(a(i;t))
. . . . . | . .     ⇒
. . . . . | . .     (islocal(kind(a(i;t)))
. . . . . | . .      ⇒
. . . . . | . .      deq-member(IdDeq;act(kind(a(i;t)));1of(a : P))
. . . . . | . .      ⇒
. . . . . | . .      2of(a : P)
. . . . . | . .      (act(kind(a(i;t)))
. . . . . | . .      ,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)
. . . . . | . . 17. ∀x:Id.
. . . . . | . .     deq-member(IdDeq;x;1of(init))
. . . . . | . .     ⇒
. . . . . | . .     s(i;0).x = 2of(init)(x)
. . . . . | . . 18. ∀a@0:Action(i).
. . . . . | . .     ¬isnull(a@0)
. . . . . | . .     ⇒
. . . . . | . .     (valtype(i;a@0) ⊆r locl(a) : 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. (λx.init(x)?•) ∈ State(ds)
. . . . . | . . 22. t' : ℕ
. . . . . | . . 23. 0≤t'
. . . . . | . . 24. True ⇒ (∀v:T. ¬P((λx.s(i;t').x),v))
. . . . . | . . 25. ¬(∃t:ℕt'. ¬isnull(a(i;t)))
. . . . . | . . 26. x : Id
. . . . . | . . 27. ¬x ∈ dom(init)
. . . . . | . . 28. ¬x ∈ dom(ds)
. . . . . | . . ⊢  s(i;0).x = •  by Unfold `top` 0 THEN Analyze
. . . . . |
. . . . . .\
. . . . . .....eq aux .....
. . . . . . 1. i : Id
. . . . . . 2. a : Id
. . . . . . 3. T : Type
. . . . . . 4. ds : x:Id fp-> Type
. . . . . . 5. P : State(ds)→T→Prop
. . . . . . 6. init : x:Id fp-> ds(x)?Void
. . . . . . 7. ∀x:Id. x ∈ dom(ds) ⇒ x ∈ dom(init)
. . . . . . 8. v : T
. . . . . . 9. P((λx.init(x)?•),v)
. . . . . . 10. w : World
. . . . . . 11. FairFifo
. . . . . . 12. FairFifo
. . . . . . 13. ∀l:IdLnk, tg:Id.
. . . . . .     (w.M(l,tg)) ⊆r if eqof(IdDeq)(source(l),i)→
. . . . . .                    (with ds: ds
. . . . . .                     init: init
. . . . . .                    action a:T
. . . . . .                     precondition a(v) is
. . . . . .                     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(1of(2of((with ds: ds
. . . . . .                                 init: init
. . . . . .                                action a:T
. . . . . .                                 precondition a(v) is
. . . . . .                                 P))))
. . . . . .       ∨ P@0 != 1of(
. . . . . .                2of(2of(2of((with ds: ds
. . . . . .                 init: init
. . . . . .                action a:T
. . . . . .                 precondition a(v) is
. . . . . .                 P)))))(a@0) ==> ∀v:1of(
. . . . . .                                      2of((with ds: ds
. . . . . .                                       init: init
. . . . . .                                      action a:T
. . . . . .                                       precondition a(v) is
```

```
. . . . . .                                          P)))(locl(a@0))?Top.
. . . . . .          ¬P@0((λx.s(i;t').x),v)
. . . . . . 16. ∀t:ℕ.
. . . . . .     ¬isnull(a(i;t))
. . . . . .     ⇒
. . . . . .     (islocal(kind(a(i;t)))
. . . . . .      ⇒
. . . . . .      deq-member(IdDeq;act(kind(a(i;t)));1of(1of(
. . . . . .                                          2of(2of(2of(
. . . . . .                                          ...))))))
. . . . . .      ⇒
. . . . . .      2of(1of(2of(2of(2of((with ds: ds
. . . . . .               init: init
. . . . . .              action a:T
. . . . . .               precondition a(v) is
. . . . . .               P))))))
. . . . . .      (act(kind(a(i;t)))
. . . . . .      ,λx.s(i;t).x
. . . . . .      ,val(a(i;t))))
. . . . . .     & (∀x:Id.
. . . . . .        deq-member(product-deq(Knd;Id;...;IdDeq);<...
. . . . . .                                                ,x>;...)
. . . . . .        ⇒
. . . . . .        s(i;t+1).x
. . . . . .        =
. . . . . .        2of(1of(2of(2of(2of(2of((with ds: ds
. . . . . .                 init: init
. . . . . .                action a:T
. . . . . .                 precondition a(v) is
. . . . . .                 P)))))))
. . . . . .        (<kind(a(i;t)),x>
. . . . . .        ,λx.s(i;t).x
. . . . . .        ,val(a(i;t))))
. . . . . .     & (∀l:IdLnk.
. . . . . .        deq-member(product-deq(Knd;...;...;...);<...
. . . . . .                                              ,l>;...)
. . . . . .        ⇒
. . . . . .        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(
. . . . . .                                1of(2of(2of(2of(2of(2of(
. . . . . .                                    (with ds: ds
. . . . . .                                     init: init
. . . . . .                                    action a:T
. . . . . .                                     precondition a(v) is
. . . . . .                                     P)))))))
. . . . . .                                (<kind(a(i;t)),l>)))
. . . . . .        else nil fi)
. . . . . .     & (∀x:Id.
. . . . . .        ¬(deq-member(IdDeq;x;1of(1of(
```

