

Inner Structure, Determinism and Modal Algebra of Multirelations

Walter Guttmann and Georg Struth

February 6, 2026

Abstract

Binary multirelations form a model of alternating nondeterminism useful for analysing games, interactions of computing systems with their environments or abstract interpretations of probabilistic programs. We investigate this alternating structure in a relational language based on power allegories extended with specific operations on multirelations. We develop algebras of modal operators over multirelations, related to concurrent dynamic logics, in this language.

Contents

| | | |
|----------|---|-----------|
| 1 | Properties of Binary Relations | 3 |
| 1.1 | Univalence, totality, determinism, and related properties . . . | 3 |
| 1.2 | Inverse image and the diagonal and graph functors | 5 |
| 1.3 | Relational domain, codomain and modalities | 6 |
| 1.4 | Residuation | 8 |
| 1.5 | Symmetric quotient | 10 |
| 2 | Properties of Power Allegories | 11 |
| 2.1 | Power transpose, epsilon, epsilonoff | 11 |
| 2.2 | Relational image functor | 12 |
| 2.3 | Unit and multiplication of powerset monad | 13 |
| 2.4 | Subset relation | 15 |
| 2.5 | Complementation relation | 16 |
| 2.6 | Kleisli lifting and Kleisli composition | 17 |
| 2.7 | Relational box | 18 |
| 3 | Basic Properties of Multirelations | 19 |
| 3.1 | Peleg composition, parallel composition (inner union) and units | 19 |
| 3.2 | Tests | 22 |
| 3.3 | Parallel subidentities | 24 |
| 3.4 | Domain | 27 |

| | | |
|----------|--|------------|
| 3.5 | Vectors | 33 |
| 3.6 | Up-closure and Parikh composition | 34 |
| 3.7 | Nonterminal and terminal multirelations | 36 |
| 3.8 | Powers | 41 |
| 3.9 | Star | 42 |
| 3.10 | Omega | 44 |
| 4 | Multirelational Properties of Power Allegories | 45 |
| 4.1 | Peleg lifting | 45 |
| 4.2 | Fusion and fission | 47 |
| 4.3 | Galois connections for multirelations | 47 |
| 4.4 | Properties of alpha, fission and fusion | 48 |
| 4.5 | Properties of fusion, fission, nu and tau | 49 |
| 4.6 | Box and diamond | 50 |
| 5 | Inner Structure | 51 |
| 5.1 | Inner union, inner intersection and inner complement | 51 |
| 5.2 | Dual | 56 |
| 5.3 | Co-composition | 57 |
| 5.4 | Inner order | 59 |
| 5.5 | Up-closure, down-closure and convex-closure | 59 |
| 6 | Powerdomain Preorders | 65 |
| 6.1 | Functional properties of multirelations | 75 |
| 6.2 | Equivalences induced by powerdomain preorders | 80 |
| 6.3 | Further results for convex-closure | 88 |
| 7 | Fusion and Fission | 92 |
| 7.1 | Atoms and co-atoms | 92 |
| 7.2 | Inner-functional properties | 93 |
| 7.3 | Fusion | 96 |
| 7.4 | Fission | 98 |
| 7.5 | Co-fusion and co-fission | 100 |
| 8 | Modalities | 103 |
| 8.1 | Tests | 103 |
| 8.2 | Domain and antidomain | 110 |
| 8.3 | Left residual | 113 |
| 8.4 | Modal operations | 116 |
| 8.5 | Goldblatt's axioms without star | 122 |
| 8.6 | Goldblatt's axioms with star | 127 |
| 8.7 | Propositional Hoare logic | 129 |

The theories formally verify results in [3, 1, 2]. See these papers for further details and related work.

The basic algebra of homogeneous binary multirelations is formalised in [4]. The present theories consider heterogeneous binary multirelations, which may have different source and target sets. While homogeneous multirelations arise as a special case where source and target sets coincide, we do not attempt to generalise the algebras of [4] to the heterogeneous case but study new concepts instead. Thus the present theories and [4] are complementary. A unification of the two approaches based on category theory is possible future work.

Algebraic structures for multirelations with Parikh composition are formalised in [5].

1 Properties of Binary Relations

theory *Relational-Properties*

imports *Main*

begin

This is a general-purpose theory for enrichments of Rel, which is still quite basic, but helpful for developing properties of multirelations.

notation *relcomp* (**infixl** $\langle ; \rangle$ 75)

notation *converse* ($\langle \smile \rangle$ [1000] 999)

type-synonym ($\langle 'a, 'b \rangle$ *rel* = ($\langle 'a \times 'b \rangle$ *set*)

lemma *modular-law*: $R ; S \cap T \subseteq (R \cap T ; S \smile) ; S$
<proof>

lemma *compl-conv*: $\neg(R \smile) = (\neg R) \smile$
<proof>

definition *top* :: ($\langle 'a, 'b \rangle$ *rel*) **where**
top = $\{(a, b) \mid a \ b. \ \text{True}\}$

abbreviation *neg* $R \equiv Id \cap \neg R$

1.1 Univalence, totality, determinism, and related properties

definition *univalent* :: ($\langle 'a, 'b \rangle$ *rel*) \Rightarrow *bool* **where**
univalent $R = (R \smile ; R \subseteq Id)$

definition *total* :: ('a,'b) rel ⇒ bool **where**
total R = (Id ⊆ R ; R[⊃])

definition *injective* :: ('a,'b) rel ⇒ bool **where**
injective R = (R ; R[⊃] ⊆ Id)

definition *surjective* :: ('a,'b) rel ⇒ bool **where**
surjective R = (Id ⊆ R[⊃] ; R)

definition *deterministic* :: ('a,'b) rel ⇒ bool **where**
deterministic R = (univalent R ∧ *total* R)

definition *bijjective* :: ('a,'b) rel ⇒ bool **where**
bijjective R = (*injective* R ∧ *surjective* R)

lemma *univalent-set*: univalent R = (∀ a b c. (a,b) ∈ R ∧ (a,c) ∈ R → b = c)
⟨proof⟩

Univalent relations feature as single-valued relations in Main.

lemma *univ-single-valued*: univalent R = single-valued R
⟨proof⟩

lemma *total-set*: *total* R = (∀ a. ∃ b. (a,b) ∈ R)
⟨proof⟩

lemma *total-var*: *total* R = (R ; top = top)
⟨proof⟩

lemma *deterministic-set*: *deterministic* R = (∀ a . ∃! B . (a,B) ∈ R)
⟨proof⟩

lemma *deterministic-var1*: *deterministic* R = (R ; -Id = -R)
⟨proof⟩

lemma *deterministic-var2*: *deterministic* R = (∀ S. R ; -S = -(R ; S))
⟨proof⟩

lemma *inj-univ*: *injective* R = univalent (R[⊃])
⟨proof⟩

lemma *injective-set*: *injective* S = (∀ a b c. (a,c) ∈ S ∧ (b,c) ∈ S → a = b)
⟨proof⟩

lemma *surj-tot*: *surjective* R = *total* (R[⊃])
⟨proof⟩

lemma *surjective-set*: *surjective* S = (∀ b. ∃ a. (a,b) ∈ S)
⟨proof⟩

lemma *surj-var*: *surjective* $R = (R^\smile ; \text{top} = \text{top})$
<proof>

lemma *bij-det*: *bijjective* $R = \text{deterministic} (R^\smile)$
<proof>

lemma *univ-relcomp*: *univalent* $R \implies \text{univalent } S \implies \text{univalent} (R ; S)$
<proof>

lemma *tot-relcomp*: *total* $R \implies \text{total } S \implies \text{total} (R ; S)$
<proof>

lemma *det-relcomp*: *deterministic* $R \implies \text{deterministic } S \implies \text{deterministic} (R ; S)$
<proof>

lemma *inj-relcomp*: *injective* $R \implies \text{injective } S \implies \text{injective} (R ; S)$
<proof>

lemma *surj-relcomp*: *surjective* $R \implies \text{surjective } S \implies \text{surjective} (R ; S)$
<proof>

lemma *bij-relcomp*: *bijjective* $R \implies \text{bijjective } S \implies \text{bijjective} (R ; S)$
<proof>

lemma *det-Id*: *deterministic* Id
<proof>

lemma *bij-Id*: *bijjective* Id
<proof>

lemma *tot-top*: *total* top
<proof>

lemma *tot-surj*: *surjective* top
<proof>

lemma *det-meet-distl*: *univalent* $R \implies R ; (S \cap T) = R ; S \cap R ; T$
<proof>

lemma *inj-meet-distr*: *injective* $T \implies (R \cap S) ; T = R ; T \cap S ; T$
<proof>

lemma *univ-modular*: *univalent* $S \implies R ; S \cap T = (R \cap T ; S^\smile) ; S$
<proof>

1.2 Inverse image and the diagonal and graph functors

definition *Invim* :: $('a, 'b) \text{ rel} \implies 'b \text{ set} \implies 'a \text{ set}$ **where**

$$\text{Invim } R = \text{Image } (R^\smile)$$

definition Δ :: 'a set \Rightarrow ('a,'a) rel ($\langle \Delta \rangle$) **where**
 $\Delta P = \{(p,p) \mid p. p \in P\}$

definition Grph :: ('a \Rightarrow 'b) \Rightarrow ('a,'b) rel **where**
 $\text{Grph } f = \{(x,y). y = f x\}$

lemma Image-Grph [*simp*]: $\text{Image} \circ \text{Grph} = \text{image}$
 $\langle \text{proof} \rangle$

1.3 Relational domain, codomain and modalities

Domain and codomain (range) maps have been defined in Main, but they return sets instead of relations.

definition dom :: ('a,'b) rel \Rightarrow ('a,'a) rel **where**
 $\text{dom } R = \text{Id} \cap R ; R^\smile$

definition cod :: ('a,'b) rel \Rightarrow ('b,'b) rel **where**
 $\text{cod } R = \text{dom } (R^\smile)$

definition rel-fdia :: ('a,'b) rel \Rightarrow ('b,'b) rel \Rightarrow ('a,'a) rel ($\langle (|-) \rangle$) [61,81] 82
where
 $|R\rangle Q = \text{dom } (R ; \text{dom } Q)$

definition rel-bdia :: ('a,'b) rel \Rightarrow ('a,'a) rel \Rightarrow ('b,'b) rel ($\langle \langle (-) \rangle \rangle$) [61,81] 82
where
 $\text{rel-bdia } R = \text{rel-fdia } (R^\smile)$

definition rel-fbox :: ('a,'b) rel \Rightarrow ('b,'b) rel \Rightarrow ('a,'a) rel ($\langle (|-) \rangle$) [61,81] 82
where
 $|R]Q = \text{neg } (\text{dom } (R ; \text{neg } (\text{dom } Q)))$

definition rel-bbox :: ('a,'b) rel \Rightarrow ('a,'a) rel \Rightarrow ('b,'b) rel ($\langle \langle (|-) \rangle \rangle$) [61,81] 82
where
 $\text{rel-bbox } R = \text{rel-fbox } (R^\smile)$

lemma rel-bdia-def-var : $\text{rel-bdia} = \text{rel-fdia} \circ \text{converse}$
 $\langle \text{proof} \rangle$

lemma dom-set : $\text{dom } R = \{(a,a) \mid a. \exists b. (a,b) \in R\}$
 $\langle \text{proof} \rangle$

lemma dom-Domain : $\text{dom} = \Delta \circ \text{Domain}$
 $\langle \text{proof} \rangle$

lemma cod-set : $\text{cod } R = \{(b,b) \mid b. \exists a. (a,b) \in R\}$
 $\langle \text{proof} \rangle$

lemma *cod-Range*: $\text{cod} = \Delta \circ \text{Range}$
<proof>

lemma *rel-fdia-set*: $|R\rangle Q = \{(a,a) \mid a. \exists b. (a,b) \in R \wedge (b,b) \in \text{dom } Q\}$
<proof>

lemma *rel-bdia-set*: $\langle R| P = \{(b,b) \mid b. \exists a. (a,b) \in R \wedge (a,a) \in \text{dom } P\}$
<proof>

lemma *rel-fbox-set*: $|R] Q = \{(a,a) \mid a. \forall b. (a,b) \in R \longrightarrow (b,b) \in \text{dom } Q\}$
<proof>

lemma *rel-bbox-set*: $[R| P = \{(b,b) \mid b. \forall a. (a,b) \in R \longrightarrow (a,a) \in \text{dom } P\}$
<proof>

lemma *dom-alt-def*: $\text{dom } R = \text{Id} \cap R ; \text{top}$
<proof>

lemma *dom-gla*: $(\text{dom } R \subseteq \text{Id} \cap S) = (R \subseteq (\text{Id} \cap S) ; R)$
<proof>

lemma *dom-gla-top*: $(\text{dom } R \subseteq \text{Id} \cap S) = (R \subseteq (\text{Id} \cap S) ; \text{top})$
<proof>

lemma *dom-subid*: $(\text{dom } R = R) = (R = \text{Id} \cap R)$
<proof>

lemma *dom-cod*: $(\text{dom } R = R) = (\text{cod } R = R)$
<proof>

lemma *dom-top*: $R ; \text{top} = \text{dom } R ; \text{top}$
<proof>

lemma *top-dom*: $\text{dom } R = \text{dom } (R ; \text{top})$
<proof>

lemma *cod-top*: $\text{cod } R = \text{Id} \cap \text{top} ; R$
<proof>

lemma *dom-conv* [*simp*]: $(\text{dom } R)^\smile = \text{dom } R$
<proof>

lemma *total-dom*: $\text{total } R = (\text{dom } R = \text{Id})$
<proof>

lemma *surj-cod*: $\text{surjective } R = (\text{cod } R = \text{Id})$
<proof>

lemma *fdia-demod*: $(|R\rangle P \subseteq \text{dom } Q) = (R ; \text{dom } P \subseteq \text{dom } Q ; R)$

$\langle proof \rangle$

lemma *bbox-demod*: $(dom P \subseteq [R] Q) = (R ; dom P \subseteq dom Q ; R)$
 $\langle proof \rangle$

lemma *bdia-demod*: $(\langle R \rangle P \subseteq dom Q) = (dom P ; R \subseteq R ; dom Q)$
 $\langle proof \rangle$

lemma *fbox-demod*: $(dom P \subseteq |R] Q) = (dom P ; R \subseteq R ; dom Q)$
 $\langle proof \rangle$

lemma *fdia-demod-top*: $(|R\rangle P \subseteq dom Q) = (R ; dom P ; top \subseteq dom Q ; top)$
 $\langle proof \rangle$

lemma *bbox-demod-top*: $(dom P \subseteq [R] Q) = (R ; dom P ; top \subseteq dom Q ; top)$
 $\langle proof \rangle$

lemma *fdia-bbox-galois*: $(|R\rangle P \subseteq dom Q) = (dom P \subseteq [R] Q)$
 $\langle proof \rangle$

lemma *bdia-fbox-galois*: $(\langle R \rangle P \subseteq dom Q) = (dom P \subseteq |R] Q)$
 $\langle proof \rangle$

lemma *fdia-bdia-conjugation*: $(|R\rangle P \subseteq neg (dom Q)) = (\langle R \rangle Q \subseteq neg (dom P))$
 $\langle proof \rangle$

lemma *bfox-bbox-conjugation*: $(neg (dom Q) \subseteq |R] P) = (neg (dom P) \subseteq [R] Q)$
 $\langle proof \rangle$

1.4 Residuation

definition *lres* :: $(a, c) rel \Rightarrow (b, c) rel \Rightarrow (a, b) rel$ (**infixl** $\langle // \rangle$ 75)
where $R // S = \{(a, b). \forall c. (b, c) \in S \longrightarrow (a, c) \in R\}$

definition *rres* :: $(c, a) rel \Rightarrow (c, b) rel \Rightarrow (a, b) rel$ (**infixl** $\langle \setminus \rangle$ 75)
where $R \setminus S = \{(b, a). \forall c. (c, b) \in R \longrightarrow (c, a) \in S\}$

lemma *rres-lres-conv*: $R \setminus S = (S^\smile // R^\smile)^\smile$
 $\langle proof \rangle$

lemma *lres-galois*: $(R ; S \subseteq T) = (R \subseteq T // S)$
 $\langle proof \rangle$

lemma *rres-galois*: $(R ; S \subseteq T) = (S \subseteq R \setminus T)$
 $\langle proof \rangle$

lemma *lres-compl*: $R // S = -(-R ; S^\smile)$
 $\langle proof \rangle$

lemma *rres-compl*: $R \setminus S = -(R^\smile ; -S)$
 ⟨proof⟩

lemma *lres-simp [simp]*: $(R \parallel R) ; R = R$
 ⟨proof⟩

lemma *rres-simp [simp]*: $R ; (R \setminus R) = R$
 ⟨proof⟩

lemma *lres-curry*: $R \parallel (T ; S) = (R \parallel S) \parallel T$
 ⟨proof⟩

lemma *rres-curry*: $(R ; S) \setminus T = S \setminus (R \setminus T)$
 ⟨proof⟩

lemma *lres-Id*: $Id \subseteq R \parallel R$
 ⟨proof⟩

lemma *det-lres*: *deterministic* $R \implies (R ; S) \parallel S = R ; (S \parallel S)$
 ⟨proof⟩

lemma *det-rres*: *deterministic* $(R^\smile) \implies S \setminus (S ; R) = (S \setminus S) ; R$
 ⟨proof⟩

lemma *rres-bij*: *bijective* $S \implies (R \setminus T) ; S = R \setminus (T ; S)$
 ⟨proof⟩

lemma *lres-bij*: *bijective* $S \implies (R \parallel T^\smile) ; S = R \parallel (T ; S)^\smile$
 ⟨proof⟩

lemma *dom-rres-top*: $(dom P \subseteq R \setminus (dom Q ; top)) = (dom P ; top \subseteq R \setminus (dom Q ; top))$
 ⟨proof⟩

lemma *dom-rres-top-var*: $(dom P \subseteq R \setminus (dom Q ; top)) = (P ; top \subseteq R \setminus (Q ; top))$
 ⟨proof⟩

lemma *fdia-rres-top*: $(|R\rangle P \subseteq dom Q) = (dom P \subseteq R \setminus (dom Q ; top))$
 ⟨proof⟩

lemma *fdia-rres-top-var*: $(|R\rangle P \subseteq dom Q) = (dom P \subseteq R \setminus (Q ; top))$
 ⟨proof⟩

lemma *dom-galois-var2*: $(|R\rangle (Id \cap P) \subseteq Id \cap Q) = (Id \cap P \subseteq R \setminus ((Id \cap Q) ; top))$
 ⟨proof⟩

lemma *rres-top*: $R \setminus (dom Q ; top) ; top = R \setminus (dom Q ; top)$

$\langle proof \rangle$

lemma *ddd-var*: $(\ |R\rangle P \subseteq dom\ Q) = (dom\ P \subseteq dom\ ((R \setminus (dom\ Q ; top)) ; top))$
 $\langle proof \rangle$

lemma *wlp-prop*: $dom\ ((R \setminus (dom\ Q ; top)) ; top) = neg\ (cod\ (neg\ (dom\ Q); R))$
 $\langle proof \rangle$

lemma *wlp-prop-var*: $dom\ ((R \setminus (dom\ Q ; top))) = neg\ (cod\ ((neg\ (dom\ Q)); R))$
 $\langle proof \rangle$

lemma *dom-demod*: $(\ |R\rangle (Id \cap P) \subseteq Id \cap Q) = (R ; (Id \cap P) \subseteq (Id \cap Q) ; R)$
 $\langle proof \rangle$

lemma *fdia-bbox-galois-var*: $(\ |R\rangle (Id \cap P) \subseteq Id \cap Q) = (Id \cap P \subseteq Id \cap -\ cod\ ((Id \cap -Q); R))$
 $\langle proof \rangle$

lemma *dom-demod-var2*: $(\ |R\rangle (Id \cap P) \subseteq Id \cap Q) = (Id \cap P \subseteq R \setminus ((Id \cap Q) ; R))$
 $\langle proof \rangle$

1.5 Symmetric quotient

definition *syq* :: $(c, a) rel \Rightarrow (c, b) rel \Rightarrow (a, b) rel$ (**infixl** \div 75)
where $R \div S = (R \setminus S) \cap (R^\smile \parallel S^\smile)$

lemma *syq-set*: $R \div S = \{(a, b). \forall c. (c, a) \in R \longleftrightarrow (c, b) \in S\}$
 $\langle proof \rangle$

lemma *converse-syq* [*simp*]: $(R \div S)^\smile = S \div R$
 $\langle proof \rangle$

lemma *syq-compl*: $R \div S = - (R^\smile ; -S) \cap - (- (R^\smile) ; S)$
 $\langle proof \rangle$

lemma *syq-compl2* [*simp*]: $-R \div -S = R \div S$
 $\langle proof \rangle$

lemma *syq-expand1*: $R ; (R \div S) = S \cap (top ; (R \div S))$
 $\langle proof \rangle$

lemma *syq-expand2*: $(R \div S) ; S^\smile = R^\smile \cap ((R \div S) ; top)$
 $\langle proof \rangle$

lemma *syq-comp1*: $(R \div S) ; (S \div T) = (R \div T) \cap (top ; (S \div T))$
 $\langle proof \rangle$

lemma *syq-comp2*: $(R \div S) ; (S \div T) = (R \div T) \cap ((R \div S) ; top)$
 ⟨proof⟩

lemma *syq-bij*: *bijjective* $T \implies (R \div S) ; T = R \div (S ; T)$
 ⟨proof⟩

end

2 Properties of Power Allegories

theory *Power-Allegories-Properties*

imports *Relational-Properties*

begin

2.1 Power transpose, epsilon, epsilonoff

definition *Lambda* :: $('a, 'b \text{ set}) \text{ rel} \Rightarrow ('a, 'b \text{ set}) \text{ rel} (\langle \Lambda \rangle)$ **where**
 $\Lambda R = \{(a, B) \mid a \in B. B = \{b. (a, b) \in R\}\}$

definition *epsilon* :: $('a, 'a \text{ set}) \text{ rel}$ **where**
 $\epsilon = \{(a, A). a \in A\}$

definition *epsilonoff* = $\{(A, a). a \in A\}$

definition *alpha* :: $('a, 'b \text{ set}) \text{ rel} \Rightarrow ('a, 'b) \text{ rel} (\langle \alpha \rangle)$ **where**
 $\alpha R = R ; \epsilon \text{off}$

[alpha](#) can be seen as a relational approximation of a multirelation. The next lemma provides a relational definition of [Lambda](#).

lemma *Lambda-syq*: $\Lambda R = R^\smile \div \epsilon$
 ⟨proof⟩

lemma *epsilonoff-epsilon*: $\epsilon \text{off} = \epsilon^\smile$
 ⟨proof⟩

lemma *alpha-set*: $\alpha R = \{(a, b) \mid a \in b. b \in \bigcup \{B. (a, B) \in R\}\}$
 ⟨proof⟩

lemma *alpha-relcomp* [*simp*]: $\alpha (R ; S) = R ; \alpha S$
 ⟨proof⟩

lemma *Lambda-epsilonoff-up1*: $f = \Lambda R \implies R = \alpha f$
 ⟨proof⟩

lemma *Lambda-epsilonoff-up2*: *deterministic* $f \implies R = \alpha f \implies f = \Lambda R$
 ⟨proof⟩

lemma *Lambda-epsiloff-up*:
assumes *deterministic f*
shows $(R = \alpha f) = (f = \Lambda R)$
 $\langle proof \rangle$

lemma *det-lambda: deterministic* (ΛR)
 $\langle proof \rangle$

lemma *Lambda-alpha-canc: deterministic* $f \implies \Lambda (\alpha f) = f$
 $\langle proof \rangle$

lemma *alpha-Lambda-canc [simp]*: $\alpha (\Lambda R) = R$
 $\langle proof \rangle$

lemma *alpha-cancel*:
assumes *deterministic f*
and *deterministic g*
shows $\alpha f = \alpha g \implies f = g$
 $\langle proof \rangle$

lemma *Lambda-fusion*:
assumes *deterministic f*
shows $\Lambda (f ; R) = f ; \Lambda R$
 $\langle proof \rangle$

lemma *Lambda-fusion-var*: $\Lambda (\Lambda R ; S) = \Lambda R ; \Lambda S$
 $\langle proof \rangle$

lemma *Lambda-epsiloff [simp]*: $\Lambda \text{epsiloff} = Id$
 $\langle proof \rangle$

lemma *alpha-epsiloff [simp]*: $\alpha Id = \text{epsiloff}$
 $\langle proof \rangle$

lemma *alpha-Sup-pres*: $\alpha (\bigcup \mathcal{R}) = (\bigcup R \in \mathcal{R}. \alpha R)$
 $\langle proof \rangle$

lemma *alpha-ord-pres*: $R \subseteq S \implies \alpha R \subseteq \alpha S$
 $\langle proof \rangle$

lemma *alpha-inf-pres*: $\alpha \{(a,A). \exists B C. A = B \cap C \wedge (a,B) \in R \wedge (a,C) \in S\}$
 $= \alpha R \cap \alpha S$
 $\langle proof \rangle$

2.2 Relational image functor

definition $\text{pow} :: ('a, 'b) \text{rel} \Rightarrow ('a \text{ set}, 'b \text{ set}) \text{rel}$ ($\langle \mathcal{P} \rangle$) **where**
 $\mathcal{P} R = \Lambda (\text{epsiloff} ; R)$

lemma *pow-set*: $\mathcal{P} R = \{(A,B). B = \text{Image } R A\}$
 ⟨proof⟩

lemma *pow-set-var*: $\mathcal{P} R = \{(A,B). B = \{b. \exists a \in A. (a,b) \in R\}\}$
 ⟨proof⟩

lemma *pow-converse-set*: $\mathcal{P} (R^\sim) = \{(Q,P). P = \{a. \exists b. (a,b) \in R \wedge b \in Q\}\}$
 ⟨proof⟩

lemma *det-pow*: *deterministic* ($\mathcal{P} R$)
 ⟨proof⟩

lemma *Lambda-pow*: $\Lambda (R ; S) = \Lambda R ; \mathcal{P} S$
 ⟨proof⟩

lemma *pow-func1* [*simp*]: $\mathcal{P} \text{Id} = \text{Id}$
 ⟨proof⟩

lemma *pow-func2*: $\mathcal{P} (R ; S) = \mathcal{P} R ; \mathcal{P} S$
 ⟨proof⟩

lemma *Grph-Image* [*simp*]: $\text{Grph} \circ \text{Image} = \mathcal{P}$
 ⟨proof⟩

lemma *lambda-alpha-idem* [*simp*]: $\Lambda (\alpha (\Lambda (\alpha R))) = \Lambda (\alpha R)$
 ⟨proof⟩

2.3 Unit and multiplication of powerset monad

definition *eta* :: (*'a*, *'a set*) *rel* ($\langle \eta \rangle$) **where**
 $\eta = \Lambda \text{Id}$

definition *mu* :: (*'a set set*, *'a set*) *rel* ($\langle \mu \rangle$) **where**
 $\mu = \text{pow } \text{epsiloff}$

lemma *eta-set*: $\eta = \{(a, \{a\}) \mid a. \text{True}\}$
 ⟨proof⟩

lemma *alpha-eta* [*simp*]: $\alpha \eta = \text{Id}$
 ⟨proof⟩

lemma *det-eta*: *deterministic* η
 ⟨proof⟩

lemma *mu-set*: $\mu = \{(A,B). B = \{b. \exists C. C \in A \wedge b \in C\}\}$
 ⟨proof⟩

lemma *det-mu*: *deterministic* μ
 ⟨proof⟩

lemma *Lambda-eta*:
assumes *deterministic R*
shows $\Lambda R = R ; \eta$
 $\langle proof \rangle$

lemma *eta-nat-trans*:
assumes *deterministic R*
shows $\eta ; \mathcal{P} R = R ; \eta$
 $\langle proof \rangle$

lemma *mu-nat-trans*:
assumes *deterministic R*
shows $\mathcal{P} (\mathcal{P} R) ; \mu = \mu ; \mathcal{P} R$
 $\langle proof \rangle$

The standard axioms for the powerset monad are derivable.

lemma *pow-monad1* [*simp*]: $\mathcal{P} \mu ; \mu = \mu ; \mu$
 $\langle proof \rangle$

lemma *pow-monad2* [*simp*]: $\mathcal{P} \eta ; \mu = Id$
 $\langle proof \rangle$

lemma *pow-monad3* [*simp*]: $\eta ; \mu = Id$
 $\langle proof \rangle$

lemma *Lambda-mu*:
assumes *deterministic R*
shows $\Lambda(R) ; \mu = R$
 $\langle proof \rangle$

lemma *pow-Lambda-mu* [*simp*]: $\mathcal{P} (\Lambda R) ; \mu = \mathcal{P} R$
 $\langle proof \rangle$

lemma *lambda-alpha-mu*: $\Lambda (\alpha R) = \Lambda R ; \mu$
 $\langle proof \rangle$

lemma *alpha-eta-pow* [*simp*]: $\alpha (\eta ; \mathcal{P} R) = R$
 $\langle proof \rangle$

lemma *eta-pow-Lambda* [*simp*]: $\eta ; \mathcal{P} R = \Lambda R$
 $\langle proof \rangle$

lemma *pow-prop1*: $\mathcal{P} R \subseteq S \implies R \subseteq \alpha (\eta ; S)$
 $\langle proof \rangle$

lemma *pow-prop-2*: $R \subseteq \mathcal{P} S \implies \alpha (\eta ; R) \subseteq S$
 $\langle proof \rangle$

lemma *pow-prop*: $R = \mathcal{P} S \implies \alpha (\eta ; R) = S$
 ⟨proof⟩

lemma *alpha-eta-id* [*simp*]: $\alpha (R ; \eta) = R$
 ⟨proof⟩

lemma *eta-alpha-idem* [*simp*]: $\alpha (\alpha R ; \eta) ; \eta = \alpha R ; \eta$
 ⟨proof⟩

lemma *lambda-eta-alpha* [*simp*]: $\Lambda (\alpha (\alpha R ; \eta)) = \Lambda (\alpha R)$
 ⟨proof⟩

lemma *eta-lambda-idem* [*simp*]: $\alpha (\Lambda (\alpha R)) ; \eta = \alpha R ; \eta$
 ⟨proof⟩

lemma *Grph-eta* [*simp*]: $Grph (\lambda x. \{x\}) = \eta$
 ⟨proof⟩

lemma *Grph-epsiloff* [*simp*]: $Grph (\lambda x. \{x\}) ; \text{epsiloff} = Id$
 ⟨proof⟩

lemma *Image-epsiloff* [*simp*]: $Image \text{epsiloff} \circ (\lambda x. \{x\}) = id$
 ⟨proof⟩

2.4 Subset relation

definition *Omega* :: ('a set, 'a set) rel (⟨Ω⟩) **where**
 $\Omega = \text{epsilon} \setminus \text{epsilon}$

lemma *Omega-set*: $\Omega = \{(A,B). A \subseteq B\}$
 ⟨proof⟩

lemma *conv-Omega*: $\Omega^\sim = \text{epsiloff} // \text{epsiloff}$
 ⟨proof⟩

lemma *epsilon-eta-Omega* [*simp*]: $\eta ; \Omega = \text{epsilon}$
 ⟨proof⟩

lemma *epsiloff-eta-Omega* [*simp*]: $\Omega^\sim ; \eta^\sim = \text{epsiloff}$
 ⟨proof⟩

lemma *epsilon-Omega* [*simp*]: $\text{epsilon} ; \Omega = \text{epsilon}$
 ⟨proof⟩

lemma *conv-Omega-epsiloff* [*simp*]: $\Omega^\sim ; \text{epsiloff} = \text{epsiloff}$
 ⟨proof⟩

lemma *Lambda-conv* [*simp*]: $(\Lambda R)^\sim = \text{epsilon} \div R^\sim$
 ⟨proof⟩

lemma *Lambda-Omega*: $\Lambda R ; \Omega = R^\sim \setminus \text{epsilon}$
 ⟨proof⟩

lemma *syq-epsiloff-prop* [simp]: $\Omega^\sim ; (\text{epsilon} \div R) = \text{epsiloff} \parallel R^\sim$
 ⟨proof⟩

lemma *pow-semicomm*: $((P, Q) \in \mathcal{P} R ; \Omega) = (\Delta P ; R \subseteq R ; \Delta Q)$
 ⟨proof⟩

