```
s-pre-init-rule1  THM

⊢  ∀i,a,x:Id, A,T:Type, c:A, P:(A→T→Prop).
|  @i: ma-single-pre-init1(x;A;c;a;T;x,v.P(x,v)) ∈ Dsys
|  & (∀D:Dsys.
|     @i: ma-single-pre-init1(x;A;c;a;T;x,v.P(x,v)) ⊆ D
|     ⇒
|     D
|     realizes es.(vartype(i;x) ⊆r A)
|                 & (∀e:E. loc(e) = i ⇒ first(e) ⇒ (x when e) = c)
|                 & (∀e:E.
|                    loc(e) = i
|                    ⇒
|                    kind(e) = locl(a) ⇒ (valtype(e) ⊆r T))
|                 & (∀e:E.
|                    loc(e) = i
|                    ⇒
|                    kind(e) = locl(a) ⇒ P((x when e),val(e)))
|                   & ((∃v:T. P(c,v))
|                      ⇒
|                      (∃e:E.
|                       loc(e) = i
|                       & kind(e) = locl(a)
|                         ∨ (∀v:T. ¬P((x after e),v)))))
| by Unfold `ma-single-pre-init1` 0 THEN UnivCD
|    THEN
|    Assert ((λs,v. P(s(x),v)) ∈ State(x : A)→T→Prop)
|
|\
| .....assertion .....
| 1. Id
| 2. Id
| 3. x : Id
| 4. A : Type
| 5. T : Type
| 6. A
| 7. P : A→T→Prop
| ⊢  (λs,v. P(s(x),v)) ∈ State(x : A)→T→Prop  by Analyze
| |
| |\
| | .....subterm .....
| | 1. Id
| | 2. Id
| | 3. x : Id
| | 4. A : Type
| | 5. T : Type
| | 6. A
| | 7. P : A→T→Prop
| | 8. s : State(x : A)
| | ⊢  (λv.P(s(x),v)) ∈ T→Prop  by GenConcl (s(x) = b)
| | |
| | |\
| | | .....wf .....
| | | 1. Id
| | | 2. Id
```

```
| | | 3. x : Id
| | | 4. A : Type
| | | 5. T : Type
| | | 6. A
| | | 7. A→T→Prop
| | | 8. s : State(x : A)
| | | ⊢  s(x) ∈ A  by Unfold ‘ma-state‘ -1 THEN DoSubsume
| | | |
| | | .....subtype_rel .....
| | | 1. Id
| | | 2. Id
| | | 3. x : Id
| | | 4. A : Type
| | | 5. T : Type
| | | 6. A
| | | 7. A→T→Prop
| | | 8. x@0:Id→x : A(x@0)?Top
| | | ⊢  x : A(x)?Top ⊆r A  by Reduce 0
| | |
| | |\
| | | .....wf .....
| | | 1. Id
| | | 2. Id
| | | 3. x : Id
| | | 4. A : Type
| | | 5. T : Type
| | | 6. A
| | | 7. A→T→Prop
| | | 8. State(x : A)
| | | ⊢  A ∈ Type  by Auto
| | |
| | .\
| | . 1. Id
| | . 2. Id
| | . 3. x : Id
| | . 4. A : Type
| | . 5. T : Type
| | . 6. A
| | . 7. P : A→T→Prop
| | . 8. s : State(x : A)
| | . 9. b : A
| | . 10. s(x) = b
| | . ⊢  (λv.P(b,v)) ∈ T→Prop  by Auto
| |
| .\
| . .....eq aux .....
| . 1. Id
| . 2. Id
| . 3. x : Id
| . 4. A : Type
| . 5. T : Type
| . 6. A
| . 7. A→T→Prop
| . ⊢  State(x : A) ∈ Type  by Auto THEN Unfold ‘s-decl‘ 0
|
```

```
.\
. 1. i : Id
. 2. a : Id
. 3. x : Id
. 4. A : Type
. 5. T : Type
. 6. c : A
. 7. P : A→T→Prop
. 8. (λs,v. P(s(x),v)) ∈ State(x : A)→T→Prop
. ⊢  @i: (with ds: x : A
. |   init: x : c
. |  action a:T
. |   precondition a(v) is
. |   λs,v. P(s(x),v))
. |  ∈ Dsys
. |  & (∀D:Dsys.
. |     @i: (with ds: x : A
. |      init: x : c
. |     action a:T
. |      precondition a(v) is
. |      λs,v. P(s(x),v)) ⊆ D
. |     ⇒
. |     D
. |     realizes es.(vartype(i;x) ⊆r A)
. |                 & (∀e:E. loc(e) = i ⇒ first(e) ⇒ (x when e) = c)
. |                 & (∀e:E.
. |                    loc(e) = i
. |                    ⇒
. |                    kind(e) = locl(a) ⇒ (valtype(e) ⊆r T))
. |                 & (∀e:E.
. |                    loc(e) = i
. |                    ⇒
. |                    kind(e) = locl(a) ⇒ P((x when e),val(e)))
. |                   & ((∃v:T. P(c,v))
. |                      ⇒
. |                      (∃e:E.
. |                       loc(e) = i
. |                       & kind(e) = locl(a)
. |                         ∨ (∀v:T. ¬P((x after e),v)))))
. | by AssertBY (∀x@0:Id. x@0 ∈ dom(x : A) ⇒ x@0 ∈ dom(x : c))
. |    (Repeat (Unfolds [‘fpf-dom‘;‘fpf-single‘] 0 THEN Reduce 0))
. |    THEN
. |    Assert (x : c ∈ x@0:Id fp-> x : A(x@0)?Void)
. |
. |\
. | .....assertion .....
. | 1. Id
. | 2. Id
. | 3. x : Id
. | 4. A : Type
. | 5. T : Type
. | 6. c : A
. | 7. P : A→T→Prop
. | 8. (λs,v. P(s(x),v)) ∈ State(x : A)→T→Prop
. | 9. ∀x@0:Id. x@0 ∈ dom(x : A) ⇒ x@0 ∈ dom(x : c)
```

```
. | ⊢  x : c ∈ x@0:Id fp-> x : A(x@0)?Void
. |   by Assert (x : A ∈ x:Id fp-> Type)
. |
. .\
. . 1. i : Id
. . 2. a : Id
. . 3. x : Id
. . 4. A : Type
. . 5. T : Type
. . 6. c : A
. . 7. P : A→T→Prop
. . 8. (λs,v. P(s(x),v)) ∈ State(x : A)→T→Prop
. . 9. ∀x@0:Id. x@0 ∈ dom(x : A) ⇒ x@0 ∈ dom(x : c)
. . 10. x : c ∈ x@0:Id fp-> x : A(x@0)?Void
. . ⊢  @i: (with ds: x : A
. . |   init: x : c
. . |  action a:T
. . |   precondition a(v) is
. . |   λs,v. P(s(x),v))
. . |  ∈ Dsys
. . |  & (∀D:Dsys.
. . |     @i: (with ds: x : A
. . |      init: x : c
. . |     action a:T
. . |      precondition a(v) is
. . |      λs,v. P(s(x),v)) ⊆ D
. . |     ⇒
. . |     D
. . |     realizes es.(vartype(i;x) ⊆r A)
. . |                 & (∀e:E.
. . |                    loc(e) = i ⇒ first(e) ⇒ (x when e) = c)
. . |                 & (∀e:E.
. . |                    loc(e) = i
. . |                    ⇒
. . |                    kind(e) = locl(a) ⇒ (valtype(e) ⊆r T))
. . |                 & (∀e:E.
. . |                    loc(e) = i
. . |                    ⇒
. . |                    kind(e) = locl(a) ⇒ P((x when e),val(e)))
. . |                   & ((∃v:T. P(c,v))
. . |                      ⇒
. . |                      (∃e:E.
. . |                       loc(e) = i
. . |                       & kind(e) = locl(a)
. . |                         ∨ (∀v:T. ¬P((x after e),v)))))
. . | by Inst Thm: s_DASH_pre_DASH_init_DASH_rule
. . |    [i;a;T;x : A;λs,v. P(s(x),v);x : c]
. . |    THEN
. . |    Reduce 0 THEN Try (Complete Auto)
. . |    THEN
. . |    Analyze -1
. . |    THEN
. . |    Analyze 0
. . |    THEN
. . |    Try Trivial
```

```
. . |
. . 1. i : Id
. . 2. a : Id
. . 3. x : Id
. . 4. A : Type
. . 5. T : Type
. . 6. c : A
. . 7. P : A→T→Prop
. . 8. (λs,v. P(s(x),v)) ∈ State(x : A)→T→Prop
. . 9. ∀x@0:Id. x@0 ∈ dom(x : A) ⇒ x@0 ∈ dom(x : c)
. . 10. x : c ∈ x@0:Id fp-> x : A(x@0)?Void
. . 11. @i: (with ds: x : A
. . |    init: x : c
. . |   action a:T
. . |    precondition a(v) is
. . |    λs,v. P(s(x),v))
. . |   ∈ Dsys
. . 12. ∀D:Dsys.
. . |   @i: (with ds: x : A
. . |    init: x : c
. . |   action a:T
. . |    precondition a(v) is
. . |    λs,v. P(s(x),v)) ⊆ D
. . |   ⇒
. . |   D
. . |   realizes es.(∃v:T. (λs,v. P(s(x),v))((λx@0.x : c(x@0)?•),v))
. . |               ⇒
. . |               (∃e:E. loc(e) = i)
. . 13. @i: (with ds: x : A
. . |    init: x : c
. . |   action a:T
. . |    precondition a(v) is
. . |    λs,v. P(s(x),v))
. . |   ∈ Dsys
. . ⊢  ∀D:Dsys.
. . |  @i: (with ds: x : A
. . |   init: x : c
. . |  action a:T
. . |   precondition a(v) is
. . |   λs,v. P(s(x),v)) ⊆ D
. . |  ⇒
. . |  D
. . |  realizes es.(vartype(i;x) ⊆r A)
. . |              & (∀e:E. loc(e) = i ⇒ first(e) ⇒ (x when e) = c)
. . |              & (∀e:E.
. . |                 loc(e) = i
. . |                 ⇒
. . |                 kind(e) = locl(a) ⇒ (valtype(e) ⊆r T))
. . |              & (∀e:E.
. . |                 loc(e) = i
. . |                 ⇒
. . |                 kind(e) = locl(a) ⇒ P((x when e),val(e)))
. . |               & ((∃v:T. P(c,v))
. . |                  ⇒
. . |                  (∃e:E.
```

```
. . |                    loc(e) = i
. . |                    & kind(e) = locl(a)
. . |                      ∨ (∀v:T. ¬P((x after e),v))))
. . | by Inst Thm: s_DASH_pre_DASH_rule1 [i;a;x;A;T;P]
. . |    THEN
. . |    Reduce 0 THEN Try (Complete Auto)
. . |    THEN
. . |    Try (Unfold `s-decl` 0)
. . |    THEN
. . |    Analyze -1
. . |
. . 1. i : Id
. . 2. a : Id
. . 3. x : Id
. . 4. A : Type
. . 5. T : Type
. . 6. c : A
. . 7. P : A→T→Prop
. . 8. (λs,v. P(s(x),v)) ∈ State(x : A)→T→Prop
. . 9. ∀x@0:Id. x@0 ∈ dom(x : A) ⇒ x@0 ∈ dom(x : c)
. . 10. x : c ∈ x@0:Id fp-> x : A(x@0)?Void
. . 11. @i: (with ds: x : A
. . |    init: x : c
. . |   action a:T
. . |    precondition a(v) is
. . |    λs,v. P(s(x),v))
. . |   ∈ Dsys
. . 12. ∀D:Dsys.
. . |   @i: (with ds: x : A
. . |    init: x : c
. . |   action a:T
. . |    precondition a(v) is
. . |    λs,v. P(s(x),v)) ⊆ D
. . |   ⇒
. . |   D
. . |   realizes es.(∃v:T. (λs,v. P(s(x),v))((λx@0.x : c(x@0)?•),v))
. . |              ⇒
. . |              (∃e:E. loc(e) = i)
. . 13. @i: (with ds: x : A
. . |    init: x : c
. . |   action a:T
. . |    precondition a(v) is
. . |    λs,v. P(s(x),v))
. . |   ∈ Dsys
. . 14. @i: ma-single-pre1(x;A;a;T;x,v.P(x,v)) ∈ Dsys
. . 15. ∀D:Dsys.
. . |   @i: ma-single-pre1(x;A;a;T;x,v.P(x,v)) ⊆ D
. . |   ⇒
. . |   D
. . |   realizes es.(vartype(i;x) ⊆r A)
. . |              & (∀e:E.
. . |                 loc(e) = i
. . |                 ⇒
. . |                 kind(e) = locl(a) ⇒ (valtype(e) ⊆r T))
. . |              & (∀e:E.
```

```
. . |                  loc(e) = i
. . |                  ⇒
. . |                  (kind(e) = locl(a) ⇒ P((x when e),val(e)))
. . |                  & (∃e':E.
. . |                     (e <loc e') ∨ e = e'
. . |                     & kind(e') = locl(a)
. . |                       ∨ (∀v:T. ¬P((x after e'),v))))
. . ⊢  ∀D:Dsys.
. . |  @i: (with ds: x : A
. . |   init: x : c
. . |  action a:T
. . |   precondition a(v) is
. . |   λs,v. P(s(x),v)) ⊆ D
. . |  ⇒
. . |  D
. . |  realizes es.(vartype(i;x) ⊆r A)
. . |              & (∀e:E. loc(e) = i ⇒ first(e) ⇒ (x when e) = c)
. . |              & (∀e:E.
. . |                 loc(e) = i
. . |                 ⇒
. . |                 kind(e) = locl(a) ⇒ (valtype(e) ⊆r T))
. . |              & (∀e:E.
. . |                 loc(e) = i
. . |                 ⇒
. . |                 kind(e) = locl(a) ⇒ P((x when e),val(e)))
. . |                & ((∃v:T. P(c,v))
. . |                   ⇒
. . |                   (∃e:E.
. . |                    loc(e) = i
. . |                    & kind(e) = locl(a)
. . |                      ∨ (∀v:T. ¬P((x after e),v))))
. . | by Inst Thm: s_DASH_init_DASH_rule [i;A;c;x]
. . |    THEN
. . |    Reduce 0 THEN Try (Complete Auto)
. . |    THEN
. . |    Try (Unfold `s-decl` 0)
. . |    THEN
. . |    Analyze -1
. . |
. . 1. i : Id
. . 2. a : Id
. . 3. x : Id
. . 4. A : Type
. . 5. T : Type
. . 6. c : A
. . 7. P : A→T→Prop
. . 8. (λs,v. P(s(x),v)) ∈ State(x : A)→T→Prop
. . 9. ∀x@0:Id. x@0 ∈ dom(x : A) ⇒ x@0 ∈ dom(x : c)
. . 10. x : c ∈ x@0:Id fp-> x : A(x@0)?Void
. . 11. @i: (with ds: x : A
. . |    init: x : c
. . |   action a:T
. . |    precondition a(v) is
. . |    λs,v. P(s(x),v))
. . |   ∈ Dsys
```

```
. . 12. ∀D:Dsys.
. . |   @i: (with ds: x : A
. . |    init: x : c
. . |   action a:T
. . |    precondition a(v) is
. . |    λs,v. P(s(x),v)) ⊆ D
. . |   ⇒
. . |   D
. . |   realizes es.(∃v:T. (λs,v. P(s(x),v))((λx@0.x : c(x@0)?•),v))
. . |               ⇒
. . |               (∃e:E. loc(e) = i)
. . 13. @i: (with ds: x : A
. . |    init: x : c
. . |   action a:T
. . |    precondition a(v) is
. . |    λs,v. P(s(x),v))
. . |   ∈ Dsys
. . 14. @i: ma-single-pre1(x;A;a;T;x,v.P(x,v)) ∈ Dsys
. . 15. ∀D:Dsys.
. . |   @i: ma-single-pre1(x;A;a;T;x,v.P(x,v)) ⊆ D
. . |   ⇒
. . |   D
. . |   realizes es.(vartype(i;x) ⊆r A)
. . |               & (∀e:E.
. . |                  loc(e) = i
. . |                  ⇒
. . |                  kind(e) = locl(a) ⇒ (valtype(e) ⊆r T))
. . |               & (∀e:E.
. . |                  loc(e) = i
. . |                  ⇒
. . |                  (kind(e) = locl(a) ⇒ P((x when e),val(e)))
. . |                  & (∃e':E.
. . |                     (e <loc e') ∨ e = e'
. . |                     & kind(e') = locl(a)
. . |                       ∨ (∀v:T. ¬P((x after e'),v))))
. . 16. @i: x : A initially x = c ∈ Dsys
. . 17. ∀D:Dsys.
. . |   @i: x : A initially x = c ⊆ D
. . |   ⇒
. . |   D
. . |   realizes es.(vartype(i;x) ⊆r A)
. . |               & (∀e:E. loc(e) = i ⇒ first(e) ⇒ (x when e) = c)
. . ⊢  ∀D:Dsys.
. . |  @i: (with ds: x : A
. . |   init: x : c
. . |  action a:T
. . |   precondition a(v) is
. . |   λs,v. P(s(x),v)) ⊆ D
. . |  ⇒
. . |  D
. . |  realizes es.(vartype(i;x) ⊆r A)
. . |              & (∀e:E. loc(e) = i ⇒ first(e) ⇒ (x when e) = c)
. . |              & (∀e:E.
. . |                 loc(e) = i
. . |                 ⇒
```

```
. . |                kind(e) = locl(a) ⇒ (valtype(e) ⊆r T))
. . |              & (∀e:E.
. . |                 loc(e) = i
. . |                 ⇒
. . |                 kind(e) = locl(a) ⇒ P((x when e),val(e)))
. . |               & ((∃v:T. P(c,v))
. . |                  ⇒
. . |                  (∃e:E.