```
. . . . . .                              2of(2of(2of(2of(2of(2of(
. . . . . .                              (with ds: ds
. . . . . .                               init: init
. . . . . .                              action a:T
. . . . . .                               precondition a(v) is
. . . . . .                               P))))))))))
. . . . . .          ⇒
. . . . . .          deq-member(KindDeq;kind(a(i;t));2of(
. . . . . .                                          1of(
. . . . . .                                          2of(2of(2of(2of(
. . . . . .                                          2of(2of(2of(
. . . . . .                                          ...)))))))))
. . . . . .                                          (x)))
. . . . . .       ⇒
. . . . . .       s(i;t).x = s(i;t+1).x)
. . . . . .    & (∀l:IdLnk, tg:Id.
. . . . . .       ¬(deq-member(product-deq(...;Id;...;...);...;...)
. . . . . .         ⇒
. . . . . .         deq-member(KindDeq;kind(a(i;t));2of(
. . . . . .                                          1of(
. . . . . .                                          2of(2of(2of(2of(
. . . . . .                                          2of(2of(2of(2of(
. . . . . .                                          2of(
. . . . . .                                          ...)))))))))))
. . . . . .                                          (<l,tg>)))
. . . . . .       ⇒
. . . . . .       w-tagged(tg; onlnk(l;m(i;t))) = nil)
. . . . . . 17. ∀x:Id.
. . . . . .     deq-member(IdDeq;x;1of(1of(2of(2of((with ds: ds
. . . . . .                                 init: init
. . . . . .                                action a:T
. . . . . .                                 precondition a(v) is
. . . . . .                                 P))))))
. . . . . .     ⇒
. . . . . .     s(i;0).x
. . . . . .     =
. . . . . .     2of(1of(2of(2of((with ds: ds
. . . . . .              init: init
. . . . . .             action a:T
. . . . . .              precondition a(v) is
. . . . . .              P)))))
. . . . . .     (x)
. . . . . . 18. ∀a@0:Action(i).
. . . . . .     ¬isnull(a@0)
. . . . . .     ⇒
. . . . . .     (valtype(i;a@0) ⊆r 1of(2of((with ds: ds
. . . . . .                                 init: init
. . . . . .                                action a:T
. . . . . .                                 precondition a(v) is
. . . . . .                                 P)))(kind(a@0))?Top)
. . . . . . 19. ∀x:Id.
. . . . . .     vartype(i;x) ⊆r if deq-member(IdDeq;x;1of(1of(
. . . . . .                                                 ...)))→
. . . . . .                           2of(1of((with ds: ds
. . . . . .                                init: init
```

```
. . . . . .                                action a:T
. . . . . .                                 precondition a(v) is
. . . . . .                                 P)))
. . . . . .                             (x)
. . . . . .                         else Top fi
. . . . . . 20. IdDeq ∈ EqDecider(Id)
. . . . . . 21. (λx.init(x)?•) ∈ State(ds)

. . . . . . 22. t' : ℕ
. . . . . . 23. 0≤t'
. . . . . . 24. True ⇒ (∀v:T. ¬P((λx.s(i;t').x),v))
. . . . . . 25. ¬(∃t:ℕt'. ¬isnull(a(i;t)))
. . . . . . ⊢  Id = Id  by Auto
END
```