2.5 Complementation relation

definition *Compl* :: ('a set, 'a set) rel (⟨C⟩) **where**
 $\mathcal{C} = \text{epsilon} \div \neg \text{epsilon}$

lemma *Compl-set*: $\mathcal{C} = \{(A, \neg A) \mid A. \text{True}\}$
 ⟨proof⟩

lemma *Compl-Compl* [simp]: $\mathcal{C} ; \mathcal{C} = \text{Id}$
 ⟨proof⟩

lemma *Compl-def-var*: $\mathcal{C} = \Lambda (\neg \text{epsiloff})$
 ⟨proof⟩

lemma *converse-Compl* [simp]: $\mathcal{C}^\sim = \mathcal{C}$
 ⟨proof⟩

lemma *det-Compl*: *deterministic* \mathcal{C}
 ⟨proof⟩

lemma *bij-Compl*: *bijjective* \mathcal{C}
 ⟨proof⟩

lemma *Compl-compl-epsiloff* [simp]: $\mathcal{C} ; \neg \text{epsiloff} = \text{epsiloff}$
 ⟨proof⟩

lemma *Compl-epsiloff* [simp]: $\mathcal{C} ; \text{epsiloff} = \neg \text{epsiloff}$
 ⟨proof⟩

lemma *compl-epsilon-Compl* [simp]: $\neg \text{epsilon} ; \mathcal{C} = \text{epsilon}$
 ⟨proof⟩

lemma *epsilon-Compl* [simp]: $\text{epsilon} ; \mathcal{C} = \neg \text{epsilon}$
 ⟨proof⟩

lemma *Lambda-Compl-var*: $\Lambda R ; \mathcal{C} = R^\sim \div \neg \text{epsilon}$
 ⟨proof⟩

lemma *Lambda-Compl*: $\Lambda R ; \mathcal{C} = \Lambda (\neg R)$

$\langle proof \rangle$

2.6 Kleisli lifting and Kleisli composition

definition $klift :: ('a, 'b \text{ set}) \text{ rel} \Rightarrow ('a \text{ set}, 'b \text{ set}) \text{ rel}$ ($\langle - \rangle_{\mathcal{P}}$ [1000] 999) **where**
 $(R)_{\mathcal{P}} = \mathcal{P} (\alpha R)$

definition $kcomp :: ('a, 'b \text{ set}) \text{ rel} \Rightarrow ('b, 'c \text{ set}) \text{ rel} \Rightarrow ('a, 'c \text{ set}) \text{ rel}$ (**infixl** $\langle - \rangle_{\mathcal{P}}$ 70) **where**
 $R \cdot_{\mathcal{P}} S = R ; (S)_{\mathcal{P}}$

lemma $klift\text{-var}: (R)_{\mathcal{P}} = \Lambda (\text{epsiloff} ; R ; \text{epsiloff})$
 $\langle proof \rangle$

lemma $klift\text{-set}: (R)_{\mathcal{P}} = \{(A, B). B = \bigcup (\text{Image } R A)\}$
 $\langle proof \rangle$

lemma $klift\text{-set-var}: (R)_{\mathcal{P}} = \{(A, B). B = \bigcup \{C. \exists a \in A. (a, C) \in R\}\}$
 $\langle proof \rangle$

lemma $klift\text{-mu}: (R)_{\mathcal{P}} = \mathcal{P} R ; \mu$
 $\langle proof \rangle$

lemma $klift\text{-empty}: (\{\}, A) \in (R)_{\mathcal{P}} \longleftrightarrow A = \{\}$
 $\langle proof \rangle$

lemma $klift\text{-ext1}: (R ; (S)_{\mathcal{P}})_{\mathcal{P}} = (R)_{\mathcal{P}} ; (S)_{\mathcal{P}}$
 $\langle proof \rangle$

lemma $klift\text{-ext2}: \text{deterministic } R \Longrightarrow \eta ; (R)_{\mathcal{P}} = R$
 $\langle proof \rangle$

lemma $klift\text{-ext3} [simp]: (\eta)_{\mathcal{P}} = Id$
 $\langle proof \rangle$

lemma $pow\text{-klift} [simp]: (R ; \eta)_{\mathcal{P}} = \mathcal{P} R$
 $\langle proof \rangle$

lemma $mu\text{-klift} [simp]: (Id)_{\mathcal{P}} = \mu$
 $\langle proof \rangle$

lemma $kcomp\text{-var}: R \cdot_{\mathcal{P}} S = R ; \mathcal{P} S ; \mu$
 $\langle proof \rangle$

lemma $kcomp\text{-assoc}: R \cdot_{\mathcal{P}} (S \cdot_{\mathcal{P}} T) = (R \cdot_{\mathcal{P}} S) \cdot_{\mathcal{P}} T$
 $\langle proof \rangle$

lemma $kcomp\text{-oner}: R \cdot_{\mathcal{P}} \eta = R$
 $\langle proof \rangle$

lemma *kcomp-one1*: $\text{deterministic } R \implies \eta \cdot_{\mathcal{P}} R = R$
 ⟨proof⟩

2.7 Relational box

definition *rbox* :: $('a, 'b) \text{ rel} \implies ('b \text{ set}, 'a \text{ set}) \text{ rel}$ **where**
 $rbox \ R = \Lambda (\text{epsiloff} \ // \ R)$

lemma *rbox-set*: $rbox \ R = \{(Q, P). P = \{a. \forall b. (a, b) \in R \longrightarrow b \in Q\}\}$
 ⟨proof⟩

lemma *rbox-exp*: $((Q, P) \in (rbox \ (R :: ('a, 'b) \text{ rel}))) = (P = -\{a. \exists b. (a, b) \in R \wedge b \in -Q\})$
 ⟨proof⟩

lemma *rbox-subset*: $rbox \ R ; \Omega^{\smile} = \{(Q, P). P \subseteq \{a. \forall b. (a, b) \in R \longrightarrow b \in Q\}\}$
 ⟨proof⟩

lemma *rbox-semicomm*: $(Q, P) \in rbox \ R ; \Omega^{\smile} = (\Delta \ P ; R \subseteq R ; \Delta \ Q)$
 ⟨proof⟩

lemma *rbox-semicomm-var*: $(Q, P) \in rbox \ R ; \Omega^{\smile} = (\Delta \ P \subseteq (R ; \Delta \ Q) \ // \ R)$
 ⟨proof⟩

lemma *rbox-omega*: $rbox \ \text{epsiloff} = \Lambda (\Omega^{\smile})$
 ⟨proof⟩

lemma *Omega-rbox*: $\Omega = (\alpha \ (rbox \ \text{epsiloff}))^{\smile}$
 ⟨proof⟩

lemma *pow-rbox*: $((Q, P) \in rbox \ R ; \Omega^{\smile}) = ((P, Q) \in \mathcal{P} \ R ; \Omega)$
 ⟨proof⟩

lemma *rbox-pow-Compl*: $rbox \ R = \mathcal{C} ; \mathcal{P} \ (R^{\smile}) ; \mathcal{C}$
 ⟨proof⟩

lemma *pow-rbox-Compl*: $\mathcal{P} \ R = \mathcal{C} ; rbox \ (R^{\smile}) ; \mathcal{C}$
 ⟨proof⟩

lemma *pow-conjugation*: $\mathcal{C} ; (\mathcal{P} \ (R^{\smile}) ; \Omega)^{\smile} = \mathcal{P} \ R ; \mathcal{C} ; \Omega^{\smile}$
 ⟨proof⟩

lemma *pow-rbox-eq*: $rbox \ R ; \Omega^{\smile} = (\mathcal{P} \ R ; \Omega)^{\smile}$
 ⟨proof⟩

end

3 Basic Properties of Multirelations

theory *Multirelations-Basics*

imports *Power-Allegories-Properties*

begin

This theory extends a previous AFP entry for multirelations with one single objects to proper multirelations in Rel.

3.1 Peleg composition, parallel composition (inner union) and units

type-synonym $(\text{'a}, \text{'b}) \text{ mrel} = (\text{'a}, \text{'b} \text{ set}) \text{ rel}$

definition $s\text{-prod} :: (\text{'a}, \text{'b}) \text{ mrel} \Rightarrow (\text{'b}, \text{'c}) \text{ mrel} \Rightarrow (\text{'a}, \text{'c}) \text{ mrel}$ (**infixl** $\langle \cdot \rangle$ 75)
where

$R \cdot S = \{(a, A). (\exists B. (a, B) \in R \wedge (\exists f. (\forall b \in B. (b, f b) \in S) \wedge A = \bigcup (f ` B)))\}$

definition $s\text{-id} :: (\text{'a}, \text{'a}) \text{ mrel}$ ($\langle 1_\sigma \rangle$) **where**
 $1_\sigma = (\bigcup a. \{(a, \{a\})\})$

definition $p\text{-prod} :: (\text{'a}, \text{'b}) \text{ mrel} \Rightarrow (\text{'a}, \text{'b}) \text{ mrel} \Rightarrow (\text{'a}, \text{'b}) \text{ mrel}$ (**infixl** $\langle \parallel \rangle$ 70)
where

$R \parallel S = \{(a, A). (\exists B C. A = B \cup C \wedge (a, B) \in R \wedge (a, C) \in S)\}$

definition $p\text{-id} :: (\text{'a}, \text{'b}) \text{ mrel}$ ($\langle 1_\pi \rangle$) **where**
 $1_\pi = (\bigcup a. \{(a, \{a\})\})$

definition $U :: (\text{'a}, \text{'b}) \text{ mrel}$ **where**
 $U = \{(a, A) \mid a \in A. \text{True}\}$

abbreviation $NC \equiv U - 1_\pi$

named-theorems *mr-simp*

declare $s\text{-prod-def}$ [*mr-simp*] $p\text{-prod-def}$ [*mr-simp*] $s\text{-id-def}$ [*mr-simp*] $p\text{-id-def}$ [*mr-simp*] $U\text{-def}$ [*mr-simp*]

lemma $s\text{-prod-idl}$ [*simp*]: $1_\sigma \cdot R = R$
<proof>

lemma $s\text{-prod-idr}$ [*simp*]: $R \cdot 1_\sigma = R$
<proof>

lemma $p\text{-prod-ild}$ [*simp*]: $1_\pi \parallel R = R$
<proof>

lemma *c-prod-idr* [*simp*]: $R \parallel 1_\pi = R$
<proof>

lemma *cl7* [*simp*]: $1_\sigma \parallel 1_\sigma = 1_\sigma$
<proof>

lemma *p-prod-assoc*: $R \parallel S \parallel T = R \parallel (S \parallel T)$
<proof>

lemma *p-prod-comm*: $R \parallel S = S \parallel R$
<proof>

lemma *subidem-par*: $R \subseteq R \parallel R$
<proof>

lemma *meet-le-par*: $R \cap S \subseteq R \parallel S$
<proof>

lemma *s-prod-distr*: $(R \cup S) \cdot T = R \cdot T \cup S \cdot T$
<proof>

lemma *s-prod-sup-distr*: $(\bigcup X) \cdot S = (\bigcup R \in X. R \cdot S)$
<proof>

lemma *s-prod-subdistl*: $R \cdot S \cup R \cdot T \subseteq R \cdot (S \cup T)$
<proof>

lemma *s-prod-sup-subdistl*: $X \neq \{\} \implies (\bigcup S \in X. R \cdot S) \subseteq R \cdot \bigcup X$
<proof>

lemma *s-prod-isol*: $R \subseteq S \implies R \cdot T \subseteq S \cdot T$
<proof>

lemma *s-prod-isor*: $R \subseteq S \implies T \cdot R \subseteq T \cdot S$
<proof>

lemma *s-prod-zero* [*simp*]: $\{\} \cdot R = \{\}$
<proof>

lemma *s-prod-wzeror*: $R \cdot \{\} \subseteq R$
<proof>

lemma *p-prod-zero* [*simp*]: $R \parallel \{\} = \{\}$
<proof>

lemma *s-prod-p-idl* [*simp*]: $1_\pi \cdot R = 1_\pi$
<proof>

lemma *p-id-st*: $R \cdot 1_\pi = \{(a, \{\}) \mid a. \exists B. (a, B) \in R\}$

$\langle proof \rangle$

lemma *c6*: $R \cdot 1_\pi \subseteq 1_\pi$
 $\langle proof \rangle$

lemma *p-prod-distl*: $R \parallel (S \cup T) = R \parallel S \cup R \parallel T$
 $\langle proof \rangle$

lemma *p-prod-sup-distl*: $R \parallel (\bigcup X) = (\bigcup S \in X. R \parallel S)$
 $\langle proof \rangle$

lemma *p-prod-isol*: $R \subseteq S \implies R \parallel T \subseteq S \parallel T$
 $\langle proof \rangle$

lemma *p-prod-isor*: $R \subseteq S \implies T \parallel R \subseteq T \parallel S$
 $\langle proof \rangle$

lemma *s-prod-assoc1*: $(R \cdot S) \cdot T \subseteq R \cdot (S \cdot T)$
 $\langle proof \rangle$

lemma *seq-conc-subdistr*: $(R \parallel S) \cdot T \subseteq R \cdot T \parallel S \cdot T$
 $\langle proof \rangle$

lemma *U-U [simp]*: $U \cdot U = U$
 $\langle proof \rangle$

lemma *U-par-idem [simp]*: $U \parallel U = U$
 $\langle proof \rangle$

lemma *p-id-NC*: $R - 1_\pi = R \cap NC$
 $\langle proof \rangle$

lemma *NC-NC [simp]*: $NC \cdot NC = NC$
 $\langle proof \rangle$

lemma *nc-par-idem [simp]*: $NC \parallel NC = NC$
 $\langle proof \rangle$

lemma *cl4*:

assumes $T \parallel T \subseteq T$

shows $R \cdot T \parallel S \cdot T \subseteq (R \parallel S) \cdot T$

$\langle proof \rangle$

lemma *cl3*: $R \cdot (S \parallel T) \subseteq R \cdot S \parallel R \cdot T$
 $\langle proof \rangle$

lemma *p-id-assoc1*: $(1_\pi \cdot R) \cdot S = 1_\pi \cdot (R \cdot S)$
 $\langle proof \rangle$

lemma *p-id-assoc2*: $(R \cdot 1_\pi) \cdot T = R \cdot (1_\pi \cdot T)$
<proof>

lemma *cl1 [simp]*: $R \cdot 1_\pi \cup R \cdot NC = R \cdot U$
<proof>

lemma *tarski-aux*:
assumes $R - 1_\pi \neq \{\}$
and $(a, A) \in NC$
shows $(a, A) \in NC \cdot ((R - 1_\pi) \cdot NC)$
<proof>

lemma *tarski*:
assumes $R - 1_\pi \neq \{\}$
shows $NC \cdot ((R - 1_\pi) \cdot NC) = NC$
<proof>

lemma *tarski-var*:
assumes $R \cap NC \neq \{\}$
shows $NC \cdot ((R \cap NC) \cdot NC) = NC$
<proof>

lemma *s-le-nc*: $1_\sigma \subseteq NC$
<proof>

lemma *U-nc [simp]*: $U \cdot NC = U$
<proof>

lemma *x-y-split [simp]*: $(R \cap NC) \cdot S \cup R \cdot \{\} = R \cdot S$
<proof>

lemma *c-nc-comp1 [simp]*: $1_\pi \cup NC = U$
<proof>

3.2 Tests

lemma *s-id-st*: $R \cap 1_\sigma = \{(a, \{a\}) \mid a. (a, \{a\}) \in R\}$
<proof>

lemma *subid-aux2*:
assumes $(a, A) \in R \cap 1_\sigma$
shows $A = \{a\}$
<proof>

lemma *s-prod-test-aux1*:
assumes $(a, A) \in R \cdot (P \cap 1_\sigma)$
shows $((a, A) \in R \wedge (\forall a \in A. (a, \{a\}) \in (P \cap 1_\sigma)))$
<proof>

lemma *s-prod-test-aux2*:

assumes $(a,A) \in R$
and $\forall a \in A. (a,\{a\}) \in S$
shows $(a,A) \in R \cdot S$
<proof>

lemma *s-prod-test*: $(a,A) \in R \cdot (P \cap 1_\sigma) \iff (a,A) \in R \wedge (\forall a \in A. (a,\{a\}) \in (P \cap 1_\sigma))$
<proof>

lemma *s-prod-test-var*: $R \cdot (P \cap 1_\sigma) = \{(a,A). (a,A) \in R \wedge (\forall a \in A. (a,\{a\}) \in (P \cap 1_\sigma))\}$
<proof>

lemma *test-s-prod-aux1*:

assumes $(a,A) \in (P \cap 1_\sigma) \cdot R$
shows $(a,\{a\}) \in (P \cap 1_\sigma) \wedge (a,A) \in R$
<proof>

lemma *test-s-prod-aux2*:

assumes $(a,A) \in R$
and $(a,\{a\}) \in P$
shows $(a,A) \in P \cdot R$
<proof>

lemma *test-s-prod*: $(a,A) \in (P \cap 1_\sigma) \cdot R \iff (a,\{a\}) \in (P \cap 1_\sigma) \wedge (a,A) \in R$
<proof>

lemma *test-s-prod-var*: $(P \cap 1_\sigma) \cdot R = \{(a,A). (a,\{a\}) \in (P \cap 1_\sigma) \wedge (a,A) \in R\}$
<proof>

lemma *test-assoc1*: $(R \cdot (P \cap 1_\sigma)) \cdot S = R \cdot ((P \cap 1_\sigma) \cdot S)$
<proof>

lemma *test-assoc2*: $((P \cap 1_\sigma) \cdot R) \cdot S = (P \cap 1_\sigma) \cdot (R \cdot S)$
<proof>

lemma *test-assoc3*: $(R \cdot S) \cdot (P \cap 1_\sigma) = R \cdot (S \cdot (P \cap 1_\sigma))$
<proof>

lemma *s-distl-test*: $(P \cap 1_\sigma) \cdot (S \cup T) = (P \cap 1_\sigma) \cdot S \cup (P \cap 1_\sigma) \cdot T$
<proof>

lemma *s-distl-sup-test*: $(P \cap 1_\sigma) \cdot \bigcup X = \bigcup_{S \in X} (P \cap 1_\sigma) \cdot S$
<proof>

lemma *subid-par-idem* [*simp*]: $(P \cap 1_\sigma) \parallel (P \cap 1_\sigma) = (P \cap 1_\sigma)$
<proof>

lemma *seq-conc-subdistr*: $(P \cap 1_\sigma) \cdot (S \parallel T) = ((P \cap 1_\sigma) \cdot S) \parallel ((P \cap 1_\sigma) \cdot T)$
 ⟨proof⟩

lemma *test-s-prod-is-meet* [simp]: $(P \cap 1_\sigma) \cdot (Q \cap 1_\sigma) = P \cap Q \cap 1_\sigma$
 ⟨proof⟩

lemma *test-p-prod-is-meet* [simp]: $(P \cap 1_\sigma) \parallel (Q \cap 1_\sigma) = (P \cap 1_\sigma) \cap (Q \cap 1_\sigma)$
 ⟨proof⟩

lemma *test-multiplicativer*: $(P \cap Q \cap 1_\sigma) \cdot T = ((P \cap 1_\sigma) \cdot T) \cap ((Q \cap 1_\sigma) \cdot T)$
 ⟨proof⟩

lemma *cl9* [simp]: $(R \cap 1_\sigma) \cdot 1_\pi \parallel 1_\sigma = R \cap 1_\sigma$
 ⟨proof⟩

lemma *s-subid-closed* [simp]: $R \cap NC \cap 1_\sigma = R \cap 1_\sigma$
 ⟨proof⟩

lemma *sub-id-le-nc*: $R \cap 1_\sigma \subseteq NC$
 ⟨proof⟩

lemma *x-y-prop*: $1_\sigma \cap ((R \cap NC) \cdot S) = 1_\sigma \cap R \cdot S$
 ⟨proof⟩

lemma *s-nc-U*: $1_\sigma \cap R \cdot NC = 1_\sigma \cap R \cdot U$
 ⟨proof⟩

lemma *sid-le-nc-var*: $1_\sigma \cap R \subseteq 1_\sigma \cap (R \parallel NC)$
 ⟨proof⟩

lemma *s-nc-par-U*: $1_\sigma \cap (R \parallel NC) = 1_\sigma \cap (R \parallel U)$
 ⟨proof⟩

lemma *s-id-par-s-prod*: $(P \cap 1_\sigma) \parallel (Q \cap 1_\sigma) = (P \cap 1_\sigma) \cdot (Q \cap 1_\sigma)$
 ⟨proof⟩

3.3 Parallel subidentities

lemma *p-id-zero-st*: $R \cap 1_\pi = \{(a, \{\}) \mid a. (a, \{\}) \in R\}$
 ⟨proof⟩

lemma *p-subid-iff*: $R \subseteq 1_\pi \iff R \cdot 1_\pi = R$
 ⟨proof⟩

lemma *p-subid-iff-var*: $R \subseteq 1_\pi \iff R \cdot \{\} = R$
 ⟨proof⟩

lemma *term-par-idem* [simp]: $(R \cap 1_\pi) \parallel (R \cap 1_\pi) = (R \cap 1_\pi)$

<proof>

lemma *c1* [*simp*]: $R \cdot 1_\pi \parallel R = R$
<proof>

lemma *p-id-zero*: $R \cap 1_\pi = R \cdot \{\}$
<proof>

lemma *cl5*: $(R \cdot S) \cdot (T \cdot \{\}) = R \cdot (S \cdot (T \cdot \{\}))$
<proof>

lemma *c4*: $(R \cdot S) \cdot 1_\pi = R \cdot (S \cdot 1_\pi)$
<proof>

lemma *c3*: $(R \parallel S) \cdot 1_\pi = R \cdot 1_\pi \parallel S \cdot 1_\pi$
<proof>

lemma *p-id-idem* [*simp*]: $(R \cdot 1_\pi) \cdot 1_\pi = R \cdot 1_\pi$
<proof>

lemma *x-c-par-idem* [*simp*]: $R \cdot 1_\pi \parallel R \cdot 1_\pi = R \cdot 1_\pi$
<proof>

lemma *x-zero-le-c*: $R \cdot \{\} \subseteq 1_\pi$
<proof>

lemma *p-subid-lb1*: $R \cdot \{\} \parallel S \cdot \{\} \subseteq R \cdot \{\}$
<proof>

lemma *p-subid-lb2*: $R \cdot \{\} \parallel S \cdot \{\} \subseteq S \cdot \{\}$
<proof>

lemma *p-subid-idem* [*simp*]: $R \cdot \{\} \parallel R \cdot \{\} = R \cdot \{\}$
<proof>

lemma *p-subid-glb*: $T \cdot \{\} \subseteq R \cdot \{\} \implies T \cdot \{\} \subseteq S \cdot \{\} \implies T \cdot \{\} \subseteq (R \cdot \{\}) \parallel (S \cdot \{\})$
<proof>

lemma *p-subid-glb-iff*: $T \cdot \{\} \subseteq R \cdot \{\} \wedge T \cdot \{\} \subseteq S \cdot \{\} \iff T \cdot \{\} \subseteq (R \cdot \{\}) \parallel (S \cdot \{\})$
<proof>

lemma *x-c-glb*: $(T::('a, 'b) mrel) \cdot 1_\pi \subseteq (R::('a, 'b) mrel) \cdot 1_\pi \implies T \cdot 1_\pi \subseteq (S::('a, 'b) mrel) \cdot 1_\pi \implies T \cdot 1_\pi \subseteq (R \cdot 1_\pi) \parallel (S \cdot 1_\pi)$
<proof>

lemma *x-c-lb1*: $R \cdot 1_\pi \parallel S \cdot 1_\pi \subseteq R \cdot 1_\pi$
<proof>

lemma *x-c-lb2*: $R \cdot 1_\pi \parallel S \cdot 1_\pi \subseteq S \cdot 1_\pi$

<proof>

lemma *x-c-glb-iff*: $(T::('a,'b) \text{ mrel}) \cdot 1_\pi \subseteq (R::('a,'b) \text{ mrel}) \cdot 1_\pi \wedge T \cdot 1_\pi \subseteq (S::('a,'b) \text{ mrel}) \cdot 1_\pi \iff T \cdot 1_\pi \subseteq (R \cdot 1_\pi) \parallel (S \cdot 1_\pi)$

<proof>

lemma *nc-iff1*: $R \subseteq NC \iff R \cap 1_\pi = \{\}$

<proof>

lemma *nc-iff2*: $R \subseteq NC \iff R \cdot \{\} = \{\}$

<proof>

lemma *zero-assoc3*: $(R \cdot S) \cdot \{\} = R \cdot (S \cdot \{\})$

<proof>

lemma *x-zero-interr*: $R \cdot \{\} \parallel S \cdot \{\} = (R \parallel S) \cdot \{\}$

<proof>

lemma *p-subid-interr*: $R \cdot T \cdot 1_\pi \parallel S \cdot T \cdot 1_\pi = (R \parallel S) \cdot T \cdot 1_\pi$

<proof>

lemma *cl2* [*simp*]: $1_\pi \cap (R \cup NC) = R \cdot \{\}$

<proof>

lemma *cl6* [*simp*]: $R \cdot \{\} \cdot S = R \cdot \{\}$

<proof>

lemma *cl11* [*simp*]: $(R \cap NC) \cdot 1_\pi \parallel NC = (R \cap NC) \cdot NC$

<proof>

lemma *x-split* [*simp*]: $(R \cap NC) \cup (R \cap 1_\pi) = R$

<proof>

lemma *x-split-var* [*simp*]: $(R \cap NC) \cup R \cdot \{\} = R$

<proof>

lemma *s-x-c* [*simp*]: $1_\sigma \cap R \cdot 1_\pi = \{\}$

<proof>

lemma *s-x-zero* [*simp*]: $1_\sigma \cap R \cdot \{\} = \{\}$

<proof>

lemma *c-nc* [*simp*]: $R \cdot 1_\pi \cap NC = \{\}$

<proof>

lemma *zero-nc* [*simp*]: $R \cdot \{\} \cap NC = \{\}$

<proof>

lemma *nc-zero* [*simp*]: $(R \cap NC) \cdot \{\} = \{\}$
<proof>

lemma *c-def* [*simp*]: $U \cdot \{\} = 1_\pi$
<proof>

lemma *U-c* [*simp*]: $U \cdot 1_\pi = 1_\pi$
<proof>

lemma *nc-c* [*simp*]: $NC \cdot 1_\pi = 1_\pi$
<proof>

lemma *nc-U* [*simp*]: $NC \cdot U = U$
<proof>

lemma *x-c-nc-split* [*simp*]: $((R \cap NC) \cdot NC) \cup (R \cdot \{\} \parallel NC) = (R \cdot 1_\pi) \parallel NC$
<proof>

lemma *x-c-U-split* [*simp*]: $R \cdot U \cup (R \cdot \{\} \parallel U) = R \cdot 1_\pi \parallel U$
<proof>

lemma *p-subid-par-eq-meet* [*simp*]: $R \cdot \{\} \parallel S \cdot \{\} = R \cdot \{\} \cap S \cdot \{\}$
<proof>

lemma *p-subid-par-eq-meet-var* [*simp*]: $R \cdot 1_\pi \parallel S \cdot 1_\pi = R \cdot 1_\pi \cap S \cdot 1_\pi$
<proof>

lemma *x-zero-add-closed*: $R \cdot \{\} \cup S \cdot \{\} = (R \cup S) \cdot \{\}$
<proof>

lemma *x-zero-meet-closed*: $R \cdot \{\} \cap S \cdot \{\} = (R \cap S) \cdot \{\}$
<proof>

lemma *scomp-univalent-pres*: *univalent* $R \implies$ *univalent* $S \implies$ *univalent* $(R \cdot S)$
<proof>

lemma *univalent s-id*
<proof>

lemma *det-peleg*: *deterministic* $R \implies$ *deterministic* $S \implies$ *deterministic* $(R \cdot S)$
<proof>

lemma *deterministic-sid*: *deterministic* 1_σ
<proof>

3.4 Domain

definition *Dom* :: $('a, 'b) \text{ mrel} \implies ('a, 'a) \text{ mrel}$ **where**

$$\text{Dom } R = \{(a, \{a\}) \mid a. \exists B. (a, B) \in R\}$$

named-theorems *mrd-simp*

declare *mr-simp* [*mrd-simp*] *Dom-def* [*mrd-simp*]

lemma *d-def-expl*: $\text{Dom } R = R \cdot 1_\pi \parallel 1_\sigma$
 ⟨*proof*⟩

lemma *s-subid-iff2*: $(R \cap 1_\sigma = R) = (\text{Dom } R = R)$
 ⟨*proof*⟩

lemma *cl8-var*: $\text{Dom } R \cdot S = R \cdot 1_\pi \parallel S$
 ⟨*proof*⟩

lemma *cl8* [*simp*]: $R \cdot 1_\pi \parallel 1_\sigma \cdot S = R \cdot 1_\pi \parallel S$
 ⟨*proof*⟩

lemma *cl10-var*: $\text{Dom } (R - 1_\pi) = 1_\sigma \cap ((R - 1_\pi) \cdot NC)$
 ⟨*proof*⟩

lemma *c10*: $(R \cap NC) \cdot 1_\pi \parallel 1_\sigma = 1_\sigma \cap ((R \cap NC) \cdot NC)$
 ⟨*proof*⟩

lemma *cl9-var* [*simp*]: $\text{Dom } (R \cap 1_\sigma) = R \cap 1_\sigma$
 ⟨*proof*⟩

lemma *d-s-id* [*simp*]: $\text{Dom } R \cap 1_\sigma = \text{Dom } R$
 ⟨*proof*⟩

lemma *d-s-id-ax*: $\text{Dom } R \subseteq 1_\sigma$
 ⟨*proof*⟩

lemma *d-assoc1*: $\text{Dom } R \cdot (S \cdot T) = (\text{Dom } R \cdot S) \cdot T$
 ⟨*proof*⟩

lemma *d-meet-distr-var*: $(\text{Dom } R \cap \text{Dom } S) \cdot T = \text{Dom } R \cdot T \cap \text{Dom } S \cdot T$
 ⟨*proof*⟩

lemma *d-idem* [*simp*]: $\text{Dom } (\text{Dom } R) = \text{Dom } R$
 ⟨*proof*⟩

lemma *cd-2-var*: $\text{Dom } (R \cdot 1_\pi) \cdot S = R \cdot 1_\pi \parallel S$
 ⟨*proof*⟩

lemma *dc-prop1* [*simp*]: $\text{Dom } R \cdot 1_\pi = R \cdot 1_\pi$
 ⟨*proof*⟩

lemma *dc-prop2* [*simp*]: $\text{Dom } (R \cdot 1_\pi) = \text{Dom } R$
 ⟨*proof*⟩

lemma *ds-prop* [*simp*]: $Dom R \parallel 1_\sigma = Dom R$
<proof>

lemma *dc* [*simp*]: $Dom 1_\pi = 1_\sigma$
<proof>

lemma *cd-iso* [*simp*]: $Dom (R \cdot 1_\pi) \cdot 1_\pi = R \cdot 1_\pi$
<proof>

lemma *dc-iso* [*simp*]: $Dom (Dom R \cdot 1_\pi) = Dom R$
<proof>

lemma *d-s-id-inter* [*simp*]: $Dom R \cdot Dom S = Dom R \cap Dom S$
<proof>

lemma *d-conc6*: $Dom (R \parallel S) = Dom R \parallel Dom S$
<proof>

lemma *d-conc-inter* [*simp*]: $Dom R \parallel Dom S = Dom R \cap Dom S$
<proof>

lemma *d-conc-s-prod-ax*: $Dom R \parallel Dom S = Dom R \cdot Dom S$
<proof>

lemma *d-rest-ax* [*simp*]: $Dom R \cdot R = R$
<proof>

lemma *d-loc-ax* [*simp*]: $Dom (R \cdot Dom S) = Dom (R \cdot S)$
<proof>

lemma *assoc-p-subid*: $(R \cdot S) \cdot (T \cdot 1_\pi) = R \cdot (S \cdot (T \cdot 1_\pi))$
<proof>

lemma *d-exp-ax* [*simp*]: $Dom (Dom R \cdot S) = Dom R \cdot Dom S$
<proof>

lemma *d-comm-ax*: $Dom R \cdot Dom S = Dom S \cdot Dom R$
<proof>

lemma *d-s-id-prop* [*simp*]: $Dom 1_\sigma = 1_\sigma$
<proof>

lemma *d-s-prod-closed* [*simp*]: $Dom (Dom R \cdot Dom S) = Dom R \cdot Dom S$
<proof>