. . |                   loc(e) = i
. . |                   & kind(e) = locl(a)
. . |                     ∨ (∀v:T. ¬P((x after e),v))))
. . | by Analyze 0 THEN Analyze 0
. . |
. . 1. i : Id
. . 2. a : Id
. . 3. x : Id
. . 4. A : Type
. . 5. T : Type
. . 6. c : A
. . 7. P : A→T→Prop
. . 8. (λs,v. P(s(x),v)) ∈ State(x : A)→T→Prop
. . 9. ∀x@0:Id. x@0 ∈ dom(x : A) ⇒ x@0 ∈ dom(x : c)
. . 10. x : c ∈ x@0:Id fp-> x : A(x@0)?Void
. . 11. @i: (with ds: x : A
. . |    init: x : c
. . |   action a:T
. . |    precondition a(v) is
. . |    λs,v. P(s(x),v))
. . |   ∈ Dsys
. . 12. ∀D:Dsys.
. . |   @i: (with ds: x : A
. . |    init: x : c
. . |   action a:T
. . |    precondition a(v) is
. . |    λs,v. P(s(x),v)) ⊆ D
. . |   ⇒
. . |   D
. . |   realizes es.(∃v:T. (λs,v. P(s(x),v))((λx@0.x : c(x@0)?•),v))
. . |                ⇒
. . |                (∃e:E. loc(e) = i)
. . 13. @i: (with ds: x : A
. . |    init: x : c
. . |   action a:T
. . |    precondition a(v) is
. . |    λs,v. P(s(x),v))
. . |   ∈ Dsys
. . 14. @i: ma-single-pre1(x;A;a;T;x,v.P(x,v)) ∈ Dsys
. . 15. ∀D:Dsys.
. . |   @i: ma-single-pre1(x;A;a;T;x,v.P(x,v)) ⊆ D
. . |   ⇒
. . |   D
. . |   realizes es.(vartype(i;x) ⊆r A)
. . |                & (∀e:E.
. . |                   loc(e) = i
. . |                   ⇒
```

```
. . |                  kind(e) = locl(a) ⇒ (valtype(e) ⊆r T))
. . |               & (∀e:E.
. . |                  loc(e) = i
. . |                  ⇒
. . |                  (kind(e) = locl(a) ⇒ P((x when e),val(e)))
. . |                  & (∃e':E.
. . |                     (e <loc e') ∨ e = e'
. . |                     & kind(e') = locl(a)
. . |                       ∨ (∀v:T. ¬P((x after e'),v))))
. . 16. @i: x : A initially x = c ∈ Dsys
. . 17. ∀D:Dsys.
. . |   @i: x : A initially x = c ⊆ D
. . |   ⇒
. . |   D
. . |   realizes es.(vartype(i;x) ⊆r A)
. . |              & (∀e:E. loc(e) = i ⇒ first(e) ⇒ (x when e) = c)
. . 18. D : Dsys
. . 19. @i: (with ds: x : A
. . |    init: x : c
. . |   action a:T
. . |    precondition a(v) is
. . |    λs,v. P(s(x),v)) ⊆ D
. . ⊢  D
. . |  realizes es.(vartype(i;x) ⊆r A)
. . |              & (∀e:E. loc(e) = i ⇒ first(e) ⇒ (x when e) = c)
. . |              & (∀e:E.
. . |                 loc(e) = i
. . |                 ⇒
. . |                 kind(e) = locl(a) ⇒ (valtype(e) ⊆r T))
. . |              & (∀e:E.
. . |                 loc(e) = i
. . |                 ⇒
. . |                 kind(e) = locl(a) ⇒ P((x when e),val(e)))
. . |                & ((∃v:T. P(c,v))
. . |                   ⇒
. . |                   (∃e:E.
. . |                    loc(e) = i
. . |                    & kind(e) = locl(a)
. . |                      ∨ (∀v:T. ¬P((x after e),v))))
. . | by InstHyp [D] -3
. . |
. . |\
. . | .....antecedent .....
. . | 1. i : Id
. . | 2. a : Id
. . | 3. x : Id
. . | 4. A : Type
. . | 5. T : Type
. . | 6. c : A
. . | 7. P : A→T→Prop
. . | 8. (λs,v. P(s(x),v)) ∈ State(x : A)→T→Prop
. . | 9. ∀x@0:Id. x@0 ∈ dom(x : A) ⇒ x@0 ∈ dom(x : c)
. . | 10. x : c ∈ x@0:Id fp-> x : A(x@0)?Void
. . | 11. @i: (with ds: x : A
. . | |    init: x : c
```

```
. . | |   action a:T
. . | |    precondition a(v) is
. . | |    λs,v. P(s(x),v))
. . | |   ∈ Dsys
. . | 12. ∀D:Dsys.
. . | |   @i: (with ds: x : A
. . | |    init: x : c
. . | |   action a:T
. . | |    precondition a(v) is
. . | |    λs,v. P(s(x),v)) ⊆ D
. . | |   ⇒
. . | |   D
. . | |   realizes es.(∃v:T. (λs,v. P(s(x),v))((λx@0.x : c(x@0)?•),v))
. . | |               ⇒
. . | |               (∃e:E. loc(e) = i)
. . | 13. @i: (with ds: x : A
. . | |    init: x : c
. . | |   action a:T
. . | |    precondition a(v) is
. . | |    λs,v. P(s(x),v))
. . | |   ∈ Dsys
. . | 14. @i: ma-single-pre1(x;A;a;T;x,v.P(x,v)) ∈ Dsys
. . | 15. ∀D:Dsys.
. . | |   @i: ma-single-pre1(x;A;a;T;x,v.P(x,v)) ⊆ D
. . | |   ⇒
. . | |   D
. . | |   realizes es.(vartype(i;x) ⊆r A)
. . | |               & (∀e:E.
. . | |                  loc(e) = i
. . | |                  ⇒
. . | |                  kind(e) = locl(a) ⇒ (valtype(e) ⊆r T))
. . | |               & (∀e:E.
. . | |                  loc(e) = i
. . | |                  ⇒
. . | |                  (kind(e) = locl(a) ⇒ P((x when e),val(e)))
. . | |                  & (∃e':E.
. . | |                     (e <loc e') ∨ e = e'
. . | |                     & kind(e') = locl(a)
. . | |                       ∨ (∀v:T. ¬P((x after e'),v))))
. . | 16. @i: x : A initially x = c ∈ Dsys
. . | 17. ∀D:Dsys.
. . | |   @i: x : A initially x = c ⊆ D
. . | |   ⇒
. . | |   D
. . | |   realizes es.(vartype(i;x) ⊆r A)
. . | |               & (∀e:E.
. . | |                  loc(e) = i ⇒ first(e) ⇒ (x when e) = c)
. . | 18. D : Dsys
. . | 19. @i: (with ds: x : A
. . | |    init: x : c
. . | |   action a:T
. . | |    precondition a(v) is
. . | |    λs,v. P(s(x),v)) ⊆ D
. . | ⊢  @i: x : A initially x = c ⊆ D
. . | | by Using
```

```
. . | |    ['D2'
. . | |     ,@i: (with ds: x : A
. . | |       init: x : c
. . | |      action a:T
. . | |       precondition a(v) is
. . | |       λs,v. P(s(x),v))]
. . | |    (BackThru
. . | |     Thm* ∀D1,D2,D3:Dsys. D1 ⊆ D2 ⇒ D2 ⊆ D3 ⇒ D1 ⊆ D3
. . | |     {d_DASH_sub_transitivity})
. . | |
. . | 1. i : Id
. . | 2. a : Id
. . | 3. x : Id
. . | 4. A : Type
. . | 5. T : Type
. . | 6. c : A
. . | 7. P : A→T→Prop
. . | 8. (λs,v. P(s(x),v)) ∈ State(x : A)→T→Prop
. . | 9. ∀x@0:Id. x@0 ∈ dom(x : A) ⇒ x@0 ∈ dom(x : c)
. . | 10. x : c ∈ x@0:Id fp-> x : A(x@0)?Void
. . | 11. @i: (with ds: x : A
. . | |    init: x : c
. . | |   action a:T
. . | |    precondition a(v) is
. . | |    λs,v. P(s(x),v))
. . | |   ∈ Dsys
. . | 12. ∀D:Dsys.
. . | |   @i: (with ds: x : A
. . | |    init: x : c
. . | |   action a:T
. . | |    precondition a(v) is
. . | |    λs,v. P(s(x),v)) ⊆ D
. . | |   ⇒
. . | |   D
. . | |   realizes es.(∃v:T. (λs,v. P(s(x),v))((λx@0.x : c(x@0)?•),v))
. . | |                ⇒
. . | |                (∃e:E. loc(e) = i)
. . | 13. @i: (with ds: x : A
. . | |    init: x : c
. . | |   action a:T
. . | |    precondition a(v) is
. . | |    λs,v. P(s(x),v))
. . | |   ∈ Dsys
. . | 14. @i: ma-single-pre1(x;A;a;T;x,v.P(x,v)) ∈ Dsys
. . | 15. ∀D:Dsys.
. . | |   @i: ma-single-pre1(x;A;a;T;x,v.P(x,v)) ⊆ D
. . | |   ⇒
. . | |   D
. . | |   realizes es.(vartype(i;x) ⊆r A)
. . | |                & (∀e:E.
. . | |                   loc(e) = i
. . | |                   ⇒
. . | |                   kind(e) = locl(a) ⇒ (valtype(e) ⊆r T))
. . | |                & (∀e:E.
. . | |                   loc(e) = i
```

```
. . | |                  ⇒
. . | |                  (kind(e) = locl(a) ⇒ P((x when e),val(e)))
. . | |                  & (∃e':E.
. . | |                     (e <loc e') ∨ e = e'
. . | |                     & kind(e') = locl(a)
. . | |                       ∨ (∀v:T. ¬P((x after e'),v))))
. . | 16. @i: x : A initially x = c ∈ Dsys
. . | 17. ∀D:Dsys.
. . | |   @i: x : A initially x = c ⊆ D
. . | |   ⇒
. . | |   D
. . | |   realizes es.(vartype(i;x) ⊆r A)
. . | |               & (∀e:E.
. . | |                  loc(e) = i ⇒ first(e) ⇒ (x when e) = c)
. . | 18. D : Dsys
. . | 19. @i: (with ds: x : A
. . | |    init: x : c
. . | |   action a:T
. . | |    precondition a(v) is
. . | |    λs,v. P(s(x),v)) ⊆ D
. . | ⊢  @i: x : A initially x = c ⊆ @i: (with ds: x : A
. . | |   init: x : c
. . | |  action a:T
. . | |   precondition a(v) is
. . | |   λs,v. P(s(x),v))
. . | | by Subst
. . | |    ((with ds: x : A
. . | |      init: x : c
. . | |     action a:T
. . | |      precondition a(v) is
. . | |      λs,v. P(s(x)
. . | |             ,v)) ∼ ma-single-pre-init1(x;A;c;a;T;y,v.P(y,v)))
. . | |    0
. . | |
. . | |\
. . | | .....equality .....
. . | | 1. i : Id
. . | | 2. a : Id
. . | | 3. x : Id
. . | | 4. A : Type
. . | | 5. T : Type
. . | | 6. c : A
. . | | 7. P : A→T→Prop
. . | | 8. (λs,v. P(s(x),v)) ∈ State(x : A)→T→Prop
. . | | 9. ∀x@0:Id. x@0 ∈ dom(x : A) ⇒ x@0 ∈ dom(x : c)
. . | | 10. x : c ∈ x@0:Id fp-> x : A(x@0)?Void
. . | | 11. @i: (with ds: x : A
. . | |      init: x : c
. . | |     action a:T
. . | |      precondition a(v) is
. . | |      λs,v. P(s(x),v))
. . | |     ∈ Dsys
. . | | 12. ∀D:Dsys.
. . | |     @i: (with ds: x : A
. . | |      init: x : c
```

```
. . | |     action a:T
. . | |      precondition a(v) is
. . | |      λs,v. P(s(x),v)) ⊆ D
. . | |     ⇒
. . | |     D
. . | |     realizes es.(∃v:T.
. . | |                  (λs,v. P(s(x),v))((λx@0.x : c(x@0)?•),v))
. . | |                 ⇒
. . | |                 (∃e:E. loc(e) = i)
. . | | 13. @i: (with ds: x : A
. . | |      init: x : c
. . | |     action a:T
. . | |      precondition a(v) is
. . | |      λs,v. P(s(x),v))
. . | |     ∈ Dsys
. . | | 14. @i: ma-single-pre1(x;A;a;T;x,v.P(x,v)) ∈ Dsys
. . | | 15. ∀D:Dsys.
. . | |     @i: ma-single-pre1(x;A;a;T;x,v.P(x,v)) ⊆ D
. . | |     ⇒
. . | |     D
. . | |     realizes es.(vartype(i;x) ⊆r A)
. . | |                 & (∀e:E.
. . | |                    loc(e) = i
. . | |                    ⇒
. . | |                    kind(e) = locl(a) ⇒ (valtype(e) ⊆r T))
. . | |                 & (∀e:E.
. . | |                    loc(e) = i
. . | |                    ⇒
. . | |                    (kind(e) = locl(a) ⇒ P((x when e),val(e)))
. . | |                    & (∃e':E.
. . | |                       (e <loc e') ∨ e = e'
. . | |                       & kind(e') = locl(a)
. . | |                         ∨ (∀v:T. ¬P((x after e'),v))))
. . | | 16. @i: x : A initially x = c ∈ Dsys
. . | | 17. ∀D:Dsys.
. . | |     @i: x : A initially x = c ⊆ D
. . | |     ⇒
. . | |     D
. . | |     realizes es.(vartype(i;x) ⊆r A)
. . | |                 & (∀e:E.
. . | |                    loc(e) = i ⇒ first(e) ⇒ (x when e) = c)
. . | | 18. D : Dsys
. . | | 19. @i: (with ds: x : A
. . | |      init: x : c
. . | |     action a:T
. . | |      precondition a(v) is
. . | |      λs,v. P(s(x),v)) ⊆ D
. . | | ⊢  (with ds: x : A
. . | |     init: x : c
. . | |    action a:T
. . | |     precondition a(v) is
. . | |     λs,v. P(s(x),v)) ∼ ma-single-pre-init1(x;A;c;a;T;y,v.P(y
. . | |                                                           ,v))
. . | |   by Unfold ‘ma-single-pre-init1‘ 0 THEN Trivial
. . | |
```

```
. . | .\
. . | . 1. i : Id
. . | . 2. a : Id
. . | . 3. x : Id
. . | . 4. A : Type
. . | . 5. T : Type
. . | . 6. c : A
. . | . 7. P : A→T→Prop
. . | . 8. (λs,v. P(s(x),v)) ∈ State(x : A)→T→Prop
. . | . 9. ∀x@0:Id. x@0 ∈ dom(x : A) ⇒ x@0 ∈ dom(x : c)
. . | . 10. x : c ∈ x@0:Id fp-> x : A(x@0)?Void
. . | . 11. @i: (with ds: x : A
. . | . |    init: x : c
. . | . |   action a:T
. . | . |    precondition a(v) is
. . | . |    λs,v. P(s(x),v))
. . | . |   ∈ Dsys
. . | . 12. ∀D:Dsys.
. . | . |   @i: (with ds: x : A
. . | . |    init: x : c
. . | . |   action a:T
. . | . |    precondition a(v) is
. . | . |    λs,v. P(s(x),v)) ⊆ D
. . | . |   ⇒
. . | . |   D
. . | . |   realizes es.(∃v:T.
. . | . |                (λs,v. P(s(x),v))((λx@0.x : c(x@0)?•),v))
. . | . |               ⇒
. . | . |               (∃e:E. loc(e) = i)
. . | . 13. @i: (with ds: x : A
. . | . |    init: x : c
. . | . |   action a:T
. . | . |    precondition a(v) is
. . | . |    λs,v. P(s(x),v))
. . | . |   ∈ Dsys
. . | . 14. @i: ma-single-pre1(x;A;a;T;x,v.P(x,v)) ∈ Dsys
. . | . 15. ∀D:Dsys.
. . | . |   @i: ma-single-pre1(x;A;a;T;x,v.P(x,v)) ⊆ D
. . | . |   ⇒
. . | . |   D
. . | . |   realizes es.(vartype(i;x) ⊆r A)
. . | . |               & (∀e:E.
. . | . |                  loc(e) = i
. . | . |                  ⇒
. . | . |                  kind(e) = locl(a) ⇒ (valtype(e) ⊆r T))
. . | . |               & (∀e:E.
. . | . |                  loc(e) = i
. . | . |                  ⇒
. . | . |                  (kind(e) = locl(a) ⇒ P((x when e),val(e)))
. . | . |                  & (∃e':E.
. . | . |                     (e <loc e') ∨ e = e'
. . | . |                     & kind(e') = locl(a)
. . | . |                       ∨ (∀v:T. ¬P((x after e'),v))))
. . | . 16. @i: x : A initially x = c ∈ Dsys
. . | . 17. ∀D:Dsys.
```

```
. . | . |   @i: x : A initially x = c ⊆ D
. . | . |   ⇒
. . | . |   D
. . | . |   realizes es.(vartype(i;x) ⊆r A)
. . | . |               & (∀e:E.
. . | . |                  loc(e) = i ⇒ first(e) ⇒ (x when e) = c)
. . | . 18. D : Dsys
. . | . 19. @i: (with ds: x : A
. . | . |    init: x : c
. . | . |   action a:T
. . | . |    precondition a(v) is
. . | . |    λs,v. P(s(x),v)) ⊆ D
. . | . ⊢  @i: x : A initially x = c ⊆ @i: ...
. . | . | by BackThru
. . | . |    Thm* ∀i:Id, A,B:MsgA. @i: A ⊆ @i: B ⟺ A ⊆ B
. . | . |    {s_DASH_at_DASH_sub_DASH_s_DASH_at}
. . | . |    THENA
. . | . |    (Auto THEN Unfold `msga-at` 0)
. . | . |
. . | . 1. i : Id
. . | . 2. a : Id
. . | . 3. x : Id
. . | . 4. A : Type
. . | . 5. T : Type
. . | . 6. c : A
. . | . 7. P : A→T→Prop
. . | . 8. (λs,v. P(s(x),v)) ∈ State(x : A)→T→Prop
. . | . 9. ∀x@0:Id. x@0 ∈ dom(x : A) ⇒ x@0 ∈ dom(x : c)
. . | . 10. x : c ∈ x@0:Id fp-> x : A(x@0)?Void
. . | . 11. @i: (with ds: x : A
. . | .     init: x : c
. . | .    action a:T
. . | .     precondition a(v) is
. . | .     λs,v. P(s(x),v))
. . | .    ∈ Dsys
. . | . 12. ∀D:Dsys.