lemma *d-p-prod-closed* [*simp*]: $Dom (Dom R \parallel Dom S) = Dom R \parallel Dom S$
<proof>

lemma *d-idem2* [*simp*]: $Dom R \cdot Dom R = Dom R$
<proof>

lemma *d-assoc*: $(Dom R \cdot Dom S) \cdot Dom T = Dom R \cdot (Dom S \cdot Dom T)$
<proof>

lemma *iso-1* [*simp*]: $Dom R \cdot 1_\pi \parallel 1_\sigma = Dom R$
<proof>

lemma *d-idem-par* [*simp*]: $Dom R \parallel Dom R = Dom R$
<proof>

lemma *d-inter-r*: $Dom R \cdot (S \parallel T) = Dom R \cdot S \parallel Dom R \cdot T$
<proof>

lemma *d-add-ax*: $Dom (R \cup S) = Dom R \cup Dom S$
<proof>

lemma *d-sup-add*: $Dom (\bigcup X) = (\bigcup R \in X. Dom R)$
<proof>

lemma *d-distl*: $Dom R \cdot (S \cup T) = Dom R \cdot S \cup Dom R \cdot T$
<proof>

lemma *d-sup-distl*: $Dom R \cdot \bigcup X = (\bigcup S \in X. Dom R \cdot S)$
<proof>

lemma *d-zero-ax* [*simp*]: $Dom \{\} = \{\}$
<proof>

lemma *d-absorb1* [*simp*]: $Dom R \cup Dom R \cdot Dom S = Dom R$
<proof>

lemma *d-absorb2* [*simp*]: $Dom R \cdot (Dom R \cup Dom S) = Dom R$
<proof>

lemma *d-dist1*: $Dom R \cdot (Dom S \cup Dom T) = Dom R \cdot Dom S \cup Dom R \cdot Dom T$
<proof>

lemma *d-dist2*: $Dom R \cup (Dom S \cdot Dom T) = (Dom R \cup Dom S) \cdot (Dom R \cup Dom T)$
<proof>

lemma *d-add-prod-closed* [*simp*]: $Dom (Dom R \cup Dom S) = Dom R \cup Dom S$
<proof>

lemma *x-zero-prop*: $R \cdot \{\} \parallel S = Dom (R \cdot \{\}) \cdot S$
<proof>

lemma *cda-add-ax*: $Dom ((R \cup S) \cdot T) = Dom (R \cdot T) \cup Dom (S \cdot T)$
 ⟨proof⟩

lemma *d-x-zero*: $Dom (R \cdot \{\}) = R \cdot \{\} \parallel 1_\sigma$
 ⟨proof⟩

lemma *cda-ax2*:
assumes $(R \parallel S) \cdot Dom T = R \cdot Dom T \parallel S \cdot Dom T$
shows $Dom ((R \parallel S) \cdot T) = Dom (R \cdot T) \cdot Dom (S \cdot T)$
 ⟨proof⟩

lemma *d-lb1*: $Dom R \cdot Dom S \subseteq Dom R$
 ⟨proof⟩

lemma *d-lb2*: $Dom R \cdot Dom S \subseteq Dom S$
 ⟨proof⟩

lemma *d-glb*: $Dom T \subseteq Dom R \wedge Dom T \subseteq Dom S \implies Dom T \subseteq Dom R \cdot Dom S$
 ⟨proof⟩

lemma *d-glb-iff*: $Dom T \subseteq Dom R \wedge Dom T \subseteq Dom S \iff Dom T \subseteq Dom R \cdot Dom S$
 ⟨proof⟩

lemma *d-interr*: $R \cdot Dom P \parallel S \cdot Dom P = (R \parallel S) \cdot Dom P$
 ⟨proof⟩

lemma *cl10-d*: $Dom (R \cap NC) = 1_\sigma \cap (R \cap NC) \cdot NC$
 ⟨proof⟩

lemma *cl11-d [simp]*: $Dom (R \cap NC) \cdot NC = (R \cap NC) \cdot NC$
 ⟨proof⟩

lemma *cl10-d-var1*: $Dom (R \cap NC) = 1_\sigma \cap R \cdot NC$
 ⟨proof⟩

lemma *cl10-d-var2*: $Dom (R \cap NC) = 1_\sigma \cap (R \cap NC) \cdot U$
 ⟨proof⟩

lemma *cl10-d-var3*: $Dom (R \cap NC) = 1_\sigma \cap R \cdot U$
 ⟨proof⟩

lemma *d-U [simp]*: $Dom U = 1_\sigma$
 ⟨proof⟩

lemma *d-nc [simp]*: $Dom NC = 1_\sigma$
 ⟨proof⟩

lemma alt-d-def-nc-nc: $Dom (R \cap NC) = 1_\sigma \cap (((R \cap NC) \cdot 1_\pi) \parallel NC)$
 ⟨proof⟩

lemma alt-d-def-nc-U: $Dom (R \cap NC) = 1_\sigma \cap (((R \cap NC) \cdot 1_\pi) \parallel U)$
 ⟨proof⟩

lemma d-def-split [simp]: $Dom (R \cap NC) \cup Dom (R \cdot \{\}) = Dom R$
 ⟨proof⟩

lemma d-def-split-var [simp]: $Dom (R \cap NC) \cup ((R \cdot \{\}) \parallel 1_\sigma) = Dom R$
 ⟨proof⟩

lemma ax7 [simp]: $(1_\sigma \cap R \cdot U) \cup (R \cdot \{\}) \parallel 1_\sigma = Dom R$
 ⟨proof⟩

lemma dom12-d: $Dom R = 1_\sigma \cap (R \cdot 1_\pi \parallel NC)$
 ⟨proof⟩

lemma dom12-d-U: $Dom R = 1_\sigma \cap (R \cdot 1_\pi \parallel U)$
 ⟨proof⟩

lemma dom-def-var: $Dom R = (R \cdot U \cap 1_\pi) \parallel 1_\sigma$
 ⟨proof⟩

lemma ax5-d [simp]: $Dom (R \cap NC) \cdot U = (R \cap NC) \cdot U$
 ⟨proof⟩

lemma ax5-0 [simp]: $Dom (R \cdot \{\}) \cdot U = R \cdot \{\} \parallel U$
 ⟨proof⟩

lemma x-c-U-split2: $Dom R \cdot NC = (R \cap NC) \cdot NC \cup (R \cdot \{\}) \parallel NC$
 ⟨proof⟩

lemma x-c-U-split3: $Dom R \cdot U = (R \cap NC) \cdot U \cup (R \cdot \{\}) \parallel U$
 ⟨proof⟩

lemma x-c-U-split-d: $Dom R \cdot U = R \cdot U \cup (R \cdot \{\}) \parallel U$
 ⟨proof⟩

lemma x-U-prop2: $R \cdot NC = Dom (R \cap NC) \cdot NC \cup R \cdot \{\}$
 ⟨proof⟩

lemma x-U-prop3: $R \cdot U = Dom (R \cap NC) \cdot U \cup R \cdot \{\}$
 ⟨proof⟩

lemma d-x-nc [simp]: $Dom (R \cdot NC) = Dom R$
 ⟨proof⟩

lemma *d-x-U* [*simp*]: $\text{Dom } (R \cdot U) = \text{Dom } R$
 ⟨*proof*⟩

lemma *d-llp1*: $\text{Dom } R \subseteq \text{Dom } S \implies R \subseteq \text{Dom } S \cdot R$
 ⟨*proof*⟩

lemma *d-llp2*: $R \subseteq \text{Dom } S \cdot R \implies \text{Dom } R \subseteq \text{Dom } S$
 ⟨*proof*⟩

lemma *demod1*: $\text{Dom } (R \cdot S) \subseteq \text{Dom } T \implies R \cdot \text{Dom } S \subseteq \text{Dom } T \cdot R$
 ⟨*proof*⟩

lemma *demod2*: $R \cdot \text{Dom } S \subseteq \text{Dom } T \cdot R \implies \text{Dom } (R \cdot S) \subseteq \text{Dom } T$
 ⟨*proof*⟩

lemma *d-meet-closed* [*simp*]: $\text{Dom } (\text{Dom } x \cap \text{Dom } y) = \text{Dom } x \cap \text{Dom } y$
 ⟨*proof*⟩

lemma *d-add-var*: $\text{Dom } P \cdot R \cup \text{Dom } Q \cdot R = \text{Dom } (P \cup Q) \cdot R$
 ⟨*proof*⟩

lemma *d-interr-U*: $\text{Dom } x \cdot U \parallel \text{Dom } y \cdot U = \text{Dom } (x \parallel y) \cdot U$
 ⟨*proof*⟩

lemma *d-meet*: $\text{Dom } x \cdot z \cap \text{Dom } y \cdot z = (\text{Dom } x \cap \text{Dom } y) \cdot z$
 ⟨*proof*⟩

lemma *cs-hom-meet*: $\text{Dom } (x \cdot 1_\pi \cap y \cdot 1_\pi) = \text{Dom } (x \cdot 1_\pi) \cap \text{Dom } (y \cdot 1_\pi)$
 ⟨*proof*⟩

lemma *iso3* [*simp*]: $\text{Dom } (\text{Dom } x \cdot U) = \text{Dom } x$
 ⟨*proof*⟩

lemma *iso4* [*simp*]: $\text{Dom } (x \cdot 1_\pi \parallel U) \cdot U = x \cdot 1_\pi \parallel U$
 ⟨*proof*⟩

lemma *iso3-sharp* [*simp*]: $\text{Dom } (\text{Dom } (x \cap NC) \cdot NC) = \text{Dom } (x \cap NC)$
 ⟨*proof*⟩

lemma *iso4-sharp* [*simp*]: $\text{Dom } ((x \cap NC) \cdot NC) \cdot NC = (x \cap NC) \cdot NC$
 ⟨*proof*⟩

3.5 Vectors

lemma *vec-iff1*:

assumes $\forall a. (\exists A. (a, A) \in R) \longrightarrow (\forall A. (a, A) \in R)$

shows $R \cdot 1_\pi \parallel U = R$

⟨*proof*⟩

lemma *vec-iff2*:

assumes $R \cdot 1_\pi \parallel U = R$

shows $(\forall a. (\exists A. (a,A) \in R) \longrightarrow (\forall A. (a,A) \in R))$

<proof>

lemma *vec-iff*: $(\forall a. (\exists A. (a,A) \in R) \longrightarrow (\forall A. (a,A) \in R)) \longleftrightarrow R \cdot 1_\pi \parallel U = R$

<proof>

lemma *U-par-zero* [*simp*]: $\{\} \cdot R \parallel U = \{\}$

<proof>

lemma *U-par-s-id* [*simp*]: $1_\sigma \cdot 1_\pi \parallel U = U$

<proof>

lemma *U-par-p-id* [*simp*]: $1_\pi \cdot 1_\pi \parallel U = U$

<proof>

lemma *U-par-nc* [*simp*]: $NC \cdot 1_\pi \parallel U = U$

<proof>

3.6 Up-closure and Parikh composition

definition *s-prod-pa* :: $('a, 'b) \text{ mrel} \Rightarrow ('b, 'c) \text{ mrel} \Rightarrow ('a, 'c) \text{ mrel}$ (**infixl** $\langle \otimes \rangle$ 75)

where

$R \otimes S = \{(a,A). (\exists B. (a,B) \in R \wedge (\forall b \in B. (b,A) \in S))\}$

lemma *U-par-st*: $(a,A) \in R \parallel U \longleftrightarrow (\exists B. B \subseteq A \wedge (a,B) \in R)$

<proof>

lemma *p-id-U*: $R \parallel U = \{(a,B). \exists A. (a,A) \in R \wedge A \subseteq B\}$

<proof>

lemma *ucl-iff*: $(\forall a A B. (a,A) \in R \wedge A \subseteq B \longrightarrow (a,B) \in R) \longleftrightarrow R \parallel U = R$

<proof>

lemma *upclosed-ext*: $R \subseteq R \parallel U$

<proof>

lemma *onelem*: $R \cdot S \parallel U \subseteq R \otimes (S \parallel U)$

<proof>

lemma *twolem*: $R \otimes (S \parallel U) \subseteq R \cdot S \parallel U$

<proof>

lemma *pe-pa-sim*: $R \cdot S \parallel U = R \otimes (S \parallel U)$

<proof>

lemma *pe-pa-sim-var*: $(R \parallel U) \cdot (S \parallel U) \parallel U = (R \parallel U) \otimes (S \parallel U)$

<proof>

lemma *pa-assoc1*: $((R \parallel U) \otimes (S \parallel U)) \otimes (T \parallel U) \subseteq (R \parallel U) \otimes ((S \parallel U) \otimes (T \parallel U))$
 ⟨proof⟩

lemma *up-closed-par-is-meet*: $(R \parallel U) \parallel (S \parallel U) = (R \parallel U) \cap (S \parallel U)$
 ⟨proof⟩

lemma *U-nc-par* [simp]: $NC \parallel U = NC$
 ⟨proof⟩

lemma *uc-par-meet*: $(R \parallel U) \cap (S \parallel U) = R \parallel U \parallel S \parallel U$
 ⟨proof⟩

lemma *uc-unc* [simp]: $R \parallel U \parallel R \parallel U = R \parallel U$
 ⟨proof⟩

lemma *uc-interr*: $(R \parallel S) \cdot (T \parallel U) = R \cdot (T \parallel U) \parallel S \cdot (T \parallel U)$
 ⟨proof⟩

lemma *iso5* [simp]: $(R \cdot 1_\pi \parallel U) \cdot 1_\pi = R \cdot 1_\pi$
 ⟨proof⟩

lemma *iso6* [simp]: $(R \cdot 1_\pi \parallel U) \cdot 1_\pi \parallel U = R \cdot 1_\pi \parallel U$
 ⟨proof⟩

lemma *sv-hom-par*: $(R \parallel S) \cdot U = R \cdot U \parallel S \cdot U$
 ⟨proof⟩

lemma *vs-hom-meet*: $Dom((R \cdot 1_\pi \parallel U) \cap (S \cdot 1_\pi \parallel U)) = Dom(R \cdot 1_\pi \parallel U) \cap Dom(S \cdot 1_\pi \parallel U)$
 ⟨proof⟩

lemma *cv-hom-meet*: $(R \cdot 1_\pi \cap S \cdot 1_\pi) \parallel U = (R \cdot 1_\pi \parallel U) \cap (S \cdot 1_\pi \parallel U)$
 ⟨proof⟩

lemma *cv-hom-par* [simp]: $R \parallel U \parallel S \parallel U = (R \parallel S) \parallel U$
 ⟨proof⟩

lemma *vc-hom-meet*: $((R \cdot 1_\pi \parallel U) \cap (S \cdot 1_\pi \parallel U)) \cdot 1_\pi = ((R \cdot 1_\pi \parallel U) \cdot 1_\pi) \cap ((S \cdot 1_\pi \parallel U) \cdot 1_\pi)$
 ⟨proof⟩

lemma *vc-hom-seq*: $((R \cdot 1_\pi \parallel U) \cdot (S \cdot 1_\pi \parallel U)) \cdot 1_\pi = ((R \cdot 1_\pi \parallel U) \cdot 1_\pi) \cdot ((S \cdot 1_\pi \parallel U) \cdot 1_\pi)$
 ⟨proof⟩

3.7 Nonterminal and terminal multirelations

definition $\tau :: ('a, 'b) \text{ mrel} \Rightarrow ('a, 'b) \text{ mrel} (\langle \tau \rangle)$ **where**
 $\tau R = R \cdot \{\}$

definition $\nu :: ('a, 'b) \text{ mrel} \Rightarrow ('a, 'b) \text{ mrel} (\langle \nu \rangle)$ **where**
 $\nu R = R \cap NC$

lemma $nc\text{-s}$ [simp]: $\nu 1_\sigma = 1_\sigma$
 ⟨proof⟩

lemma $nc\text{-scomp-closed}$: $\nu R \cdot \nu S \subseteq NC$
 ⟨proof⟩

lemma $nc\text{-scomp-closed-alt}$ [simp]: $\nu (\nu R \cdot \nu S) = \nu R \cdot \nu S$
 ⟨proof⟩

lemma $nc\text{-ccomp-closed}$: $\nu R \parallel \nu S \subseteq NC$
 ⟨proof⟩

lemma $nc\text{-ccomp-closed-alt}$ [simp]: $\nu (R \parallel \nu S) = R \parallel \nu S$
 ⟨proof⟩

lemma $tarski\text{-prod}$: $(\nu R \cdot NC) \cdot (\nu S \cdot NC) = (\text{if } \nu S = \{\} \text{ then } \{\} \text{ else } \nu R \cdot NC)$
 ⟨proof⟩

lemma $nc\text{-prod-aux}$ [simp]: $(\nu R \cdot NC) \cdot NC = \nu R \cdot NC$
 ⟨proof⟩

lemma $nc\text{-vec-add-closed}$: $(\nu R \cdot NC \cup \nu S \cdot NC) \cdot NC = \nu R \cdot NC \cup \nu S \cdot NC$
 ⟨proof⟩

lemma $nc\text{-vec-par-is-meet}$: $\nu R \cdot NC \parallel \nu S \cdot NC = \nu R \cdot NC \cap \nu S \cdot NC$
 ⟨proof⟩

lemma $nc\text{-vec-meet-closed}$: $(\nu R \cdot NC \cap \nu S \cdot NC) \cdot NC = \nu R \cdot NC \cap \nu S \cdot NC$
 ⟨proof⟩

lemma $nc\text{-vec-par-closed}$: $(\nu R \cdot NC \parallel \nu S \cdot NC) \cdot NC = \nu R \cdot NC \parallel \nu S \cdot NC$
 ⟨proof⟩

lemma $nc\text{-vec-seq-closed}$: $((\nu R \cdot NC) \cdot (\nu S \cdot NC)) \cdot NC = (\nu R \cdot NC) \cdot (\nu S \cdot NC)$
 ⟨proof⟩

lemma $iso5\text{-sharp}$ [simp]: $(\nu R \cdot 1_\pi \parallel NC) \cdot 1_\pi = \nu R \cdot 1_\pi$
 ⟨proof⟩

lemma $iso6\text{-sharp}$ [simp]: $(\nu R \cdot NC \cdot 1_\pi) \parallel NC = \nu R \cdot NC$

<proof>

lemma *nsv-hom-par*: $(R \parallel S) \cdot NC = R \cdot NC \parallel S \cdot NC$
<proof>

lemma *nvs-hom-meet*: $Dom (\nu R \cdot NC \cap \nu S \cdot NC) = Dom (\nu R \cdot NC) \cap Dom (\nu S \cdot NC)$
<proof>

lemma *ncv-hom-meet*: $R \cdot 1_\pi \cap S \cdot 1_\pi \parallel NC = (R \cdot 1_\pi \parallel NC) \cap (S \cdot 1_\pi \parallel NC)$
<proof>

lemma *ncv-hom-par*: $(R \parallel S) \parallel NC = R \parallel NC \parallel S \parallel NC$
<proof>

lemma *nvc-hom-meet*: $(\nu R \cdot NC \cap \nu S \cdot NC) \cdot 1_\pi = (\nu R \cdot NC) \cdot 1_\pi \cap (\nu S \cdot NC) \cdot 1_\pi$
<proof>

lemma *tau-int*: $\tau R \leq R$
<proof>

lemma *nu-int*: $\nu R \leq R$
<proof>

lemma *tau-ret [simp]*: $\tau (\tau R) = \tau R$
<proof>

lemma *nu-ret [simp]*: $\nu (\nu R) = \nu R$
<proof>

lemma *tau-iso*: $R \leq S \implies \tau R \leq \tau S$
<proof>

lemma *nu-iso*: $R \leq S \implies \nu R \leq \nu S$
<proof>

lemma *tau-zero [simp]*: $\tau \{\} = \{\}$
<proof>

lemma *nu-zero [simp]*: $\nu \{\} = \{\}$
<proof>

lemma *tau-s [simp]*: $\tau 1_\sigma = \{\}$
<proof>

lemma *tau-c [simp]*: $\tau 1_\pi = 1_\pi$
<proof>

lemma *nu-c* [*simp*]: $\nu 1_\pi = \{\}$
<proof>

lemma *tau-nc* [*simp*]: $\tau NC = \{\}$
<proof>

lemma *nu-nc* [*simp*]: $\nu NC = NC$
<proof>

lemma *tau-U* [*simp*]: $\tau U = 1_\pi$
<proof>

lemma *nu-U* [*simp*]: $\nu U = NC$
<proof>

lemma *tau-add* [*simp*]: $\tau (R \cup S) = \tau R \cup \tau S$
<proof>

lemma *nu-add* [*simp*]: $\nu (R \cup S) = \nu R \cup \nu S$
<proof>

lemma *tau-meet* [*simp*]: $\tau (R \cap S) = \tau R \cap \tau S$
<proof>

lemma *nu-meet* [*simp*]: $\nu (R \cap S) = \nu R \cap \nu S$
<proof>

lemma *tau-seq*: $\tau (R \cdot S) = \tau R \cup \nu R \cdot \tau S$
<proof>

lemma *tau-par* [*simp*]: $\tau (R \parallel S) = \tau R \parallel \tau S$
<proof>

lemma *nu-par-aux1*: $R \parallel \tau S = \text{Dom} (\tau S) \cdot R$
<proof>

lemma *nu-par-aux3* [*simp*]: $\nu (\nu R \parallel \tau S) = \nu R \parallel \tau S$
<proof>

lemma *nu-par-aux4* [*simp*]: $\nu (\tau R \parallel \tau S) = \{\}$
<proof>

lemma *nu-par*: $\nu (R \parallel S) = \text{Dom} (\tau R) \cdot \nu S \cup \text{Dom} (\tau S) \cdot \nu R \cup (\nu R \parallel \nu S)$
<proof>

lemma *sprod-tau-nu*: $R \cdot S = \tau R \cup \nu R \cdot S$
<proof>

lemma *pprod-tau-nu*: $R \parallel S = (\nu R \parallel \nu S) \cup \text{Dom} (\tau R) \cdot \nu S \cup \text{Dom} (\tau S) \cdot \nu R$

$R \cup (\tau R \parallel \tau S)$
<proof>

lemma *tau-idem* [*simp*]: $\tau R \cdot \tau R = \tau R$
<proof>

lemma *tau-interr*: $(R \parallel S) \cdot \tau T = R \cdot \tau T \parallel S \cdot \tau T$
<proof>

lemma *tau-le-c*: $\tau R \leq 1_\pi$
<proof>

lemma *c-le-tauc*: $1_\pi \leq \tau 1_\pi$
<proof>

lemma *x-alpha-tau* [*simp*]: $\nu R \cup \tau R = R$
<proof>

lemma *alpha-tau-zero* [*simp*]: $\nu (\tau R) = \{\}$
<proof>

lemma *tau-alpha-zero* [*simp*]: $\tau (\nu R) = \{\}$
<proof>

lemma *sprod-tau-nu-var* [*simp*]: $\nu (\nu R \cdot S) = \nu (R \cdot S)$
<proof>

lemma *tau-s-prod* [*simp*]: $\tau (R \cdot S) = R \cdot \tau S$
<proof>

lemma *alpha-fp*: $\nu R = R \longleftrightarrow R \cdot \{\} = \{\}$
<proof>

lemma *p-prod-tau-alpha*: $R \parallel S = (R \parallel \nu S) \cup (\nu R \parallel S) \cup (\tau R \parallel \tau S)$
<proof>

lemma *p-prod-tau-alpha-var*: $R \parallel S = (R \parallel \nu S) \cup (\nu R \parallel S) \cup \tau (R \parallel S)$
<proof>

lemma *alpha-par*: $\nu (R \parallel S) = (\nu R \parallel S) \cup (R \parallel \nu S)$
<proof>

lemma *alpha-tau* [*simp*]: $\nu (R \cdot \tau S) = \{\}$
<proof>

lemma *nu-par-prop*: $\nu R = R \implies \nu (R \parallel S) = R \parallel S$
<proof>

lemma *tau-seq-prop*: $\tau R = R \implies R \cdot S = R$

<proof>

lemma tau-seq-prop2: $\tau R = R \implies \tau (R \cdot S) = R \cdot S$
<proof>

lemma d-nu: $\nu (Dom R \cdot S) = Dom R \cdot \nu S$
<proof>

lemma nu-ideal1: $\nu R = R \implies S \leq R \implies \nu S = S$
<proof>

lemma tau-ideal1: $\tau R = R \implies S \leq R \implies \tau S = S$
<proof>

lemma nu-ideal2: $\nu R = R \implies \nu S = S \implies \nu (R \cup S) = R \cup S$
<proof>

lemma tau-ideal2: $\tau R = R \implies \tau S = S \implies \tau (R \cup S) = R \cup S$
<proof>

lemma tau-add-precong: $\tau R \leq \tau S \implies \tau (R \cup T) \leq \tau (S \cup T)$
<proof>

lemma tau-meet-precong: $\tau R \leq \tau S \implies \tau (R \cap T) \leq \tau (S \cap T)$
<proof>

lemma tau-par-precong: $\tau R \leq \tau S \implies \tau (R \parallel T) \leq \tau (S \parallel T)$
<proof>

lemma tau-seq-precongl: $\tau R \leq \tau S \implies \tau (T \cdot R) \leq \tau (T \cdot S)$
<proof>

lemma nu-add-precong: $\nu R \leq \nu S \implies \nu (R \cup T) \leq \nu (S \cup T)$
<proof>

lemma nu-meet-precong: $\nu R \leq \nu S \implies \nu (R \cap T) \leq \nu (S \cap T)$
<proof>

lemma nu-seq-precongr: $\nu R \leq \nu S \implies \nu (R \cdot T) \leq \nu (S \cdot T)$
<proof>

definition

$$tcg R S = (\tau R \leq \tau S \wedge \tau S \leq \tau R)$$

definition

$$ncg R S = (\nu R \leq \nu S \wedge \nu S \leq \nu R)$$

lemma tcg-refl: $tcg R R$
<proof>

lemma *tcg-trans*: $tcg\ R\ S \implies tcg\ S\ T \implies tcg\ R\ T$
<proof>

lemma *tcg-sym*: $tcg\ R\ S \implies tcg\ S\ R$
<proof>

lemma *ncg-refl*: $ncg\ R\ R$
<proof>

lemma *ncg-trans*: $ncg\ R\ S \implies ncg\ S\ T \implies ncg\ R\ T$
<proof>

lemma *ncg-sym*: $ncg\ R\ S \implies ncg\ S\ R$
<proof>

lemma *tcg-alt*: $tcg\ R\ S = (\tau\ R = \tau\ S)$
<proof>

lemma *ncg-alt*: $ncg\ R\ S = (\nu\ R = \nu\ S)$
<proof>

lemma *tcg-add*: $\tau\ R = \tau\ S \implies \tau\ (R \cup T) = \tau\ (S \cup T)$
<proof>

lemma *tcg-meet*: $\tau\ R = \tau\ S \implies \tau\ (R \cap T) = \tau\ (S \cap T)$
<proof>

lemma *tcg-par*: $\tau\ R = \tau\ S \implies \tau\ (R \parallel T) = \tau\ (S \parallel T)$
<proof>

lemma *tcg-seql*: $\tau\ R = \tau\ S \implies \tau\ (T \cdot R) = \tau\ (T \cdot S)$
<proof>

lemma *ncg-add*: $\nu\ R = \nu\ S \implies \nu\ (R \cup T) = \nu\ (S \cup T)$
<proof>

lemma *ncg-meet*: $\nu\ R = \nu\ S \implies \nu\ (R \cap T) = \nu\ (S \cap T)$
<proof>

lemma *ncg-seqr*: $\nu\ R = \nu\ S \implies \nu\ (R \cdot T) = \nu\ (S \cdot T)$
<proof>

3.8 Powers

primrec *p-power* :: $('a, 'a)\ mrel \Rightarrow nat \Rightarrow ('a, 'a)\ mrel$ **where**
 $p\text{-power}\ R\ 0 = 1_\sigma \mid$
 $p\text{-power}\ R\ (Suc\ n) = R \cdot p\text{-power}\ R\ n$

primrec *power-rd* :: ('a,'a) mrel \Rightarrow nat \Rightarrow ('a,'a) mrel **where**
power-rd R 0 = {} |
power-rd R (Suc n) = $1_\sigma \cup R \cdot \text{power-rd } R \ n$

primrec *power-sq* :: ('a,'a) mrel \Rightarrow nat \Rightarrow ('a,'a) mrel **where**
power-sq R 0 = 1_σ |
power-sq R (Suc n) = $1_\sigma \cup R \cdot \text{power-sq } R \ n$

lemma *power-rd-chain*: *power-rd* R n \leq *power-rd* R (n + 1)
 <proof>

lemma *power-sq-chain*: *power-sq* R n \leq *power-sq* R (n + 1)
 <proof>

lemma *pow-chain*: *p-power* ($1_\sigma \cup R$) n \leq *p-power* ($1_\sigma \cup R$) (n + 1)
 <proof>

lemma *pow-prop*: *p-power* ($1_\sigma \cup R$) (n + 1) = $1_\sigma \cup R \cdot \text{p-power } (1_\sigma \cup R) \ n$
 <proof>

lemma *power-rd-le-sq*: *power-rd* R n \leq *power-sq* R n
 <proof>

lemma *power-sq-le-rd*: *power-sq* R n \leq *power-rd* R (Suc n)
 <proof>

lemma *power-sq-power*: *power-sq* R n = *p-power* ($1_\sigma \cup R$) n
 <proof>

3.9 Star

lemma *iso-prop*: mono ($\lambda X. S \cup R \cdot X$)
 <proof>

lemma *gfp-lfp-prop*: *gfp* ($\lambda X. R \cdot X$) \cup *lfp* ($\lambda X. S \cup R \cdot X$) \subseteq *gfp* ($\lambda X. S \cup R \cdot X$)
 <proof>

definition *star* :: ('a,'a) mrel \Rightarrow ('a,'a) mrel **where**
star R = *lfp* ($\lambda X. s\text{-id} \cup R \cdot X$)

lemma *star-unfold*: $1_\sigma \cup R \cdot \text{star } R \leq \text{star } R$
 <proof>

lemma *star-induct*: $1_\sigma \cup R \cdot S \leq S \implies \text{star } R \leq S$
 <proof>

lemma *star-refl*: $1_\sigma \leq \text{star } R$
 <proof>

lemma *star-unfold-part*: $R \cdot \text{star } R \leq \text{star } R$
 ⟨proof⟩

lemma *star-ext-aux*: $R \leq R \cdot \text{star } R$
 ⟨proof⟩

lemma *star-ext*: $R \leq \text{star } R$
 ⟨proof⟩

lemma *star-co-trans*: $\text{star } R \leq \text{star } R \cdot \text{star } R$
 ⟨proof⟩

lemma *star-iso*: $R \leq S \implies \text{star } R \leq \text{star } S$
 ⟨proof⟩

lemma *star-unfold-eq* [simp]: $1_\sigma \cup R \cdot \text{star } R = \text{star } R$
 ⟨proof⟩

lemma *nu-star1*:
 assumes $\bigwedge(R::('a, 'a) \text{ mrel}) (S::('a, 'a) \text{ mrel}) (T::('a, 'a) \text{ mrel}). R \cdot (S \cdot T) = (R \cdot S) \cdot T$
 shows $\text{star } (R::('a, 'a) \text{ mrel}) \leq \text{star } (\nu R) \cdot (1_\sigma \cup \tau R)$
 ⟨proof⟩

lemma *nu-star2*:
 assumes $\bigwedge(R::('a, 'a) \text{ mrel}). \text{star } R \cdot \text{star } R \leq \text{star } R$
 shows $\text{star } (\nu (R::('a, 'a) \text{ mrel})) \cdot (1_\sigma \cup \tau R) \leq \text{star } R$
 ⟨proof⟩

lemma *nu-star*:
 assumes $\bigwedge(R::('a, 'a) \text{ mrel}). \text{star } R \cdot \text{star } R \leq \text{star } R$
 and $\bigwedge(R::('a, 'a) \text{ mrel}) (S::('a, 'a) \text{ mrel}) (T::('a, 'a) \text{ mrel}). R \cdot (S \cdot T) = (R \cdot S) \cdot T$
 shows $\text{star } (\nu (R::('a, 'a) \text{ mrel})) \cdot (1_\sigma \cup \tau R) = \text{star } R$
 ⟨proof⟩

lemma *tau-star*: $\text{star } (\tau R) = 1_\sigma \cup \tau R$
 ⟨proof⟩

lemma *tau-star-var*:
 assumes $\bigwedge(R::('a, 'a) \text{ mrel}) (S::('a, 'a) \text{ mrel}) (T::('a, 'a) \text{ mrel}). R \cdot (S \cdot T) = (R \cdot S) \cdot T$
 and $\bigwedge(R::('a, 'a) \text{ mrel}). \text{star } R \cdot \text{star } R \leq \text{star } R$
 shows $\tau (\text{star } (R::('a, 'a) \text{ mrel})) = \text{star } (\nu R) \cdot \tau R$
 ⟨proof⟩

lemma *nu-star-sub*: $\text{star } (\nu R) \leq \nu (\text{star } R)$
 ⟨proof⟩

lemma *nu-star-nu* [simp]: $\nu (\text{star } (\nu R)) = \text{star } (\nu R)$
 ⟨proof⟩

lemma *nu-star-tau* [simp]: $\nu (\text{star } (\tau R)) = 1_\sigma$
 ⟨proof⟩

lemma *tau-star-tau* [simp]: $\tau (\text{star } (\tau R)) = \tau R$
 ⟨proof⟩

lemma *tau-star-nu* [simp]: $\tau (\text{star } (\nu R)) = \{\}$
 ⟨proof⟩

lemma *d-star-unfold* [simp]: $\text{Dom } S \cup \text{Dom } (R \cdot \text{Dom } (\text{star } R \cdot S)) = \text{Dom } (\text{star } R \cdot S)$
 ⟨proof⟩

lemma *d-star-sim1*:

assumes $\bigwedge R S T. \text{Dom } (T::('a,'b) \text{ mrel}) \cup (R::('a,'a) \text{ mrel}) \cdot (S::('a,'a) \text{ mrel})$
 $\leq S \implies \text{star } R \cdot \text{Dom } T \leq S$
shows $(R::('a,'a) \text{ mrel}) \cdot \text{Dom } (T::('a,'b) \text{ mrel}) \leq \text{Dom } T \cdot (S::('a,'a) \text{ mrel})$
 $\implies \text{star } R \cdot \text{Dom } T \leq \text{Dom } T \cdot \text{star } S$
 ⟨proof⟩

lemma *d-star-induct*:

assumes $\bigwedge R S T. \text{Dom } (T::('a,'b) \text{ mrel}) \cup (R::('a,'a) \text{ mrel}) \cdot (S::('a,'a) \text{ mrel})$
 $\leq S \implies \text{star } R \cdot \text{Dom } T \leq S$
shows $\text{Dom } ((R::('a,'a) \text{ mrel}) \cdot (S::('a,'a) \text{ mrel})) \leq \text{Dom } S \implies \text{Dom } (\text{star } R \cdot S) \leq \text{Dom } S$
 ⟨proof⟩

3.10 Omega

definition *omega* :: $('a,'a) \text{ mrel} \Rightarrow ('a,'a) \text{ mrel}$ **where**
 $\text{omega } R \equiv \text{gfp } (\lambda X. R \cdot X)$

lemma *om-unfold*: $\text{omega } R \leq R \cdot \text{omega } R$
 ⟨proof⟩

lemma *om-coinduct*: $S \leq R \cdot S \implies S \leq \text{omega } R$
 ⟨proof⟩

lemma *om-unfold-eq* [simp]: $R \cdot \text{omega } R = \text{omega } R$
 ⟨proof⟩

lemma *om-iso*: $R \leq S \implies \text{omega } R \leq \text{omega } S$
 ⟨proof⟩

lemma *zero-om* [simp]: $\text{omega } \{\} = \{\}$

<proof>

lemma *s-id-om* [*simp*]: $\text{omega } 1_\sigma = U$
<proof>

lemma *p-id-om* [*simp*]: $\text{omega } 1_\pi = 1_\pi$
<proof>

lemma *nc-om* [*simp*]: $\text{omega } NC = U$
<proof>

lemma *U-om* [*simp*]: $\text{omega } U = U$
<proof>

lemma *tau-om1*: $\tau R \leq \tau (\text{omega } R)$
<proof>

lemma *tau-om2* [*simp*]: $\text{omega } (\tau R) = \tau R$
<proof>

lemma *tau-om3*: $\text{omega } (\tau R) \leq \tau (\text{omega } R)$
<proof>

lemma *om-nu-tau*: $\text{omega } (\nu R) \cup \text{star } (\nu R) \cdot \tau R \leq \text{omega } R$
<proof>

end

4 Multirelational Properties of Power Allegories

theory *Power-Allegories-Multirelations*

imports *Multirelations-Basics*

begin

We start with random little properties.

lemma *eta-s-id*: $\eta = s\text{-id}$
<proof>

lemma *Lambda-empty* [*simp*]: $\Lambda \{\} = p\text{-id}$
<proof>

lemma *alpha-pid* [*simp*]: $\alpha p\text{-id} = \{\}$
<proof>

4.1 Peleg lifting

definition *plift* :: $(\text{'a}, \text{'b}) \text{ mrel} \Rightarrow (\text{'a set}, \text{'b set}) \text{ rel } (\text{<-_*>} [1000] 999)$ **where**

$$R_* = \{(A,B). \exists f. (\forall a \in A. (a, f(a)) \in R) \wedge B = \bigcup (f \text{ ` } A)\}$$

lemma *pcomp-pltft*: $R \cdot S = R ; S_*$
 ⟨proof⟩

lemma *det-pltft-klift*: *deterministic* $R \implies R_* = (R)_{\mathcal{P}}$
 ⟨proof⟩

lemma *pltft-ext2* [*simp*]: $\eta ; R_* = R$
 ⟨proof⟩

lemma *pltftext-3* [*simp*]: $\eta_* = Id$
 ⟨proof⟩

lemma *d-dom-pltft*: $(Dom R)_* = dom (R_*)$
 ⟨proof⟩

lemma *d-pid-pltft*: $(Dom R)_* \subseteq Id$
 ⟨proof⟩

lemma *d-pltft-sub*: $A \subseteq B \implies (B,B) \in (Dom R)_* \implies (A,A) \in (Dom R)_*$
 ⟨proof⟩

lemma *pltft-empty*: $(\{\}, A) \in R_* \longleftrightarrow A = \{\}$
 ⟨proof⟩

lemma *univ-pltft-klift*:
assumes *univalent* R
shows $R_* = (Dom R)_* ; (R)_{\mathcal{P}}$
 ⟨proof⟩

lemma *pltft-ext1*:
assumes *univalent* f
shows $(R ; f_*)_* = R_* ; f_*$
 ⟨proof⟩

lemma *pltft-assoc-univ*: *univalent* $f \implies (R \cdot S) \cdot f = R \cdot (S \cdot f)$
 ⟨proof⟩

lemma *Lambda-funct*: $\Lambda (R ; S) = \Lambda R \cdot \Lambda S$
 ⟨proof⟩

lemma *eta-funct*: $R ; S ; \eta = (R ; \eta) \cdot (S ; \eta)$
 ⟨proof⟩

lemma *alpha-funct-det*: *deterministic* $R \implies$ *deterministic* $S \implies \alpha (R \cdot S) = \alpha R ; \alpha S$
 ⟨proof⟩

lemma *pcomp-det*: *deterministic* $S \implies R \cdot S = R ; (S)_{\mathcal{P}}$
 ⟨proof⟩

lemma *pcomp-det2*: *deterministic* $R \implies$ *deterministic* $S \implies (R \cdot S)_{\mathcal{P}} = (R)_{\mathcal{P}} ; (S)_{\mathcal{P}}$
 ⟨proof⟩

lemma *pcomp-alpha*: $\alpha (R \cdot S) = R ; \alpha ((S)_*)$
 ⟨proof⟩

4.2 Fusion and fission

definition *fus* :: $('a, 'b) \text{ mrel} \Rightarrow ('a, 'b) \text{ mrel}$ **where**
 $fus R = \Lambda (\alpha R)$

definition *fis* :: $('a, 'b) \text{ mrel} \Rightarrow ('a, 'b) \text{ mrel}$ **where**
 $fis R = \alpha R ; \eta$

lemma *fus-set*: $fus R = \{(a, B) \mid a B. B = \bigcup (\text{Image } R \{a\})\}$
 ⟨proof⟩

lemma *fis-set*: $fis R = \{(a, \{b\}) \mid a b. b \in \bigcup (\text{Image } R \{a\})\}$
 ⟨proof⟩

lemma *fis-det-comp*: *deterministic* $R \implies$ *deterministic* $S \implies fis (R \cdot S) = fis R \cdot fis S$
 ⟨proof⟩

lemma *fis-fix-det*: *deterministic* $R = (fus R = R)$
 ⟨proof⟩

4.3 Galois connections for multirelations

lemma *sub-subh*: $R \subseteq S \implies R \subseteq S ; (\text{epsiloff} \parallel \text{epsiloff})$
 ⟨proof⟩

lemma *alpha-Lambda-galois*: $(\alpha R \subseteq S) = (R \subseteq \Lambda S ; (\text{epsiloff} \parallel \text{epsiloff}))$
 ⟨proof⟩

lemma *alpha-Lambda-galois-set*: $(\alpha R \subseteq S) = (R \subseteq \{(a, A). \exists B. (a, B) \in \Lambda S \wedge A \subseteq B\})$
 ⟨proof⟩

lemma *epsiloff-eta-lres*: $\text{epsiloff} ; \eta \subseteq \text{epsiloff} \parallel \text{epsiloff}$
 ⟨proof⟩

lemma *eta-alpha-galois*: $(R ; \eta \subseteq S ; (\text{epsiloff} \parallel \text{epsiloff})) = (R \subseteq \alpha S)$
 ⟨proof⟩

lemma *eta-alpha-galois-set*: $(R ; \eta \subseteq \{(a,A). \exists B. (a,B) \in S \wedge A \subseteq B\}) = (R \subseteq \alpha S)$

<proof>

lemma *Lambda-iso*: $R \subseteq S \implies \Lambda R \subseteq \Lambda S ; (\text{epsiloff} \parallel \text{epsiloff})$

<proof>

lemma *eta-iso*: $R \subseteq S \implies R ; \eta \subseteq S ; \eta ; (\text{epsiloff} \parallel \text{epsiloff})$

<proof>

lemma *alpha-iso*: $R \subseteq S ; (\text{epsiloff} \parallel \text{epsiloff}) \implies \alpha R \subseteq \alpha S$

<proof>

lemma *Lambda-canc-dcl*: $R \subseteq \Lambda (\alpha R) ; (\text{epsiloff} \parallel \text{epsiloff})$

<proof>

lemma *eta-canc-dcl*: $\alpha R ; \eta \subseteq R ; (\text{epsiloff} \parallel \text{epsiloff})$

<proof>

lemma *alpha-surj*: *surj* α

<proof>

lemma *Lambda-inj*: *inj* Λ

<proof>

lemma *eta-inj*: *inj* $(\lambda x. x ; \eta)$

<proof>

lemma *fus-least-odet*:

assumes $\Lambda (\alpha S) = S$

and $R \subseteq S ; (\text{epsiloff} \parallel \text{epsiloff})$

shows $\Lambda (\alpha R) \subseteq S ; (\text{epsiloff} \parallel \text{epsiloff})$

<proof>

lemma *fis-greatest-idet*:

assumes $\alpha S ; \eta = S$

and $S \subseteq R ; (\text{epsiloff} \parallel \text{epsiloff})$

shows $S \subseteq \alpha R ; \eta ; (\text{epsiloff} \parallel \text{epsiloff})$

<proof>

lemma *fis-fus-galois*: $(\alpha R ; \eta \subseteq S ; (\text{epsiloff} \parallel \text{epsiloff})) = (R \subseteq \Lambda (\alpha S) ;$

$(\text{epsiloff} \parallel \text{epsiloff}))$

<proof>

4.4 Properties of alpha, fission and fusion

lemma *alpha-lax*: $\alpha (R \cdot S) \subseteq \alpha R ; \alpha S$

<proof>

lemma *alpha-down* [*simp*]: $\alpha (R ; \Omega^\smile) = \alpha R$
 ⟨*proof*⟩

lemma *fis-fis* [*simp*]: $fis \circ fis = fis$
 ⟨*proof*⟩

lemma *fus-fus* [*simp*]: $fus \circ fus = fus$
 ⟨*proof*⟩

lemma *fis-fus* [*simp*]: $fis \circ fus = fis$
 ⟨*proof*⟩

lemma *fus-fis* [*simp*]: $fus \circ fis = fus$
 ⟨*proof*⟩

lemma *fis-alpha*: $fis R \cdot S = \alpha R ; S$
 ⟨*proof*⟩

lemma *fis-lax*: $fis (R \cdot S) \subseteq fis R \cdot fis S$
 ⟨*proof*⟩

lemma *klift-fus*: $(R)_{\mathcal{P}} = fus (epsilon\text{loff} ; R)$
 ⟨*proof*⟩

lemma *fus-eta-klift*: $fus R = \eta ; (R)_{\mathcal{P}}$
 ⟨*proof*⟩

lemma *fus-Lambda-mu*: $fus R = \Lambda R ; \mu$
 ⟨*proof*⟩

4.5 Properties of fusion, fission, nu and tau

lemma *alpha-tau* [*simp*]: $\alpha (\tau R) = \{\}$
 ⟨*proof*⟩

lemma *alpha-nu* [*simp*]: $\alpha (\nu R) = \alpha R$
 ⟨*proof*⟩

lemma *nu-fis* [*simp*]: $\nu (fis R) = fis R$
 ⟨*proof*⟩

lemma *nu-fis-var*: $\nu (fis R) = fis (\nu R)$
 ⟨*proof*⟩

lemma *tau-fis* [*simp*]: $\tau (fis R) = \{\}$
 ⟨*proof*⟩

Properties of tests and domain

lemma *subid-plit*: $(P \cap \eta)_* = \{(A, A) \mid A. \forall a \in A. (a, \{a\}) \in (P \cap \eta)\}$
 ⟨*proof*⟩

lemma *U-subid*: $R ; (P \cap \eta)_* = R \cap U ; (P \cap \eta)_*$
 ⟨proof⟩

lemma *subid-plift-down*: $U ; (P \cap \eta)_* ; \Omega^\smile = U ; (P \cap \eta)_*$
 ⟨proof⟩

lemma *nu-subid-plift*: $\nu (R ; (P \cap \eta)_*) = \nu R ; (P \cap \eta)_*$
 ⟨proof⟩

lemma *dom-fis1*: $\text{dom} (fis R) = \text{dom} (\alpha R)$
 ⟨proof⟩

lemma *dom-fis2*: $\text{dom} (fis R) = \text{dom} (\alpha (\nu R))$
 ⟨proof⟩

lemma *dom-fis3*: $\text{dom} (fis R) = \text{dom} (\nu R)$
 ⟨proof⟩

lemma *dom-fis4*: $\text{dom} (fis R) = \text{dom} (\nu (fus R))$
 ⟨proof⟩

lemma *dom-alpha*: $\text{dom} (\alpha R ; (P \cap \eta)) = \text{dom} (\nu (R ; \Omega^\smile) ; (P \cap \eta)_*)$
 ⟨proof⟩

4.6 Box and diamond

definition *box* :: ('a, 'b) mrel \Rightarrow ('b set, 'a set) rel **where**
 $box R = rbox (\alpha R)$

definition *dia* :: ('a, 'b) mrel \Rightarrow ('b set, 'a set) rel **where**
 $dia R = \mathcal{P} ((\alpha R)^\smile)$

lemma *box-set*: $box R = \{(B, A). A = \{a. \forall C. (a, C) \in R \longrightarrow C \subseteq B\}\}$
 ⟨proof⟩

lemma *dia-set*: $dia R = \{(B, A). A = \{a. \exists C. (a, C) \in R \wedge C \cap B \neq \{\}\}\}$
 ⟨proof⟩

lemma *box-Omega*: $box R = \Lambda (\Omega^\smile // R)$
 ⟨proof⟩

end

theory *Multirelations*

imports *Power-Allegories-Multirelations*

begin

lemma *nonempty-set-card*:
assumes *finite S*
shows $S \neq \{\}$ \longleftrightarrow $\text{card } S \geq 1$
 $\langle \text{proof} \rangle$

no-notation *one-class.one* $\langle 1 \rangle$
no-notation *times-class.times* (**infixl** $\langle * \rangle$ 70)

no-notation *rel-fdia* $\langle (| -) \rangle$ [61,81] 82)
no-notation *rel-bdia* $\langle (\langle - | - \rangle) \rangle$ [61,81] 82)
no-notation *rel-fbox* $\langle (| -] \rangle$ [61,81] 82)
no-notation *rel-bbox* $\langle ([- | \rangle) \rangle$ [61,81] 82)

declare *s-prod-pa-def* [*mr-simp*]

notation *s-prod* (**infixl** $\langle * \rangle$ 70)
notation *s-id* $\langle 1 \rangle$

lemma *sp-oi-subdist*:
 $(P \cap Q) * (R \cap S) \subseteq P * R$
 $\langle \text{proof} \rangle$

lemma *sp-oi-subdist-2*:
 $(P \cap Q) * (R \cap S) \subseteq (P * R) \cap (Q * S)$
 $\langle \text{proof} \rangle$

5 Inner Structure

5.1 Inner union, inner intersection and inner complement

abbreviation *inner-union* (**infixl** $\langle \cup \cup \rangle$ 65)
where *inner-union* \equiv *p-prod*

definition *inner-intersection* $:: ('a, 'b) \text{ mrel} \Rightarrow ('a, 'b) \text{ mrel} \Rightarrow ('a, 'b) \text{ mrel}$ (**infixl** $\langle \cap \cap \rangle$ 65) **where**
 $R \cap \cap S \equiv \{ (a, B) . \exists C D . B = C \cap D \wedge (a, C) \in R \wedge (a, D) \in S \}$

definition *inner-complement* $:: ('a, 'b) \text{ mrel} \Rightarrow ('a, 'b) \text{ mrel}$ ($\langle \sim \rightarrow$ [80] 80) **where**
 $\sim R \equiv \{ (a, B) . (a, -B) \in R \}$

abbreviation *iu-unit* $\langle 1_{\cup \cup} \rangle$
where $1_{\cup \cup} \equiv$ *p-id*

definition *ii-unit* $:: ('a, 'a) \text{ mrel}$ $\langle 1_{\cap \cap} \rangle$
where $1_{\cap \cap} \equiv \{ (a, UNIV) \mid a . \text{True} \}$

declare *inner-intersection-def* [*mr-simp*] *inner-complement-def* [*mr-simp*]
ii-unit-def [*mr-simp*]

lemma *iu-assoc*:
 $(R \cup S) \cup T = R \cup (S \cup T)$
<proof>

lemma *iu-commute*:
 $R \cup S = S \cup R$
<proof>

lemma *iu-unit*:
 $R \cup 1_{\cup} = R$
<proof>

lemma *ii-assoc*:
 $(R \cap S) \cap T = R \cap (S \cap T)$
<proof>

lemma *ii-commute*:
 $R \cap S = S \cap R$
<proof>

lemma *ii-unit [simp]*:
 $R \cap 1_{\cap} = R$
<proof>

lemma *pa-ic*:
 $\sim(R \otimes \sim S) = R \otimes S$
<proof>

lemma *ic-involutive [simp]*:
 $\sim\sim R = R$
<proof>

lemma *ic-injective*:
 $\sim R = \sim S \implies R = S$
<proof>

lemma *ic-antidist-iu*:
 $\sim(R \cup S) = \sim R \cap \sim S$
<proof>

lemma *ic-antidist-ii*:
 $\sim(R \cap S) = \sim R \cup \sim S$
<proof>

lemma *ic-iu-unit [simp]*:
 $\sim 1_{\cup} = 1_{\cap}$
<proof>

lemma *ic-ii-unit [simp]*:

$$\sim 1 \cap \cap = 1 \cup \cup$$

<proof>

lemma *ii-unit-split-iu* [simp]:

$$1 \cup \cup \sim 1 = 1 \cap \cap$$

<proof>

lemma *aux-1*:

$$B = \{a\} \cap D \implies \neg D = \{a\} \implies B = \{\}$$

<proof>

lemma *iu-unit-split-ii* [simp]:

$$1 \cap \cap \sim 1 = 1 \cup \cup$$

<proof>

lemma *iu-right-dist-ou*:

$$(R \cup S) \cup \cup T = (R \cup \cup T) \cup (S \cup \cup T)$$

<proof>

lemma *ii-right-dist-ou*:

$$(R \cup S) \cap \cap T = (R \cap \cap T) \cup (S \cap \cap T)$$

<proof>

lemma *iu-left-isotone*:

$$R \subseteq S \implies R \cup \cup T \subseteq S \cup \cup T$$

<proof>

lemma *iu-right-isotone*:

$$R \subseteq S \implies T \cup \cup R \subseteq T \cup \cup S$$

<proof>

lemma *iu-isotone*:

$$R \subseteq S \implies P \subseteq Q \implies R \cup \cup P \subseteq S \cup \cup Q$$

<proof>

lemma *ii-left-isotone*:

$$R \subseteq S \implies R \cap \cap T \subseteq S \cap \cap T$$

<proof>

lemma *ii-right-isotone*:

$$R \subseteq S \implies T \cap \cap R \subseteq T \cap \cap S$$

<proof>

lemma *ii-isotone*:

$$R \subseteq S \implies P \subseteq Q \implies R \cap \cap P \subseteq S \cap \cap Q$$

<proof>

lemma *iu-right-subdist-ii*:

$$(R \cap \cap S) \cup \cup T \subseteq (R \cup \cup T) \cap \cap (S \cup \cup T)$$

$\langle proof \rangle$

lemma *ii-right-subdist-iu*:

$$(R \cup\cup S) \cap\cap T \subseteq (R \cap\cap T) \cup\cup (S \cap\cap T)$$

$\langle proof \rangle$

lemma *ic-isotone*:

$$R \subseteq S \implies \sim R \subseteq \sim S$$

$\langle proof \rangle$

lemma *ic-bot* [*simp*]:

$$\sim\{\} = \{\}$$

$\langle proof \rangle$

lemma *ic-top* [*simp*]:

$$\sim U = U$$

$\langle proof \rangle$

lemma *ic-dist-ou*:

$$\sim(R \cup S) = \sim R \cup \sim S$$

$\langle proof \rangle$

lemma *ic-dist-oi*:

$$\sim(R \cap S) = \sim R \cap \sim S$$

$\langle proof \rangle$

lemma *ic-dist-oc*:

$$\sim\sim R = \sim(\sim R)$$

$\langle proof \rangle$

lemma *ii-sub-idempotent*:

$$R \subseteq R \cap\cap R$$

$\langle proof \rangle$

definition *inner-Union* :: ($'i \Rightarrow ('a, 'b) \text{ mrel} \Rightarrow 'i \text{ set} \Rightarrow ('a, 'b) \text{ mrel} \langle \cup\cup \text{-} \rangle$)
[80,80] 80) **where**

$$\cup\cup X|I \equiv \{ (a, B) . \exists f . B = (\cup i \in I . f i) \wedge (\forall i \in I . (a, f i) \in X i) \}$$

definition *inner-Intersection* :: ($'i \Rightarrow ('a, 'b) \text{ mrel} \Rightarrow 'i \text{ set} \Rightarrow ('a, 'b) \text{ mrel} \langle \cap\cap \text{-} \rangle$)
[80,80] 80) **where**

$$\cap\cap X|I \equiv \{ (a, B) . \exists f . B = (\cap i \in I . f i) \wedge (\forall i \in I . (a, f i) \in X i) \}$$

declare *inner-Union-def* [*mr-simp*] *inner-Intersection-def* [*mr-simp*]

lemma *iU-empty*:

$$\cup\cup X|\{\} = 1_{\cup\cup}$$

$\langle proof \rangle$

lemma *iI-empty*:

$$\bigcap \bigcap X|\{\} = 1_{\cap\cap}$$

<proof>

lemma *ic-antidist-iU*:

$$\sim \bigcup \bigcup X|I = \bigcap \bigcap (\text{inner-complement o } X)|I$$

<proof>

lemma *ic-antidist-iI*:

$$\sim \bigcap \bigcap X|I = \bigcup \bigcup (\text{inner-complement o } X)|I$$

<proof>

lemma *iu-right-dist-oU*:

$$\bigcup X \cup\cup T = (\bigcup R \in X . R \cup\cup T)$$

<proof>

lemma *ii-right-dist-oU*:

$$\bigcup X \cap\cap T = (\bigcup R \in X . R \cap\cap T)$$

<proof>

lemma *iu-right-subdist-iI*:

$$\bigcap \bigcap X|I \cup\cup T \subseteq \bigcap \bigcap (\lambda i . X i \cup\cup T)|I$$

<proof>

lemma *ii-right-subdist-iU*:

$$\bigcup \bigcup X|I \cap\cap T \subseteq \bigcup \bigcup (\lambda i . X i \cap\cap T)|I$$

<proof>

lemma *ic-dist-oU*:

$$\sim \bigcup X = \bigcup (\text{inner-complement ' } X)$$

<proof>

lemma *ic-dist-oI*:

$$\sim \bigcap X = \bigcap (\text{inner-complement ' } X)$$

<proof>

lemma *sp-left-subdist-iU*:

$$R * (\bigcup \bigcup X|I) \subseteq \bigcup \bigcup (\lambda i . R * X i)|I$$

<proof>

lemma *sp-right-subdist-iU*:

$$(\bigcup \bigcup X|I) * R \subseteq \bigcup \bigcup (\lambda i . X i * R)|I$$

<proof>

lemma *sp-right-dist-iU*:

assumes $\forall J::'a \text{ set} . J \neq \{\} \longrightarrow (\bigcup \bigcup (\lambda j . R)|J) \subseteq R$
shows $(\bigcup \bigcup X|I) * R = \bigcup \bigcup (\lambda i . X i * R)|(I::'a \text{ set})$
<proof>

5.2 Dual

abbreviation $dual :: ('a, 'b) mrel \Rightarrow ('a, 'b) mrel \langle \cdot^d \rangle [100] 100$
where $R^d \equiv \sim -R$

lemma $dual$:

$$R^d = \{ (a, B) . (a, -B) \notin R \}$$

$\langle proof \rangle$

declare $dual$ [$mr-simp$]

lemma $dual-antitone$:

$$R \subseteq S \Longrightarrow S^d \subseteq R^d$$

$\langle proof \rangle$

lemma $ic-oc-dual$:

$$\sim R = -R^d$$

$\langle proof \rangle$

lemma $dual-involutive$ [$simp$]:

$$R^{dd} = R$$

$\langle proof \rangle$

lemma $dual-antidist-ou$:

$$(R \cup S)^d = R^d \cap S^d$$

$\langle proof \rangle$

lemma $dual-antidist-oi$:

$$(R \cap S)^d = R^d \cup S^d$$

$\langle proof \rangle$

lemma $dual-dist-oc$:

$$(-R)^d = -R^d$$

$\langle proof \rangle$

lemma $dual-dist-ic$:

$$(\sim R)^d = \sim R^d$$

$\langle proof \rangle$

lemma $dual-antidist-oU$:

$$(\bigcup X)^d = \bigcap (dual \cdot X)$$

$\langle proof \rangle$

lemma $dual-antidist-oI$:

$$(\bigcap X)^d = \bigcup (dual \cdot X)$$

$\langle proof \rangle$

5.3 Co-composition

definition *co-prod* :: ('a,'b) mrel \Rightarrow ('b,'c) mrel \Rightarrow ('a,'c) mrel (**infixl** \odot 70)

where

$$R \odot S \equiv \{ (a,C) . \exists B . (a,B) \in R \wedge (\exists f . (\forall b \in B . (b,f b) \in S) \wedge C = \bigcap \{ f b \mid b . b \in B \}) \}$$

lemma *co-prod-im*:

$$R \odot S = \{ (a,C) . \exists B . (a,B) \in R \wedge (\exists f . (\forall b \in B . (b,f b) \in S) \wedge C = \bigcap ((\lambda x . f x) ` B)) \}$$

<proof>

lemma *co-prod-iff*:

$$(a,C) \in (R \odot S) \iff (\exists B . (a,B) \in R \wedge (\exists f . (\forall b \in B . (b,f b) \in S) \wedge C = \bigcap \{ f b \mid b . b \in B \}))$$

<proof>

declare *co-prod-im* [*mr-simp*]

lemma *co-prod*:

$$R \odot S = \sim(R * \sim S)$$

<proof>

lemma *cp-left-isotone*:

$$R \subseteq S \implies R \odot T \subseteq S \odot T$$

<proof>

lemma *cp-right-isotone*:

$$R \subseteq S \implies T \odot R \subseteq T \odot S$$

<proof>

lemma *cp-isotone*:

$$R \subseteq S \implies P \subseteq Q \implies R \odot P \subseteq S \odot Q$$

<proof>

lemma *ic-dist-cp*:

$$\sim(R \odot S) = R * \sim S$$

<proof>

lemma *ic-dist-sp*:

$$\sim(R * S) = R \odot \sim S$$

<proof>

lemma *ic-cp-ic-unit*:

$$\sim R = R \odot \sim 1$$

<proof>

lemma *cp-left-zero* [*simp*]:

$$\{\} \odot R = \{\}$$

<proof>

lemma *cp-left-unit* [*simp*]:

$$1 \odot R = R$$

<proof>

lemma *cp-ic-unit* [*simp*]:

$$\sim 1 \odot \sim 1 = 1$$

<proof>

lemma *cp-right-dist-ou*:

$$(R \cup S) \odot T = (R \odot T) \cup (S \odot T)$$

<proof>

lemma *cp-left-iu-unit* [*simp*]:

$$1_{\cup\cup} \odot R = 1_{\cap\cap}$$

<proof>

lemma *cp-right-ii-unit*:

$$R \odot 1_{\cap\cap} \subseteq R \cup\cup \sim R$$

<proof>

lemma *sp-right-iu-unit*:

$$R * 1_{\cup\cup} \subseteq R \cap\cap \sim R$$

<proof>

lemma *cp-left-subdist-ii*:

$$R \odot (S \cap\cap T) \subseteq (R \odot S) \cap\cap (R \odot T)$$

<proof>

lemma *cp-right-subantidist-iu*:

$$(R \cup\cup S) \odot T \subseteq (R \odot T) \cap\cap (S \odot T)$$

<proof>

lemma *cp-right-antidist-iu*:

assumes $T \cap\cap T \subseteq T$

shows $(R \cup\cup S) \odot T = (R \odot T) \cap\cap (S \odot T)$

<proof>

lemma *cp-right-dist-oU*:

$$\bigcup X \odot T = \bigcup_{R \in X} R \odot T$$

<proof>

lemma *cp-left-subdist-iI*:

$$R \odot (\bigcap \bigcap X | I) \subseteq \bigcap \bigcap (\lambda i . R \odot X i) | I$$

<proof>

lemma *cp-right-subantidist-iU*:

$$(\bigcup \bigcup X | I) \odot R \subseteq \bigcap \bigcap (\lambda i . X i \odot R) | I$$

<proof>

lemma *cp-right-antidist-iU*:
assumes $\forall J :: 'a \text{ set} . J \neq \{\}$ $\longrightarrow (\bigcap (\lambda j . R)|J) \subseteq R$
shows $(\bigcup X|I) \odot R = \bigcap (\lambda i . X i \odot R)|(I :: 'a \text{ set})$
<proof>

5.4 Inner order

definition *inner-order-iu* :: $'a \times 'b \text{ set} \Rightarrow 'a \times 'b \text{ set} \Rightarrow \text{bool}$ (**infix** $\langle \preceq_{\cup\cup} \rangle$ 50)

where

$$x \preceq_{\cup\cup} y \equiv \text{fst } x = \text{fst } y \wedge \text{snd } x \subseteq \text{snd } y$$

definition *inner-order-ii* :: $'a \times 'b \text{ set} \Rightarrow 'a \times 'b \text{ set} \Rightarrow \text{bool}$ (**infix** $\langle \preceq_{\cap\cap} \rangle$ 50)

where

$$x \preceq_{\cap\cap} y \equiv \text{fst } x = \text{fst } y \wedge \text{snd } x \supseteq \text{snd } y$$

lemma *inner-order-dual*:

$$x \preceq_{\cup\cup} y \longleftrightarrow y \preceq_{\cap\cap} x$$

<proof>

interpretation *inner-order-iu*: *order* $(\preceq_{\cup\cup}) \lambda x y . x \preceq_{\cup\cup} y \wedge x \neq y$