. . | .    @i: (with ds: x : A
. . | .     init: x : c
. . | .    action a:T
. . | .     precondition a(v) is
. . | .     λs,v. P(s(x),v)) ⊆ D
. . | .    ⇒
. . | .    D
. . | .    realizes es.(∃v:T.
. . | .                 (λs,v. P(s(x),v))((λx@0.x : c(x@0)?·),v))
. . | .                ⇒
. . | .                (∃e:E. loc(e) = i)
. . | . 13. @i: (with ds: x : A
. . | .     init: x : c
. . | .    action a:T
. . | .     precondition a(v) is
. . | .     λs,v. P(s(x),v))
. . | .    ∈ Dsys
. . | . 14. @i: ma-single-pre1(x;A;a;T;x,v.P(x,v)) ∈ Dsys
. . | . 15. ∀D:Dsys.
```

```
. . | .     @i: ma-single-pre1(x;A;a;T;x,v.P(x,v)) ⊆ D
. . | .     ⇒
. . | .     D
. . | .     realizes es.(vartype(i;x) ⊆r A)
. . | .                 & (∀e:E.
. . | .                    loc(e) = i
. . | .                    ⇒
. . | .                    kind(e) = locl(a) ⇒ (valtype(e) ⊆r T))
. . | .                 & (∀e:E.
. . | .                    loc(e) = i
. . | .                    ⇒
. . | .                    (kind(e) = locl(a) ⇒ P((x when e),val(e)))
. . | .                    & (∃e':E.
. . | .                       (e <loc e') ∨ e = e'
. . | .                       & kind(e') = locl(a)
. . | .                         ∨ (∀v:T. ¬P((x after e'),v))))
. . | . 16. @i: x : A initially x = c ∈ Dsys
. . | . 17. ∀D:Dsys.
. . | .     @i: x : A initially x = c ⊆ D
. . | .     ⇒
. . | .     D
. . | .     realizes es.(vartype(i;x) ⊆r A)
. . | .                 & (∀e:E.
. . | .                    loc(e) = i ⇒ first(e) ⇒ (x when e) = c)
. . | . 18. D : Dsys
. . | . 19. @i: (with ds: x : A
. . | .      init: x : c
. . | .     action a:T
. . | .      precondition a(v) is
. . | .      λs,v. P(s(x),v)) ⊆ D
. . | . ⊢  x : A initially x = c ⊆ ...
. . | .   by Repeat
. . | .      (Unfolds
. . | .       ['ma-single-init'
. . | .       ;'ma-single-pre-init'
. . | .       ;'ma-single-pre-init1'
. . | .       ;'ma-sub'
. . | .       ;'mk-ma']
. . | .       0
. . | .       THEN
. . | .       Reduce 0)
. . | .      THEN
. . | .      Try
. . | .      (BackThru
. . | .       Thm* ∀B,eq,g:Top.  ⊆ g    {fpf_DASH_empty_DASH_sub})
. . | .      THEN
. . | .      Try
. . | .      (BackThru
. . | .       Thm* ∀B:(A→Type), eq:EqDecider(A), f,g:a:A fp-> B(a).
. . | .            f = g ⇒ f ⊆ g
. . | .       {fpf_DASH_sub_weakening})
. . | .      THEN
. . | .      Try
. . | .      (BackThru
. . | .       Thm* ∀A:Type, f:a:A fp-> Type, eq:EqDecider(A), x:A,
```

```
. . | .             z:Type. f(x)?z ∈ Type
. . | .       {fpf_DASH_cap_DASH_wf_DASH_univ})
. . |
. . .\
. . . 1. i : Id
. . . 2. a : Id
. . . 3. x : Id
. . . 4. A : Type
. . . 5. T : Type
. . . 6. c : A
. . . 7. P : A→T→Prop
. . . 8. (λs,v. P(s(x),v)) ∈ State(x : A)→T→Prop
. . . 9. ∀x@0:Id. x@0 ∈ dom(x : A) ⇒ x@0 ∈ dom(x : c)
. . . 10. x : c ∈ x@0:Id fp-> x : A(x@0)?Void
. . . 11. @i: (with ds: x : A
. . . |    init: x : c
. . . |   action a:T
. . . |    precondition a(v) is
. . . |    λs,v. P(s(x),v))
. . . |   ∈ Dsys
. . . 12. ∀D:Dsys.
. . . |   @i: (with ds: x : A
. . . |    init: x : c
. . . |   action a:T
. . . |    precondition a(v) is
. . . |    λs,v. P(s(x),v)) ⊆ D
. . . |   ⇒
. . . |   D
. . . |   realizes es.(∃v:T. (λs,v. P(s(x),v))((λx@0.x : c(x@0)?•),v))
. . . |               ⇒
. . . |               (∃e:E. loc(e) = i)
. . . 13. @i: (with ds: x : A
. . . |    init: x : c
. . . |   action a:T
. . . |    precondition a(v) is
. . . |    λs,v. P(s(x),v))
. . . |   ∈ Dsys
. . . 14. @i: ma-single-pre1(x;A;a;T;x,v.P(x,v)) ∈ Dsys
. . . 15. ∀D:Dsys.
. . . |   @i: ma-single-pre1(x;A;a;T;x,v.P(x,v)) ⊆ D
. . . |   ⇒
. . . |   D
. . . |   realizes es.(vartype(i;x) ⊆r A)
. . . |               & (∀e:E.
. . . |                  loc(e) = i
. . . |                  ⇒
. . . |                  kind(e) = locl(a) ⇒ (valtype(e) ⊆r T))
. . . |               & (∀e:E.
. . . |                  loc(e) = i
. . . |                  ⇒
. . . |                  (kind(e) = locl(a) ⇒ P((x when e),val(e)))
. . . |                  & (∃e':E.
. . . |                     (e <loc e') ∨ e = e'
. . . |                     & kind(e') = locl(a)
. . . |                       ∨ (∀v:T. ¬P((x after e'),v))))
```

```
. . . 16. @i: x : A initially x = c ∈ Dsys
. . . 17. ∀D:Dsys.
. . . |   @i: x : A initially x = c ⊆ D
. . . |   ⇒
. . . |   D
. . . |   realizes es.(vartype(i;x) ⊆r A)
. . . |              & (∀e:E.
. . . |                 loc(e) = i ⇒ first(e) ⇒ (x when e) = c)
. . . 18. D : Dsys
. . . 19. @i: (with ds: x : A
. . . |    init: x : c
. . . |   action a:T
. . . |    precondition a(v) is
. . . |    λs,v. P(s(x),v)) ⊆ D
. . . 20. D
. . . |   realizes es.(vartype(i;x) ⊆r A)
. . . |              & (∀e:E.
. . . |                 loc(e) = i ⇒ first(e) ⇒ (x when e) = c)
. . . ⊢  D
. . . |  realizes es.(vartype(i;x) ⊆r A)
. . . |             & (∀e:E.
. . . |                loc(e) = i ⇒ first(e) ⇒ (x when e) = c)
. . . |             & (∀e:E.
. . . |                loc(e) = i
. . . |                ⇒
. . . |                kind(e) = locl(a) ⇒ (valtype(e) ⊆r T))
. . . |             & (∀e:E.
. . . |                loc(e) = i
. . . |                ⇒
. . . |                kind(e) = locl(a) ⇒ P((x when e),val(e)))
. . . |               & ((∃v:T. P(c,v))
. . . |                  ⇒
. . . |                  (∃e:E.
. . . |                   loc(e) = i
. . . |                   & kind(e) = locl(a)
. . . |                     ∨ (∀v:T. ¬P((x after e),v))))
. . . | by RepeatFor 2 (Thin -4) THEN InstHyp [D] -4
. . . |
. . . |\
. . . | .....antecedent .....
. . . | 1. i : Id
. . . | 2. a : Id
. . . | 3. x : Id
. . . | 4. A : Type
. . . | 5. T : Type
. . . | 6. c : A
. . . | 7. P : A→T→Prop
. . . | 8. (λs,v. P(s(x),v)) ∈ State(x : A)→T→Prop
. . . | 9. ∀x@0:Id. x@0 ∈ dom(x : A) ⇒ x@0 ∈ dom(x : c)
. . . | 10. x : c ∈ x@0:Id fp-> x : A(x@0)?Void
. . . | 11. @i: (with ds: x : A
. . . | |    init: x : c
. . . | |   action a:T
. . . | |    precondition a(v) is
. . . | |    λs,v. P(s(x),v))
```

```
. . . | |   ∈ Dsys
. . . | 12. ∀D:Dsys.
. . . | |   @i: (with ds: x : A
. . . | |    init: x : c
. . . | |   action a:T
. . . | |    precondition a(v) is
. . . | |    λs,v. P(s(x),v)) ⊆ D
. . . | |   ⇒
. . . | |   D
. . . | |   realizes es.(∃v:T.
. . . | |                (λs,v. P(s(x),v))((λx@0.x : c(x@0)?•),v))
. . . | |               ⇒
. . . | |               (∃e:E. loc(e) = i)
. . . | 13. @i: (with ds: x : A
. . . | |    init: x : c
. . . | |   action a:T
. . . | |    precondition a(v) is
. . . | |    λs,v. P(s(x),v))
. . . | |   ∈ Dsys
. . . | 14. @i: ma-single-pre1(x;A;a;T;x,v.P(x,v)) ∈ Dsys
. . . | 15. ∀D:Dsys.
. . . | |   @i: ma-single-pre1(x;A;a;T;x,v.P(x,v)) ⊆ D
. . . | |   ⇒
. . . | |   D
. . . | |   realizes es.(vartype(i;x) ⊆r A)
. . . | |               & (∀e:E.
. . . | |                  loc(e) = i
. . . | |                  ⇒
. . . | |                  kind(e) = locl(a) ⇒ (valtype(e) ⊆r T))
. . . | |               & (∀e:E.
. . . | |                  loc(e) = i
. . . | |                  ⇒
. . . | |                  (kind(e) = locl(a) ⇒ P((x when e),val(e)))
. . . | |                  & (∃e':E.
. . . | |                     (e <loc e') ∨ e = e'
. . . | |                     & kind(e') = locl(a)
. . . | |                       ∨ (∀v:T. ¬P((x after e'),v))))
. . . | 16. D : Dsys
. . . | 17. @i: (with ds: x : A
. . . | |    init: x : c
. . . | |   action a:T
. . . | |    precondition a(v) is
. . . | |    λs,v. P(s(x),v)) ⊆ D
. . . | 18. D
. . . | |   realizes es.(vartype(i;x) ⊆r A)
. . . | |               & (∀e:E.
. . . | |                  loc(e) = i ⇒ first(e) ⇒ (x when e) = c)
. . . | ⊢  @i: ma-single-pre1(x;A;a;T;x,v.P(x,v)) ⊆ D
. . . | | by Using
. . . | |    ['D2'
. . . | |     ,@i: (with ds: x : A
. . . | |       init: x : c
. . . | |      action a:T
. . . | |       precondition a(v) is
. . . | |       λs,v. P(s(x),v))]
```

```
. . . | |    (BackThru
. . . | |     Thm* ∀D1,D2,D3:Dsys. D1 ⊆ D2 ⇒ D2 ⊆ D3 ⇒ D1 ⊆ D3
. . . | |     {d_DASH_sub_transitivity})
. . . | |
. . . | 1. i : Id
. . . | 2. a : Id
. . . | 3. x : Id
. . . | 4. A : Type
. . . | 5. T : Type
. . . | 6. c : A
. . . | 7. P : A→T→Prop
. . . | 8. (λs,v. P(s(x),v)) ∈ State(x : A)→T→Prop
. . . | 9. ∀x@0:Id. x@0 ∈ dom(x : A) ⇒ x@0 ∈ dom(x : c)
. . . | 10. x : c ∈ x@0:Id fp-> x : A(x@0)?Void
. . . | 11. @i: (with ds: x : A
. . . | |    init: x : c
. . . | |   action a:T
. . . | |    precondition a(v) is
. . . | |    λs,v. P(s(x),v))
. . . | |   ∈ Dsys
. . . | 12. ∀D:Dsys.
. . . | |   @i: (with ds: x : A
. . . | |    init: x : c
. . . | |   action a:T
. . . | |    precondition a(v) is
. . . | |    λs,v. P(s(x),v)) ⊆ D
. . . | |   ⇒
. . . | |   D
. . . | |   realizes es.(∃v:T.
. . . | |                (λs,v. P(s(x),v))((λx@0.x : c(x@0)?·),v))
. . . | |               ⇒
. . . | |               (∃e:E. loc(e) = i)
. . . | 13. @i: (with ds: x : A
. . . | |    init: x : c
. . . | |   action a:T
. . . | |    precondition a(v) is
. . . | |    λs,v. P(s(x),v))
. . . | |   ∈ Dsys
. . . | 14. @i: ma-single-pre1(x;A;a;T;x,v.P(x,v)) ∈ Dsys
. . . | 15. ∀D:Dsys.
. . . | |   @i: ma-single-pre1(x;A;a;T;x,v.P(x,v)) ⊆ D
. . . | |   ⇒
. . . | |   D
. . . | |   realizes es.(vartype(i;x) ⊆r A)
. . . | |               & (∀e:E.
. . . | |                  loc(e) = i
. . . | |                  ⇒
. . . | |                  kind(e) = locl(a) ⇒ (valtype(e) ⊆r T))
. . . | |               & (∀e:E.
. . . | |                  loc(e) = i
. . . | |                  ⇒
. . . | |                  (kind(e) = locl(a) ⇒ P((x when e),val(e)))
. . . | |                  & (∃e':E.
. . . | |                     (e <loc e') ∨ e = e'
. . . | |                     & kind(e') = locl(a)
```

```
. . . | |                        ∨ (∀v:T. ¬P((x after e'),v))))
. . . | 16. D : Dsys
. . . | 17. @i: (with ds: x : A
. . . | |    init: x : c
. . . | |   action a:T
. . . | |    precondition a(v) is
. . . | |    λs,v. P(s(x),v)) ⊆ D
. . . | 18. D
. . . | |   realizes es.(vartype(i;x) ⊆r A)
. . . | |               & (∀e:E.
. . . | |                  loc(e) = i ⇒ first(e) ⇒ (x when e) = c)
. . . | ⊢  @i: ma-single-pre1(x;A;a;T;x,v.P(x
. . . | |                                   ,v)) ⊆ @i: (with ds: x : A
. . . | |   init: x : c
. . . | |  action a:T
. . . | |   precondition a(v) is
. . . | |   λs,v. P(s(x),v))
. . . | | by Subst
. . . | |    ((with ds: x : A
. . . | |      init: x : c
. . . | |     action a:T
. . . | |      precondition a(v) is
. . . | |      λs,v. P(s(x)
. . . | |             ,v)) ∼ ma-single-pre-init1(x;A;c;a;T;y,v.P(y
. . . | |                                                        ,v)))
. . . | |    0
. . . | |
. . . | |\
. . . | | .....equality .....
. . . | | 1. i : Id
. . . | | 2. a : Id
. . . | | 3. x : Id
. . . | | 4. A : Type
. . . | | 5. T : Type
. . . | | 6. c : A
. . . | | 7. P : A→T→Prop
. . . | | 8. (λs,v. P(s(x),v)) ∈ State(x : A)→T→Prop
. . . | | 9. ∀x@0:Id. x@0 ∈ dom(x : A) ⇒ x@0 ∈ dom(x : c)
. . . | | 10. x : c ∈ x@0:Id fp-> x : A(x@0)?Void
. . . | | 11. @i: (with ds: x : A
. . . | |      init: x : c
. . . | |     action a:T
. . . | |      precondition a(v) is
. . . | |      λs,v. P(s(x),v))
. . . | |     ∈ Dsys
. . . | | 12. ∀D:Dsys.
. . . | |     @i: (with ds: x : A
. . . | |      init: x : c
. . . | |     action a:T
. . . | |      precondition a(v) is
. . . | |      λs,v. P(s(x),v)) ⊆ D
. . . | |     ⇒
. . . | |     D
. . . | |     realizes es.(∃v:T.
. . . | |                  (λs,v. P(s(x),v))((λx@0.x : c(x@0)?•),v))
```

```
. . . | |                ⇒
. . . | |                (∃e:E. loc(e) = i)
. . . | | 13. @i: (with ds: x : A
. . . | |      init: x : c
. . . | |     action a:T
. . . | |      precondition a(v) is
. . . | |      λs,v. P(s(x),v))
. . . | |     ∈ Dsys
. . . | | 14. @i: ma-single-pre1(x;A;a;T;x,v.P(x,v)) ∈ Dsys
. . . | | 15. ∀D:Dsys.
. . . | |     @i: ma-single-pre1(x;A;a;T;x,v.P(x,v)) ⊆ D
. . . | |     ⇒
. . . | |     D
. . . | |     realizes es.(vartype(i;x) ⊆r A)
. . . | |                 & (∀e:E.
. . . | |                    loc(e) = i
. . . | |                    ⇒
. . . | |                    kind(e) = locl(a) ⇒ (valtype(e) ⊆r T))
. . . | |                 & (∀e:E.
. . . | |                    loc(e) = i
. . . | |                    ⇒
. . . | |                    (kind(e) = locl(a)
. . . | |                     ⇒
. . . | |                     P((x when e),val(e)))
. . . | |                    & (∃e':E.
. . . | |                       (e <loc e') ∨ e = e'
. . . | |                       & kind(e') = locl(a)
. . . | |                         ∨ (∀v:T. ¬P((x after e'),v))))
. . . | | 16. D : Dsys
. . . | | 17. @i: (with ds: x : A
. . . | |      init: x : c
. . . | |     action a:T
. . . | |      precondition a(v) is
. . . | |      λs,v. P(s(x),v)) ⊆ D
. . . | | 18. D
. . . | |     realizes es.(vartype(i;x) ⊆r A)
. . . | |                 & (∀e:E.