<proof>

5.5 Up-closure, down-closure and convex-closure

abbreviation *up* :: $('a, 'b) \text{ mrel} \Rightarrow ('a, 'b) \text{ mrel}$ $(\langle \uparrow \rangle [100] 100)$

where $R \uparrow \equiv R \cup\cup U$

abbreviation *down* :: $('a, 'b) \text{ mrel} \Rightarrow ('a, 'b) \text{ mrel}$ $(\langle \downarrow \rangle [100] 100)$

where $R \downarrow \equiv R \cap\cap U$

abbreviation *convex* :: $('a, 'b) \text{ mrel} \Rightarrow ('a, 'b) \text{ mrel}$ $(\langle \updownarrow \rangle [100] 100)$

where $R \updownarrow \equiv R \uparrow \cap R \downarrow$

lemma *up*:

$$R \uparrow = \{ (a, B) . \exists C . (a, C) \in R \wedge C \subseteq B \}$$

<proof>

lemma *down*:

$$R \downarrow = \{ (a, B) . \exists C . (a, C) \in R \wedge B \subseteq C \}$$

<proof>

lemma *convex*:

$$R \updownarrow = \{ (a, B) . \exists C D . (a, C) \in R \wedge (a, D) \in R \wedge C \subseteq B \wedge B \subseteq D \}$$

<proof>

declare *up* [*mr-simp*] *down* [*mr-simp*] *convex* [*mr-simp*]

lemma *ic-up*:

$$\sim(R \uparrow) = (\sim R) \downarrow$$

$\langle proof \rangle$

lemma *ic-down*:

$$\sim(R\downarrow) = (\sim R)\uparrow$$

$\langle proof \rangle$

lemma *ic-convex*:

$$\sim(R\updownarrow) = (\sim R)\updownarrow$$

$\langle proof \rangle$

lemma *up-isotone*:

$$R \subseteq S \implies R\uparrow \subseteq S\uparrow$$

$\langle proof \rangle$

lemma *up-increasing*:

$$R \subseteq R\uparrow$$

$\langle proof \rangle$

lemma *up-idempotent* [*simp*]:

$$R\uparrow\uparrow = R\uparrow$$

$\langle proof \rangle$

lemma *up-dist-ou*:

$$(R \cup S)\uparrow = R\uparrow \cup S\uparrow$$

$\langle proof \rangle$

lemma *up-dist-iu*:

$$(R \cup\cup S)\uparrow = R\uparrow \cup\cup S\uparrow$$

$\langle proof \rangle$

lemma *up-dist-ii*:

$$(R \cap\cap S)\uparrow = R\uparrow \cap\cap S\uparrow$$

$\langle proof \rangle$

lemma *down-isotone*:

$$R \subseteq S \implies R\downarrow \subseteq S\downarrow$$

$\langle proof \rangle$

lemma *down-increasing*:

$$R \subseteq R\downarrow$$

$\langle proof \rangle$

lemma *down-idempotent* [*simp*]:

$$R\downarrow\downarrow = R\downarrow$$

$\langle proof \rangle$

lemma *down-dist-ou*:

$$(R \cup S)\downarrow = R\downarrow \cup S\downarrow$$

$\langle proof \rangle$

lemma *down-dist-iu*:

$$(R \cup\cup S)\downarrow = R\downarrow \cup\cup S\downarrow$$

<proof>

lemma *down-dist-ii*:

$$(R \cap\cap S)\downarrow = R\downarrow \cap\cap S\downarrow$$

<proof>

lemma *convex-isotone*:

$$R \subseteq S \implies R\uparrow \subseteq S\uparrow$$

<proof>

lemma *convex-increasing*:

$$R \subseteq R\uparrow$$

<proof>

lemma *convex-idempotent [simp]*:

$$R\uparrow\uparrow = R\uparrow$$

<proof>

lemma *down-sp*:

$$R\downarrow = R * (1_{\cup\cup} \cup 1)$$

<proof>

lemma *up-cp*:

$$R\uparrow = \sim R \odot (1_{\cap\cap} \cup \sim 1)$$

<proof>

lemma *down-dist-sp*:

$$(R * S)\downarrow = R * S\downarrow$$

<proof>

lemma *up-dist-cp*:

$$(R \odot S)\uparrow = R \odot S\uparrow$$

<proof>

lemma *iu-up-oi*:

$$R\uparrow \cup\cup S\uparrow = R\uparrow \cap S\uparrow$$

<proof>

lemma *ii-down-oi*:

$$R\downarrow \cap\cap S\downarrow = R\downarrow \cup S\downarrow$$

<proof>

lemma *down-dist-ii-oi*:

$$R\downarrow \cap S\downarrow = (R \cap\cap S)\downarrow$$

<proof>

lemma *up-dist-iu-oi*:

$$R\uparrow \cap S\uparrow = (R \cup S)\uparrow$$

<proof>

lemma *oi-down-sub-up*:

$$R\downarrow \cap S\uparrow \subseteq (R\downarrow \cap S)\uparrow$$

<proof>

lemma *oi-down-up*:

$$R\downarrow \cap S = \{\} \implies R \cap S\uparrow = \{\}$$

<proof>

lemma *oi-down-up-iff*:

$$R\downarrow \cap S = \{\} \iff R \cap S\uparrow = \{\}$$

<proof>

lemma *down-double-complement-up*:

$$R\downarrow \subseteq S \iff R \subseteq -((-S)\uparrow)$$

<proof>

lemma *up-double-complement-down*:

$$R\uparrow \subseteq S \iff R \subseteq -((-S)\downarrow)$$

<proof>

lemma *below-up-oi-down*:

$$R \subseteq R\uparrow \cap R\downarrow$$

<proof>

lemma *cp-pa-sim*:

$$(R \odot S)\downarrow = R \otimes S\downarrow$$

<proof>

lemma *domain-up-down-conjugate*:

$$(R\uparrow \cap S) * 1_{\cup\cup} = (R \cap S\downarrow) * 1_{\cup\cup}$$

<proof>

lemma *down-below-sp-top*:

$$R\downarrow \subseteq R * U$$

<proof>

lemma *down-oi-up-closed*:

assumes $Q\uparrow = Q$

shows $R\downarrow \cap Q \subseteq (R \cap Q)\downarrow$

<proof>

lemma *up-dist-oU*:

$$(\bigcup X)\uparrow = \bigcup (\text{up } X)$$

<proof>

lemma *up-dist-iU*:
assumes $I \neq \{\}$
shows $(\bigcup\bigcup X|I)\uparrow = \bigcup\bigcup (up \ o \ X)|I$
 $\langle proof \rangle$

lemma *up-dist-iI*:
 $(\bigcap\bigcap X|I)\uparrow = \bigcap\bigcap (up \ o \ X)|I$
 $\langle proof \rangle$

lemma *down-dist-oU*:
 $(\bigcup X)\downarrow = \bigcup (down \ ' \ X)$
 $\langle proof \rangle$

lemma *down-dist-iU*:
 $(\bigcup\bigcup X|I)\downarrow = \bigcup\bigcup (down \ o \ X)|I$
 $\langle proof \rangle$

lemma *down-dist-iI*:
assumes $I \neq \{\}$
shows $(\bigcap\bigcap X|I)\downarrow = \bigcap\bigcap (down \ o \ X)|I$
 $\langle proof \rangle$

lemma *iU-up-oI*:
assumes $I \neq \{\}$
shows $\bigcup\bigcup (up \ o \ X)|I = \bigcap (up \ ' \ X \ ' \ I)$
 $\langle proof \rangle$

lemma *iI-down-oI*:
assumes $I \neq \{\}$
shows $\bigcap\bigcap (down \ o \ X)|I = \bigcap (down \ ' \ X \ ' \ I)$
 $\langle proof \rangle$

lemma *down-dist-iI-oI*:
 $\bigcap (down \ ' \ X \ ' \ I) = (\bigcap\bigcap X|I)\downarrow$
 $\langle proof \rangle$

lemma *up-dist-iU-oI*:
 $\bigcap (up \ ' \ X \ ' \ I) = (\bigcup\bigcup X|I)\uparrow$
 $\langle proof \rangle$

lemma *iu-up*:
 $(R \cup\cup R)\uparrow = R\uparrow$
 $\langle proof \rangle$

lemma *ii-down*:
 $(R \cap\cap R)\downarrow = R\downarrow$
 $\langle proof \rangle$

lemma *iU-up*:
 assumes $I \neq \{\}$
 shows $(\bigcup (\lambda j . R)|I)\uparrow = R\uparrow$
 $\langle proof \rangle$

lemma *iI-down*:
 assumes $I \neq \{\}$
 shows $(\bigcap (\lambda j . R)|I)\downarrow = R\downarrow$
 $\langle proof \rangle$

lemma *iu-unit-up*:
 $1_{UU}\uparrow = U$
 $\langle proof \rangle$

lemma *iu-unit-down*:
 $1_{UU}\downarrow = 1_{UU}$
 $\langle proof \rangle$

lemma *iu-unit-convex*:
 $1_{UU}\updownarrow = 1_{UU}$
 $\langle proof \rangle$

lemma *ii-unit-up*:
 $1_{II}\uparrow = 1_{II}$
 $\langle proof \rangle$

lemma *ii-unit-down*:
 $1_{II}\downarrow = U$
 $\langle proof \rangle$

lemma *ii-unit-convex*:
 $1_{II}\updownarrow = 1_{II}$
 $\langle proof \rangle$

lemma *sp-unit-down*:
 $1\downarrow = 1 \cup 1_{UU}$
 $\langle proof \rangle$

lemma *sp-unit-convex*:
 $1\updownarrow = 1$
 $\langle proof \rangle$

lemma *top-up*:
 $U\uparrow = U$
 $\langle proof \rangle$

lemma *top-down*:
 $U\downarrow = U$
 $\langle proof \rangle$

lemma *top-convex*:

$$U\downarrow = U$$

<proof>

lemma *bot-up*:

$$\{\}\uparrow = \{\}$$

<proof>

lemma *bot-down*:

$$\{\}\downarrow = \{\}$$

<proof>

lemma *bot-convex*:

$$\{\}\downarrow\uparrow = \{\}$$

<proof>

lemma *down-oi-up-convex*:

$$(R\downarrow \cap S\uparrow)\downarrow\uparrow = R\downarrow \cap S\uparrow$$

<proof>

lemma *convex-iff-down-oi-up*:

$$Q = Q\downarrow\uparrow \iff (\exists R S . Q = R\downarrow \cap S\uparrow)$$

<proof>

lemma *convex-closed-oI*:

$$(\bigcap R \in X . R\downarrow\uparrow)\downarrow\uparrow = (\bigcap R \in X . R\downarrow\uparrow)$$

<proof>

lemma *convex-closed-oi*:

$$(R\downarrow\uparrow \cap S\downarrow\uparrow)\downarrow\uparrow = R\downarrow\uparrow \cap S\downarrow\uparrow$$

<proof>

lemma

$$(R\downarrow\uparrow \cup S\downarrow\uparrow)\downarrow\uparrow = R\downarrow\uparrow \cup S\downarrow\uparrow$$

nitpick*[expect=genuine,card=1,3]*
<proof>

6 Powerdomain Preorders

abbreviation *lower-less-eq* :: ('a,'b) mrel \Rightarrow ('a,'b) mrel \Rightarrow bool (**infixl** $\sqsubseteq\downarrow$ 50)

where

$$R \sqsubseteq\downarrow S \equiv R \subseteq S\downarrow$$

abbreviation *upper-less-eq* :: ('a,'b) mrel \Rightarrow ('a,'b) mrel \Rightarrow bool (**infixl** $\sqsubseteq\uparrow$

50) **where**

$$R \sqsubseteq\uparrow S \equiv S \subseteq R\uparrow$$

abbreviation *convex-less-eq* :: ('a,'b) mrel \Rightarrow ('a,'b) mrel \Rightarrow bool (**infixl** $\sqsubseteq\downarrow\uparrow$)

50) **where**

$$R \sqsubseteq\updownarrow S \equiv R \sqsubseteq\downarrow S \wedge R \sqsubseteq\uparrow S$$

abbreviation *Convex-less-eq* :: ('a,'b) mrel \Rightarrow ('a,'b) mrel \Rightarrow bool (**infixl** $\langle\sqsubseteq\updownarrow\rangle$)

50) **where**

$$R \sqsubseteq\updownarrow S \equiv R \subseteq S\updownarrow$$

lemma *lower-less-eq*:

$$R \sqsubseteq\downarrow S \longleftrightarrow (\forall a B . (a,B) \in R \longrightarrow (\exists C . (a,C) \in S \wedge B \subseteq C))$$

<proof>

lemma *upper-less-eq*:

$$R \sqsubseteq\uparrow S \longleftrightarrow (\forall a C . (a,C) \in S \longrightarrow (\exists B . (a,B) \in R \wedge B \subseteq C))$$

<proof>

lemma *Convex-less-eq*:

$$R \sqsubseteq\updownarrow S \longleftrightarrow (\forall a C . (a,C) \in R \longrightarrow (\exists B D . (a,B) \in S \wedge (a,D) \in S \wedge B \subseteq C \wedge C \subseteq D))$$

<proof>

lemma *Convex-lower-upper*:

$$R \sqsubseteq\updownarrow S \longleftrightarrow R \sqsubseteq\downarrow S \wedge S \sqsubseteq\uparrow R$$

<proof>

lemma *lower-reflexive*:

$$R \sqsubseteq\downarrow R$$

<proof>

lemma *upper-reflexive*:

$$R \sqsubseteq\uparrow R$$

<proof>

lemma *convex-reflexive*:

$$R \sqsubseteq\updownarrow R$$

<proof>

lemma *Convex-reflexive*:

$$R \sqsubseteq\updownarrow R$$

<proof>

lemma *lower-transitive*:

$$R \sqsubseteq\downarrow S \Longrightarrow S \sqsubseteq\downarrow T \Longrightarrow R \sqsubseteq\downarrow T$$

<proof>

lemma *upper-transitive*:

$$R \sqsubseteq\uparrow S \Longrightarrow S \sqsubseteq\uparrow T \Longrightarrow R \sqsubseteq\uparrow T$$

<proof>

lemma *convex-transitive*:

$$R \sqsubseteq\uparrow S \implies S \sqsubseteq\uparrow T \implies R \sqsubseteq\uparrow T$$

<proof>

lemma *Convex-transitive:*

$$R \sqsubseteq\uparrow S \implies S \sqsubseteq\uparrow T \implies R \sqsubseteq\uparrow T$$

<proof>

lemma *bot-lower-least:*

$$\{\} \sqsubseteq\downarrow R$$

<proof>

lemma *top-upper-least:*

$$U \sqsubseteq\uparrow R$$

<proof>

lemma *bot-Convex-least:*

$$\{\} \sqsubseteq\uparrow R$$

<proof>

lemma *top-lower-greatest:*

$$R \sqsubseteq\downarrow U$$

<proof>

lemma *bot-upper-greatest:*

$$R \sqsubseteq\uparrow \{\}$$

<proof>

lemma *top-Convex-greatest:*

$$R \sqsubseteq\uparrow U$$

<proof>

lemma *lower-ii-increasing:*

$$R \sqsubseteq\downarrow R \cup\cup R$$

<proof>

lemma *upper-ii-increasing:*

$$R \sqsubseteq\uparrow R \cup\cup S$$

<proof>

lemma *convex-ii-increasing:*

$$R \sqsubseteq\uparrow R \cup\cup R$$

<proof>

lemma *Convex-ii-increasing:*

$$R \sqsubseteq\uparrow R \cup\cup R$$

<proof>

lemma *lower-ii-decreasing:*

$$R \cap\cap S \sqsubseteq\downarrow R$$

$\langle proof \rangle$

lemma *upper-ii-decreasing*:

$$R \cap R \sqsubseteq \uparrow R$$

$\langle proof \rangle$

lemma *convex-ii-decreasing*:

$$R \cap R \sqsubseteq \downarrow R$$

$\langle proof \rangle$

lemma *Convex-ii-increasing*:

$$R \sqsubseteq \downarrow R \cap R$$

$\langle proof \rangle$

lemma *iu-lower-left-isotone*:

$$R \sqsubseteq \downarrow S \implies R \cup T \sqsubseteq \downarrow S \cup T$$

$\langle proof \rangle$

lemma *iu-upper-left-isotone*:

$$R \sqsubseteq \uparrow S \implies R \cup T \sqsubseteq \uparrow S \cup T$$

$\langle proof \rangle$

lemma *iu-convex-left-isotone*:

$$R \sqsubseteq \downarrow S \implies R \cup T \sqsubseteq \downarrow S \cup T$$

$\langle proof \rangle$

lemma *iu-Convex-left-isotone*:

$$R \sqsubseteq \downarrow S \implies R \cup T \sqsubseteq \downarrow S \cup T$$

$\langle proof \rangle$

lemma *iu-lower-right-isotone*:

$$R \sqsubseteq \downarrow S \implies T \cup R \sqsubseteq \downarrow T \cup S$$

$\langle proof \rangle$

lemma *iu-upper-right-isotone*:

$$R \sqsubseteq \uparrow S \implies T \cup R \sqsubseteq \uparrow T \cup S$$

$\langle proof \rangle$

lemma *iu-convex-right-isotone*:

$$R \sqsubseteq \downarrow S \implies T \cup R \sqsubseteq \downarrow T \cup S$$

$\langle proof \rangle$

lemma *iu-Convex-right-isotone*:

$$R \sqsubseteq \downarrow S \implies T \cup R \sqsubseteq \downarrow T \cup S$$

$\langle proof \rangle$

lemma *iu-lower-isotone*:

$$R \sqsubseteq \downarrow S \implies P \sqsubseteq \downarrow Q \implies R \cup P \sqsubseteq \downarrow S \cup Q$$

$\langle proof \rangle$

lemma *iu-upper-isotone*:

$$R \sqsubseteq\uparrow S \implies P \sqsubseteq\uparrow Q \implies R \sqcup\sqcup P \sqsubseteq\uparrow S \sqcup\sqcup Q$$

<proof>

lemma *iu-convex-isotone*:

$$R \sqsubseteq\downarrow S \implies P \sqsubseteq\downarrow Q \implies R \sqcup\sqcup P \sqsubseteq\downarrow S \sqcup\sqcup Q$$

<proof>

lemma *iu-Convex-isotone*:

$$R \sqsubseteq\downarrow S \implies P \sqsubseteq\downarrow Q \implies R \sqcup\sqcup P \sqsubseteq\downarrow S \sqcup\sqcup Q$$

<proof>

lemma *ii-lower-left-isotone*:

$$R \sqsubseteq\downarrow S \implies R \sqcap\sqcap T \sqsubseteq\downarrow S \sqcap\sqcap T$$

<proof>

lemma *ii-upper-left-isotone*:

$$R \sqsubseteq\uparrow S \implies R \sqcap\sqcap T \sqsubseteq\uparrow S \sqcap\sqcap T$$

<proof>

lemma *ii-convex-left-isotone*:

$$R \sqsubseteq\downarrow S \implies R \sqcap\sqcap T \sqsubseteq\downarrow S \sqcap\sqcap T$$

<proof>

lemma *ii-Convex-left-isotone*:

$$R \sqsubseteq\downarrow S \implies R \sqcap\sqcap T \sqsubseteq\downarrow S \sqcap\sqcap T$$

<proof>

lemma *ii-lower-right-isotone*:

$$R \sqsubseteq\downarrow S \implies T \sqcap\sqcap R \sqsubseteq\downarrow T \sqcap\sqcap S$$

<proof>

lemma *ii-upper-right-isotone*:

$$R \sqsubseteq\uparrow S \implies T \sqcap\sqcap R \sqsubseteq\uparrow T \sqcap\sqcap S$$

<proof>

lemma *ii-convex-right-isotone*:

$$R \sqsubseteq\downarrow S \implies T \sqcap\sqcap R \sqsubseteq\downarrow T \sqcap\sqcap S$$

<proof>

lemma *ii-Convex-right-isotone*:

$$R \sqsubseteq\downarrow S \implies T \sqcap\sqcap R \sqsubseteq\downarrow T \sqcap\sqcap S$$

<proof>

lemma *ii-lower-isotone*:

$$R \sqsubseteq\downarrow S \implies P \sqsubseteq\downarrow Q \implies R \sqcap\sqcap P \sqsubseteq\downarrow S \sqcap\sqcap Q$$

<proof>

lemma *ii-upper-isotone:*

$$R \sqsubseteq\uparrow S \implies P \sqsubseteq\uparrow Q \implies R \sqcap P \sqsubseteq\uparrow S \sqcap Q$$

<proof>

lemma *ii-convex-isotone:*

$$R \sqsubseteq\updownarrow S \implies P \sqsubseteq\updownarrow Q \implies R \sqcap P \sqsubseteq\updownarrow S \sqcap Q$$

<proof>

lemma *ii-Convex-isotone:*

$$R \sqsubseteq\updownarrow S \implies P \sqsubseteq\updownarrow Q \implies R \sqcap P \sqsubseteq\updownarrow S \sqcap Q$$

<proof>

lemma *ou-lower-left-isotone:*

$$R \sqsubseteq\downarrow S \implies R \cup T \sqsubseteq\downarrow S \cup T$$

<proof>

lemma *ou-upper-left-isotone:*

$$R \sqsubseteq\uparrow S \implies R \cup T \sqsubseteq\uparrow S \cup T$$

<proof>

lemma *ou-convex-left-isotone:*

$$R \sqsubseteq\updownarrow S \implies R \cup T \sqsubseteq\updownarrow S \cup T$$

<proof>

lemma *ou-Convex-left-isotone:*

$$R \sqsubseteq\updownarrow S \implies R \cup T \sqsubseteq\updownarrow S \cup T$$

<proof>

lemma *ou-lower-right-isotone:*

$$R \sqsubseteq\downarrow S \implies T \cup R \sqsubseteq\downarrow T \cup S$$

<proof>

lemma *ou-upper-right-isotone:*

$$R \sqsubseteq\uparrow S \implies T \cup R \sqsubseteq\uparrow T \cup S$$

<proof>

lemma *ou-convex-right-isotone:*

$$R \sqsubseteq\updownarrow S \implies T \cup R \sqsubseteq\updownarrow T \cup S$$

<proof>

lemma *ou-Convex-right-isotone:*

$$R \sqsubseteq\updownarrow S \implies T \cup R \sqsubseteq\updownarrow T \cup S$$

<proof>

lemma *ou-lower-isotone:*

$$R \sqsubseteq\downarrow S \implies P \sqsubseteq\downarrow Q \implies R \cup P \sqsubseteq\downarrow S \cup Q$$

<proof>

lemma *ou-upper-isotone:*

$$R \sqsubseteq\uparrow S \implies P \sqsubseteq\uparrow Q \implies R \cup P \sqsubseteq\uparrow S \cup Q$$

<proof>

lemma *ou-convex-isotone:*

$$R \sqsubseteq\updownarrow S \implies P \sqsubseteq\updownarrow Q \implies R \cup P \sqsubseteq\updownarrow S \cup Q$$

<proof>

lemma *ou-Convex-isotone:*

$$R \sqsubseteq\updownarrow S \implies P \sqsubseteq\updownarrow Q \implies R \cup P \sqsubseteq\updownarrow S \cup Q$$

<proof>

lemma *sp-lower-left-isotone:*

$$R \sqsubseteq\downarrow S \implies T * R \sqsubseteq\downarrow T * S$$

<proof>

lemma *sp-upper-left-isotone:*

$$R \sqsubseteq\uparrow S \implies T * R \sqsubseteq\uparrow T * S$$

<proof>

lemma *sp-convex-left-isotone:*

$$R \sqsubseteq\updownarrow S \implies T * R \sqsubseteq\updownarrow T * S$$

<proof>

lemma *sp-Convex-left-isotone:*

$$R \sqsubseteq\updownarrow S \implies T * R \sqsubseteq\updownarrow T * S$$

<proof>

lemma *cp-lower-left-isotone:*

$$R \sqsubseteq\downarrow S \implies T \odot R \sqsubseteq\downarrow T \odot S$$

<proof>

lemma *cp-upper-left-isotone:*

$$R \sqsubseteq\uparrow S \implies T \odot R \sqsubseteq\uparrow T \odot S$$

<proof>

lemma *cp-convex-left-isotone:*

$$R \sqsubseteq\updownarrow S \implies T \odot R \sqsubseteq\updownarrow T \odot S$$

<proof>

lemma *cp-Convex-left-isotone:*

$$R \sqsubseteq\updownarrow S \implies T \odot R \sqsubseteq\updownarrow T \odot S$$

<proof>

lemma *lower-ic-upper:*

$$R \sqsubseteq\downarrow S \iff \sim S \sqsubseteq\uparrow \sim R$$

<proof>

lemma *upper-ic-lower:*

$$R \sqsubseteq\uparrow S \iff \sim S \sqsubseteq\downarrow \sim R$$

<proof>

lemma *convex-ic:*

$$R \sqsubseteq\Downarrow S \iff \sim S \sqsubseteq\Downarrow \sim R$$

<proof>

lemma *Convex-ic:*

$$R \sqsubseteq\Downarrow S \iff \sim R \sqsubseteq\Downarrow \sim S$$

<proof>

lemma *up-lower-isotone:*

$$R \sqsubseteq\Downarrow S \implies R\uparrow \sqsubseteq\Downarrow S\uparrow$$

<proof>

lemma *up-upper-isotone:*

$$R \sqsubseteq\Uparrow S \implies R\uparrow \sqsubseteq\Uparrow S\uparrow$$

<proof>

lemma *up-convex-isotone:*

$$R \sqsubseteq\Downarrow S \implies R\uparrow \sqsubseteq\Downarrow S\uparrow$$

<proof>

lemma *up-Convex-isotone:*

$$R \sqsubseteq\Downarrow S \implies R\uparrow \sqsubseteq\Downarrow S\uparrow$$

<proof>

lemma *down-lower-isotone:*

$$R \sqsubseteq\Downarrow S \implies R\downarrow \sqsubseteq\Downarrow S\downarrow$$

<proof>

lemma *down-upper-isotone:*

$$R \sqsubseteq\Uparrow S \implies R\downarrow \sqsubseteq\Uparrow S\downarrow$$

<proof>

lemma *down-convex-isotone:*

$$R \sqsubseteq\Downarrow S \implies R\downarrow \sqsubseteq\Downarrow S\downarrow$$

<proof>

lemma *down-Convex-isotone:*

$$R \sqsubseteq\Downarrow S \implies R\downarrow \sqsubseteq\Downarrow S\downarrow$$

<proof>

lemma *convex-lower-isotone:*

$$R \sqsubseteq\Downarrow S \implies R\downarrow \sqsubseteq\Downarrow S\downarrow$$

<proof>

lemma *convex-upper-isotone:*

$$R \sqsubseteq\Uparrow S \implies R\downarrow \sqsubseteq\Uparrow S\downarrow$$

<proof>

lemma *convex-convex-isotone*:

$$R \sqsubseteq\uparrow S \implies R\uparrow \sqsubseteq\uparrow S\uparrow$$

<proof>

lemma *convex-Convex-isotone*:

$$R \sqsubseteq\uparrow S \implies R\uparrow \sqsubseteq\uparrow S\uparrow$$

<proof>

lemma *subset-lower*:

$$R \subseteq S \implies R \sqsubseteq\downarrow S$$

<proof>

lemma *subset-upper*:

$$R \subseteq S \implies S \sqsubseteq\uparrow R$$

<proof>

lemma *subset-Convex*:

$$R \subseteq S \implies R \sqsubseteq\uparrow S$$

<proof>

lemma *oi-subset-lower-left-isotone*:

$$R \subseteq S \implies R \cap T \sqsubseteq\downarrow S \cap T$$

<proof>

lemma *oi-subset-upper-left-antitone*:

$$R \subseteq S \implies S \cap T \sqsubseteq\uparrow R \cap T$$

<proof>

lemma *oi-subset-Convex-left-isotone*:

$$R \subseteq S \implies R \cap T \sqsubseteq\uparrow S \cap T$$

<proof>

lemma *oi-subset-lower-right-isotone*:

$$R \subseteq S \implies T \cap R \sqsubseteq\downarrow T \cap S$$

<proof>

lemma *oi-subset-upper-right-antitone*:

$$R \subseteq S \implies T \cap S \sqsubseteq\uparrow T \cap R$$

<proof>

lemma *oi-subset-Convex-right-isotone*:

$$R \subseteq S \implies T \cap R \sqsubseteq\uparrow T \cap S$$

<proof>

lemma *oi-subset-lower-isotone*:

$$R \subseteq S \implies P \subseteq Q \implies R \cap P \sqsubseteq\downarrow S \cap Q$$

<proof>

lemma *oi-subset-upper-antitone*:

$$R \subseteq S \implies P \subseteq Q \implies S \cap Q \sqsubseteq\uparrow R \cap P$$

<proof>

lemma *oi-subset-Convex-isotone*:

$$R \subseteq S \implies P \subseteq Q \implies R \cap P \sqsubseteq\Downarrow S \cap Q$$

<proof>

lemma *sp-ii-unit-lower*:

$$R * 1_{\cup\cup} \sqsubseteq\downarrow R$$

<proof>

lemma *cp-ii-unit-upper*:

$$R \sqsubseteq\uparrow R \odot 1_{\cap\cap}$$

<proof>

lemma *lower-ii-down*:

$$R \sqsubseteq\downarrow S \iff R\downarrow = (R \cap\cap S)\downarrow$$

<proof>

lemma *lower-ii-lower-bound*:

$$R \sqsubseteq\downarrow S \iff R \subseteq R \cap\cap S$$

<proof>

lemma *upper-ii-up*:

$$R \sqsubseteq\uparrow S \iff S\uparrow = (R \cup\cup S)\uparrow$$

<proof>

lemma *upper-ii-upper-bound*:

$$R \sqsubseteq\uparrow S \iff S \subseteq R \cup\cup S$$

<proof>

lemma

$$R \sqsubseteq\downarrow S \iff R = R \cap\cap S$$

nitpick*[expect=genuine,card=1]*
<proof>

lemma

$$R \sqsubseteq\uparrow S \iff S = R \cup\cup S$$

nitpick*[expect=genuine,card=1]*
<proof>

lemma *convex-oi-Convex-ii*:

$$R\downarrow \cap S\downarrow \sqsubseteq\Downarrow R \cup\cup S$$

<proof>

lemma *convex-oi-Convex-ii*:

$$R\downarrow \cap S\downarrow \sqsubseteq\Downarrow R \cap\cap S$$

<proof>

lemma *convex-oi-iu-ii*:

$$R\downarrow \cap S\uparrow = (R \cup\cup S)\uparrow \cap (R \cap\cap S)\downarrow$$

<proof>

lemma *ii-lower-iu*:

$$R \cap\cap S \sqsubseteq\downarrow R \cup\cup S$$

<proof>

lemma *ii-upper-iu*:

$$R \cap\cap S \sqsubseteq\uparrow R \cup\cup S$$

<proof>

lemma *ii-convex-iu*:

$$R \cap\cap S \sqsubseteq\updownarrow R \cup\cup S$$

<proof>

lemma *convex-oi-iu-ii-convex*:

$$R\downarrow \cap S\uparrow = (R \cup\cup S)\downarrow \cap (R \cap\cap S)\updownarrow$$

<proof>

6.1 Functional properties of multirelations

lemma *id-one-converse*:

$$Id = 1 ; 1\sim$$

<proof>

lemma *dom-explicit*:

$$Dom R = R ; U \cap 1$$

<proof>

lemma *dom-explicit-2*:

$$Dom R = R ; top \cap 1$$

<proof>

lemma *total-dom*:

$$total R \longleftrightarrow Dom R = 1$$

<proof>

lemma *total-eq*:

$$total R \longleftrightarrow 1_{\cup\cup} = R * 1_{\cup\cup}$$

<proof>

lemma *domain-pointwise*:

$$x \in R * 1_{\cup\cup} \longleftrightarrow (\exists a B . (a,B) \in R \wedge x = (a,\{\}))$$