. . . | |                    loc(e) = i ⇒ first(e) ⇒ (x when e) = c)
. . . | | ⊢  (with ds: x : A
. . . | |     init: x : c
. . . | |    action a:T
. . . | |     precondition a(v) is
. . . | |     λs,v. P(s(x)
. . . | |            ,v)) ∼ ma-single-pre-init1(x;A;c;a;T;y,v.P(y,v))
. . . | |   by Unfold ‘ma-single-pre-init1‘ 0 THEN Trivial
. . . | |
. . . | .\
. . . | . 1. i : Id
. . . | . 2. a : Id
. . . | . 3. x : Id
. . . | . 4. A : Type
. . . | . 5. T : Type
. . . | . 6. c : A
. . . | . 7. P : A→T→Prop
. . . | . 8. (λs,v. P(s(x),v)) ∈ State(x : A)→T→Prop
```

```
. . . | . 9. ∀x@0:Id. x@0 ∈ dom(x : A) ⇒ x@0 ∈ dom(x : c)
. . . | . 10. x : c ∈ x@0:Id fp-> x : A(x@0)?Void
. . . | . 11. @i: (with ds: x : A
. . . | . |    init: x : c
. . . | . |   action a:T
. . . | . |    precondition a(v) is
. . . | . |    λs,v. P(s(x),v))
. . . | . |   ∈ Dsys
. . . | . 12. ∀D:Dsys.
. . . | . |   @i: (with ds: x : A
. . . | . |    init: x : c
. . . | . |   action a:T
. . . | . |    precondition a(v) is
. . . | . |    λs,v. P(s(x),v)) ⊆ D
. . . | . |   ⇒
. . . | . |   D
. . . | . |   realizes es.(∃v:T.
. . . | . |                (λs,v. P(s(x),v))((λx@0.x : c(x@0)?•),v))
. . . | . |               ⇒
. . . | . |               (∃e:E. loc(e) = i)
. . . | . 13. @i: (with ds: x : A
. . . | . |    init: x : c
. . . | . |   action a:T
. . . | . |    precondition a(v) is
. . . | . |    λs,v. P(s(x),v))
. . . | . |   ∈ Dsys
. . . | . 14. @i: ma-single-pre1(x;A;a;T;x,v.P(x,v)) ∈ Dsys
. . . | . 15. ∀D:Dsys.
. . . | . |   @i: ma-single-pre1(x;A;a;T;x,v.P(x,v)) ⊆ D
. . . | . |   ⇒
. . . | . |   D
. . . | . |   realizes es.(vartype(i;x) ⊆r A)
. . . | . |               & (∀e:E.
. . . | . |                  loc(e) = i
. . . | . |                  ⇒
. . . | . |                  kind(e) = locl(a) ⇒ (valtype(e) ⊆r T))
. . . | . |               & (∀e:E.

. . . | . |                  loc(e) = i
. . . | . |                  ⇒
. . . | . |                  (kind(e) = locl(a)
. . . | . |                   ⇒
. . . | . |                   P((x when e),val(e)))
. . . | . |                  & (∃e':E.
. . . | . |                     (e <loc e') ∨ e = e'
. . . | . |                     & kind(e') = locl(a)
. . . | . |                       ∨ (∀v:T. ¬P((x after e'),v))))
. . . | . 16. D : Dsys
. . . | . 17. @i: (with ds: x : A
. . . | . |    init: x : c
. . . | . |   action a:T
. . . | . |    precondition a(v) is
. . . | . |    λs,v. P(s(x),v)) ⊆ D
. . . | . 18. D
. . . | . |   realizes es.(vartype(i;x) ⊆r A)
. . . | . |               & (∀e:E.
```

```
. . . | . |                  loc(e) = i ⇒ first(e) ⇒ (x when e) = c)
. . . | . ⊢  @i: ma-single-pre1(x;A;a;T;x,v.P(x
. . . | . |                                  ,v)) ⊆ @i: ...
. . . | . | by BackThru
. . . | . |    Thm* ∀i:Id, A,B:MsgA. @i: A ⊆ @i: B ⟺ A ⊆ B
. . . | . |    {s_DASH_at_DASH_sub_DASH_s_DASH_at}
. . . | . |    THENA
. . . | . |    (Auto THEN Unfold `msga-at` 0)
. . . | . |
. . . | . 1. i : Id
. . . | . 2. a : Id
. . . | . 3. x : Id
. . . | . 4. A : Type
. . . | . 5. T : Type
. . . | . 6. c : A
. . . | . 7. P : A→T→Prop
. . . | . 8. (λs,v. P(s(x),v)) ∈ State(x : A)→T→Prop
. . . | . 9. ∀x@0:Id. x@0 ∈ dom(x : A) ⇒ x@0 ∈ dom(x : c)
. . . | . 10. x : c ∈ x@0:Id fp-> x : A(x@0)?Void
. . . | . 11. @i: (with ds: x : A
. . . | . |    init: x : c
. . . | . |   action a:T
. . . | . |    precondition a(v) is
. . . | . |    λs,v. P(s(x),v))
. . . | . |   ∈ Dsys
. . . | . 12. ∀D:Dsys.
. . . | . |   @i: (with ds: x : A
. . . | . |    init: x : c
. . . | . |   action a:T
. . . | . |    precondition a(v) is
. . . | . |    λs,v. P(s(x),v)) ⊆ D
. . . | . |   ⇒
. . . | . |   D
. . . | . |   realizes es.(∃v:T.
. . . | . |                (λs,v. P(s(x),v))((λx@0.x : c(x@0)?•),v))
. . . | . |               ⇒
. . . | . |               (∃e:E. loc(e) = i)
. . . | . 13. @i: (with ds: x : A
. . . | . |    init: x : c
. . . | . |   action a:T
. . . | . |    precondition a(v) is
. . . | . |    λs,v. P(s(x),v))
. . . | . |   ∈ Dsys
. . . | . 14. @i: ma-single-pre1(x;A;a;T;x,v.P(x,v)) ∈ Dsys
. . . | . 15. ∀D:Dsys.
. . . | . |   @i: ma-single-pre1(x;A;a;T;x,v.P(x,v)) ⊆ D
. . . | . |   ⇒
. . . | . |   D
. . . | . |   realizes es.(vartype(i;x) ⊆r A)
. . . | . |               & (∀e:E.
. . . | . |                  loc(e) = i
. . . | . |                  ⇒
. . . | . |                  kind(e) = locl(a) ⇒ (valtype(e) ⊆r T))
. . . | . |               & (∀e:E.
. . . | . |                  loc(e) = i
```

```
. . . | . |                  ⇒
. . . | . |                  (kind(e) = locl(a)
. . . | . |                   ⇒
. . . | . |                   P((x when e),val(e)))
. . . | . |                  & (∃e':E.
. . . | . |                     (e <loc e') ∨ e = e'
. . . | . |                     & kind(e') = locl(a)
. . . | . |                       ∨ (∀v:T. ¬P((x after e'),v))))
. . . | . 16. D : Dsys
. . . | . 17. @i: (with ds: x : A
. . . | . |    init: x : c
. . . | . |   action a:T
. . . | . |    precondition a(v) is
. . . | . |    λs,v. P(s(x),v)) ⊆ D
. . . | . 18. D
. . . | . |   realizes es.(vartype(i;x) ⊆r A)
. . . | . |               & (∀e:E.
. . . | . |                  loc(e) = i ⇒ first(e) ⇒ (x when e) = c)
. . . | . ⊢  ma-single-pre1(x;A;a;T;x,v.P(x
. . . | . |                               ,v)) ⊆ ...
. . . | . | by Repeat
. . . | . |    (Unfolds
. . . | . |     [‘ma-single-pre1‘
. . . | . |     ;‘ma-single-pre‘
. . . | . |     ;‘ma-single-pre-init‘
. . . | . |     ;‘ma-single-pre-init1‘
. . . | . |     ;‘ma-sub‘
. . . | . |     ;‘mk-ma‘]
. . . | . |     0
. . . | . |     THEN
. . . | . |     Reduce 0)
. . . | . |    THEN
. . . | . |    Try
. . . | . |    (BackThru
. . . | . |     Thm* ∀B,eq,g:Top.  ⊆ g    {fpf_DASH_empty_DASH_sub}
. . . | . |     THEN
. . . | . |     Complete Auto)
. . . | . |    THEN
. . . | . |    Try
. . . | . |    (BackThru
. . . | . |     Thm* ∀B:(A→Type), eq:EqDecider(A), f,g:a:A fp-> B(a).
. . . | . |          f = g ⇒ f ⊆ g
. . . | . |     {fpf_DASH_sub_weakening}
. . . | . |     THEN
. . . | . |     Complete Auto)
. . . | . |
. . . | . 1. i : Id
. . . | . 2. a : Id
. . . | . 3. x : Id
. . . | . 4. A : Type
. . . | . 5. T : Type
. . . | . 6. c : A
. . . | . 7. P : A→T→Prop
. . . | . 8. (λs,v. P(s(x),v)) ∈ State(x : A)→T→Prop
. . . | . 9. ∀x@0:Id. x@0 ∈ dom(x : A) ⇒ x@0 ∈ dom(x : c)
```

```
. . . | . 10. x : c ∈ x@0:Id fp-> x : A(x@0)?Void
. . . | . 11. @i: (with ds: x : A
. . . | . |    init: x : c
. . . | . |   action a:T
. . . | . |    precondition a(v) is
. . . | . |    λs,v. P(s(x),v))
. . . | . |   ∈ Dsys
. . . | . 12. ∀D:Dsys.
. . . | . |   @i: (with ds: x : A
. . . | . |    init: x : c
. . . | . |   action a:T
. . . | . |    precondition a(v) is
. . . | . |    λs,v. P(s(x),v)) ⊆ D
. . . | . |   ⇒
. . . | . |   D
. . . | . |   realizes es.(∃v:T.
. . . | . |                (λs,v. P(s(x),v))((λx@0.x : c(x@0)?•),v))
. . . | . |               ⇒
. . . | . |               (∃e:E. loc(e) = i)
. . . | . 13. @i: (with ds: x : A
. . . | . |    init: x : c
. . . | . |   action a:T
. . . | . |    precondition a(v) is
. . . | . |    λs,v. P(s(x),v))
. . . | . |   ∈ Dsys
. . . | . 14. @i: ma-single-pre1(x;A;a;T;x,v.P(x,v)) ∈ Dsys
. . . | . 15. ∀D:Dsys.
. . . | . |   @i: ma-single-pre1(x;A;a;T;x,v.P(x,v)) ⊆ D
. . . | . |   ⇒
. . . | . |   D
. . . | . |   realizes es.(vartype(i;x) ⊆r A)
. . . | . |               & (∀e:E.
. . . | . |                  loc(e) = i
. . . | . |                  ⇒
. . . | . |                  kind(e) = locl(a) ⇒ (valtype(e) ⊆r T))
. . . | . |               & (∀e:E.
. . . | . |                  loc(e) = i
. . . | . |                  ⇒
. . . | . |                  (kind(e) = locl(a)
. . . | . |                   ⇒
. . . | . |                   P((x when e),val(e)))
. . . | . |                  & (∃e':E.
. . . | . |                     (e <loc e') ∨ e = e'
. . . | . |                     & kind(e') = locl(a)
. . . | . |                       ∨ (∀v:T. ¬P((x after e'),v))))
. . . | . 16. D : Dsys
. . . | . 17. @i: (with ds: x : A
. . . | . |    init: x : c
. . . | . |   action a:T
. . . | . |    precondition a(v) is
. . . | . |    λs,v. P(s(x),v)) ⊆ D
. . . | . 18. D
. . . | . |   realizes es.(vartype(i;x) ⊆r A)
. . . | . |               & (∀e:E.
. . . | . |                  loc(e) = i ⇒ first(e) ⇒ (x when e) = c)
```

```
. . . | . ⊢  a : λ2s,v. P(s(x),v) ⊆ a : λs,v. P(s(x),v)
. . . | . | by Unfold ‘so_lambda‘ 0
. . . | . |
. . . | . 1. i : Id
. . . | . 2. a : Id
. . . | . 3. x : Id
. . . | . 4. A : Type
. . . | . 5. T : Type
. . . | . 6. c : A
. . . | . 7. P : A→T→Prop
. . . | . 8. (λs,v. P(s(x),v)) ∈ State(x : A)→T→Prop
. . . | . 9. ∀x@0:Id. x@0 ∈ dom(x : A) ⇒ x@0 ∈ dom(x : c)
. . . | . 10. x : c ∈ x@0:Id fp-> x : A(x@0)?Void
. . . | . 11. @i: (with ds: x : A
. . . | . |    init: x : c
. . . | . |   action a:T
. . . | . |    precondition a(v) is
. . . | . |    λs,v. P(s(x),v))
. . . | . |   ∈ Dsys
. . . | . 12. ∀D:Dsys.
. . . | . |   @i: (with ds: x : A
. . . | . |    init: x : c
. . . | . |   action a:T
. . . | . |    precondition a(v) is
. . . | . |    λs,v. P(s(x),v)) ⊆ D
. . . | . |   ⇒
. . . | . |   D
. . . | . |   realizes es.(∃v:T.
. . . | . |                (λs,v. P(s(x),v))((λx@0.x : c(x@0)?•),v))
. . . | . |               ⇒
. . . | . |               (∃e:E. loc(e) = i)
. . . | . 13. @i: (with ds: x : A
. . . | . |    init: x : c
. . . | . |   action a:T
. . . | . |    precondition a(v) is
. . . | . |    λs,v. P(s(x),v))
. . . | . |   ∈ Dsys
. . . | . 14. @i: ma-single-pre1(x;A;a;T;x,v.P(x,v)) ∈ Dsys
. . . | . 15. ∀D:Dsys.
. . . | . |   @i: ma-single-pre1(x;A;a;T;x,v.P(x,v)) ⊆ D
. . . | . |   ⇒
. . . | . |   D
. . . | . |   realizes es.(vartype(i;x) ⊆r A)
. . . | . |               & (∀e:E.
. . . | . |                  loc(e) = i
. . . | . |                  ⇒
. . . | . |                  kind(e) = locl(a) ⇒ (valtype(e) ⊆r T))
. . . | . |               & (∀e:E.
. . . | . |                  loc(e) = i
. . . | . |                  ⇒
. . . | . |                  (kind(e) = locl(a)
. . . | . |                   ⇒
. . . | . |                   P((x when e),val(e)))
. . . | . |                  & (∃e':E.
. . . | . |                     (e <loc e') ∨ e = e'
```

```
. . . | . |                     & kind(e') = locl(a)
. . . | . |                       ∨ (∀v:T. ¬P((x after e'),v))))
. . . | . 16. D : Dsys
. . . | . 17. @i: (with ds: x : A
. . . | . |    init: x : c
. . . | . |   action a:T
. . . | . |    precondition a(v) is
. . . | . |    λs,v. P(s(x),v)) ⊆ D
. . . | . 18. D
. . . | . |   realizes es.(vartype(i;x) ⊆r A)
. . . | . |               & (∀e:E.
. . . | . |                  loc(e) = i ⇒ first(e) ⇒ (x when e) = c)
. . . | . ⊢  a : λs,v. P(s(x),v) ⊆ a : λs,v. P(s(x),v)
. . . | . | by Unfold `fpf-cap` 0
. . . | . |    THEN
. . . | . |    BackThru
. . . | . |    Thm* ∀B:(A→Type), x:A, v:B(x), eqa:EqDecider(A).
. . . | . |         x : v ⊆ x : v
. . . | . |    {fpf_DASH_single_DASH_sub_DASH_reflexive}
. . . | . |    THEN
. . . | . |    Try (Complete Auto)
. . . | . |    THEN
. . . | . |    Fold `fpf-cap` 0
. . . | . |
. . . | . |\
. . . | . | 1. i : Id
. . . | . | 2. a : Id
. . . | . | 3. x : Id
. . . | . | 4. A : Type
. . . | . | 5. T : Type
. . . | . | 6. c : A
. . . | . | 7. P : A→T→Prop
. . . | . | 8. (λs,v. P(s(x),v)) ∈ State(x : A)→T→Prop
. . . | . | 9. ∀x@0:Id. x@0 ∈ dom(x : A) ⇒ x@0 ∈ dom(x : c)
. . . | . | 10. x : c ∈ x@0:Id fp-> x : A(x@0)?Void
. . . | . | 11. @i: (with ds: x : A
. . . | . | |    init: x : c
. . . | . | |   action a:T
. . . | . | |    precondition a(v) is
. . . | . | |    λs,v. P(s(x),v))
. . . | . | |   ∈ Dsys
. . . | . | 12. ∀D:Dsys.
. . . | . | |   @i: (with ds: x : A
. . . | . | |    init: x : c
. . . | . | |   action a:T
. . . | . | |    precondition a(v) is
. . . | . | |    λs,v. P(s(x),v)) ⊆ D
. . . | . | |   ⇒
. . . | . | |   D
. . . | . | |   realizes es.(∃v:T.
. . . | . | |                (λs,v. P(s(x),v))((λx@0.x : c(x@0)?•),v))
. . . | . | |               ⇒
. . . | . | |               (∃e:E. loc(e) = i)
. . . | . | 13. @i: (with ds: x : A
. . . | . | |    init: x : c
```

```
. . . | . | |   action a:T
. . . | . | |    precondition a(v) is
. . . | . | |    λs,v. P(s(x),v))
. . . | . | |   ∈ Dsys
. . . | . | 14. @i: ma-single-pre1(x;A;a;T;x,v.P(x,v)) ∈ Dsys
. . . | . | 15. ∀D:Dsys.
. . . | . | |   @i: ma-single-pre1(x;A;a;T;x,v.P(x,v)) ⊆ D
. . . | . | |   ⇒
. . . | . | |   D
. . . | . | |   realizes es.(vartype(i;x) ⊆r A)
. . . | . | |               & (∀e:E.
. . . | . | |                  loc(e) = i
. . . | . | |                  ⇒
. . . | . | |                  kind(e) = locl(a) ⇒ (valtype(e) ⊆r T))
. . . | . | |               & (∀e:E.