<proof>

card only works for finite sets

lemma *univalent-2*:

univalent $R \iff (\forall a . \text{finite } \{ B . (a,B) \in R \} \wedge \text{card } \{ B . (a,B) \in R \} \leq \text{one-class.one})$
<proof>

lemma *univalent-3*:

univalent $R \iff (\forall S . R * 1_{\cup\cup} = S * 1_{\cup\cup} \wedge S \subseteq R \longrightarrow S = R)$
<proof>

lemma *total-2*:

total $R \iff (\forall a . \{ B . (a,B) \in R \} \neq \{\})$
<proof>

lemma *total-3*:

total $R \iff (\forall a . \text{finite } \{ B . (a,B) \in R \} \longrightarrow \text{card } \{ B . (a,B) \in R \} \geq \text{one-class.one})$
<proof>

lemma *total-4*: *total* $R \iff 1_{\cup\cup} \subseteq R * 1_{\cup\cup}$

<proof>

lemma *deterministic-2*:

deterministic $R \iff (\forall a . \text{card } \{ B . (a,B) \in R \} = \text{one-class.one})$
<proof>

lemma *univalent-convex*:

assumes *univalent* S

shows $S = S \downarrow$

<proof>

lemma *univalent-iu-idempotent*:

assumes *univalent* S

shows $S = S \cup\cup S$

<proof>

lemma *univalent-ii-idempotent*:

assumes *univalent* S

shows $S = S \cap\cap S$

<proof>

lemma *univalent-down-iu-idempotent*:

assumes *univalent* S

shows $S = S \downarrow \cup\cup S$

<proof>

lemma *univalent-up-ii-idempotent*:

assumes *univalent* S

shows $S = S \uparrow \cap\cap S$

<proof>

lemma *univalent-convex-iu-idempotent*:

assumes *univalent S*

shows $S = S \Downarrow \cupcup S$

<proof>

lemma *univalent-convex-ii-idempotent*:

assumes *univalent S*

shows $S = S \Downarrow \capcap S$

<proof>

lemma *univalent-iu-closed*:

univalent R \implies *univalent S* \implies *univalent (R \cupcup S)*

<proof>

lemma *univalent-ii-closed*:

univalent R \implies *univalent S* \implies *univalent (R \capcap S)*

<proof>

lemma *total-lower*:

total R \longleftrightarrow $1 \cupcup \sqsubseteq\downarrow R$

<proof>

lemma *total-upper*:

total R \longleftrightarrow $R \sqsubseteq\uparrow 1 \capcap$

<proof>

lemma *total-lower-iu*:

assumes *total T*

shows $R \sqsubseteq\downarrow R \cupcup T$

<proof>

lemma *total-upper-ii*:

assumes *total T*

shows $R \capcap T \sqsubseteq\uparrow R$

<proof>

lemma *total-univalent-lower-iu*:

assumes *total T*

and *univalent S*

and $T \sqsubseteq\downarrow S$

shows $T \cupcup S = S$

<proof>

lemma *total-iu-closed*:

total R \implies *total S* \implies *total (R \cupcup S)*

<proof>

lemma *total-ii-closed*:

total R \implies *total S* \implies *total (R \capcap S)*

<proof>

lemma *deterministic-lower:*

assumes *deterministic V*

shows $R \sqsubseteq\downarrow V \iff (\forall a B C . (a,B) \in R \wedge (a,C) \in V \longrightarrow B \subseteq C)$
<proof>

lemma *deterministic-upper:*

assumes *deterministic V*

shows $V \sqsubseteq\uparrow R \iff (\forall a B C . (a,B) \in R \wedge (a,C) \in V \longrightarrow C \subseteq B)$
<proof>

lemma *deterministic-iu-closed:*

deterministic R \implies *deterministic S* \implies *deterministic (R $\cup\cup$ S)*

<proof>

lemma *deterministic-ii-closed:*

deterministic R \implies *deterministic S* \implies *deterministic (R $\cap\cap$ S)*

<proof>

lemma *total-univalent-lower-implies-upper:*

assumes *total T*

and *univalent S*

and $T \sqsubseteq\downarrow S$

shows $T \sqsubseteq\uparrow S$

<proof>

lemma *total-univalent-lower-implies-convex:*

assumes *total T*

and *univalent S*

and $T \sqsubseteq\downarrow S$

shows $T \sqsubseteq\updownarrow S$

<proof>

lemma *total-univalent-upper-implies-lower:*

assumes *total T*

and *univalent S*

and $S \sqsubseteq\uparrow T$

shows $S \sqsubseteq\downarrow T$

<proof>

lemma *total-univalent-upper-implies-convex:*

assumes *total T*

and *univalent S*

and $S \sqsubseteq\uparrow T$

shows $S \sqsubseteq\updownarrow T$

<proof>

lemma *deterministic-lower-upper:*

assumes *deterministic T*
and *deterministic S*
shows $S \sqsubseteq\downarrow T \longleftrightarrow S \sqsubseteq\uparrow T$
<proof>

lemma *deterministic-lower-convex:*
assumes *deterministic T*
and *deterministic S*
shows $S \sqsubseteq\downarrow T \longleftrightarrow S \sqsubseteq\uparrow\downarrow T$
<proof>

lemma *deterministic-upper-convex:*
assumes *deterministic T*
and *deterministic S*
shows $S \sqsubseteq\uparrow T \longleftrightarrow S \sqsubseteq\downarrow\uparrow T$
<proof>

lemma *total-down-sp-sp-down:*
assumes *total T*
shows $R\downarrow * T \subseteq R * T\downarrow$
<proof>

lemma *total-down-sp-semi-commute:*
total T $\implies R\downarrow * T \subseteq (R * T)\downarrow$
<proof>

lemma *total-down-dist-sp:*
total T $\implies (R * T)\downarrow = R\downarrow * T\downarrow$
<proof>

lemma *univalent-ic-closed:*
univalent R \longleftrightarrow *univalent ($\sim R$)*
<proof>

lemma *total-ic-closed:*
total R \longleftrightarrow *total ($\sim R$)*
<proof>

lemma *deterministic-ic-closed:*
deterministic R \longleftrightarrow *deterministic ($\sim R$)*
<proof>

lemma *iu-unit-deterministic:*
deterministic ($1_{\cup\cup}$)
<proof>

lemma *ii-unit-deterministic:*
deterministic ($1_{\cap\cap}$)
<proof>

lemma *univalent-upper-iu*:
assumes *univalent R*
shows $(R \sqsubseteq\uparrow S) \longleftrightarrow (R \cup\cup S = S)$
 $\langle proof \rangle$

lemma *univalent-lower-ii*:
assumes *univalent S*
shows $(R \sqsubseteq\downarrow S) = (R \cap\cap S = R)$
 $\langle proof \rangle$

6.2 Equivalences induced by powerdomain preorders

abbreviation *lower-eq* :: $('a, 'b) \text{ mrel} \Rightarrow ('a, 'b) \text{ mrel} \Rightarrow \text{bool}$ (**infixl** $\langle =\downarrow \rangle$ 50)
where
 $R =\downarrow S \equiv R \sqsubseteq\downarrow S \wedge S \sqsubseteq\downarrow R$

abbreviation *upper-eq* :: $('a, 'b) \text{ mrel} \Rightarrow ('a, 'b) \text{ mrel} \Rightarrow \text{bool}$ (**infixl** $\langle =\uparrow \rangle$ 50)
where
 $R =\uparrow S \equiv R \sqsubseteq\uparrow S \wedge S \sqsubseteq\uparrow R$

abbreviation *convex-eq* :: $('a, 'b) \text{ mrel} \Rightarrow ('a, 'b) \text{ mrel} \Rightarrow \text{bool}$ (**infixl** $\langle =\Downarrow \rangle$ 50)
where
 $R =\Downarrow S \equiv R \sqsubseteq\Downarrow S \wedge S \sqsubseteq\Downarrow R$

lemma *Convex-eq*:
 $R =\Downarrow S \equiv R \sqsubseteq\Downarrow S \wedge S \sqsubseteq\Downarrow R$
 $\langle proof \rangle$

lemma *convex-lower-upper*:
 $R =\Downarrow S \longleftrightarrow R =\downarrow S \wedge R =\uparrow S$
 $\langle proof \rangle$

lemma *lower-eq-down*:
 $R =\downarrow S \longleftrightarrow R\downarrow = S\downarrow$
 $\langle proof \rangle$

lemma *upper-eq-up*:
 $R =\uparrow S \longleftrightarrow R\uparrow = S\uparrow$
 $\langle proof \rangle$

lemma *convex-eq-convex*:
 $R =\Downarrow S \longleftrightarrow R\Downarrow = S\Downarrow$
 $\langle proof \rangle$

lemma *lower-eq*:
 $R =\downarrow S \longleftrightarrow (\forall a B . (\exists C . (a, C) \in R \wedge B \subseteq C) \longleftrightarrow (\exists C . (a, C) \in S \wedge B \subseteq C))$
 $\langle proof \rangle$

lemma *upper-eq*:

$$R =\uparrow S \iff (\forall a C . (\exists B . (a,B) \in R \wedge B \subseteq C) \iff (\exists B . (a,B) \in S \wedge B \subseteq C))$$

<proof>

lemma *lower-eq-reflexive*:

$$R =\downarrow R$$

<proof>

lemma *upper-eq-reflexive*:

$$R =\uparrow R$$

<proof>

lemma *convex-eq-reflexive*:

$$R =\Downarrow R$$

<proof>

lemma *lower-eq-symmetric*:

$$R =\downarrow S \implies S =\downarrow R$$

<proof>

lemma *upper-eq-symmetric*:

$$R =\uparrow S \implies S =\uparrow R$$

<proof>

lemma *convex-eq-symmetric*:

$$R =\Downarrow S \implies S =\Downarrow R$$

<proof>

lemma *lower-eq-transitive*:

$$R =\downarrow S \implies S =\downarrow T \implies R =\downarrow T$$

<proof>

lemma *upper-eq-transitive*:

$$R =\uparrow S \implies S =\uparrow T \implies R =\uparrow T$$

<proof>

lemma *convex-eq-transitive*:

$$R =\Downarrow S \implies S =\Downarrow T \implies R =\Downarrow T$$

<proof>

lemma *ou-lower-eq-left-congruence*:

$$R =\downarrow S \implies R \cup T =\downarrow S \cup T$$

<proof>

lemma *ou-upper-eq-left-congruence*:

$$R =\uparrow S \implies R \cup T =\uparrow S \cup T$$

<proof>

lemma *ou-convex-eq-left-congruence*:

$$R =\Downarrow S \implies R \cup T =\Downarrow S \cup T$$

<proof>

lemma *ou-lower-eq-right-congruence*:

$$R =\Downarrow S \implies T \cup R =\Downarrow T \cup S$$

<proof>

lemma *ou-upper-eq-right-congruence*:

$$R =\Uparrow S \implies T \cup R =\Uparrow T \cup S$$

<proof>

lemma *ou-convex-eq-right-congruence*:

$$R =\Downarrow S \implies T \cup R =\Downarrow T \cup S$$

<proof>

lemma *ou-lower-eq-congruence*:

$$R =\Downarrow S \implies P =\Downarrow Q \implies R \cup P =\Downarrow S \cup Q$$

<proof>

lemma *ou-upper-eq-congruence*:

$$R =\Uparrow S \implies P =\Uparrow Q \implies R \cup P =\Uparrow S \cup Q$$

<proof>

lemma *ou-convex-eq-congruence*:

$$R =\Downarrow S \implies P =\Downarrow Q \implies R \cup P =\Downarrow S \cup Q$$

<proof>

lemma *iu-lower-eq-left-congruence*:

$$R =\Downarrow S \implies R \cup\cup T =\Downarrow S \cup\cup T$$

<proof>

lemma *iu-upper-eq-left-congruence*:

$$R =\Uparrow S \implies R \cup\cup T =\Uparrow S \cup\cup T$$

<proof>

lemma *iu-convex-eq-left-congruence*:

$$R =\Downarrow S \implies R \cup\cup T =\Downarrow S \cup\cup T$$

<proof>

lemma *iu-lower-eq-right-congruence*:

$$R =\Downarrow S \implies T \cup\cup R =\Downarrow T \cup\cup S$$

<proof>

lemma *iu-upper-eq-right-congruence*:

$$R =\Uparrow S \implies T \cup\cup R =\Uparrow T \cup\cup S$$

<proof>

lemma *iu-convex-eq-right-congruence*:

$$R =\Downarrow S \implies T \cup\cup R =\Downarrow T \cup\cup S$$

<proof>

lemma *iu-lower-eq-congruence*:

$$R =\Downarrow S \implies P =\Downarrow Q \implies R \cup\cup P =\Downarrow S \cup\cup Q$$

<proof>

lemma *iu-upper-eq-congruence*:

$$R =\Uparrow S \implies P =\Uparrow Q \implies R \cup\cup P =\Uparrow S \cup\cup Q$$

<proof>

lemma *iu-convex-eq-congruence*:

$$R =\Downarrow S \implies P =\Downarrow Q \implies R \cup\cup P =\Downarrow S \cup\cup Q$$

<proof>

lemma *ii-lower-eq-left-congruence*:

$$R =\Downarrow S \implies R \cap\cap T =\Downarrow S \cap\cap T$$

<proof>

lemma *ii-upper-eq-left-congruence*:

$$R =\Uparrow S \implies R \cap\cap T =\Uparrow S \cap\cap T$$

<proof>

lemma *ii-convex-eq-left-congruence*:

$$R =\Downarrow S \implies R \cap\cap T =\Downarrow S \cap\cap T$$

<proof>

lemma *ii-lower-eq-right-congruence*:

$$R =\Downarrow S \implies T \cap\cap R =\Downarrow T \cap\cap S$$

<proof>

lemma *ii-upper-eq-right-congruence*:

$$R =\Uparrow S \implies T \cap\cap R =\Uparrow T \cap\cap S$$

<proof>

lemma *ii-convex-eq-right-congruence*:

$$R =\Downarrow S \implies T \cap\cap R =\Downarrow T \cap\cap S$$

<proof>

lemma *ii-lower-eq-congruence*:

$$R =\Downarrow S \implies P =\Downarrow Q \implies R \cap\cap P =\Downarrow S \cap\cap Q$$

<proof>

lemma *ii-upper-eq-congruence*:

$$R =\Uparrow S \implies P =\Uparrow Q \implies R \cap\cap P =\Uparrow S \cap\cap Q$$

<proof>

lemma *ii-convex-eq-congruence*:

$$R =\Downarrow S \implies P =\Downarrow Q \implies R \sqcap P =\Downarrow S \sqcap Q$$

<proof>

lemma *sp-lower-eq-left-congruence:*

$$R =\Downarrow S \implies T * R =\Downarrow T * S$$

<proof>

lemma *sp-upper-eq-left-congruence:*

$$R =\Uparrow S \implies T * R =\Uparrow T * S$$

<proof>

lemma *sp-convex-eq-left-congruence:*

$$R =\Downarrow S \implies T * R =\Downarrow T * S$$

<proof>

lemma *cp-lower-eq-left-congruence:*

$$R =\Downarrow S \implies T \odot R =\Downarrow T \odot S$$

<proof>

lemma *cp-upper-eq-left-congruence:*

$$R =\Uparrow S \implies T \odot R =\Uparrow T \odot S$$

<proof>

lemma *cp-convex-eq-left-congruence:*

$$R =\Downarrow S \implies T \odot R =\Downarrow T \odot S$$

<proof>

lemma *lower-eq-ic-upper:*

$$R =\Downarrow S \iff \sim R =\Uparrow \sim S$$

<proof>

lemma *upper-eq-ic-lower:*

$$R =\Uparrow S \iff \sim R =\Downarrow \sim S$$

<proof>

lemma *convex-eq-ic-lower:*

$$R =\Downarrow S \iff \sim R =\Downarrow \sim S$$

<proof>

lemma *up-lower-eq-congruence:*

$$R =\Downarrow S \implies R\uparrow =\Downarrow S\uparrow$$

<proof>

lemma *up-upper-eq-congruence:*

$$R =\Uparrow S \implies R\uparrow =\Uparrow S\uparrow$$

<proof>

lemma *up-convex-eq-congruence:*

$$R =\Downarrow S \implies R\uparrow =\Downarrow S\uparrow$$

<proof>

lemma *down-lower-eq-congruence:*

$$R = \downarrow S \implies R \downarrow = \downarrow S \downarrow$$

<proof>

lemma *down-upper-eq-congruence:*

$$R = \uparrow S \implies R \downarrow = \uparrow S \downarrow$$

<proof>

lemma *down-convex-eq-congruence:*

$$R = \Downarrow S \implies R \downarrow = \Downarrow S \downarrow$$

<proof>

lemma *convex-lower-eq-congruence:*

$$R = \downarrow S \implies R \Uparrow = \downarrow S \Uparrow$$

<proof>

lemma *convex-upper-eq-congruence:*

$$R = \uparrow S \implies R \Uparrow = \uparrow S \Uparrow$$

<proof>

lemma *convex-convex-eq-congruence:*

$$R = \Downarrow S \implies R \Uparrow = \Downarrow S \Uparrow$$

<proof>

lemma *univalent-lower-eq-subset:*

assumes *univalent* S

and $S = \downarrow R$

shows $S \subseteq R$

<proof>

lemma *univalent-lower-eq:*

assumes *univalent* R

and *univalent* S

and $R = \downarrow S$

shows $R = S$

<proof>

lemma *univalent-lower-eq-iff:*

assumes *univalent* R

and *univalent* S

shows $(R = \downarrow S) \iff (R = S)$

<proof>

lemma *univalent-upper-eq-subset:*

assumes *univalent* S

and $S = \uparrow R$

shows $S \subseteq R$

$\langle proof \rangle$

lemma *univalent-upper-eq*:
 assumes *univalent* R
 and *univalent* S
 and $R = \uparrow S$
 shows $R = S$
 $\langle proof \rangle$

lemma *univalent-upper-eq-iff*:
 assumes *univalent* R
 and *univalent* S
 shows $(R = \uparrow S) \longleftrightarrow (R = S)$
 $\langle proof \rangle$

lemma *univalent-convex-eq-iff*:
 assumes *univalent* R
 and *univalent* S
 shows $(R = \Downarrow S) \longleftrightarrow (R = S)$
 $\langle proof \rangle$

lemma *total-univalent-upper-ii*:
 assumes *total* T
 and *univalent* S
 and $S \sqsubseteq \uparrow T$
 shows $T \cap \cap S = S$
 $\langle proof \rangle$

lemma *lower-eq-down-closed*:
 $R = \downarrow R \downarrow$
 $\langle proof \rangle$

lemma *upper-eq-up-closed*:
 $R = \uparrow R \uparrow$
 $\langle proof \rangle$

lemma *convex-eq-up-closed*:
 $R = \Downarrow R \Downarrow$
 $\langle proof \rangle$

lemma *lower-join*:
 $(\forall P . Q \sqsubseteq \downarrow P \longleftrightarrow R \sqsubseteq \downarrow P \wedge S \sqsubseteq \downarrow P) \longleftrightarrow Q = \downarrow R \cup S$
 $\langle proof \rangle$

lemma *lower-meet*:
 $(\forall P . P \sqsubseteq \downarrow Q \longleftrightarrow P \sqsubseteq \downarrow R \wedge P \sqsubseteq \downarrow S) \longleftrightarrow Q = \downarrow R \cap \cap S$
 $\langle proof \rangle$

lemma *upper-join*:

$$(\forall P . Q \sqsubseteq\uparrow P \iff R \sqsubseteq\uparrow P \wedge S \sqsubseteq\uparrow P) \iff Q =\uparrow R \cup\cup S$$

<proof>

lemma *upper-meet:*

$$(\forall P . P \sqsubseteq\uparrow Q \iff P \sqsubseteq\uparrow R \wedge P \sqsubseteq\uparrow S) \iff Q =\uparrow R \cup S$$

<proof>

lemma *lower-ii-idempotent:*

$$R \cap\cap R =\downarrow R$$

<proof>

lemma *upper-iu-idempotent:*

$$R \cup\cup R =\uparrow R$$

<proof>

lemma *lower-iI-idempotent:*

$$I \neq \{\} \implies (\cap\cap(\lambda j . R)|I) =\downarrow R$$

<proof>

lemma *upper-iU-idempotent:*

$$I \neq \{\} \implies (\cup\cup(\lambda j . R)|I) =\uparrow R$$

<proof>

lemma *down-closed-intersection-closed:*

$$R = R\downarrow \implies \forall I . I \neq \{\} \longrightarrow (\cap\cap(\lambda j . R)|I) \subseteq R$$

<proof>

lemma *up-closed-union-closed:*

$$R = R\uparrow \implies \forall I . I \neq \{\} \longrightarrow (\cup\cup(\lambda j . R)|I) \subseteq R$$

<proof>

lemma *ou-down-lower-eq-ou:*

$$R\downarrow \cup S\downarrow =\downarrow R \cup S$$

<proof>

lemma *oi-down-lower-eq-ii:*

$$R\downarrow \cap S\downarrow =\downarrow R \cap\cap S$$

<proof>

lemma *ou-up-upper-eq-ou:*

$$R\uparrow \cup S\uparrow =\uparrow R \cup S$$

<proof>

lemma *oi-up-upper-eq-iu:*

$$R\uparrow \cap S\uparrow =\uparrow R \cup\cup S$$

<proof>

lemma *oU-down-lower-eq-oU:*

$$(\cup R \in X . R\downarrow) =\downarrow \cup X$$

<proof>

lemma *oI-down-lower-eq-iI*:

$$(\bigcap_{i \in I} . X \downarrow) = \downarrow \bigcap \bigcap X | I$$

<proof>

lemma *oU-up-upper-eq-oU*:

$$(\bigcup_{R \in X} . R \uparrow) = \uparrow \bigcup X$$

<proof>

lemma *oI-up-upper-eq-iI*:

$$(\bigcap_{i \in I} . X \uparrow) = \uparrow \bigcup \bigcup X | I$$

<proof>

lemma *down-order-lower*:

$$R \downarrow \subseteq S \downarrow \longleftrightarrow R \sqsubseteq \downarrow S$$

<proof>

lemma *up-order-upper*:

$$R \uparrow \subseteq S \uparrow \longleftrightarrow S \sqsubseteq \uparrow R$$

<proof>

lemma *convex-order-lower-upper*:

$$R \updownarrow \subseteq S \updownarrow \longleftrightarrow R \sqsubseteq \downarrow S \wedge S \sqsubseteq \uparrow R$$

<proof>

lemma *convex-order-Convex*:

$$R \updownarrow \subseteq S \updownarrow \longleftrightarrow R \sqsubseteq \updownarrow S$$

<proof>

6.3 Further results for convex-closure

lemma *convex-down*:

$$R \updownarrow \downarrow = R \downarrow$$

<proof>

lemma *convex-up*:

$$R \updownarrow \uparrow = R \uparrow$$

<proof>

lemma *iu-dist-oi-convex*:

assumes $R = R \updownarrow$

and $S = S \updownarrow$

and $T = T \updownarrow$

shows $(R \cap S) \cup T = (R \cup T) \cap (S \cup T)$

nitpick $[expect=genuine,card=1]$

<proof>

lemma *ii-dist-oi-convex*:

assumes $R = R\uparrow$
and $S = S\uparrow$
and $T = T\uparrow$
shows $(R \cap S) \cap T = (R \cap T) \cap (S \cap T)$
nitpick[*expect=genuine,card=1*]
<proof>

lemma *oI-up-closed*:
assumes $\forall R \in X . R\uparrow = R$
shows $(\bigcap X)\uparrow = \bigcap X$
<proof>

lemma *oI-down-closed*:
assumes $\forall R \in X . R\downarrow = R$
shows $(\bigcap X)\downarrow = \bigcap X$
<proof>

lemma *oI-convex-closed*:
assumes $\forall R \in X . R\uparrow = R$
shows $(\bigcap X)\uparrow = \bigcap X$
<proof>

lemma *up-dist-Union*:
 $(\bigcup X)\uparrow = \bigcup \{ R\uparrow \mid R . R \in X \}$
<proof>

lemma *down-dist-Union*:
 $(\bigcup X)\downarrow = \bigcup \{ R\downarrow \mid R . R \in X \}$
<proof>

lemma *convex-dist-Union*:
 $(\bigcup X)\uparrow = \bigcup \{ R\uparrow \mid R . R \in X \}$
nitpick[*expect=genuine,card=1,2*]
<proof>

lemma *up-dist-Inter*:
 $(\bigcap X)\uparrow = \bigcap \{ R\uparrow \mid R . R \in X \}$
nitpick[*expect=genuine,card=1*]
<proof>

lemma *down-dist-Inter*:
 $(\bigcap X)\downarrow = \bigcap \{ R\downarrow \mid R . R \in X \}$
nitpick[*expect=genuine,card=1*]
<proof>

lemma *convex-dist-Inter*:
 $(\bigcap X)\uparrow = \bigcap \{ R\uparrow \mid R . R \in X \}$
nitpick[*expect=genuine,card=1,2*]
<proof>

lemma *Inter-convex-closed*:

$$(\bigcap X)\downarrow = \bigcap X$$

nitpick[*expect=genuine,card=1,2*]

<proof>

abbreviation *convex-iu* (**infixl** $\langle \cup\cup\downarrow \rangle$ 70)

where $R \cup\cup\downarrow S \equiv (R \cup\cup S)\downarrow$

lemma *convex-iu*:

$$R \cup\cup\downarrow S = (R\downarrow \cup\cup S\downarrow) \cap R\uparrow \cap S\uparrow$$

<proof>

lemma *convex-iu-sub*:

$$R\downarrow \cup\cup S \subseteq R \cup\cup\downarrow S$$

<proof>

lemma *convex-iu-convex-left*:

$$R \cup\cup\downarrow S = R\downarrow \cup\cup\downarrow S$$

<proof>

lemma *convex-iu-convex-right*:

$$R \cup\cup\downarrow S = R \cup\cup\downarrow S\downarrow$$

<proof>

lemma *convex-iu-convex*:

$$R \cup\cup\downarrow S = R\downarrow \cup\cup\downarrow S\downarrow$$

<proof>

lemma *convex-iu-assoc*:

$$(R \cup\cup\downarrow S) \cup\cup\downarrow T = R \cup\cup\downarrow (S \cup\cup\downarrow T)$$

<proof>

lemma *convex-iu-comm*:

$$R \cup\cup\downarrow S = S \cup\cup\downarrow R$$

<proof>

lemma *convex-iu-unit*:

$$R = R\downarrow \implies R \cup\cup\downarrow 1_{\cup\cup} = R$$

<proof>

abbreviation *convex-ii* (**infixl** $\langle \cap\cap\downarrow \rangle$ 70)

where $R \cap\cap\downarrow S \equiv (R \cap\cap S)\downarrow$

lemma *convex-ii*:

$$R \cap\cap\downarrow S = (R\uparrow \cap\cap S\uparrow) \cap R\downarrow \cap S\downarrow$$

<proof>

lemma *convex-ii-sub*:

$$R\downarrow \cap\cap S \subseteq R \cap\cap\downarrow S$$

<proof>

lemma *convex-ii-convex-left:*

$$R \cap\cap\downarrow S = R\downarrow \cap\cap\downarrow S$$

<proof>

lemma *convex-ii-convex-right:*

$$R \cap\cap\downarrow S = R \cap\cap\downarrow S\downarrow$$

<proof>

lemma *convex-ii-convex:*

$$R \cap\cap\downarrow S = R\downarrow \cap\cap\downarrow S\downarrow$$

<proof>

lemma *convex-ii-assoc:*

$$(R \cap\cap\downarrow S) \cap\cap\downarrow T = R \cap\cap\downarrow (S \cap\cap\downarrow T)$$

<proof>

lemma *convex-ii-comm:*

$$R \cap\cap\downarrow S = S \cap\cap\downarrow R$$

<proof>

lemma *convex-ii-unit:*

$$R = R\downarrow \implies R \cap\cap\downarrow 1_{\cap\cap} = R$$

<proof>

lemma *convex-ii-ic:*

$$\sim(R \cup\cup\downarrow S) = \sim R \cap\cap\downarrow \sim S$$

<proof>

lemma *convex-ii-ic:*

$$\sim(R \cap\cap\downarrow S) = \sim R \cup\cup\downarrow \sim S$$

<proof>

abbreviation *convex-sup* :: ('a,'b) mrel set \Rightarrow ('a,'b) mrel ($\cup\downarrow$) **where**

$$\cup\downarrow X \equiv (\cup X)\downarrow$$

lemma *convex-sup-convex:*

$$\cup\downarrow X = (\cup\downarrow X)\downarrow$$

<proof>

lemma *convex-sup-inter:*

$$\cup\downarrow X = \cap\{ Y . Y = Y\downarrow \wedge \cup X \subseteq Y \}$$

<proof>

lemma *convex-ii-dist-convex-sup:*

$$\cup\downarrow X \cup\cup\downarrow S = \cup\downarrow\{ R \cup\cup\downarrow S \mid R . R \in X \}$$

<proof>

lemma *convex-ii-dist-convex-sup*:
 $\bigcup\downarrow X \text{ } \text{ } \text{ } \text{ } S = \bigcup\downarrow\{ R \text{ } \text{ } \text{ } S \mid R . R \in X \}$
<proof>

lemma *convex-dist-sup*:
 $(\bigcup X)\downarrow = \bigcup\downarrow\{ R\downarrow \mid R . R \in X \}$
<proof>

7 Fusion and Fission

7.1 Atoms and co-atoms

definition *atoms* :: ('a,'b) mrel ($\langle A_{\cup\cup} \rangle$)
where $A_{\cup\cup} \equiv \{ (a, \{b\}) \mid a \text{ } b . \text{True} \}$

definition *co-atoms* :: ('a,'b) mrel ($\langle A_{\cap\cap} \rangle$)
where $A_{\cap\cap} \equiv \{ (a, \text{UNIV} - \{b\}) \mid a \text{ } b . \text{True} \}$

declare *atoms-def* [*mr-simp*] *co-atoms-def* [*mr-simp*]

lemma *atoms-solution*:
 $A_{\cup\cup}\uparrow = -1_{\cup\cup}$
<proof>

lemma *atoms-least-solution*:
assumes $R\uparrow = -1_{\cup\cup}$
shows $A_{\cup\cup} \subseteq R$
<proof>

lemma *ic-atoms*:
 $\sim A_{\cup\cup} = A_{\cap\cap}$
<proof>

lemma *ic-co-atoms*:
 $\sim A_{\cap\cap} = A_{\cup\cup}$
<proof>

lemma *co-atoms-solution*:
 $A_{\cap\cap}\downarrow = -1_{\cap\cap}$
<proof>

lemma *co-atoms-least-solution*:
assumes $R\downarrow = -1_{\cap\cap}$
shows $A_{\cap\cap} \subseteq R$
<proof>

lemma *iu-unit-atoms-disjoint*:
 $1_{\cup\cup} \cap A_{\cup\cup} = \{\}$

<proof>

lemma *ii-unit-co-atoms-disjoint*:

$$1_{\cap\cap} \cap A_{\cap\cap} = \{\}$$

<proof>

lemma *atoms-sp-idempotent*:

$$A_{\cup\cup} * A_{\cup\cup} = A_{\cup\cup}$$

<proof>

lemma *atoms-sp-cp*:

$$(R \cap A_{\cup\cup}) * S = (R \cap A_{\cup\cup}) \odot S$$

<proof>

7.2 Inner-functional properties

abbreviation *inner-univalent* :: ('a,'b) mrel \Rightarrow bool **where**

$$\textit{inner-univalent } R \equiv R \subseteq 1_{\cup\cup} \cup A_{\cup\cup}$$

abbreviation *inner-total* :: ('a,'b) mrel \Rightarrow bool **where**

$$\textit{inner-total } R \equiv R \subseteq -1_{\cup\cup}$$

abbreviation *inner-deterministic* :: ('a,'b) mrel \Rightarrow bool **where**

$$\textit{inner-deterministic } R \equiv \textit{inner-total } R \wedge \textit{inner-univalent } R$$

lemma *inner-deterministic-atoms*:

$$\textit{inner-deterministic } R \longleftrightarrow R \subseteq A_{\cup\cup}$$

<proof>

lemma *inner-univalent*:

$$\textit{inner-univalent } R \longleftrightarrow (\forall a b c B . (a,B) \in R \wedge b \in B \wedge c \in B \longrightarrow b = c)$$

<proof>

lemma *inner-univalent-2*:

$$\textit{inner-univalent } R \longleftrightarrow (\forall a B . (a,B) \in R \longrightarrow \textit{finite } B \wedge \textit{card } B \leq \textit{one-class.one})$$

<proof>

lemma *inner-total*:

$$\textit{inner-total } R \longleftrightarrow (\forall a B . (a,B) \in R \longrightarrow (\exists b . b \in B))$$