. . . | . | |                  loc(e) = i
. . . | . | |                  ⇒
. . . | . | |                  (kind(e) = locl(a)
. . . | . | |                   ⇒
. . . | . | |                   P((x when e),val(e)))
. . . | . | |                  & (∃e':E.
. . . | . | |                     (e <loc e') ∨ e = e'
. . . | . | |                     & kind(e') = locl(a)
. . . | . | |                       ∨ (∀v:T. ¬P((x after e'),v))))
. . . | . | 16. D : Dsys
. . . | . | 17. @i: (with ds: x : A
. . . | . | |    init: x : c
. . . | . | |   action a:T
. . . | . | |    precondition a(v) is
. . . | . | |    λs,v. P(s(x),v)) ⊆ D
. . . | . | 18. D
. . . | . | |   realizes es.(vartype(i;x) ⊆r A)
. . . | . | |               & (∀e:E.
. . . | . | |                  loc(e) = i
. . . | . | |                  ⇒
. . . | . | |                  first(e) ⇒ (x when e) = c)
. . . | . | ⊢  (λa@0.State(x : A)→locl(a) : T(locl(a@0))?Top→Prop)
. . . | . | |  ∈ Id→Type  by Auto
. . . | . | |
. . . | . | .....subterm .....
. . . | . | 1. i : Id
. . . | . | 2. a : Id
. . . | . | 3. x : Id
. . . | . | 4. A : Type
. . . | . | 5. T : Type
. . . | . | 6. c : A
. . . | . | 7. P : A→T→Prop
. . . | . | 8. (λs,v. P(s(x),v)) ∈ State(x : A)→T→Prop
. . . | . | 9. ∀x@0:Id. x@0 ∈ dom(x : A) ⇒ x@0 ∈ dom(x : c)
. . . | . | 10. x : c ∈ x@0:Id fp-> x : A(x@0)?Void
. . . | . | 11. @i: (with ds: x : A
. . . | . |     init: x : c
. . . | . |    action a:T
. . . | . |     precondition a(v) is
. . . | . |     λs,v. P(s(x),v))
```

```
. . . | . |     ∈ Dsys
. . . | . | 12. ∀D:Dsys.
. . . | . |     @i: (with ds: x : A
. . . | . |      init: x : c
. . . | . |     action a:T
. . . | . |      precondition a(v) is
. . . | . |      λs,v. P(s(x),v)) ⊆ D
. . . | . |     ⇒
. . . | . |     D
. . . | . |     realizes es.(∃v:T.
. . . | . |                  (λs,v. P(s(x),v))((λx@0.x : c(x@0)?•),v))
. . . | . |                 ⇒
. . . | . |                 (∃e:E. loc(e) = i)
. . . | . | 13. @i: (with ds: x : A
. . . | . |      init: x : c
. . . | . |     action a:T
. . . | . |      precondition a(v) is
. . . | . |      λs,v. P(s(x),v))
. . . | . |     ∈ Dsys
. . . | . | 14. @i: ma-single-pre1(x;A;a;T;x,v.P(x,v)) ∈ Dsys
. . . | . | 15. ∀D:Dsys.
. . . | . |     @i: ma-single-pre1(x;A;a;T;x,v.P(x,v)) ⊆ D
. . . | . |     ⇒
. . . | . |     D
. . . | . |     realizes es.(vartype(i;x) ⊆r A)
. . . | . |                 & (∀e:E.
. . . | . |                    loc(e) = i
. . . | . |                    ⇒
. . . | . |                    kind(e) = locl(a) ⇒ (valtype(e) ⊆r T))
. . . | . |                 & (∀e:E.
. . . | . |                    loc(e) = i
. . . | . |                    ⇒
. . . | . |                    (kind(e) = locl(a)
. . . | . |                     ⇒
. . . | . |                     P((x when e),val(e)))
. . . | . |                    & (∃e':E.
. . . | . |                       (e <loc e') ∨ e = e'
. . . | . |                       & kind(e') = locl(a)
. . . | . |                         ∨ (∀v:T. ¬P((x after e'),v))))
. . . | . | 16. D : Dsys
. . . | . | 17. @i: (with ds: x : A
. . . | . |      init: x : c
. . . | . |     action a:T
. . . | . |      precondition a(v) is
. . . | . |      λs,v. P(s(x),v)) ⊆ D
. . . | . | 18. D
. . . | . |     realizes es.(vartype(i;x) ⊆r A)
. . . | . |                 & (∀e:E.
. . . | . |                    loc(e) = i
. . . | . |                    ⇒
. . . | . |                    first(e) ⇒ (x when e) = c)
. . . | . | 19. a@0 : Id
. . . | . | 20. State(x : A)
. . . | . | ⊢  locl(a) : T(locl(a@0))?Top ∈ Type
. . . | . |   by BackThru
```

```
. . . | . |      Thm* ∀A:Type, f:a:A fp-> Type, eq:EqDecider(A), x:A,
. . . | . |           z:Type. f(x)?z ∈ Type
. . . | . |      {fpf_DASH_cap_DASH_wf_DASH_univ}
. . . | . |
. . . | . .\
. . . | . . 1. i : Id
. . . | . . 2. a : Id
. . . | . . 3. x : Id
. . . | . . 4. A : Type
. . . | . . 5. T : Type
. . . | . . 6. c : A
. . . | . . 7. P : A→T→Prop
. . . | . . 8. (λs,v. P(s(x),v)) ∈ State(x : A)→T→Prop
. . . | . . 9. ∀x@0:Id. x@0 ∈ dom(x : A) ⇒ x@0 ∈ dom(x : c)
. . . | . . 10. x : c ∈ x@0:Id fp-> x : A(x@0)?Void
. . . | . . 11. @i: (with ds: x : A
. . . | . . |    init: x : c
. . . | . . |   action a:T
. . . | . . |    precondition a(v) is
. . . | . . |    λs,v. P(s(x),v))
. . . | . . |   ∈ Dsys
. . . | . . 12. ∀D:Dsys.
. . . | . . |   @i: (with ds: x : A
. . . | . . |    init: x : c
. . . | . . |   action a:T
. . . | . . |    precondition a(v) is
. . . | . . |    λs,v. P(s(x),v)) ⊆ D
. . . | . . |   ⇒
. . . | . . |   D
. . . | . . |   realizes es.(∃v:T.
. . . | . . |                (λs,v. P(s(x),v))((λx@0.x : c(x@0)?·),v))
. . . | . . |               ⇒
. . . | . . |               (∃e:E. loc(e) = i)
. . . | . . 13. @i: (with ds: x : A
. . . | . . |    init: x : c
. . . | . . |   action a:T
. . . | . . |    precondition a(v) is
. . . | . . |    λs,v. P(s(x),v))
. . . | . . |   ∈ Dsys
. . . | . . 14. @i: ma-single-pre1(x;A;a;T;x,v.P(x,v)) ∈ Dsys
. . . | . . 15. ∀D:Dsys.
. . . | . . |   @i: ma-single-pre1(x;A;a;T;x,v.P(x,v)) ⊆ D
. . . | . . |   ⇒
. . . | . . |   D
. . . | . . |   realizes es.(vartype(i;x) ⊆r A)
. . . | . . |              & (∀e:E.
. . . | . . |                 loc(e) = i
. . . | . . |                 ⇒
. . . | . . |                 kind(e) = locl(a) ⇒ (valtype(e) ⊆r T))
. . . | . . |              & (∀e:E.
. . . | . . |                 loc(e) = i
. . . | . . |                 ⇒
. . . | . . |                 (kind(e) = locl(a)
. . . | . . |                  ⇒
. . . | . . |                  P((x when e),val(e)))
```

```
. . . | . . |                  & (∃e':E.
. . . | . . |                     (e <loc e') ∨ e = e'
. . . | . . |                     & kind(e') = locl(a)
. . . | . . |                       ∨ (∀v:T. ¬P((x after e'),v))))
. . . | . . 16. D : Dsys
. . . | . . 17. @i: (with ds: x : A
. . . | . . |    init: x : c
. . . | . . |   action a:T
. . . | . . |    precondition a(v) is
. . . | . . |    λs,v. P(s(x),v)) ⊆ D
. . . | . . 18. D
. . . | . . |   realizes es.(vartype(i;x) ⊆r A)
. . . | . . |               & (∀e:E.
. . . | . . |                  loc(e) = i
. . . | . . |                  ⇒
. . . | . . |                  first(e) ⇒ (x when e) = c)
. . . | . . ⊢  (λs,v. P(s(x),v))
. . . | . . |  ∈ State(x : A)→locl(a) : T(locl(a))?Top→Prop
. . . | . . | by RW0
. . . | . . |    Thm* ∀eq:EqDecider(A), x:A, v,z:Top. x : v(x)?z ∼ v
. . . | . . |    {fpf_DASH_cap_DASH_single1}
. . . | . . |    0
. . . | . . |
. . . | . . 1. i : Id
. . . | . . 2. a : Id
. . . | . . 3. x : Id
. . . | . . 4. A : Type
. . . | . . 5. T : Type
. . . | . . 6. c : A
. . . | . . 7. P : A→T→Prop
. . . | . . 8. (λs,v. P(s(x),v)) ∈ State(x : A)→T→Prop
. . . | . . 9. ∀x@0:Id. x@0 ∈ dom(x : A) ⇒ x@0 ∈ dom(x : c)
. . . | . . 10. x : c ∈ x@0:Id fp-> x : A(x@0)?Void
. . . | . . 11. @i: (with ds: x : A
. . . | . .     init: x : c
. . . | . .    action a:T
. . . | . .     precondition a(v) is
. . . | . .     λs,v. P(s(x),v))
. . . | . .    ∈ Dsys
. . . | . . 12. ∀D:Dsys.
. . . | . .    @i: (with ds: x : A
. . . | . .     init: x : c
. . . | . .    action a:T
. . . | . .     precondition a(v) is
. . . | . .     λs,v. P(s(x),v)) ⊆ D
. . . | . .    ⇒
. . . | . .    D
. . . | . .    realizes es.(∃v:T.
. . . | . .                 (λs,v. P(s(x),v))((λx@0.x : c(x@0)?•),v))
. . . | . .                ⇒
. . . | . .                (∃e:E. loc(e) = i)
. . . | . . 13. @i: (with ds: x : A
. . . | . .     init: x : c
. . . | . .    action a:T
. . . | . .     precondition a(v) is
```

```
. . . | . .      λs,v. P(s(x),v))
. . . | . .     ∈ Dsys
. . . | . . 14. @i: ma-single-pre1(x;A;a;T;x,v.P(x,v)) ∈ Dsys
. . . | . . 15. ∀D:Dsys.
. . . | . .     @i: ma-single-pre1(x;A;a;T;x,v.P(x,v)) ⊆ D
. . . | . .     ⇒
. . . | . .     D
. . . | . .     realizes es.(vartype(i;x) ⊆r A)
. . . | . .                 & (∀e:E.
. . . | . .                    loc(e) = i
. . . | . .                    ⇒
. . . | . .                    kind(e) = locl(a) ⇒ (valtype(e) ⊆r T))
. . . | . .                 & (∀e:E.
. . . | . .                    loc(e) = i
. . . | . .                    ⇒
. . . | . .                    (kind(e) = locl(a)
. . . | . .                     ⇒
. . . | . .                     P((x when e),val(e)))
. . . | . .                    & (∃e':E.
. . . | . .                       (e <loc e') ∨ e = e'
. . . | . .                       & kind(e') = locl(a)
. . . | . .                         ∨ (∀v:T. ¬P((x after e'),v))))
. . . | . . 16. D : Dsys
. . . | . . 17. @i: (with ds: x : A
. . . | . .      init: x : c
. . . | . .     action a:T
. . . | . .      precondition a(v) is
. . . | . .      λs,v. P(s(x),v)) ⊆ D
. . . | . . 18. D
. . . | . .     realizes es.(vartype(i;x) ⊆r A)
. . . | . .                 & (∀e:E.
. . . | . .                    loc(e) = i
. . . | . .                    ⇒
. . . | . .                    first(e) ⇒ (x when e) = c)
. . . | . . ⊢  (λs,v. P(s(x),v)) ∈ State(x : A)→T→Prop
. . . | . .   by NthHypSq 8 THEN Analyze THEN Try Trivial
. . . |
. . . .\
. . . . 1. i : Id
. . . . 2. a : Id
. . . . 3. x : Id
. . . . 4. A : Type
. . . . 5. T : Type
. . . . 6. c : A
. . . . 7. P : A→T→Prop
. . . . 8. (λs,v. P(s(x),v)) ∈ State(x : A)→T→Prop
. . . . 9. ∀x@0:Id. x@0 ∈ dom(x : A) ⇒ x@0 ∈ dom(x : c)
. . . . 10. x : c ∈ x@0:Id fp-> x : A(x@0)?Void
. . . . 11. @i: (with ds: x : A
. . . . |    init: x : c
. . . . |   action a:T
. . . . |    precondition a(v) is
. . . . |    λs,v. P(s(x),v))
. . . . |   ∈ Dsys
. . . . 12. ∀D:Dsys.
```

```
. . . . |   @i: (with ds: x : A
. . . . |    init: x : c
. . . . |   action a:T
. . . . |    precondition a(v) is
. . . . |    λs,v. P(s(x),v)) ⊆ D
. . . . |   ⇒
. . . . |   D
. . . . |   realizes es.(∃v:T.
. . . . |                (λs,v. P(s(x),v))((λx@0.x : c(x@0)?·),v))
. . . . |               ⇒
. . . . |               (∃e:E. loc(e) = i)
. . . . 13. @i: (with ds: x : A
. . . . |    init: x : c
. . . . |   action a:T
. . . . |    precondition a(v) is
. . . . |    λs,v. P(s(x),v))
. . . . |   ∈ Dsys
. . . . 14. @i: ma-single-pre1(x;A;a;T;x,v.P(x,v)) ∈ Dsys
. . . . 15. ∀D:Dsys.
. . . . |   @i: ma-single-pre1(x;A;a;T;x,v.P(x,v)) ⊆ D
. . . . |   ⇒
. . . . |   D
. . . . |   realizes es.(vartype(i;x) ⊆r A)
. . . . |               & (∀e:E.
. . . . |                  loc(e) = i
. . . . |                  ⇒
. . . . |                  kind(e) = locl(a) ⇒ (valtype(e) ⊆r T))
. . . . |               & (∀e:E.
. . . . |                  loc(e) = i
. . . . |                  ⇒
. . . . |                  (kind(e) = locl(a) ⇒ P((x when e),val(e)))
. . . . |                  & (∃e':E.

. . . . |                     (e <loc e') ∨ e = e'
. . . . |                     & kind(e') = locl(a)
. . . . |                       ∨ (∀v:T. ¬P((x after e'),v))))
. . . . 16. D : Dsys
. . . . 17. @i: (with ds: x : A
. . . . |    init: x : c
. . . . |   action a:T
. . . . |    precondition a(v) is
. . . . |    λs,v. P(s(x),v)) ⊆ D
. . . . 18. D
. . . . |   realizes es.(vartype(i;x) ⊆r A)
. . . . |               & (∀e:E.
. . . . |                  loc(e) = i ⇒ first(e) ⇒ (x when e) = c)
. . . . 19. D
. . . . |   realizes es.(vartype(i;x) ⊆r A)
. . . . |               & (∀e:E.
. . . . |                  loc(e) = i
. . . . |                  ⇒
. . . . |                  kind(e) = locl(a) ⇒ (valtype(e) ⊆r T))
. . . . |               & (∀e:E.
. . . . |                  loc(e) = i
. . . . |                  ⇒
. . . . |                  (kind(e) = locl(a) ⇒ P((x when e),val(e)))
```

```
. . . . |                  & (∃e':E.
. . . . |                     (e <loc e') ∨ e = e'
. . . . |                     & kind(e') = locl(a)
. . . . |                       ∨ (∀v:T. ¬P((x after e'),v))))
. . . . ⊢  D
. . . . |  realizes es.(vartype(i;x) ⊆r A)
. . . . |              & (∀e:E.
. . . . |                 loc(e) = i ⇒ first(e) ⇒ (x when e) = c)
. . . . |              & (∀e:E.
. . . . |                 loc(e) = i
. . . . |                 ⇒
. . . . |                 kind(e) = locl(a) ⇒ (valtype(e) ⊆r T))
. . . . |              & (∀e:E.
. . . . |                 loc(e) = i
. . . . |                 ⇒
. . . . |                 kind(e) = locl(a) ⇒ P((x when e),val(e)))
. . . . |               & ((∃v:T. P(c,v))
. . . . |                  ⇒
. . . . |                  (∃e:E.
. . . . |                   loc(e) = i
. . . . |                   & kind(e) = locl(a)
. . . . |                     ∨ (∀v:T. ¬P((x after e),v))))
. . . . | by RepeatFor 3 (Thin -5) THEN InstHyp [D] -5
. . . . |
. . . . 1. i : Id
. . . . 2. a : Id
. . . . 3. x : Id
. . . . 4. A : Type
. . . . 5. T : Type
. . . . 6. c : A
. . . . 7. P : A→T→Prop
. . . . 8. (λs,v. P(s(x),v)) ∈ State(x : A)→T→Prop
. . . . 9. ∀x@0:Id. x@0 ∈ dom(x : A) ⇒ x@0 ∈ dom(x : c)
. . . . 10. x : c ∈ x@0:Id fp-> x : A(x@0)?Void
. . . . 11. @i: (with ds: x : A
. . . . |    init: x : c
. . . . |   action a:T
. . . . |    precondition a(v) is
. . . . |    λs,v. P(s(x),v))
. . . . |   ∈ Dsys
. . . . 12. ∀D:Dsys.
. . . . |   @i: (with ds: x : A
. . . . |    init: x : c
. . . . |   action a:T
. . . . |    precondition a(v) is
. . . . |    λs,v. P(s(x),v)) ⊆ D
. . . . |   ⇒
. . . . |   D
. . . . |   realizes es.(∃v:T.
. . . . |                 (λs,v. P(s(x),v))((λx@0.x : c(x@0)?•),v))
. . . . |               ⇒
. . . . |               (∃e:E. loc(e) = i)
. . . . 13. D : Dsys
. . . . 14. @i: (with ds: x : A
. . . . |    init: x : c
```

```
. . . . |   action a:T
. . . . |    precondition a(v) is
. . . . |    λs,v. P(s(x),v)) ⊆ D
. . . . 15. D
. . . . |   realizes es.(vartype(i;x) ⊆r A)
. . . . |               & (∀e:E.
. . . . |                  loc(e) = i ⇒ first(e) ⇒ (x when e) = c)
. . . . 16. D
. . . . |   realizes es.(vartype(i;x) ⊆r A)
. . . . |               & (∀e:E.
. . . . |                  loc(e) = i
. . . . |                  ⇒
. . . . |                  kind(e) = locl(a) ⇒ (valtype(e) ⊆r T))
. . . . |               & (∀e:E.
. . . . |                  loc(e) = i
. . . . |                  ⇒
. . . . |                  (kind(e) = locl(a) ⇒ P((x when e),val(e)))
. . . . |                  & (∃e':E.
. . . . |                     (e <loc e') ∨ e = e'
. . . . |                     & kind(e') = locl(a)
. . . . |                       ∨ (∀v:T. ¬P((x after e'),v))))
. . . . 17. D
. . . . |   realizes es.(∃v:T.
. . . . |                (λs,v. P(s(x),v))((λx@0.x : c(x@0)?•),v))
. . . . |               ⇒
. . . . |               (∃e:E. loc(e) = i)
. . . . ⊢  D
. . . . |  realizes es.(vartype(i;x) ⊆r A)
. . . . |              & (∀e:E.
. . . . |                 loc(e) = i ⇒ first(e) ⇒ (x when e) = c)
. . . . |              & (∀e:E.
. . . . |                 loc(e) = i
. . . . |                 ⇒
. . . . |                 kind(e) = locl(a) ⇒ (valtype(e) ⊆r T))
. . . . |              & (∀e:E.
. . . . |                 loc(e) = i
. . . . |                 ⇒
. . . . |                 kind(e) = locl(a) ⇒ P((x when e),val(e)))
. . . . |               & ((∃v:T. P(c,v))
. . . . |                  ⇒
. . . . |                  (∃e:E.
. . . . |                   loc(e) = i
. . . . |                   & kind(e) = locl(a)
. . . . |                     ∨ (∀v:T. ¬P((x after e),v))))
. . . . | by All (Unfold `d-realizes`)
. . . . |
. . . . 1. i : Id
. . . . 2. a : Id
. . . . 3. x : Id
. . . . 4. A : Type
. . . . 5. T : Type
. . . . 6. c : A
. . . . 7. P : A→T→Prop
. . . . 8. (λs,v. P(s(x),v)) ∈ State(x : A)→T→Prop
. . . . 9. ∀x@0:Id. x@0 ∈ dom(x : A) ⇒ x@0 ∈ dom(x : c)
```

```
. . . . 10. x : c ∈ x@0:Id fp-> x : A(x@0)?Void
. . . . 11. @i: (with ds: x : A
. . . . |    init: x : c
. . . . |   action a:T
. . . . |    precondition a(v) is
. . . . |    λs,v. P(s(x),v))
. . . . |   ∈ Dsys
. . . . 12. ∀D:Dsys.
. . . . |   @i: (with ds: x : A
. . . . |    init: x : c
. . . . |   action a:T
. . . . |    precondition a(v) is
. . . . |    λs,v. P(s(x),v)) ⊆ D
. . . . |   ⇒
. . . . |   (∀D':Dsys.
. . . . |    D ⊆ D'
. . . . |    ⇒
. . . . |    (∀w:World, p:FairFifo.
. . . . |     PossibleWorld(D';w)
. . . . |     ⇒
. . . . |     (∃v:T. (λs,v. P(s(x),v))((λx@0.x : c(x@0)?•),v))
. . . . |     ⇒
. . . . |     (∃e:E. loc(e) = i)))
. . . . 13. D : Dsys
. . . . 14. @i: (with ds: x : A
. . . . |    init: x : c
. . . . |   action a:T
. . . . |    precondition a(v) is
. . . . |    λs,v. P(s(x),v)) ⊆ D
. . . . 15. ∀D':Dsys.
. . . . |   D ⊆ D'
. . . . |   ⇒
. . . . |   (∀w:World, p:FairFifo.
. . . . |    PossibleWorld(D';w)
. . . . |    ⇒
. . . . |    (vartype(i;x) ⊆r A)
. . . . |    & (∀e:E. loc(e) = i ⇒ first(e) ⇒ (x when e) = c))
. . . . 16. ∀D':Dsys.
. . . . |   D ⊆ D'
. . . . |   ⇒
. . . . |   (∀w:World, p:FairFifo.
. . . . |    PossibleWorld(D';w)
. . . . |    ⇒
. . . . |    (vartype(i;x) ⊆r A)
. . . . |    & (∀e:E.
. . . . |       loc(e) = i ⇒ kind(e) = locl(a) ⇒ (valtype(e) ⊆r T))
. . . . |    & (∀e:E.
. . . . |       loc(e) = i
. . . . |       ⇒
. . . . |       (kind(e) = locl(a) ⇒ P((x when e),val(e)))
. . . . |       & (∃e':E.
. . . . |          (e <loc e') ∨ e = e'
. . . . |          & kind(e') = locl(a)
. . . . |            ∨ (∀v:T. ¬P((x after e'),v)))))
. . . . 17. ∀D':Dsys.
```

```
. . . . |   D ⊆ D'
. . . . |   ⇒
. . . . |   (∀w:World, p:FairFifo.
. . . . |    PossibleWorld(D';w)
. . . . |    ⇒
. . . . |    (∃v:T. (λs,v. P(s(x),v))((λx@0.x : c(x@0)?•),v))
. . . . |    ⇒
. . . . |    (∃e:E. loc(e) = i))
. . . . ⊢  ∀D':Dsys.
. . . . |  D ⊆ D'
. . . . |  ⇒
. . . . |  (∀w:World, p:FairFifo.
. . . . |   PossibleWorld(D';w)
. . . . |   ⇒
. . . . |   (vartype(i;x) ⊆r A)
. . . . |   & (∀e:E. loc(e) = i ⇒ first(e) ⇒ (x when e) = c)
. . . . |   & (∀e:E.
. . . . |      loc(e) = i ⇒ kind(e) = locl(a) ⇒ (valtype(e) ⊆r T))
. . . . |   & (∀e:E.
. . . . |      loc(e) = i
. . . . |      ⇒
. . . . |      kind(e) = locl(a) ⇒ P((x when e),val(e)))
. . . . |     & ((∃v:T. P(c,v))
. . . . |        ⇒
. . . . |        (∃e:E.
. . . . |         loc(e) = i
. . . . |         & kind(e) = locl(a) ∨ (∀v:T. ¬P((x after e),v)))))
. . . . | by RepeatFor 6 (Analyze 0)
. . . . |    THEN
. . . . |    AllHyps
. . . . |    (λh.InstHyp [D';w;p] h THENA Complete (Reduce 0))
. . . . |
. . . . |\
. . . . | 1. i : Id
. . . . | 2. a : Id
. . . . | 3. x : Id
. . . . | 4. A : Type
. . . . | 5. T : Type
. . . . | 6. c : A
. . . . | 7. P : A→T→Prop
. . . . | 8. (λs,v. P(s(x),v)) ∈ State(x : A)→T→Prop
. . . . | 9. ∀x@0:Id. x@0 ∈ dom(x : A) ⇒ x@0 ∈ dom(x : c)
. . . . | 10. x : c ∈ x@0:Id fp-> x : A(x@0)?Void
. . . . | 11. @i: (with ds: x : A
. . . . |      init: x : c
. . . . |     action a:T
. . . . |      precondition a(v) is
. . . . |      λs,v. P(s(x),v))
. . . . |     ∈ Dsys
. . . . | 12. ∀D:Dsys.
. . . . |     @i: (with ds: x : A
. . . . |      init: x : c
. . . . |     action a:T
. . . . |      precondition a(v) is
. . . . |      λs,v. P(s(x),v)) ⊆ D
```

```
. . . . |     ⇒
. . . . |     (∀D':Dsys.
. . . . |      D ⊆ D'
. . . . |      ⇒
. . . . |      (∀w:World, p:FairFifo.
. . . . |       PossibleWorld(D';w)
. . . . |       ⇒
. . . . |       (∃v:T. (λs,v. P(s(x),v))((λx@0.x : c(x@0)?·),v))
. . . . |       ⇒
. . . . |       (∃e:E. loc(e) = i)))
. . . . | 13. D : Dsys
. . . . | 14. @i: (with ds: x : A
. . . . |      init: x : c
. . . . |     action a:T
. . . . |      precondition a(v) is
. . . . |      λs,v. P(s(x),v)) ⊆ D
. . . . | 15. ∀D':Dsys.
. . . . |     D ⊆ D'
. . . . |     ⇒
. . . . |     (∀w:World, p:FairFifo.
. . . . |      PossibleWorld(D';w)
. . . . |      ⇒
. . . . |      (vartype(i;x) ⊆r A)
. . . . |      & (∀e:E. loc(e) = i ⇒ first(e) ⇒ (x when e) = c))
. . . . | 16. ∀D':Dsys.
. . . . |     D ⊆ D'
. . . . |     ⇒
. . . . |     (∀w:World, p:FairFifo.
. . . . |      PossibleWorld(D';w)
. . . . |      ⇒
. . . . |      (vartype(i;x) ⊆r A)
. . . . |      & (∀e:E.
. . . . |         loc(e) = i
. . . . |         ⇒
. . . . |         kind(e) = locl(a) ⇒ (valtype(e) ⊆r T))
. . . . |      & (∀e:E.
. . . . |         loc(e) = i
. . . . |         ⇒
. . . . |         (kind(e) = locl(a) ⇒ P((x when e),val(e)))
. . . . |         & (∃e':E.
. . . . |            (e <loc e') ∨ e = e'
. . . . |            & kind(e') = locl(a)
. . . . |              ∨ (∀v:T. ¬P((x after e'),v)))))
. . . . | 17. ∀D':Dsys.
. . . . |     D ⊆ D'
. . . . |     ⇒
. . . . |     (∀w:World, p:FairFifo.
. . . . |      PossibleWorld(D';w)
. . . . |      ⇒
. . . . |      (∃v:T. (λs,v. P(s(x),v))((λx@0.x : c(x@0)?·),v))
. . . . |      ⇒
. . . . |      (∃e:E. loc(e) = i))
. . . . | 18. D' : Dsys
. . . . | 19. D ⊆ D'
. . . . | 20. w : World
```

```
. . . . | 21. p : FairFifo
. . . . | 22. PossibleWorld(D';w)

. . . . | 23. (vartype(i;x) ⊆r A)
. . . . |     & (∀e:E.
. . . . |        loc(e) = i ⇒ kind(e) = locl(a) ⇒ (valtype(e) ⊆r T))
. . . . |     & (∀e:E.
. . . . |        loc(e) = i
. . . . |        ⇒
. . . . |        (kind(e) = locl(a) ⇒ P((x when e),val(e)))
. . . . |        & (∃e':E.
. . . . |           (e <loc e') ∨ e = e'
. . . . |           & kind(e') = locl(a)
. . . . |             ∨ (∀v:T. ¬P((x after e'),v))))
. . . . | 24. (vartype(i;x) ⊆r A)
. . . . |     & (∀e:E. loc(e) = i ⇒ first(e) ⇒ (x when e) = c)
. . . . | ⊢  (vartype(i;x) ⊆r A)
. . . . |    & (∀e:E. loc(e) = i ⇒ first(e) ⇒ (x when e) = c)
. . . . |    & (∀e:E.
. . . . |       loc(e) = i ⇒ kind(e) = locl(a) ⇒ (valtype(e) ⊆r T))
. . . . |   by All Reduce THEN SplitAndHyps THEN BetterSplitAndConcl
. . . . |      THEN
. . . . |      Try Trivial
. . . . |
. . . . .\
. . . . . 1. i : Id
. . . . . 2. a : Id
. . . . . 3. x : Id
. . . . . 4. A : Type
. . . . . 5. T : Type
. . . . . 6. c : A
. . . . . 7. P : A→T→Prop
. . . . . 8. (λs,v. P(s(x),v)) ∈ State(x : A)→T→Prop
. . . . . 9. ∀x@0:Id. x@0 ∈ dom(x : A) ⇒ x@0 ∈ dom(x : c)
. . . . . 10. x : c ∈ x@0:Id fp-> x : A(x@0)?Void
. . . . . 11. @i: (with ds: x : A
. . . . . |    init: x : c
. . . . . |   action a:T
. . . . . |    precondition a(v) is
. . . . . |    λs,v. P(s(x),v))
. . . . . |   ∈ Dsys
. . . . . 12. ∀D:Dsys.
. . . . . |   @i: (with ds: x : A
. . . . . |    init: x : c
. . . . . |   action a:T
. . . . . |    precondition a(v) is
. . . . . |    λs,v. P(s(x),v)) ⊆ D
. . . . . |   ⇒
. . . . . |   (∀D':Dsys.
. . . . . |    D ⊆ D'
. . . . . |    ⇒
. . . . . |    (∀w:World, p:FairFifo.
. . . . . |     PossibleWorld(D';w)
. . . . . |     ⇒
. . . . . |     (∃v:T. (λs,v. P(s(x),v))((λx@0.x : c(x@0)?•),v))
. . . . . |     ⇒
```

```
. . . . . |     (∃e:E. loc(e) = i)))
. . . . . 13. D : Dsys
. . . . . 14. @i: (with ds: x : A
. . . . . |    init: x : c
. . . . . |   action a:T
. . . . . |    precondition a(v) is
. . . . . |    λs,v. P(s(x),v)) ⊆ D
. . . . . 15. ∀D':Dsys.
. . . . . |   D ⊆ D'
. . . . . |   ⇒
. . . . . |   (∀w:World, p:FairFifo.
. . . . . |    PossibleWorld(D';w)
. . . . . |    ⇒
. . . . . |    (vartype(i;x) ⊆r A)
. . . . . |    & (∀e:E. loc(e) = i ⇒ first(e) ⇒ (x when e) = c))
. . . . . 16. ∀D':Dsys.
. . . . . |   D ⊆ D'
. . . . . |   ⇒
. . . . . |   (∀w:World, p:FairFifo.
. . . . . |    PossibleWorld(D';w)
. . . . . |    ⇒
. . . . . |    (vartype(i;x) ⊆r A)
. . . . . |    & (∀e:E.
. . . . . |       loc(e) = i
. . . . . |       ⇒
. . . . . |       kind(e) = locl(a) ⇒ (valtype(e) ⊆r T))
. . . . . |    & (∀e:E.
. . . . . |       loc(e) = i
. . . . . |       ⇒
. . . . . |       (kind(e) = locl(a) ⇒ P((x when e),val(e)))
. . . . . |       & (∃e':E.
. . . . . |          (e <loc e') ∨ e = e'
. . . . . |          & kind(e') = locl(a)
. . . . . |            ∨ (∀v:T. ¬P((x after e'),v)))))
. . . . . 17. ∀D':Dsys.
. . . . . |   D ⊆ D'
. . . . . |   ⇒
. . . . . |   (∀w:World, p:FairFifo.
. . . . . |    PossibleWorld(D';w)
. . . . . |    ⇒
. . . . . |    (∃v:T. (λs,v. P(s(x),v))((λx@0.x : c(x@0)?·),v))
. . . . . |    ⇒
. . . . . |    (∃e:E. loc(e) = i))
. . . . . 18. D' : Dsys
. . . . . 19. D ⊆ D'
. . . . . 20. w : World
. . . . . 21. p : FairFifo

. . . . . 22. PossibleWorld(D';w)
. . . . . 23. (vartype(i;x) ⊆r A)
. . . . . |   & (∀e:E. loc(e) = i ⇒ first(e) ⇒ (x when e) = c)
. . . . . |   & (∀e:E.
. . . . . |      loc(e) = i ⇒ kind(e) = locl(a) ⇒ (valtype(e) ⊆r T))
. . . . . 24. (vartype(i;x) ⊆r A)
. . . . . |   & (∀e:E. loc(e) = i ⇒ first(e) ⇒ (x when e) = c)
. . . . . |   & (∀e:E.
```

```
. . . . . |      loc(e) = i ⇒ kind(e) = locl(a) ⇒ (valtype(e) ⊆r T))
. . . . . 25. (vartype(i;x) ⊆r A)
. . . . . |   & (∀e:E.
. . . . . |      loc(e) = i ⇒ kind(e) = locl(a) ⇒ (valtype(e) ⊆r T))
. . . . . |   & (∀e:E.
. . . . . |      loc(e) = i
. . . . . |      ⇒
. . . . . |      (kind(e) = locl(a) ⇒ P((x when e),val(e)))
. . . . . |      & (∃e':E.
. . . . . |         (e <loc e') ∨ e = e'
. . . . . |         & kind(e') = locl(a)
. . . . . |           ∨ (∀v:T. ¬P((x after e'),v))))
. . . . . 26. (vartype(i;x) ⊆r A)
. . . . . |   & (∀e:E. loc(e) = i ⇒ first(e) ⇒ (x when e) = c)
. . . . . ⊢  (∀e:E.
. . . . . |   loc(e) = i ⇒ kind(e) = locl(a) ⇒ P((x when e),val(e)))
. . . . . |  & ((∃v:T. P(c,v))
. . . . . |     ⇒
. . . . . |     (∃e:E.
. . . . . |      loc(e) = i
. . . . . |      & kind(e) = locl(a) ∨ (∀v:T. ¬P((x after e),v))))
. . . . . | by All Reduce THEN SplitAndHyps THEN BetterSplitAndConcl
. . . . . |    THEN
. . . . . |    Try Trivial
. . . . . |
. . . . . |\
. . . . . | 1. i : Id
. . . . . | 2. a : Id
. . . . . | 3. x : Id
. . . . . | 4. A : Type
. . . . . | 5. T : Type
. . . . . | 6. c : A
. . . . . | 7. P : A→T→Prop
. . . . . | 8. (λs,v. P(s(x),v)) ∈ State(x : A)→T→Prop
. . . . . | 9. ∀x@0:Id. x@0 ∈ dom(x : A) ⇒ x@0 ∈ dom(x : c)
. . . . . | 10. x : c ∈ x@0:Id fp-> x : A(x@0)?Void
. . . . . | 11. @i: (with ds: x : A
. . . . . |      init: x : c
. . . . . |     action a:T
. . . . . |      precondition a(v) is
. . . . . |      λs,v. P(s(x),v))
. . . . . |     ∈ Dsys
. . . . . | 12. ∀D:Dsys.
. . . . . |     @i: (with ds: x : A
. . . . . |      init: x : c
. . . . . |     action a:T
. . . . . |      precondition a(v) is
. . . . . |      λs,v. P(s(x),v)) ⊆ D
. . . . . |     ⇒
. . . . . |     (∀D':Dsys.
. . . . . |      D ⊆ D'
. . . . . |      ⇒
. . . . . |      (∀w:World, p:FairFifo.
. . . . . |       PossibleWorld(D';w)
. . . . . |       ⇒
```

```
. . . . . |       (∃v:T. P(c,v)) ⇒ (∃e:E. loc(e) = i)))
. . . . . | 13. D : Dsys
. . . . . | 14. @i: (with ds: x : A
. . . . . |      init: x : c
. . . . . |     action a:T
. . . . . |      precondition a(v) is
. . . . . |      λs,v. P(s(x),v)) ⊆ D
. . . . . | 15. ∀D':Dsys.
. . . . . |     D ⊆ D'
. . . . . |     ⇒
. . . . . |     (∀w:World, p:FairFifo.
. . . . . |      PossibleWorld(D';w)
. . . . . |      ⇒
. . . . . |      (vartype(i;x) ⊆r A)
. . . . . |      & (∀e:E. loc(e) = i ⇒ first(e) ⇒ (x when e) = c))
. . . . . | 16. ∀D':Dsys.
. . . . . |     D ⊆ D'
. . . . . |     ⇒
. . . . . |     (∀w:World, p:FairFifo.
. . . . . |      PossibleWorld(D';w)
. . . . . |      ⇒
. . . . . |      (vartype(i;x) ⊆r A)
. . . . . |      & (∀e:E.
. . . . . |         loc(e) = i
. . . . . |         ⇒
. . . . . |         kind(e) = locl(a) ⇒ (valtype(e) ⊆r T))
. . . . . |      & (∀e:E.
. . . . . |         loc(e) = i
. . . . . |         ⇒
. . . . . |         (kind(e) = locl(a) ⇒ P((x when e),val(e)))
. . . . . |         & (∃e':E.
. . . . . |            (e <loc e') ∨ e = e'
. . . . . |            & kind(e') = locl(a)
. . . . . |              ∨ (∀v:T. ¬P((x after e'),v)))))
. . . . . | 17. ∀D':Dsys.
. . . . . |     D ⊆ D'
. . . . . |     ⇒
. . . . . |     (∀w:World, p:FairFifo.
. . . . . |      PossibleWorld(D';w)
. . . . . |      ⇒
. . . . . |      (∃v:T. P(c,v)) ⇒ (∃e:E. loc(e) = i))
. . . . . | 18. D' : Dsys
. . . . . | 19. D ⊆ D'
. . . . . | 20. w : World
. . . . . | 21. p : FairFifo
. . . . . | 22. PossibleWorld(D';w)
. . . . . | 23. vartype(i;x) ⊆r A
. . . . . | 24. ∀e:E. loc(e) = i ⇒ first(e) ⇒ (x when e) = c
. . . . . | 25. ∀e:E.
. . . . . |     loc(e) = i ⇒ kind(e) = locl(a) ⇒ (valtype(e) ⊆r T)
. . . . . | 26. vartype(i;x) ⊆r A
. . . . . | 27. ∀e:E. loc(e) = i ⇒ first(e) ⇒ (x when e) = c
. . . . . | 28. ∀e:E.
. . . . . |     loc(e) = i ⇒ kind(e) = locl(a) ⇒ (valtype(e) ⊆r T)
. . . . . | 29. vartype(i;x) ⊆r A
```

```
. . . . . | 30. ∀e:E.
. . . . . |     loc(e) = i ⇒ kind(e) = locl(a) ⇒ (valtype(e) ⊆r T)
. . . . . | 31. ∀e:E.
. . . . . |     loc(e) = i
. . . . . |     ⇒
. . . . . |     (kind(e) = locl(a) ⇒ P((x when e),val(e)))
. . . . . |     & (∃e':E.
. . . . . |        (e <loc e') ∨ e = e'
. . . . . |        & kind(e') = locl(a) ∨ (∀v:T. ¬P((x after e'),v)))
. . . . . | 32. vartype(i;x) ⊆r A
. . . . . | 33. ∀e:E. loc(e) = i ⇒ first(e) ⇒ (x when e) = c
. . . . . | ⊢  ∀e:E.
. . . . . |    loc(e) = i ⇒ kind(e) = locl(a) ⇒ P((x when e),val(e))
. . . . . |   by ParallelOp -3 THEN ParallelLast
. . . . . |
. . . . . .\
. . . . . . 1. i : Id
. . . . . . 2. a : Id
. . . . . . 3. x : Id
. . . . . . 4. A : Type
. . . . . . 5. T : Type
. . . . . . 6. c : A
. . . . . . 7. P : A→T→Prop
. . . . . . 8. (λs,v. P(s(x),v)) ∈ State(x : A)→T→Prop
. . . . . . 9. ∀x@0:Id. x@0 ∈ dom(x : A) ⇒ x@0 ∈ dom(x : c)
. . . . . . 10. x : c ∈ x@0:Id fp-> x : A(x@0)?Void
. . . . . . 11. @i: (with ds: x : A
. . . . . . |    init: x : c
. . . . . . |   action a:T
. . . . . . |    precondition a(v) is
. . . . . . |    λs,v. P(s(x),v))
. . . . . . |   ∈ Dsys
. . . . . . 12. ∀D:Dsys.
. . . . . . |   @i: (with ds: x : A
. . . . . . |    init: x : c
. . . . . . |   action a:T
. . . . . . |    precondition a(v) is
. . . . . . |    λs,v. P(s(x),v)) ⊆ D
. . . . . . |   ⇒
. . . . . . |   (∀D':Dsys.
. . . . . . |    D ⊆ D'
. . . . . . |    ⇒
. . . . . . |    (∀w:World, p:FairFifo.
. . . . . . |     PossibleWorld(D';w)
. . . . . . |     ⇒
. . . . . . |     (∃v:T. P(c,v)) ⇒ (∃e:E. loc(e) = i)))
. . . . . . 13. D : Dsys
. . . . . . 14. @i: (with ds: x : A
. . . . . . |    init: x : c
. . . . . . |   action a:T
. . . . . . |    precondition a(v) is
. . . . . . |    λs,v. P(s(x),v)) ⊆ D
. . . . . . 15. ∀D':Dsys.
. . . . . . |   D ⊆ D'
. . . . . . |   ⇒
```

```
. . . . . |   (∀w:World, p:FairFifo.
. . . . . |    PossibleWorld(D';w)
. . . . . |    ⇒
. . . . . |    (vartype(i;x) ⊆r A)
. . . . . |    & (∀e:E. loc(e) = i ⇒ first(e) ⇒ (x when e) = c))
. . . . . 16. ∀D':Dsys.
. . . . . |   D ⊆ D'
. . . . . |   ⇒
. . . . . |   (∀w:World, p:FairFifo.
. . . . . |    PossibleWorld(D';w)
. . . . . |    ⇒
. . . . . |    (vartype(i;x) ⊆r A)
. . . . . |    & (∀e:E.
. . . . . |       loc(e) = i
. . . . . |       ⇒
. . . . . |       kind(e) = locl(a) ⇒ (valtype(e) ⊆r T))
. . . . . |    & (∀e:E.
. . . . . |       loc(e) = i
. . . . . |       ⇒
. . . . . |       (kind(e) = locl(a) ⇒ P((x when e),val(e)))
. . . . . |       & (∃e':E.
. . . . . |          (e <loc e') ∨ e = e'
. . . . . |          & kind(e') = locl(a)
. . . . . |            ∨ (∀v:T. ¬P((x after e'),v)))))
. . . . . 17. ∀D':Dsys.
. . . . . |   D ⊆ D'
. . . . . |   ⇒
. . . . . |   (∀w:World, p:FairFifo.
. . . . . |    PossibleWorld(D';w)
. . . . . |    ⇒
. . . . . |    (∃v:T. P(c,v)) ⇒ (∃e:E. loc(e) = i))
. . . . . 18. D' : Dsys
. . . . . 19. D ⊆ D'
. . . . . 20. w : World
. . . . . 21. p : FairFifo
. . . . . 22. PossibleWorld(D';w)
. . . . . 23. vartype(i;x) ⊆r A
. . . . . 24. ∀e:E. loc(e) = i ⇒ first(e) ⇒ (x when e) = c
. . . . . 25. ∀e:E.
. . . . . |   loc(e) = i ⇒ kind(e) = locl(a) ⇒ (valtype(e) ⊆r T)
. . . . . 26. vartype(i;x) ⊆r A
. . . . . 27. ∀e:E. loc(e) = i ⇒ first(e) ⇒ (x when e) = c
. . . . . 28. ∀e:E.
. . . . . |   loc(e) = i ⇒ kind(e) = locl(a) ⇒ (valtype(e) ⊆r T)
. . . . . 29. vartype(i;x) ⊆r A
. . . . . 30. ∀e:E.
. . . . . |   loc(e) = i ⇒ kind(e) = locl(a) ⇒ (valtype(e) ⊆r T)
. . . . . 31. ∀e:E.
. . . . . |   loc(e) = i
. . . . . |   ⇒
. . . . . |   (kind(e) = locl(a) ⇒ P((x when e),val(e)))
. . . . . |   & (∃e':E.
. . . . . |      (e <loc e') ∨ e = e'
. . . . . |      & kind(e') = locl(a) ∨ (∀v:T. ¬P((x after e'),v)))
. . . . . 32. vartype(i;x) ⊆r A
```

```
. . . . . 33. ∀e:E. loc(e) = i ⇒ first(e) ⇒ (x when e) = c
. . . . . 34. ∀e:E.
. . . . . |   loc(e) = i
. . . . . |   ⇒
. . . . . |   kind(e) = locl(a) ⇒ P((x when e),val(e))
. . . . . ⊢  (∃v:T. P(c,v))
. . . . . |  ⇒
. . . . . |  (∃e:E.
. . . . . |   loc(e) = i
. . . . . |   & kind(e) = locl(a) ∨ (∀v:T. ¬P((x after e),v)))
. . . . . | by Auto
. . . . . |
. . . . . 1. i : Id
. . . . . 2. a : Id
. . . . . 3. x : Id
. . . . . 4. A : Type
. . . . . 5. T : Type
. . . . . 6. c : A
. . . . . 7. P : A→T→Prop
. . . . . 8. (λs,v. P(s(x),v)) ∈ State(x : A)→T→Prop
. . . . . 9. ∀x@0:Id. x@0 ∈ dom(x : A) ⇒ x@0 ∈ dom(x : c)
. . . . . 10. x : c ∈ x@0:Id fp-> x : A(x@0)?Void
. . . . . 11. @i: (with ds: x : A
. . . . . |    init: x : c
. . . . . |   action a:T
. . . . . |    precondition a(v) is
. . . . . |    λs,v. P(s(x),v))
. . . . . |   ∈ Dsys
. . . . . 12. ∀D:Dsys.
. . . . . |   @i: (with ds: x : A
. . . . . |    init: x : c
. . . . . |   action a:T
. . . . . |    precondition a(v) is
. . . . . |    λs,v. P(s(x),v)) ⊆ D
. . . . . |   ⇒
. . . . . |   (∀D':Dsys.
. . . . . |    D ⊆ D'
. . . . . |    ⇒
. . . . . |    (∀w:World, p:FairFifo.
. . . . . |     PossibleWorld(D';w)
. . . . . |     ⇒
. . . . . |     (∃v:T. P(c,v)) ⇒ (∃e:E. loc(e) = i)))
. . . . . 13. D : Dsys
. . . . . 14. @i: (with ds: x : A
. . . . . |    init: x : c
. . . . . |   action a:T
. . . . . |    precondition a(v) is
. . . . . |    λs,v. P(s(x),v)) ⊆ D
. . . . . 15. ∀D':Dsys.
. . . . . |   D ⊆ D'
. . . . . |   ⇒
. . . . . |   (∀w:World, p:FairFifo.
. . . . . |    PossibleWorld(D';w)
. . . . . |    ⇒
. . . . . |    (vartype(i;x) ⊆r A)
```

```
. . . . . |    & (∀e:E. loc(e) = i ⇒ first(e) ⇒ (x when e) = c))
. . . . . 16. ∀D':Dsys.
. . . . . |   D ⊆ D'
. . . . . |   ⇒
. . . . . |   (∀w:World, p:FairFifo.
. . . . . |    PossibleWorld(D';w)
. . . . . |    ⇒
. . . . . |    (vartype(i;x) ⊆r A)
. . . . . |    & (∀e:E.
. . . . . |       loc(e) = i
. . . . . |       ⇒
. . . . . |       kind(e) = locl(a) ⇒ (valtype(e) ⊆r T))
. . . . . |    & (∀e:E.
. . . . . |       loc(e) = i
. . . . . |       ⇒
. . . . . |       (kind(e) = locl(a) ⇒ P((x when e),val(e)))
. . . . . |       & (∃e':E.
. . . . . |          (e <loc e') ∨ e = e'
. . . . . |          & kind(e') = locl(a)
. . . . . |            ∨ (∀v:T. ¬P((x after e'),v)))))
. . . . . 17. ∀D':Dsys.
. . . . . |   D ⊆ D'
. . . . . |   ⇒
. . . . . |   (∀w:World, p:FairFifo.
. . . . . |    PossibleWorld(D';w)
. . . . . |    ⇒
. . . . . |    (∃v:T. P(c,v)) ⇒ (∃e:E. loc(e) = i))
. . . . . 18. D' : Dsys
. . . . . 19. D ⊆ D'
. . . . . 20. w : World
. . . . . 21. p : FairFifo
. . . . . 22. PossibleWorld(D';w)
. . . . . 23. vartype(i;x) ⊆r A
. . . . . 24. ∀e:E. loc(e) = i ⇒ first(e) ⇒ (x when e) = c
. . . . . 25. ∀e:E.
. . . . . |   loc(e) = i ⇒ kind(e) = locl(a) ⇒ (valtype(e) ⊆r T)
. . . . . 26. vartype(i;x) ⊆r A
. . . . . 27. ∀e:E. loc(e) = i ⇒ first(e) ⇒ (x when e) = c
. . . . . 28. ∀e:E.
. . . . . |   loc(e) = i ⇒ kind(e) = locl(a) ⇒ (valtype(e) ⊆r T)
. . . . . 29. vartype(i;x) ⊆r A
. . . . . 30. ∀e:E.
. . . . . |   loc(e) = i ⇒ kind(e) = locl(a) ⇒ (valtype(e) ⊆r T)
. . . . . 31. ∀e:E.
. . . . . |   loc(e) = i
. . . . . |   ⇒
. . . . . |   (kind(e) = locl(a) ⇒ P((x when e),val(e)))
. . . . . |   & (∃e':E.
. . . . . |      (e <loc e') ∨ e = e'
. . . . . |      & kind(e') = locl(a) ∨ (∀v:T. ¬P((x after e'),v)))
. . . . . 32. vartype(i;x) ⊆r A
. . . . . 33. ∀e:E. loc(e) = i ⇒ first(e) ⇒ (x when e) = c
. . . . . 34. ∀e:E.
. . . . . |   loc(e) = i
. . . . . |   ⇒
```

```
. . . . . |   kind(e) = locl(a) ⇒ P((x when e),val(e))
. . . . . 35. ∃v:T. P(c,v)
. . . . . ⊢  ∃e:E.
. . . . . |  loc(e) = i
. . . . . |  & kind(e) = locl(a) ∨ (∀v:T. ¬P((x after e),v))
. . . . . | by AllHyps
. . . . . |    (λh.InstHyp [D';w;p] h THENA Complete (Reduce 0))
. . . . . |    THEN
. . . . . |    ExRepD
. . . . . |    THEN
. . . . . |    InstHyp [e] -3
. . . . . |    THEN
. . . . . |    ParallelLast
. . . . . |    THEN
. . . . . |    ExRepD
. . . . . |
. . . . . |\
. . . . . | 1. i : Id
. . . . . | 2. a : Id
. . . . . | 3. x : Id
. . . . . | 4. A : Type
. . . . . | 5. T : Type
. . . . . | 6. c : A
. . . . . | 7. P : A→T→Prop
. . . . . | 8. (λs,v. P(s(x),v)) ∈ State(x : A)→T→Prop
. . . . . | 9. ∀x@0:Id. x@0 ∈ dom(x : A) ⇒ x@0 ∈ dom(x : c)
. . . . . | 10. x : c ∈ x@0:Id fp-> x : A(x@0)?Void
. . . . . | 11. @i: (with ds: x : A
. . . . . |      init: x : c
. . . . . |     action a:T
. . . . . |      precondition a(v) is
. . . . . |      λs,v. P(s(x),v))
. . . . . |     ∈ Dsys
. . . . . | 12. ∀D:Dsys.
. . . . . |     @i: (with ds: x : A
. . . . . |      init: x : c
. . . . . |     action a:T
. . . . . |      precondition a(v) is
. . . . . |      λs,v. P(s(x),v)) ⊆ D
. . . . . |     ⇒
. . . . . |     (∀D':Dsys.
. . . . . |      D ⊆ D'
. . . . . |      ⇒
. . . . . |      (∀w:World, p:FairFifo.
. . . . . |       PossibleWorld(D';w)
. . . . . |       ⇒
. . . . . |       (∃v:T. P(c,v)) ⇒ (∃e:E. loc(e) = i)))
. . . . . | 13. D : Dsys
. . . . . | 14. @i: (with ds: x : A
. . . . . |      init: x : c
. . . . . |     action a:T
. . . . . |      precondition a(v) is
. . . . . |      λs,v. P(s(x),v)) ⊆ D
. . . . . | 15. ∀D':Dsys.
. . . . . |     D ⊆ D'
```

```
. . . . . |     ⇒
. . . . . |     (∀w:World, p:FairFifo.
. . . . . |      PossibleWorld(D';w)
. . . . . |      ⇒
. . . . . |      (vartype(i;x) ⊆r A)
. . . . . |      & (∀e:E. loc(e) = i ⇒ first(e) ⇒ (x when e) = c))
. . . . . | 16. ∀D':Dsys.
. . . . . |     D ⊆ D'
. . . . . |     ⇒
. . . . . |     (∀w:World, p:FairFifo.
. . . . . |      PossibleWorld(D';w)
. . . . . |      ⇒
. . . . . |      (vartype(i;x) ⊆r A)
. . . . . |      & (∀e:E.
. . . . . |         loc(e) = i
. . . . . |         ⇒
. . . . . |         kind(e) = locl(a) ⇒ (valtype(e) ⊆r T))
. . . . . |      & (∀e:E.
. . . . . |         loc(e) = i
. . . . . |         ⇒
. . . . . |         (kind(e) = locl(a) ⇒ P((x when e),val(e)))
. . . . . |         & (∃e':E.
. . . . . |            (e <loc e') ∨ e = e'
. . . . . |            & kind(e') = locl(a)
. . . . . |              ∨ (∀v:T. ¬P((x after e'),v)))))
. . . . . | 17. ∀D':Dsys.
. . . . . |     D ⊆ D'
. . . . . |     ⇒
. . . . . |     (∀w:World, p:FairFifo.
. . . . . |      PossibleWorld(D';w)
. . . . . |      ⇒
. . . . . |      (∃v:T. P(c,v)) ⇒ (∃e:E. loc(e) = i))
. . . . . | 18. D' : Dsys
. . . . . | 19. D ⊆ D'
. . . . . | 20. w : World
. . . . . | 21. p : FairFifo
. . . . . | 22. PossibleWorld(D';w)
. . . . . | 23. vartype(i;x) ⊆r A
. . . . . | 24. ∀e:E. loc(e) = i ⇒ first(e) ⇒ (x when e) = c
. . . . . | 25. ∀e:E.
. . . . . |     loc(e) = i ⇒ kind(e) = locl(a) ⇒ (valtype(e) ⊆r T)
. . . . . | 26. vartype(i;x) ⊆r A
. . . . . | 27. ∀e:E. loc(e) = i ⇒ first(e) ⇒ (x when e) = c
. . . . . | 28. ∀e:E.
. . . . . |     loc(e) = i ⇒ kind(e) = locl(a) ⇒ (valtype(e) ⊆r T)
. . . . . | 29. vartype(i;x) ⊆r A
. . . . . | 30. ∀e:E.
. . . . . |     loc(e) = i ⇒ kind(e) = locl(a) ⇒ (valtype(e) ⊆r T)
. . . . . | 31. ∀e:E.
. . . . . |     loc(e) = i
. . . . . |     ⇒
. . . . . |     (kind(e) = locl(a) ⇒ P((x when e),val(e)))
. . . . . |     & (∃e':E.
. . . . . |        (e <loc e') ∨ e = e'
. . . . . |        & kind(e') = locl(a)
```

```
. . . . . | ∨ (∀v:T. ¬P((x after e'),v)))
. . . . . | 32. vartype(i;x) ⊆r A
. . . . . | 33. ∀e:E. loc(e) = i ⇒ first(e) ⇒ (x when e) = c
. . . . . | 34. ∀e:E.
. . . . . | loc(e) = i
. . . . . | ⇒
. . . . . | kind(e) = locl(a) ⇒ P((x when e),val(e))
. . . . . | 35. v : T
. . . . . | 36. P(c,v)
. . . . . | 37. e : E
. . . . . | 38. loc(e) = i
. . . . . | 39. vartype(i;x) ⊆r A
. . . . . | 40. ∀e:E.
. . . . . | loc(e) = i ⇒ kind(e) = locl(a) ⇒ (valtype(e) ⊆r T)
. . . . . | 41. ∀e:E.
. . . . . | loc(e) = i
. . . . . | ⇒
. . . . . | (kind(e) = locl(a) ⇒ P((x when e),val(e)))
. . . . . | & (∃e':E.
. . . . . | (e <loc e') ∨ e = e'
. . . . . | & kind(e') = locl(a)
. . . . . | ∨ (∀v:T. ¬P((x after e'),v)))
. . . . . | 42. vartype(i;x) ⊆r A
. . . . . | 43. ∀e:E. loc(e) = i ⇒ first(e) ⇒ (x when e) = c
. . . . . | 44. kind(e) = locl(a) ⇒ P((x when e),val(e))
. . . . . | 45. e' : E
. . . . . | 46. (e <loc e') ∨ e = e'
. . . . . | 47. kind(e') = locl(a) ∨ (∀v:T. ¬P((x after e'),v))
. . . . . | ⊢ loc(e') = i by UseLocInfo Auto
. . . . . |
. . . . . .\
. . . . . . 1. i : Id
. . . . . . 2. a : Id
. . . . . . 3. x : Id
. . . . . . 4. A : Type
. . . . . . 5. T : Type
. . . . . . 6. c : A
. . . . . . 7. P : A→T→Prop
. . . . . . 8. (λs,v. P(s(x),v)) ∈ State(x : A)→T→Prop
. . . . . . 9. ∀x@0:Id. x@0 ∈ dom(x : A) ⇒ x@0 ∈ dom(x : c)
. . . . . . 10. x : c ∈ x@0:Id fp-> x : A(x@0)?Void
. . . . . . 11. @i: (with ds: x : A
. . . . . . | init: x : c
. . . . . . | action a:T
. . . . . . | precondition a(v) is
. . . . . . | λs,v. P(s(x),v))
. . . . . . | ∈ Dsys
. . . . . . 12. ∀D:Dsys.
. . . . . . | @i: (with ds: x : A
. . . . . . | init: x : c
. . . . . . | action a:T
. . . . . . | precondition a(v) is
. . . . . . | λs,v. P(s(x),v)) ⊆ D
. . . . . . | ⇒
. . . . . . | (∀D':Dsys.
```

```
. . . . . |    D ⊆ D'
. . . . . |    ⇒
. . . . . |    (∀w:World, p:FairFifo.
. . . . . |     PossibleWorld(D';w)
. . . . . |     ⇒
. . . . . |     (∃v:T. P(c,v)) ⇒ (∃e:E. loc(e) = i)))
. . . . . 13. D : Dsys
. . . . . 14. @i: (with ds: x : A
. . . . . |    init: x : c
. . . . . |   action a:T
. . . . . |    precondition a(v) is
. . . . . |    λs,v. P(s(x),v)) ⊆ D
. . . . . 15. ∀D':Dsys.
. . . . . |   D ⊆ D'
. . . . . |   ⇒
. . . . . |   (∀w:World, p:FairFifo.
. . . . . |    PossibleWorld(D';w)
. . . . . |    ⇒
. . . . . |    (vartype(i;x) ⊆r A)
. . . . . |    & (∀e:E. loc(e) = i ⇒ first(e) ⇒ (x when e) = c))
. . . . . 16. ∀D':Dsys.
. . . . . |   D ⊆ D'
. . . . . |   ⇒
. . . . . |   (∀w:World, p:FairFifo.
. . . . . |    PossibleWorld(D';w)
. . . . . |    ⇒
. . . . . |    (vartype(i;x) ⊆r A)
. . . . . |    & (∀e:E.
. . . . . |       loc(e) = i
. . . . . |       ⇒
. . . . . |       kind(e) = locl(a) ⇒ (valtype(e) ⊆r T))
. . . . . |    & (∀e:E.
. . . . . |       loc(e) = i
. . . . . |       ⇒
. . . . . |       (kind(e) = locl(a) ⇒ P((x when e),val(e)))
. . . . . |       & (∃e':E.
. . . . . |          (e <loc e') ∨ e = e'
. . . . . |          & kind(e') = locl(a)
. . . . . |            ∨ (∀v:T. ¬P((x after e'),v)))))
. . . . . 17. ∀D':Dsys.
. . . . . |   D ⊆ D'
. . . . . |   ⇒
. . . . . |   (∀w:World, p:FairFifo.
. . . . . |    PossibleWorld(D';w)
. . . . . |    ⇒
. . . . . |    (∃v:T. P(c,v)) ⇒ (∃e:E. loc(e) = i))
. . . . . 18. D' : Dsys
. . . . . 19. D ⊆ D'
. . . . . 20. w : World
. . . . . 21. p : FairFifo
. . . . . 22. PossibleWorld(D';w)
. . . . . 23. vartype(i;x) ⊆r A
. . . . . 24. ∀e:E. loc(e) = i ⇒ first(e) ⇒ (x when e) = c
. . . . . 25. ∀e:E.
. . . . . |   loc(e) = i ⇒ kind(e) = locl(a) ⇒ (valtype(e) ⊆r T)
```

```
. . . . . 26. vartype(i;x) ⊆r A
. . . . . 27. ∀e:E. loc(e) = i ⇒ first(e) ⇒ (x when e) = c
. . . . . 28. ∀e:E.
. . . . . |   loc(e) = i ⇒ kind(e) = locl(a) ⇒ (valtype(e) ⊆r T)
. . . . . 29. vartype(i;x) ⊆r A
. . . . . 30. ∀e:E.
. . . . . |   loc(e) = i ⇒ kind(e) = locl(a) ⇒ (valtype(e) ⊆r T)
. . . . . 31. ∀e:E.
. . . . . |   loc(e) = i
. . . . . |   ⇒
. . . . . |   (kind(e) = locl(a) ⇒ P((x when e),val(e)))
. . . . . |   & (∃e':E.
. . . . . |      (e <loc e') ∨ e = e'
. . . . . |      & kind(e') = locl(a)
. . . . . |        ∨ (∀v:T. ¬P((x after e'),v)))
. . . . . 32. vartype(i;x) ⊆r A
. . . . . 33. ∀e:E. loc(e) = i ⇒ first(e) ⇒ (x when e) = c
. . . . . 34. ∀e:E.
. . . . . |   loc(e) = i
. . . . . |   ⇒
. . . . . |   kind(e) = locl(a) ⇒ P((x when e),val(e))
. . . . . 35. v : T
. . . . . 36. P(c,v)
. . . . . 37. e : E
. . . . . 38. loc(e) = i
. . . . . 39. vartype(i;x) ⊆r A
. . . . . 40. ∀e:E.
. . . . . |   loc(e) = i ⇒ kind(e) = locl(a) ⇒ (valtype(e) ⊆r T)
. . . . . 41. ∀e:E.
. . . . . |   loc(e) = i
. . . . . |   ⇒
. . . . . |   (kind(e) = locl(a) ⇒ P((x when e),val(e)))
. . . . . |   & (∃e':E.
. . . . . |      (e <loc e') ∨ e = e'
. . . . . |      & kind(e') = locl(a)
. . . . . |        ∨ (∀v:T. ¬P((x after e'),v)))
. . . . . 42. vartype(i;x) ⊆r A
. . . . . 43. ∀e:E. loc(e) = i ⇒ first(e) ⇒ (x when e) = c
. . . . . 44. kind(e) = locl(a) ⇒ P((x when e),val(e))
. . . . . 45. e' : E
. . . . . 46. (e <loc e') ∨ e = e'
. . . . . 47. kind(e') = locl(a) ∨ (∀v:T. ¬P((x after e'),v))

. . . . . 48. e1 : E
. . . . . 49. loc(e1) = i
. . . . . 50. T
. . . . . ⊢  (x after e1) ∈ A  by DoSubsume
. . . . . |
. . . . . .....subtype_rel .....
. . . . . 1. i : Id
. . . . . 2. a : Id
. . . . . 3. x : Id
. . . . . 4. A : Type
. . . . . 5. T : Type
. . . . . 6. c : A
. . . . . 7. P : A→T→Prop
```

```
. . . . . 8. (λs,v. P(s(x),v)) ∈ State(x : A)→T→Prop
. . . . . 9. ∀x@0:Id. x@0 ∈ dom(x : A) ⇒ x@0 ∈ dom(x : c)
. . . . . 10. x : c ∈ x@0:Id fp-> x : A(x@0)?Void
. . . . . 11. @i: (with ds: x : A
. . . . . init: x : c
. . . . . action a:T
. . . . . precondition a(v) is
. . . . . λs,v. P(s(x),v))
. . . . . ∈ Dsys
. . . . . 12. ∀D:Dsys.
. . . . . @i: (with ds: x : A
. . . . . init: x : c
. . . . . action a:T
. . . . . precondition a(v) is
. . . . . λs,v. P(s(x),v)) ⊆ D
. . . . . ⇒
. . . . . (∀D':Dsys.
. . . . . D ⊆ D'
. . . . . ⇒
. . . . . (∀w:World, p:FairFifo.
. . . . . PossibleWorld(D';w)
. . . . . ⇒
. . . . . (∃v:T. P(c,v)) ⇒ (∃e:E. loc(e) = i)))
. . . . . 13. D : Dsys
. . . . . 14. @i: (with ds: x : A
. . . . . init: x : c
. . . . . action a:T
. . . . . precondition a(v) is
. . . . . λs,v. P(s(x),v)) ⊆ D
. . . . . 15. ∀D':Dsys.
. . . . . D ⊆ D'
. . . . . ⇒
. . . . . (∀w:World, p:FairFifo.
. . . . . PossibleWorld(D';w)
. . . . . ⇒
. . . . . (vartype(i;x) ⊆r A)
. . . . . & (∀e:E. loc(e) = i ⇒ first(e) ⇒ (x when e) = c))
. . . . . 16. ∀D':Dsys.
. . . . . D ⊆ D'
. . . . . ⇒
. . . . . (∀w:World, p:FairFifo.
. . . . . PossibleWorld(D';w)
. . . . . ⇒
. . . . . (vartype(i;x) ⊆r A)
. . . . . & (∀e:E.
. . . . . loc(e) = i
. . . . . ⇒
. . . . . kind(e) = locl(a) ⇒ (valtype(e) ⊆r T))
. . . . . & (∀e:E.
. . . . . loc(e) = i
. . . . . ⇒
. . . . . (kind(e) = locl(a) ⇒ P((x when e),val(e)))
. . . . . & (∃e':E.
. . . . . (e <loc e') ∨ e = e'
. . . . . & kind(e') = locl(a)
```

```
. . . . . .                ∨ (∀v:T. ¬P((x after e'),v)))))
. . . . . . 17. ∀D':Dsys.
. . . . . .     D ⊆ D'
. . . . . .     ⇒
. . . . . .     (∀w:World, p:FairFifo.
. . . . . .      PossibleWorld(D';w)
. . . . . .      ⇒
. . . . . .      (∃v:T. P(c,v)) ⇒ (∃e:E. loc(e) = i))
. . . . . . 18. D' : Dsys
. . . . . . 19. D ⊆ D'
. . . . . . 20. w : World
. . . . . . 21. p : FairFifo
. . . . . . 22. PossibleWorld(D';w)
. . . . . . 23. vartype(i;x) ⊆r A
. . . . . . 24. ∀e:E. loc(e) = i ⇒ first(e) ⇒ (x when e) = c
. . . . . . 25. ∀e:E.
. . . . . .     loc(e) = i ⇒ kind(e) = locl(a) ⇒ (valtype(e) ⊆r T)
. . . . . . 26. vartype(i;x) ⊆r A
. . . . . . 27. ∀e:E. loc(e) = i ⇒ first(e) ⇒ (x when e) = c
. . . . . . 28. ∀e:E.
. . . . . .     loc(e) = i ⇒ kind(e) = locl(a) ⇒ (valtype(e) ⊆r T)
. . . . . . 29. vartype(i;x) ⊆r A
. . . . . . 30. ∀e:E.
. . . . . .     loc(e) = i ⇒ kind(e) = locl(a) ⇒ (valtype(e) ⊆r T)
. . . . . . 31. ∀e:E.
. . . . . .     loc(e) = i
. . . . . .     ⇒
. . . . . .     (kind(e) = locl(a) ⇒ P((x when e),val(e)))
. . . . . .     & (∃e':E.
. . . . . .        (e <loc e') ∨ e = e'
. . . . . .        & kind(e') = locl(a)
. . . . . .          ∨ (∀v:T. ¬P((x after e'),v)))
. . . . . . 32. vartype(i;x) ⊆r A
. . . . . . 33. ∀e:E. loc(e) = i ⇒ first(e) ⇒ (x when e) = c
. . . . . . 34. ∀e:E.
. . . . . .     loc(e) = i
. . . . . .     ⇒
. . . . . .     kind(e) = locl(a) ⇒ P((x when e),val(e))
. . . . . . 35. v : T
. . . . . . 36. P(c,v)
. . . . . . 37. e : E
. . . . . . 38. loc(e) = i
. . . . . . 39. vartype(i;x) ⊆r A
. . . . . . 40. ∀e:E.
. . . . . .     loc(e) = i ⇒ kind(e) = locl(a) ⇒ (valtype(e) ⊆r T)
. . . . . . 41. ∀e:E.
. . . . . .     loc(e) = i
. . . . . .     ⇒
. . . . . .     (kind(e) = locl(a) ⇒ P((x when e),val(e)))
. . . . . .     & (∃e':E.
. . . . . .        (e <loc e') ∨ e = e'
. . . . . .        & kind(e') = locl(a)
. . . . . .          ∨ (∀v:T. ¬P((x after e'),v)))
. . . . . . 42. vartype(i;x) ⊆r A
. . . . . . 43. ∀e:E. loc(e) = i ⇒ first(e) ⇒ (x when e) = c
```

```
. . . . . 44. kind(e) = locl(a) ⇒ P((x when e),val(e))
. . . . . 45. e' : E
. . . . . 46. (e <loc e') ∨ e = e'
. . . . . 47. kind(e') = locl(a) ∨ (∀v:T. ¬P((x after e'),v))
. . . . . 48. e1 : E
. . . . . 49. loc(e1) = i
. . . . . 50. T
. . . . . ⊢  vartype(loc(e1);x) ⊆r A  by HypSubst -2 0
END
```