<proof>

lemma *inner-total-2*:

$$\textit{inner-total } R \longleftrightarrow (\forall a B . (a,B) \in R \longrightarrow B \neq \{\})$$

<proof>

lemma *inner-total-3*:

$$\textit{inner-total } R \longleftrightarrow (\forall a B . (a,B) \in R \wedge \textit{finite } B \longrightarrow \textit{card } B \geq \textit{one-class.one})$$

<proof>

lemma *inner-deterministic:*

inner-deterministic $R \iff (\forall a B . (a,B) \in R \implies (\exists! b . b \in B))$
<proof>

lemma *inner-deterministic-2:*

inner-deterministic $R \iff (\forall a B . (a,B) \in R \implies \text{card } B = \text{one-class.one})$
<proof>

lemma *inner-deterministic-sp-unit:*

inner-deterministic 1
<proof>

lemma *inner-univalent-down:*

assumes *inner-univalent* S
shows $S\downarrow \subseteq S \cup 1_{\cup\cup}$
<proof>

lemma *inner-deterministic-lower-eq:*

assumes *inner-deterministic* V
and *inner-deterministic* W
and $V =\downarrow W$
shows $V = W$
<proof>

lemma *inner-total-down-closed:*

inner-total $T \implies R \subseteq T \implies \text{inner-total } R$
<proof>

lemma *inner-univalent-down-closed:*

inner-univalent $T \implies R \subseteq T \implies \text{inner-univalent } R$
<proof>

lemma *inner-deterministic-down-closed:*

inner-deterministic $T \implies R \subseteq T \implies \text{inner-deterministic } R$
<proof>

lemma *inner-univalent-conver:*

assumes *inner-univalent* R
shows $R = R\downarrow$
<proof>

lemma *inner-deterministic-alt-closure:*

inner-deterministic $R = (R \text{ O } \text{converse } 1 \text{ O } 1 = R)$
<proof>

lemma *inner-deterministic-s-id-conv-epsiloff:*

inner-deterministic $R \implies R \text{ O } \text{converse } s\text{-id} = R \text{ O } \text{epsiloff}$
<proof>

lemma *inner-deterministic-lower-iff*:

assumes *inner-deterministic R*
and *inner-deterministic S*
shows $(R \sqsubseteq\downarrow S) \longleftrightarrow (R \subseteq S)$
<proof>

lemma *inner-deterministic-upper-iff*:

assumes *inner-deterministic R*
and *inner-deterministic S*
shows $(R \sqsubseteq\uparrow S) \longleftrightarrow (S \subseteq R)$
<proof>

lemma *inner-deterministic-lower-eq-iff*:

assumes *inner-deterministic R*
and *inner-deterministic S*
shows $(R =\downarrow S) \longleftrightarrow (R = S)$
<proof>

lemma *inner-deterministic-upper-eq-iff*:

assumes *inner-deterministic R*
and *inner-deterministic S*
shows $(R =\uparrow S) \longleftrightarrow (R = S)$
<proof>

lemma *inner-deterministic-convex-eq-iff*:

assumes *inner-deterministic R*
and *inner-deterministic S*
shows $(R =\updownarrow S) \longleftrightarrow (R = S)$
<proof>

lemma

inner-univalent R \implies *inner-univalent S* \implies *inner-univalent (R $\cup\cup$ S)*
nitpick[*expect=genuine,card=1,2*]
<proof>

lemma *inner-univalent-ii-closed*:

inner-univalent R \implies *inner-univalent S* \implies *inner-univalent (R $\cap\cap$ S)*
<proof>

lemma *inner-total-iu-closed*:

inner-total R \implies *inner-total S* \implies *inner-total (R $\cup\cup$ S)*
<proof>

lemma

inner-total R \implies *inner-total S* \implies *inner-total (R $\cap\cap$ S)*
nitpick[*expect=genuine,card=1,2*]
<proof>

7.3 Fusion

lemma *fusion-set*:

$$\text{fus } R \equiv \{ (a, B) . B = \bigcup \{ C . (a, C) \in R \} \}$$

<proof>

declare *fusion-set* [*mr-simp*]

lemma *fusion-lower-increasing*:

$$R \sqsubseteq\downarrow \text{fus } R$$

<proof>

lemma *fusion-deterministic*:

$$\text{deterministic } (\text{fus } R)$$

<proof>

lemma *fusion-least*:

assumes $R \sqsubseteq\downarrow S$
and *deterministic* S
shows $\text{fus } R \sqsubseteq\downarrow S$
<proof>

lemma *fusion-unique*:

assumes $\forall R . R \sqsubseteq\downarrow f R$
and $\forall R . \text{deterministic } (f R)$
and $\forall R S . R \sqsubseteq\downarrow S \wedge \text{deterministic } S \longrightarrow f R \sqsubseteq\downarrow S$
shows $f T = \text{fus } T$
<proof>

lemma *fusion-down-char*:

$$(\text{fus } R)\downarrow = -((-(R\downarrow) \cap A_{\cup\cup})\uparrow)$$

<proof>

lemma *fusion-up-char*:

$$(\text{fus } R)\uparrow = -((\sim(R\downarrow) \cap A_{\cap\cap})\downarrow)$$

<proof>

lemma *fusion-up-char-2*:

$$(\text{fus } R)\uparrow = -(((R\downarrow) \cap A_{\cup\cup}) * \sim I)\downarrow$$

<proof>

lemma *fusion-char*:

$$\text{fus } R = -((-(R\downarrow) \cap A_{\cup\cup})\uparrow) \cap -((\sim(R\downarrow) \cap A_{\cap\cap})\downarrow)$$

<proof>

lemma *fusion-char-2*:

$$\text{fus } R = -((-(R\downarrow) \cap A_{\cup\cup})\uparrow) \cap -(((R\downarrow) \cap A_{\cup\cup}) * \sim I)\downarrow$$

<proof>

lemma *fusion-lower-isotone*:

$R \sqsubseteq\downarrow S \implies \text{fus } R \sqsubseteq\downarrow \text{fus } S$
 ⟨proof⟩

lemma *fusion-iu-idempotent*:
 $\text{fus } R \cup\cup \text{fus } R = \text{fus } R$
 ⟨proof⟩

lemma *fusion-down*:
 $\text{fus } R = \text{fus } (R\downarrow)$
 ⟨proof⟩

lemma *fusion-iu-total*:
 $\text{total } T \implies T \cup\cup \text{fus } T = \text{fus } T$
 ⟨proof⟩

lemma *fusion-deterministic-fixpoint*:
 $\text{deterministic } R \longleftrightarrow R = \text{fus } R$
 ⟨proof⟩

abbreviation *non-empty* :: ('a,'b) mrel \Rightarrow ('a,'b) mrel (⟨ne \rightarrow [100] 100)
 where $ne R \equiv R \cap -1 \cup\cup$

lemma *non-empty*:
 $ne R = \{ (a,B) \mid a B . (a,B) \in R \wedge B \neq \{\} \}$
 ⟨proof⟩

lemma *ne-equality*:
 $ne R = R \longleftrightarrow R \subseteq -1 \cup\cup$
 ⟨proof⟩

lemma *ne-dist-ou*:
 $ne (R \cup S) = ne R \cup ne S$
 ⟨proof⟩

lemma *ne-down-idempotent*:
 $ne ((ne (R\downarrow))\downarrow) = ne (R\downarrow)$
 ⟨proof⟩

lemma *ne-up*:
 $(ne R)\uparrow = ne R * 1\uparrow$
 ⟨proof⟩

lemma *ne-dist-down-sp*:
 $ne (R\downarrow * S) = ne (R\downarrow) * ne S$
 ⟨proof⟩

lemma *total-ne-down-dist-sp*:
 $\text{total } T \implies ne ((R * T)\downarrow) = ne (R\downarrow) * ne (T\downarrow)$
 ⟨proof⟩

lemma *inner-univalent-char*:

inner-univalent $S \iff (\forall R . \text{fus } R = \text{fus } S \wedge R \sqsubseteq\downarrow S \implies \text{ne } R = \text{ne } S)$
<proof>

lemma *ne-dist-oU*:

$\text{ne } (\bigcup X) = \bigcup (\text{non-empty } X)$
<proof>

7.4 Fission

lemma *fission-set*:

$\text{fis } R = \{ (a, \{b\}) \mid a \text{ } b . \exists B . (a, B) \in R \wedge b \in B \}$
<proof>

declare *fission-set* [*mr-simp*]

lemma *fission-var*:

$\text{fis } R = R\downarrow \cap A_{\cup\cup}$
<proof>

lemma *fission-lower-decreasing*:

$\text{fis } R \sqsubseteq\downarrow R$
<proof>

lemma *fission-inner-deterministic*:

inner-deterministic ($\text{fis } R$)
<proof>

lemma *fission-greatest*:

assumes $S \sqsubseteq\downarrow R$
and *inner-deterministic* S
shows $S \sqsubseteq\downarrow \text{fis } R$
<proof>

lemma *fission-unique*:

assumes $\forall R . f R \sqsubseteq\downarrow R$
and $\forall R . \text{inner-deterministic } (f R)$
and $\forall R S . S \sqsubseteq\downarrow R \wedge \text{inner-deterministic } S \implies S \sqsubseteq\downarrow f R$
shows $f T = \text{fis } T$
<proof>

lemma *fission-lower-isotone*:

$R \sqsubseteq\downarrow S \implies \text{fis } R \sqsubseteq\downarrow \text{fis } S$
<proof>

lemma *fission-idempotent*:

$\text{fis } (\text{fis } R) = \text{fis } R$
<proof>

lemma *fission-top*:

$$\text{fis } U = A_{\cup\cup}$$

<proof>

lemma *fission-down*:

$$\text{fis } R = \text{fis } (R\downarrow)$$

<proof>

lemma *fission-ne-fixpoint*:

$$\text{fis } R = \text{ne } (\text{fis } R)$$

<proof>

lemma *fission-down-ne-fixpoint*:

$$\text{fis } R = \text{ne } ((\text{fis } R)\downarrow)$$

<proof>

lemma *fission-inner-deterministic-fixpoint*:

$$\text{inner-deterministic } R \longleftrightarrow R = \text{fis } R$$

<proof>

lemma *fission-sp-subdist*:

$$\text{fis } (R * S) \subseteq \text{fis } R * \text{fis } S$$

<proof>

lemma *fission-sp-total-dist*:

assumes *total* T

shows $\text{fis } (R * T) = \text{fis } R * \text{fis } T$

<proof>

lemma *fission-dist-ou*:

$$\text{fis } (R \cup S) = \text{fis } R \cup \text{fis } S$$

<proof>

lemma *fission-sp-iu-unit*:

$$\text{fis } (R * 1_{\cup\cup}) = \{\}$$

<proof>

lemma *fission-fusion-lower-decreasing*:

$$\text{fis } (\text{fus } R) \sqsubseteq\downarrow R$$

<proof>

lemma *fission-fusion-lower-increasing*:

$$R \sqsubseteq\downarrow \text{fus } (\text{fis } R)$$

<proof>

lemma *fission-fusion-galois*:

$$\text{fis } R \sqsubseteq\downarrow S \longleftrightarrow R \sqsubseteq\downarrow \text{fus } S$$

<proof>

lemma *fission-fusion*:

$$\text{fis } (\text{fus } R) = \text{fis } R$$

<proof>

lemma *fusion-fission*:

$$\text{fus } (\text{fis } R) = \text{fus } R$$

<proof>

lemma *same-fusion-fission-lower*:

$$\text{fus } R = \text{fus } S \implies \text{fis } R \sqsubseteq\downarrow S$$

<proof>

lemma *fission-below-ne-down-fusion*:

$$\text{fis } R \subseteq \text{ne } ((\text{fus } R)\downarrow)$$

<proof>

lemma *ne-fusion-fission*:

$$(\text{ne } ((\text{fus } R)\downarrow))\uparrow = (\text{fis } R)\uparrow$$

<proof>

lemma *fission-up-ne-down-up*:

$$(\text{fis } R)\uparrow = (\text{ne } (R\downarrow))\uparrow$$

<proof>

lemma *fusion-idempotent*:

$$\text{fus } (\text{fus } R) = \text{fus } R$$

<proof>

lemma *fission-dist-oU*:

$$\text{fis } (\bigcup X) = \bigcup (\text{fis } ' X)$$

<proof>

7.5 Co-fusion and co-fission

definition *co-fusion* :: ('a,'b) mrel \Rightarrow ('a,'b) mrel ($\langle \sqcap \sqcap \rightarrow [80] 80 \rangle$) **where**

$$\sqcap \sqcap R \equiv \{ (a,B) . B = \bigcap \{ C . (a,C) \in R \} \}$$

declare *co-fusion-def* [*mr-simp*]

lemma *co-fusion-upper-decreasing*:

$$\sqcap \sqcap R \sqsubseteq\uparrow R$$

<proof>

lemma *co-fusion-deterministic*:

$$\text{deterministic } (\sqcap \sqcap R)$$

<proof>

lemma *co-fusion-greatest*:

assumes $S \sqsubseteq \uparrow R$
and *deterministic* S
shows $S \sqsubseteq \uparrow \sqcap \sqcap R$
<proof>

lemma *co-fusion-unique*:
assumes $\forall R . f R \sqsubseteq \uparrow R$
and $\forall R . \text{deterministic } (f R)$
and $\forall R S . S \sqsubseteq \uparrow R \wedge \text{deterministic } S \longrightarrow S \sqsubseteq \uparrow f R$
shows $f T = \sqcap \sqcap T$
<proof>

lemma *co-fusion-up-char*:
 $(\sqcap \sqcap R) \uparrow = -((-(R \uparrow) \cap A_{\cap \cap}) \downarrow)$
<proof>

lemma *co-fusion-down-char*:
 $(\sqcap \sqcap R) \downarrow = -((\sim(R \uparrow) \cap A_{\cup \cup}) \uparrow)$
<proof>

lemma *co-fusion-down-char-2*:
 $(\sqcap \sqcap R) \downarrow = -(((R \uparrow) \cap A_{\cap \cap}) \odot \sim I) \uparrow)$
<proof>

lemma *co-fusion-char*:
 $\sqcap \sqcap R = -((-(R \uparrow) \cap A_{\cap \cap}) \downarrow) \cap -((\sim(R \uparrow) \cap A_{\cup \cup}) \uparrow)$
<proof>

lemma *co-fusion-char-2*:
 $\sqcap \sqcap R = -((-(R \uparrow) \cap A_{\cap \cap}) \downarrow) \cap -(((R \uparrow) \cap A_{\cap \cap}) \odot \sim I) \uparrow)$
<proof>

lemma *co-fusion-upper-isotone*:
 $R \sqsubseteq \uparrow S \implies \sqcap \sqcap R \sqsubseteq \uparrow \sqcap \sqcap S$
<proof>

lemma *co-fusion-ii-idempotent*:
 $\sqcap \sqcap R \cap \sqcap \sqcap R = \sqcap \sqcap R$
<proof>

lemma *co-fusion-up*:
 $\sqcap \sqcap R = \sqcap \sqcap (R \uparrow)$
<proof>

lemma *co-fusion-ii-total*:
 $\text{total } T \implies T \cap \sqcap \sqcap T = \sqcap \sqcap T$
<proof>

lemma *co-fusion-deterministic-fixpoint*:

deterministic $R \longleftrightarrow R = \prod \prod R$
 ⟨proof⟩

abbreviation *co-fission* :: $(a, b) \text{ mrel} \Rightarrow (a, b) \text{ mrel} (\text{at}_{\cap\cap} \rightarrow [80] 80)$ **where**
 $\text{at}_{\cap\cap} R \equiv R \uparrow \cap A_{\cap\cap}$

lemma *co-fission*:
 $\text{at}_{\cap\cap} R = \{ (a, B) \mid a B . (\exists b . -B = \{b\}) \wedge (\exists C . (a, C) \in R \wedge C \subseteq B) \}$
 ⟨proof⟩

declare *co-fission* [*mr-simp*]

lemma *co-fission-upper-increasing*:
 $R \sqsubseteq \uparrow \text{at}_{\cap\cap} R$
 ⟨proof⟩

lemma *co-fission-ic-inner-deterministic*:
inner-deterministic $(\sim \text{at}_{\cap\cap} R)$
 ⟨proof⟩

lemma *co-fission-least*:
assumes $R \sqsubseteq \uparrow S$
and *inner-deterministic* $(\sim S)$
shows $\text{at}_{\cap\cap} R \sqsubseteq \uparrow S$
 ⟨proof⟩

lemma *co-fission-unique*:
assumes $\forall R . R \sqsubseteq \uparrow f R$
and $\forall R . \text{inner-deterministic} (\sim f R)$
and $\forall R S . R \sqsubseteq \uparrow S \wedge \text{inner-deterministic} (\sim S) \longrightarrow f R \sqsubseteq \uparrow S$
shows $f T = \text{at}_{\cap\cap} T$
 ⟨proof⟩

lemma *co-fission-upper-isotone*:
 $R \sqsubseteq \uparrow S \Longrightarrow \text{at}_{\cap\cap} R \sqsubseteq \uparrow \text{at}_{\cap\cap} S$
 ⟨proof⟩

lemma *co-fission-idempotent*:
 $\text{at}_{\cap\cap} (\text{at}_{\cap\cap} R) = \text{at}_{\cap\cap} R$
 ⟨proof⟩

lemma *co-fission-top*:
 $\text{at}_{\cap\cap} U = A_{\cap\cap}$
 ⟨proof⟩

lemma *co-fission-up*:
 $\text{at}_{\cap\cap} R = \text{at}_{\cap\cap} (R \uparrow)$
 ⟨proof⟩

lemma *co-fission-ic-inner-deterministic-fixpoint:*
inner-deterministic $(\sim R) \longleftrightarrow R = at_{\cap\cap} R$
 ⟨proof⟩

lemma *co-fusion-co-fission-upper-decreasing:*
 $\cap\cap(at_{\cap\cap} R) \sqsubseteq\uparrow R$
 ⟨proof⟩

lemma *co-fission-co-fusion-upper-increasing:*
 $R \sqsubseteq\uparrow at_{\cap\cap} (\cap\cap R)$
 ⟨proof⟩

lemma *co-fusion-co-fission-galois:*
 $\cap\cap R \sqsubseteq\uparrow S \longleftrightarrow R \sqsubseteq\uparrow at_{\cap\cap} S$
 ⟨proof⟩

lemma *co-fission-co-fusion:*
 $at_{\cap\cap} (\cap\cap R) = at_{\cap\cap} R$
 ⟨proof⟩

lemma *co-fusion-co-fission:*
 $\cap\cap(at_{\cap\cap} R) = \cap\cap R$
 ⟨proof⟩

lemma *same-co-fusion-co-fission-upper:*
 $\cap\cap R = \cap\cap S \implies S \sqsubseteq\uparrow at_{\cap\cap} R$
 ⟨proof⟩

lemma *co-fusion-idempotent:*
 $\cap\cap(\cap\cap R) = \cap\cap R$
 ⟨proof⟩

8 Modalities

8.1 Tests

abbreviation *test* :: $(\prime a, \prime a) \text{ mrel} \Rightarrow \text{bool}$ where
 $\text{test } R \equiv R \subseteq 1$

lemma *test:*
 $\text{test } R \longleftrightarrow (\forall a B . (a, B) \in R \longrightarrow B = \{a\})$
 ⟨proof⟩

lemma *test-fix:* $\text{test } R \equiv R \cap 1_\sigma = R$
 ⟨proof⟩

lemma *test-ou-closed:*
 $\text{test } p \implies \text{test } q \implies \text{test } (p \cup q)$
 ⟨proof⟩

lemma *test-oi-closed*:

$test\ p \implies test\ (p \cap q)$
<proof>

abbreviation *test-complement* :: ('a,'a) mrel \Rightarrow ('a,'a) mrel ($\lrcorner \rightarrow$ [80] 80)

where

$\lrcorner R \equiv -R \cap 1$

lemma *test-complement-closed*:

$test\ (\lrcorner p)$
<proof>

lemma *test-double-complement*:

$test\ p \longleftrightarrow p = \lrcorner \lrcorner p$
<proof>

lemma *test-complement*:

$(a, \{a\}) \in \lrcorner p \longleftrightarrow \neg (a, \{a\}) \in p$
<proof>

declare *test-complement* [*mr-simp*]

lemma *test-complement-antitone*:

assumes *test p*
shows $p \subseteq q \longleftrightarrow \lrcorner q \subseteq \lrcorner p$
<proof>

lemma *test-complement-huntington*:

$test\ p \implies p = \lrcorner (\lrcorner p \cup \lrcorner q) \cup \lrcorner (\lrcorner p \cup q)$
<proof>

abbreviation *test-implication* :: ('a,'a) mrel \Rightarrow ('a,'a) mrel \Rightarrow ('a,'a) mrel

(**infixl** \rightarrow 65) **where**

$p \rightarrow q \equiv \lrcorner p \cup q$

lemma *test-implication-closed*:

$test\ q \implies test\ (p \rightarrow q)$
<proof>

lemma *test-implication*:

$(a, \{a\}) \in p \rightarrow q \longleftrightarrow ((a, \{a\}) \in p \longrightarrow (a, \{a\}) \in q)$
<proof>

declare *test-implication* [*mr-simp*]

lemma *test-implication-left-antitone*:

assumes *test p*
shows $p \subseteq r \implies r \rightarrow q \subseteq p \rightarrow q$

<proof>

lemma *test-implication-right-isotone:*

assumes *test p*

shows $q \subseteq r \implies p \rightarrow q \subseteq p \rightarrow r$

<proof>

lemma *test-sp-idempotent:*

test p $\implies p * p = p$

<proof>

lemma *test-sp:*

assumes *test p*

shows $p * R = (p * U) \cap R$

<proof>

lemma *sp-test:*

test p $\implies R * p = R \cap (U * p)$

<proof>

lemma *sp-test-dist-oi:*

test p $\implies (R \cap S) * p = (R * p) \cap (S * p)$

<proof>

lemma *sp-test-dist-oi-left:*

test p $\implies (R \cap S) * p = (R * p) \cap S$

<proof>

lemma *sp-test-dist-oi-right:*

test p $\implies (R \cap S) * p = R \cap (S * p)$

<proof>

lemma *sp-test-sp-oi-left:*

test p $\implies (R \cap (U * p)) * T = R * p * T$

<proof>

lemma *sp-test-sp-oi-right:*

test p $\implies R * ((p * U) \cap T) = R * p * T$

<proof>

lemma *test-sp-ne:*

test p $\implies p * ne R = ne (p * R)$

<proof>

lemma *ne-sp-test:*

test p $\implies ne R * p = ne (R * p)$

<proof>

lemma *top-sp-test-down-closed:*

assumes *test p*
shows $U * p = (U * p)\downarrow$
 $\langle proof \rangle$

lemma *oc-top-sp-test-up-closed*:
 $test\ p \implies \neg(U * p) = (\neg(U * p))\uparrow$
 $\langle proof \rangle$

lemma *top-sp-test*:
 $test\ p \implies (a, B) \in U * p \iff (\forall b \in B . (b, \{b\}) \in p)$
 $\langle proof \rangle$

lemma *oc-top-sp-test*:
 $test\ p \implies (a, B) \in \neg(U * p) \iff (\exists b \in B . (b, \{b\}) \notin p)$
 $\langle proof \rangle$

declare *top-sp-test* [*mr-simp*] *oc-top-sp-test* [*mr-simp*]

lemma *oc-top-sp-test-0*:
 $\neg 1_{\cup\cup} * \wr p = ne\ (U * \wr p)$
 $\langle proof \rangle$

lemma *oc-top-sp-test-1*:
assumes *test p*
shows $\neg(U * p) = (ne\ (U * \wr p))\uparrow$
 $\langle proof \rangle$

lemma *oc-top-sp-test-2*:
 $test\ p \implies \neg(U * p) = (\neg 1_{\cup\cup} * \wr p)\uparrow$
 $\langle proof \rangle$

lemma *split-sp-test*:
assumes *test p*
shows $R = (R * p) \cup (ne\ R \cap (ne\ (R\downarrow * \wr p))\uparrow)$
 $\langle proof \rangle$

lemma *top-sp-test-down-iff-1*:
assumes *test p*
shows $R \subseteq U * p \iff R\downarrow \subseteq U * p$
 $\langle proof \rangle$

lemma *test-ne*:
 $test\ p \implies ne\ p = p$
 $\langle proof \rangle$

lemma *ne-test-up*:
 $test\ p \implies ne\ (p\uparrow) = p\uparrow$
 $\langle proof \rangle$

lemma *ne-sp-test-up*:

$$\text{test } p \implies (ne (R * p))\uparrow = ne R * p\uparrow$$

<proof>

lemma *ne-down-sp-test-up*:

$$\text{test } p \implies ne (R\downarrow * p\uparrow) = ne (R\downarrow) * p\uparrow$$

<proof>

lemma *test-up-sp*:

$$\text{test } p \implies p\uparrow = p * 1\uparrow$$

<proof>

lemma *top-test-oi-top-complement*:

$$\text{test } p \implies (U * p) \cap (U * \imath p) = 1_{\cup\cup}$$

<proof>

lemma *sp-test-oi-complement*:

$$\text{test } p \implies (R * p) \cap (R * \imath p) = R \cap 1_{\cup\cup}$$

<proof>

lemma *ne-top-sp-test-complement*:

assumes *test p*
shows $ne (U * p) * \imath p = \{\}$

<proof>

lemma *complement-test-sp-top*:

assumes *test p*
shows $-(p * U) = \imath p * U$

<proof>

lemma *top-sp-test-shunt*:

assumes *test p*
shows $R \subseteq U * p \longrightarrow R * \imath p \subseteq 1_{\cup\cup}$

<proof>

lemma *top-sp-test-down-iff-2*:

assumes *test p*
shows $R\downarrow \subseteq U * p \longleftrightarrow R\downarrow * \imath p \subseteq 1_{\cup\cup}$

<proof>

lemma *top-sp-test-down-iff-3*:

$$R\downarrow * \imath p \subseteq 1_{\cup\cup} \longleftrightarrow ne (R\downarrow) * \imath p \subseteq \{\}$$

<proof>

lemma *top-sp-test-down-iff-4*:

assumes *test p*
shows $R\downarrow \cap (U * \imath p) \subseteq 1_{\cup\cup} \longleftrightarrow R\downarrow \subseteq 1_{\cup\cup} \cup (U * p)$

<proof>

lemma *top-sp-test-down-iff-5*:

assumes *test p*

shows $R\downarrow \subseteq U * p \longleftrightarrow R\downarrow \subseteq 1_{UU} \cup (U * p)$
<proof>

lemma *iu-test-sp-left-zero*:

assumes $q \subseteq 1_{UU}$

shows $q * R = q$
<proof>

lemma *test-iu-test-split*:

$t \subseteq 1 \cup 1_{UU} \longleftrightarrow (\exists p q . p \subseteq 1 \wedge q \subseteq 1_{UU} \wedge t = p \cup q)$
<proof>

lemma *test-iu-test-sp-assoc-1*:

$t \subseteq 1 \cup 1_{UU} \implies t * (R * S) = (t * R) * S$
<proof>

lemma *test-iu-test-sp-assoc-2*:

$t \subseteq 1_{UU} \implies R * (t * S) = (R * t) * S$
<proof>

lemma *test-iu-test-sp-assoc-3*:

assumes $t \subseteq 1 \cup 1_{UU}$

shows $R * (t * S) = (R * t) * S$
<proof>

lemma *test-iu-test-sp-assoc-4*:

$t \subseteq 1_{UU} \implies R * (S * t) = (R * S) * t$
<proof>

lemma *test-iu-test-sp-assoc-5*:

assumes $t \subseteq 1 \cup 1_{UU}$

shows $R * (S * t) = (R * S) * t$
<proof>

lemma *inner-deterministic-sp-assoc*:

assumes *inner-univalent t*

shows $t * (R * S) = (t * R) * S$
<proof>

lemma *iu-unit-below-top-sp-test*:

$1_{UU} \subseteq U * R$

<proof>

lemma *ne-oi-complement-top-sp-test-1*:

$ne (R \cap -(U * S)) = R \cap -(U * S)$

<proof>

lemma *ne-oi-complement-top-sp-test-2*:
 $ne\ R \cap -(U * S) = R \cap -(U * S)$
 ⟨proof⟩

lemma *schroeder-test*:
assumes *test p*
shows $R * p \subseteq S \longleftrightarrow -S * p \subseteq -R$
 ⟨proof⟩

lemma *complement-test-sp-test*:
 $test\ p \implies -p * p \subseteq -1$
 ⟨proof⟩

lemma *test-sp-commute*:
 $test\ p \implies test\ q \implies p * q = q * p$
 ⟨proof⟩

lemma *test-shunting*:
assumes *test p*
and *test q*
and *test r*
shows $p * q \subseteq r \longleftrightarrow p \subseteq r \cup \setminus q$
 ⟨proof⟩

lemma *test-sp-is-iu*:
 $test\ p \implies test\ q \implies p * q = p \cup \cup q$
 ⟨proof⟩

lemma *test-set*:
 $test\ p \implies p = \{ (a, \{a\}) \mid a . (a, \{a\}) \in p \}$
 ⟨proof⟩

lemma *test-sp-is-ii*:
assumes *test p*
and *test q*
shows $p * q = p \cap \cap q$
 ⟨proof⟩

lemma *test-galois-1*:
assumes *test p*
and *test q*
shows $p * q \subseteq r \longleftrightarrow q \subseteq p \rightarrow r$
 ⟨proof⟩

lemma *test-sp-shunting*:
assumes *test p*
shows $\setminus p * R \subseteq \{\} \longleftrightarrow R \subseteq p * R$
 ⟨proof⟩

lemma *test-oU-closed*:
 $\forall p \in X . \text{test } p \implies \text{test } (\bigcup X)$
 $\langle \text{proof} \rangle$

lemma *test-oI-closed*:
 $\exists p \in X . \text{test } p \implies \text{test } (\bigcap X)$
 $\langle \text{proof} \rangle$

lemma *sp-test-dist-oI*:
assumes *test* p
and $X \neq \{\}$
shows $(\bigcap X) * p = (\bigcap R \in X . R * p)$
 $\langle \text{proof} \rangle$

lemma *test-iU-is-iI*:
assumes $\forall i \in I . \text{test } (X \ i)$
and $I \neq \{\}$
shows $\bigcup \bigcup X | I = \bigcap \bigcap X | I$
 $\langle \text{proof} \rangle$

lemma *test-iU-is-oI*:
assumes $\forall i \in I . \text{test } (X \ i)$
and $I \neq \{\}$
shows $\bigcup \bigcup X | I = \bigcap (X \ ' \ I)$
 $\langle \text{proof} \rangle$

8.2 Domain and antidomain

declare *Dom-def* [*mr-simp*]

abbreviation *aDom* :: $('a, 'b) \text{ mrel} \Rightarrow ('a, 'a) \text{ mrel}$ **where**
 $a\text{Dom } R \equiv \lambda \text{ Dom } R$

lemma *ad-set*: $a\text{Dom } R = \{(a, \{a\}) \mid a. \neg(\exists A. (a, A) \in R)\}$
 $\langle \text{proof} \rangle$

lemma *d-test*:
 $\text{test } (\text{Dom } R)$
 $\langle \text{proof} \rangle$

lemma *ad-test*:
 $\text{test } (a\text{Dom } R)$
 $\langle \text{proof} \rangle$

lemma *ad-expl*:
 $a\text{Dom } R = -((R * 1_{\cup\cup}) \cup\cup 1) \cap 1$
 $\langle \text{proof} \rangle$

lemma *ad-expl-2*:

$aDom (R::('a,'b) mrel) = -((R * (1_{\cup\cup}::('b,'a) mrel))\uparrow) \cap (1::('a,'a) mrel)$
 ⟨proof⟩

lemma *aDom*:

$aDom R = \{ (a, \{a\}) \mid a . \neg(\exists B . (a, B) \in R) \}$
 ⟨proof⟩

declare *aDom* [*mr-simp*]

lemma *d-down-oi-up-1*:

$Dom (R\downarrow \cap S) = Dom (R \cap S\uparrow)$
 ⟨proof⟩

lemma *d-down-oi-up-2*:

$Dom (R\downarrow \cap S) = Dom (R\downarrow \cap S\uparrow)$
 ⟨proof⟩

lemma *d-ne-down-dp-complement-test*:

assumes *test p*

shows $Dom (R \cap -(U * p)) = Dom (ne (R\downarrow) * \wr p)$
 ⟨proof⟩

lemma *d-strict*:

$R = \{\} \longleftrightarrow Dom R = \{\}$
 ⟨proof⟩

lemma *d-sp-strict*:

$R * S = \{\} \longleftrightarrow R * Dom S = \{\}$
 ⟨proof⟩

lemma *d-complement-ad*:

$Dom R = \wr aDom R$
 ⟨proof⟩

lemma *down-sp-below-iu-unit*:

$R\downarrow * S \subseteq 1_{\cup\cup} \longleftrightarrow R \subseteq U * aDom (ne S)$
 ⟨proof⟩

lemma *ad-sp-bot*:

$aDom R * R = \{\}$
 ⟨proof⟩

lemma *sp-top-d*:

$R * U \subseteq Dom R * U$
 ⟨proof⟩

lemma *d-sp-top*:

$Dom (R * U) = Dom R$
 ⟨proof⟩

lemma *d-down*:

$$\text{Dom } (R\downarrow) = \text{Dom } R$$

<proof>

lemma *d-up*:

$$\text{Dom } (R\uparrow) = \text{Dom } R$$

<proof>

lemma *d-isotone*:

$$R \subseteq S \implies \text{Dom } R \subseteq \text{Dom } S$$

<proof>

lemma *ad-antitone*:

$$R \subseteq S \implies a\text{Dom } S \subseteq a\text{Dom } R$$

<proof>

lemma *d-dist-ou*:

$$\text{Dom } (R \cup S) = \text{Dom } R \cup \text{Dom } S$$

<proof>

lemma *d-dist-iu*:

$$\text{Dom } (R \cup\cup S) = \text{Dom } R * \text{Dom } S$$

<proof>

lemma *d-dist-ii*:

$$\text{Dom } (R \cap\cap S) = \text{Dom } R * \text{Dom } S$$

<proof>

lemma *d-loc*:

$$\text{Dom } (R * \text{Dom } S) = \text{Dom } (R * S)$$

<proof>

lemma *ad-loc*:

$$a\text{Dom } (R * \text{Dom } S) = a\text{Dom } (R * S)$$

<proof>

lemma *d-ne-down*:

$$\text{Dom } (ne (R\downarrow)) = \text{Dom } (ne R)$$

<proof>

lemma *ne-sp-iu-unit-up*:

$$ne R = R \implies (R * 1_{\cup\cup})\uparrow = R * U$$

<proof>

lemma *ne-d-expl*:

$$ne R = R \implies \text{Dom } R = R * U \cap 1$$

<proof>

lemma *ne-a-expl*:

$$ne\ R = R \implies aDom\ R = -(R * U) \cap 1$$

<proof>

lemma *d-dist-oU*:

$$Dom\ (\bigcup X) = \bigcup (Dom\ ' X)$$

<proof>

lemma *d-dist-iU-iI*:

$$Dom\ (\bigcup \bigcup X|I) = Dom\ (\bigcap \bigcap X|I)$$

<proof>

lemma *d-dist-iU-oI*:

assumes $I \neq \{\}$

shows $Dom\ (\bigcup \bigcup X|I) = \bigcap (Dom\ ' X\ ' I)$

<proof>

8.3 Left residual

definition *sp-lres* :: $('a, 'c)\ mrel \Rightarrow ('b, 'c)\ mrel \Rightarrow ('a, 'b)\ mrel$ (**infixl** $\langle \circ \rangle$ 65)

where

$$Q \circ R \equiv \{ (a, B) . \forall f . (\forall b \in B . (b, f\ b) \in R) \longrightarrow (a, \bigcup \{ f\ b \mid b . b \in B \}) \in Q \}$$

declare *sp-lres-def* [*mr-simp*]

lemma *sp-lres-galois*:

$$S * R \subseteq Q \longleftrightarrow S \subseteq Q \circ R$$

<proof>

lemma *sp-lres-expl*:

$$Q \circ R = \bigcup \{ S . S * R \subseteq Q \}$$

<proof>

lemma *bot-sp-lres-d*:

$$\{\} \circ R = \{\} \circ Dom\ R$$

<proof>

lemma *bot-sp-lres-expl*:

$$\{\} \circ R = -(U * Dom\ R)$$

<proof>

lemma *sp-lres-sp-below*:

$$(Q \circ R) * R \subseteq Q$$

<proof>

lemma *sp-lres-left-isotone*:

$$Q \subseteq S \implies Q \circ R \subseteq S \circ R$$

<proof>

lemma *sp-lres-right-antitone*:
 $S \subseteq R \implies Q \circ R \subseteq Q \circ S$
 ⟨proof⟩

lemma *sp-lres-down-closed-1*:
 $Q \downarrow \circ R = Q \downarrow \circ R \downarrow$
 ⟨proof⟩

lemma *sp-lres-down-closed-2*:
 assumes $R \downarrow = R$
 and *total* T
 shows $(R \circ T) \downarrow = R \circ T$
 ⟨proof⟩

lemma *down-sp-sp*:
 $R \downarrow * S = R * (1_{UU} \cup S)$
 ⟨proof⟩

lemma *iu-unit-sp-lres-iu-unit-ou*:
 $U * aDom (ne R) = 1_{UU} \circ (1_{UU} \cup R)$
 ⟨proof⟩

lemma *bot-sl-below-complement-d*:
 $\{\} \circ R \subseteq - Dom R$
 ⟨proof⟩

lemma *sp-unit-oi-bot-sp-lres*:
 $1 \cap - Dom R = 1 \cap (\{\} \circ R)$
 ⟨proof⟩

lemma *ad-explicit-d*:
 $aDom R = -(U * Dom R) \cap 1$
 ⟨proof⟩

lemma *top-test-sp-lres-total-expl-1*:
 assumes *test* p
 shows $\forall S . S \downarrow \subseteq (U * p) \circ R \iff S \subseteq U * aDom (R \cap -(U * p))$
 ⟨proof⟩

lemma *top-test-sp-lres-total-expl-2*:
 assumes *test* p
 and *total* T
 shows $(U * p) \circ T = U * aDom (T \cap -(U * p))$
 ⟨proof⟩

lemma *top-test-sp-lres-total-expl-3*:
 assumes *test* p
 shows $((U * p) \circ R) \cap 1 = aDom (R \cap -(U * p))$

<proof>

lemma *top-test-sp-lres-total-expl-4:*

assumes *test p*

shows $aDom (ne (R\downarrow) * \wr p) = ((U * p) \circledast R) \cap 1$

<proof>

lemma *oi-complement-top-sp-test-top-1:*

assumes *test p*

shows $(R \cap -(U * p)) * U = (R\downarrow \cap -(U * p)) * U$

<proof>

lemma *oi-complement-top-sp-test-top-2:*

assumes *test p*

shows $(R\downarrow \cap -(U * p)) * U = ne (R\downarrow) * \wr p * U$

<proof>

lemma *oi-complement-top-sp-test-top-3:*

assumes *test p*

shows $(R\downarrow \cap -(U * p)) * U = ne (R\downarrow) * -(p * U)$

<proof>

lemma *split-sp-test-2:*

test p $\implies R \subseteq R * p \cup ne (R\downarrow) * (\wr p)\uparrow$

<proof>

lemma *split-sp-test-3:*

test p $\implies R \subseteq R * p \cup R\downarrow * (\wr p)\uparrow$

<proof>

lemma *split-sp-test-4:*

assumes *test p*

and *test q*

shows $R * (p \cup q) \subseteq R * p \cup ne (R\downarrow) * q\uparrow$

<proof>

lemma *split-sp-test-5:*

assumes *test p*

and *test q*

shows $R * (p \cup q) \subseteq R * p \cup R\downarrow * q\uparrow$

<proof>

lemma *split-sp-test-6:*

assumes *test p*

and *test q*

shows $Dom (R * (p \cup q)) \subseteq Dom (R * p \cup ne (R\downarrow) * q)$

<proof>

lemma *split-sp-test-7:*

assumes *test p*
and *test q*
shows $Dom (ne (R\downarrow) * (p \cup q)) = Dom (ne (R\downarrow) * p \cup ne (R\downarrow) * q)$
 $\langle proof \rangle$

lemma *test-sp-left-dist-iu-1:*
 $test\ p \implies p * (R \cup\cup S) = p * R \cup\cup S$
 $\langle proof \rangle$

lemma *test-sp-left-dist-iu-2:*
 $test\ p \implies p * (R \cup\cup S) = R \cup\cup p * S$
 $\langle proof \rangle$

lemma *d-sp-below-iu-down:*
 $Dom\ R * S \subseteq (R \cup\cup S)\downarrow$
 $\langle proof \rangle$

lemma *d-sp-ne-down-below-ne-iu-down:*
 $Dom\ R * ne (S\downarrow) \subseteq ne ((R \cup\cup S)\downarrow)$
 $\langle proof \rangle$

lemma *top-test:*
 $test\ p \implies U * p = \{ (a, B) . (\forall b \in B . (b, \{b\}) \in p) \}$
 $\langle proof \rangle$

lemma *iu-oi-complement-top-test-ou-up:*
 $test\ p \implies (R \cup\cup S) \cap -(U * p) \subseteq ((R \cup S) \cap -(U * p))\uparrow$
 $\langle proof \rangle$

lemma *d-ne-iu-down-sp-test-ou:*
assumes *test p*
shows $Dom (ne ((R \cup\cup S)\downarrow) * p) \subseteq Dom ((ne (R\downarrow) \cup ne (S\downarrow)) * p)$
 $\langle proof \rangle$

lemma *test-sp-left-dist-iU:*
assumes *test p*
and $I \neq \{\}$
shows $p * (\bigcup\bigcup X|I) = \bigcup\bigcup (\lambda i . p * X\ i)|I$
 $\langle proof \rangle$

8.4 Modal operations

definition *adia* :: $('a, 'b) mrel \implies ('b, 'b) mrel \implies ('a, 'a) mrel (\langle | - \rangle \rightarrow [50, 90] 95)$
where

$$|R\rangle p \equiv \{ (a, \{a\}) \mid a . \exists B . (a, B) \in R \wedge (\forall b \in B . (b, \{b\}) \in p) \}$$

definition *abox* :: $('a, 'b) mrel \implies ('b, 'b) mrel \implies ('a, 'a) mrel (\langle | - \rangle \rightarrow [50, 90] 95)$
where

$$|R\rangle p \equiv \{ (a, \{a\}) \mid a . \forall B . (a, B) \in R \longrightarrow (\forall b \in B . (b, \{b\}) \in p) \}$$

definition $edia :: ('a,'b) mrel \Rightarrow ('b,'b) mrel \Rightarrow ('a,'a) mrel (\lrcorner | - \rceil) \rightarrow [50,90]$
 95) **where**

$|R\rceil p \equiv \{ (a,\{a\}) \mid a . \exists B . (a,B) \in R \wedge (\exists b \in B . (b,\{b\}) \in p) \}$

definition $ebox :: ('a,'b) mrel \Rightarrow ('b,'b) mrel \Rightarrow ('a,'a) mrel (\lrcorner | - \rfloor) \rightarrow [50,90]$ 95)
where

$|R\rfloor p \equiv \{ (a,\{a\}) \mid a . \forall B . (a,B) \in R \longrightarrow (\exists b \in B . (b,\{b\}) \in p) \}$

declare $adia-def$ [*mr-simp*] $abox-def$ [*mr-simp*] $edia-def$ [*mr-simp*] $ebox-def$ [*mr-simp*]

lemma $adia$:

assumes $test\ p$

shows $|R\rceil p = Dom\ (R * p)$

<proof>

lemma $abox-1$:

assumes $test\ p$

shows $|R\rfloor p = aDom\ (R \cap \lrcorner (U * p))$

<proof>

lemma $abox$:

assumes $test\ p$

shows $|R\rfloor p = aDom\ (ne\ (R\downarrow) * \wr p)$

<proof>

lemma $edia-1$:

assumes $test\ p$

shows $|R\rceil p = Dom\ (R \cap \lrcorner (U * \wr p))$

<proof>

lemma $edia$:

assumes $test\ p$

shows $|R\rceil p = Dom\ (ne\ (R\downarrow) * p)$

<proof>

lemma $ebox$:

assumes $test\ p$

shows $|R\rfloor p = aDom\ (R * \wr p)$

<proof>

lemma $abox-2$:

assumes $test\ p$

shows $|R\rfloor p = \lrcorner ((R \cap \lrcorner (U * p)) * U) \cap 1$

<proof>

lemma $abox-3$:

assumes $test\ p$

shows $|R]p = -(ne (R\downarrow) * \wr p * U) \cap 1$
 $\langle proof \rangle$

lemma *abox-4*:
assumes *test p*
shows $|R]p = ((U * p) \odot R) \cap 1$
 $\langle proof \rangle$

lemma *abox-ebox*:
assumes *test p*
shows $|R]p = |ne (R\downarrow)]p$
 $\langle proof \rangle$

lemma *abox-edia*:
assumes *test p*
shows $|R]p = \wr |R\rangle(\wr p)$
 $\langle proof \rangle$

lemma *abox-adia*:
assumes *test p*
shows $|R]p = \wr |ne (R\downarrow)\rangle(\wr p)$
 $\langle proof \rangle$

lemma *edia-adia*:
assumes *test p*
shows $|R\rangle p = |ne (R\downarrow)\rangle p$
 $\langle proof \rangle$

lemma *edia-abox*:
assumes *test p*
shows $|R\rangle p = \wr |R](\wr p)$
 $\langle proof \rangle$

lemma *edia-ebox*:
assumes *test p*
shows $|R\rangle p = \wr |ne (R\downarrow)](\wr p)$
 $\langle proof \rangle$

lemma *abox-ne-down*:
assumes *test p*
shows $|R]p = |ne (R\downarrow)]p$
 $\langle proof \rangle$

lemma *edia-ne-down*:
assumes *test p*
shows $|R\rangle p = |ne (R\downarrow)\rangle p$
 $\langle proof \rangle$

lemma *adia-up*:

assumes $test\ p$
shows $|R\rangle p = |R\uparrow\rangle p$
 $\langle proof \rangle$

lemma *ebox-up*:
assumes $test\ p$
shows $|R]]p = |R\uparrow]]p$
 $\langle proof \rangle$

lemma *adia-ebox*:
assumes $test\ p$
shows $|R\rangle p = \iota |R]](\iota\ p)$
 $\langle proof \rangle$

lemma *ebox-adia*:
assumes $test\ p$
shows $|R]]p = \iota |R\rangle(\iota\ p)$
 $\langle proof \rangle$

lemma *abox-down*:
assumes $test\ p$
shows $|R]p = |R\downarrow]p$
 $\langle proof \rangle$

lemma *edia-down*:
assumes $test\ p$
shows $|R\rangle\rangle p = |R\downarrow\rangle\rangle p$
 $\langle proof \rangle$

lemma *fusion-oi-complement-top-test-up*:
 $test\ p \implies fus\ R \cap -(U * p) \subseteq (R \cap -(U * p))\uparrow$
 $\langle proof \rangle$

lemma *adia-left-isotone*:
 $test\ p \implies R \subseteq S \implies |R\rangle p \subseteq |S\rangle p$
 $\langle proof \rangle$

lemma *adia-right-isotone*:
 $test\ p \implies test\ q \implies p \subseteq q \implies |R\rangle p \subseteq |R\rangle q$
 $\langle proof \rangle$

lemma *abox-left-antitone*:
 $test\ p \implies R \subseteq S \implies |S]p \subseteq |R]p$
 $\langle proof \rangle$

lemma *abox-right-isotone*:
 $test\ p \implies test\ q \implies p \subseteq q \implies |R]p \subseteq |R]q$
 $\langle proof \rangle$

lemma *edia-left-isotone*:

test $p \implies R \subseteq S \implies |R\rangle\rangle p \subseteq |S\rangle\rangle p$

<proof>

lemma *edia-right-isotone*:

test $p \implies \text{test } q \implies p \subseteq q \implies |R\rangle\rangle p \subseteq |R\rangle\rangle q$

<proof>

lemma *ebox-left-antitone*:

test $p \implies R \subseteq S \implies |S]]p \subseteq |R]]p$

<proof>

lemma *ebox-right-isotone*:

test $p \implies \text{test } q \implies p \subseteq q \implies |R]]p \subseteq |R]]q$

<proof>

lemma *edia-fusion*:

assumes *test* p

shows $|R\rangle\rangle p = |fus R\rangle\rangle p$

<proof>

lemma *abox-fusion*:

assumes *test* p

shows $|R]p = |fus R]p$

<proof>

lemma *abox-fission*:

assumes *test* p

shows $|R]p = |fis R]p$

<proof>

lemma *edia-fission*:

assumes *test* p

shows $|R\rangle\rangle p = |fis R\rangle\rangle p$

<proof>

lemma *fission-below*:

$fis R \subseteq S \iff (\forall a b B . (a,B) \in R \wedge b \in B \implies (a,\{b\}) \in S)$

<proof>

lemma *below-fission-up*:

$S \subseteq (fis R)\uparrow \iff (\forall a B . (a,B) \in S \implies (\exists C . (a,C) \in R \wedge C \cap B \neq \{\}))$

<proof>

lemma *ebox-below-abox*:

assumes *test* p

and $fis R \subseteq S$

shows $|S]]p \subseteq |R]]p$

<proof>

lemma *abox-below-ebox*:

assumes *test p*
and $S \subseteq (fis\ R)\uparrow$
shows $|R]p \subseteq |S]]p$
<proof>

lemma *abox-eq-ebox*:

assumes *test p*
and $fis\ R \subseteq S$
and $S \subseteq (fis\ R)\uparrow$
shows $|R]p = |S]]p$
<proof>

lemma *abox-eq-ebox-sufficient*:

$S = fis\ R \vee S = ne\ (R\downarrow) \vee S = (ne\ (R\downarrow))\uparrow \longrightarrow fis\ R \subseteq S \wedge S \subseteq (fis\ R)\uparrow$
<proof>

lemma *ebox-fission-abox*:

test p $\implies |R]p = |fis\ R]]p$
<proof>

lemma *ebox-down-ne-up-abox*:

test p $\implies |R]p = |(ne\ (R\downarrow))\uparrow]]p$
<proof>

lemma *same-fusion*:

assumes $fis\ R \sqsubseteq\downarrow S$
and $S \sqsubseteq\downarrow fus\ R$
shows $fis\ R = fis\ S$
<proof>

lemma *same-abox*:

assumes $fis\ R \sqsubseteq\downarrow S$
and $S \sqsubseteq\downarrow fus\ R$
and *test p*
shows $|R]p = |S]p$
<proof>

lemma *abox-ebox-inner-deterministic*:

assumes *test p*
and *inner-deterministic R*
shows $|R]p = |R]]p$
<proof>

lemma *adia-edia-inner-deterministic*:

assumes *test p*
and *inner-deterministic R*
shows $|R\rangle p = |R\rangle\rangle p$

$\langle proof \rangle$

lemma *abox-adia-deterministic*:

assumes *test p*
and *deterministic R*
shows $|R]p = |R\rangle p$
 $\langle proof \rangle$

lemma *ebox-edia-deterministic*:

assumes *test p*
and *deterministic R*
shows $|R]]p = |R\rangle p$
 $\langle proof \rangle$

lemma *abox-ebox-fusion*:

assumes *test p*
shows $|fis R]p = |fis R]]p$
 $\langle proof \rangle$

lemma *abox-fission-edia-fusion*:

assumes *test p*
shows $|fis R]p = |fus R\rangle p$
 $\langle proof \rangle$

lemma *abox-adia-fusion*:

assumes *test p*
shows $|fus R]p = |fus R\rangle p$
 $\langle proof \rangle$

8.5 Goldblatt's axioms without star

lemma *abox-sp-unit*:

$|R]1 = 1$
 $\langle proof \rangle$

lemma *ou-unit-abox*:

$test\ p \implies |\{\}p = 1$
 $\langle proof \rangle$

lemma *ou-unit-test-implication*:

$test\ p \implies \{\} \rightarrow p = 1$
 $\langle proof \rangle$

lemma *sp-unit-abox*:

$test\ p \implies |1]p = p$
 $\langle proof \rangle$

lemma *sp-unit-test-implication*:

$test\ p \implies 1 \rightarrow p = p$

$\langle proof \rangle$

lemma *test-abox-ebox*:

$test\ p \implies test\ q \implies |q]p = |q]]p$
 $\langle proof \rangle$

lemma *test-abox*:

$test\ p \implies test\ q \implies |q]p = q \rightarrow p$
 $\langle proof \rangle$

lemma *abox-ou-adia-sp-unit*:

assumes *test p*
shows $|R]p \cup |R]1 = 1$
 $\langle proof \rangle$

lemma *d-test-sp*:

$test\ p \implies Dom\ (p * R) = p * Dom\ R$
 $\langle proof \rangle$

lemma *ad-test-sp*:

$test\ p \implies aDom\ (p * R) = \wr p \cup aDom\ R$
 $\langle proof \rangle$

lemma *adia-test-sp*:

$test\ p \implies test\ q \implies |p * R\rangle q = p * |R\rangle q$
 $\langle proof \rangle$

lemma *ebox-test-sp*:

$test\ p \implies test\ q \implies |p * R]]q = \wr p \cup |R]]q$
 $\langle proof \rangle$

lemma *abox-test-sp*:

assumes *test p*
and *test q*
shows $|p * R]q = \wr p \cup |R]q$
 $\langle proof \rangle$

lemma *abox-test-sp-2*:

$test\ p \implies test\ q \implies p \cup |R]q = |\wr p * R]q$
 $\langle proof \rangle$

lemma *abox-test-sp-3*:

$test\ p \implies test\ q \implies p \rightarrow |R]q = |p * R]q$
 $\langle proof \rangle$

lemma *fission-sp-dist*:

$fis\ (R * S) = fis\ (R * Dom\ S) * fis\ S$
 $\langle proof \rangle$

lemma *abox-test*:

test $p \implies \text{test} (|R\rangle p)$

<proof>

lemma *adia-test*:

test $p \implies \text{test} (|R\rangle p)$

<proof>

lemma *ebox-test*:

test $p \implies \text{test} (|R\rangle\!\rangle p)$

<proof>

lemma *edia-test*:

test $p \implies \text{test} (|R\rangle\!\rangle p)$

<proof>

lemma *abox-sp*:

assumes *test* p

and *test* q

shows $|R\rangle(p * q) = |R\rangle p * |R\rangle q$

<proof>

lemma *adia-ou-below-ne-down*:

assumes *test* p

shows $|R\rangle(p \cup \wr q) \subseteq |R\rangle p \cup |ne (R\downarrow)\rangle(\wr q)$

<proof>

lemma *abox-adia-mp*:

assumes *test* p

and *test* q

shows $|R\rangle(p \rightarrow q) * |R\rangle p \subseteq |R\rangle q$

<proof>

lemma *adia-abox-mp*:

assumes *test* p

and *test* q

shows $|R\rangle p * |R\rangle(p \rightarrow q) \subseteq |R\rangle q$

<proof>

lemma *abox-implication-adia*:

assumes *test* p

and *test* q

shows $|R\rangle(p \rightarrow q) \subseteq |R\rangle p \rightarrow |R\rangle q$

<proof>

lemma *abox-adia-implication*:

assumes *test* p

and *test* q

shows $|R\rangle p \subseteq |R\rangle q \rightarrow |R\rangle(p * q)$

$\langle proof \rangle$

lemma *abox-mp*:

assumes *test p*

and *test q*

shows $|R]p * |R](p \rightarrow q) \subseteq |R]q$

$\langle proof \rangle$

lemma *abox-implication*:

assumes *test p*

and *test q*

shows $|R](p \rightarrow q) \subseteq |R]p \rightarrow |R]q$

$\langle proof \rangle$

lemma *ebox-left-dist-ou*:

assumes *test p*

shows $|R \cup S]]p = |R]]p * |S]]p$

$\langle proof \rangle$

lemma *abox-left-dist-ou*:

assumes *test p*

shows $|R \cup S]p = |R]p * |S]p$

$\langle proof \rangle$

lemma *adia-left-dist-ou*:

assumes *test p*

shows $|R \cup S\rangle p = |R\rangle p \cup |S\rangle p$

$\langle proof \rangle$

lemma *edia-left-dist-ou*:

assumes *test p*

shows $|R \cup S\rangle\rangle p = |R\rangle\rangle p \cup |S\rangle\rangle p$

$\langle proof \rangle$

lemma *abox-dist-iu-1*:

assumes *test p*

shows $|R \cup\cup S]p = |Dom R * ne (S\downarrow)]p * |Dom S * ne (R\downarrow)]p$

$\langle proof \rangle$

lemma *abox-dist-iu-2*:

assumes *test p*

shows $|R \cup\cup S]p = |Dom R * S]p * |Dom S * R]p$

$\langle proof \rangle$

lemma *abox-dist-iu-3*:

assumes *test p*

shows $|R \cup\cup S]p = (|R]1 \rightarrow |S]p) * (|S]1 \rightarrow |R]p)$

$\langle proof \rangle$

lemma *abox-adia-sp-one-set*:

$$|R||S\rangle 1 = \{ (a, \{a\}) \mid a . \forall B . (a, B) \in R \longrightarrow (\forall b \in B . \exists D . (b, D) \in S) \}$$

<proof>

lemma *abox-abox-set*:

$$|R||S\rangle p = \{ (a, \{a\}) \mid a . \forall B . (a, B) \in R \longrightarrow (\forall C . (\exists b \in B . (b, C) \in S) \longrightarrow (\forall c \in C . (c, \{c\}) \in p)) \}$$

<proof>

lemma *sp-abox-set*:

$$|R * S\rangle p = \{ (a, \{a\}) \mid a . \forall B . (a, B) \in R \longrightarrow (\forall C . (\exists f . (\forall b \in B . (b, f b) \in S) \wedge C = \bigcup \{ f b \mid b . b \in B \}) \longrightarrow (\forall c \in C . (c, \{c\}) \in p)) \}$$

<proof>

lemma *abox-sp-1*:

assumes *test p*

shows $|R||S\rangle 1 * |R * S\rangle p \subseteq |R||S\rangle p$

<proof>

lemma *abox-sp-2*:

assumes *test p*

shows $|R||S\rangle p = |R\downarrow * S\rangle p$

<proof>

lemma *abox-sp-3*:

assumes *test p*

shows $|R||S\rangle p \subseteq |R * S\rangle p$

<proof>

lemma *abox-sp-4*:

assumes *test p*

shows $|R * S\rangle p \subseteq |R||S\rangle 1 \rightarrow |R||S\rangle p$

<proof>

lemma *abox-sp-5*:

assumes *test p*

shows $|R||S\rangle 1 * |R * S\rangle p = |R||S\rangle 1 * |R||S\rangle p$

<proof>

lemma *abox-sp-6*:

assumes *test p*

shows $|R||S\rangle 1 \rightarrow |R * S\rangle p = |R||S\rangle 1 \rightarrow |R||S\rangle p$

<proof>

lemma *abox-sp-7*:

assumes *test p*

and *total S*

shows $|R * S\rangle p = |R||S\rangle p$

<proof>

lemma *adia-sp-associative*:
assumes *test p*
shows $|Q * (R * S)\rangle p = |(Q * R) * S\rangle p$
 $\langle proof \rangle$

lemma *ebox-sp-associative*:
assumes *test p*
shows $|Q * (R * S)] p = |(Q * R) * S] p$
 $\langle proof \rangle$

lemma *edia-sp-associative*:
assumes *test p*
shows $|Q * (R * S)\rangle\rangle p = |(Q * R) * S\rangle\rangle p$
 $\langle proof \rangle$

lemma *abox-sp-associative*:
assumes *test p*
shows $|Q * (R * S)] p = |(Q * R) * S] p$
 $\langle proof \rangle$

lemma *abox-oI*:
assumes $X \neq \{\}$
shows $|R] \cap X = (\bigcap p \in X . |R] p)$
 $\langle proof \rangle$

lemma *ebox-left-dist-oU*:
assumes $X \neq \{\}$
shows $|\bigcup X]] p = (\bigcap R \in X . |R]] p)$
 $\langle proof \rangle$

lemma *abox-left-dist-oU*:
assumes $X \neq \{\}$
shows $|\bigcup X] p = (\bigcap R \in X . |R] p)$
 $\langle proof \rangle$

lemma *adia-left-dist-oU*:
 $|\bigcup X\rangle p = (\bigcup R \in X . |R\rangle p)$
 $\langle proof \rangle$

lemma *edia-left-dist-oU*:
 $|\bigcup X\rangle\rangle p = (\bigcup R \in X . |R\rangle\rangle p)$
 $\langle proof \rangle$

8.6 Goldblatt's axioms with star

unbundle *no rtrancl-syntax*
notation *star* $\langle \leftarrow * \rangle$ [1000] 999

lemma *star-induct-1*:

assumes $1 \subseteq X$
and $R * X \subseteq X$
shows $R^* \subseteq X$
<proof>

lemma *star-induct*:

assumes $S \subseteq 1 \cup 1_{\cup\cup}$
and $S \subseteq X$
and $R * X \subseteq X$
shows $R^* * S \subseteq X$
<proof>

lemma *star-total*:

total (R^*)
<proof>

lemma *star-down*:

$R^* \downarrow = (R \downarrow)^* \cup 1_{\cup\cup}$
<proof>

lemma *ne-star-down*:

$ne (R^* \downarrow) = ne ((R \downarrow)^*)$
<proof>

lemma *ne-down-star*:

$ne ((R \downarrow)^*) = (ne (R \downarrow))^*$
<proof>

lemma *abox-star-unfold*:

$test p \implies |R^*]p = p * |R]|R^*]p$
<proof>

lemma *star-sp-test-commute*:

assumes $S \subseteq 1 \cup 1_{\cup\cup}$
and $Q * S \subseteq S * R$
shows $Q^* * S \subseteq S * R^*$
<proof>

lemma *adia-star-induct*:

assumes *test* p
shows $|R]p \subseteq p \longleftrightarrow |R^*]p \subseteq p$
<proof>

lemma *ebox-star-induct*:

assumes *test* p
shows $p \subseteq |R]]p \longleftrightarrow p \subseteq |R^*]]p$
<proof>

lemma *abox-star-induct*:
 assumes *test p*
 shows $p \subseteq |R]p \longleftrightarrow p \subseteq |R^*]p$
 ⟨*proof*⟩

lemma *edia-star-induct*:
 assumes *test p*
 shows $|R\rangle\rangle p \subseteq p \longleftrightarrow |R^*\rangle\rangle p \subseteq p$
 ⟨*proof*⟩

lemma *abox-star-induct-1*:
 assumes *test p*
 and *test q*
 and $q \subseteq p * |R]q$
 shows $q \subseteq |R^*]p$
 ⟨*proof*⟩

lemma *adia-star-induct-1*:
 assumes *test p*
 and *test q*
 and $p \cup |R\rangle q \subseteq q$
 shows $|R^*\rangle p \subseteq q$
 ⟨*proof*⟩

lemma *abox-segerberg*:
 assumes *test p*
 shows $|R^*](p \rightarrow |R]p) \subseteq p \rightarrow |R^*]p$
 ⟨*proof*⟩

lemma *abox-segerberg-adia*:
 assumes *test p*
 shows $|R^*](|R\rangle p \rightarrow p) \subseteq |R^*\rangle p \rightarrow p$
 ⟨*proof*⟩

lemma *s-p-id-sp*:
 ($s-id \cup p-id) * R = R \cup p-id$
 ⟨*proof*⟩

8.7 Propositional Hoare logic

abbreviation *hoare* :: $('a, 'a) mrel \Rightarrow ('a, 'b) mrel \Rightarrow ('b, 'b) mrel \Rightarrow bool$ ($\langle - \{ \} - \rangle$)
 [50,60,50] 95)
 where $p \{ \{ R \} \} q \equiv p \subseteq |R]q$

abbreviation *if-then-else* :: $('a, 'a) mrel \Rightarrow ('a, 'b) mrel \Rightarrow ('a, 'b) mrel \Rightarrow ('a, 'b) mrel$
 where *if-then-else* $p R S \equiv p * R \cup \wr p * S$

abbreviation *while-do* :: $('a, 'a) mrel \Rightarrow ('a, 'a) mrel \Rightarrow ('a, 'a) mrel$

where $\text{while-do } p \ R \equiv (p * R)^* * \wr p$

lemma *hoare-skip*:

assumes $\text{test } p$
shows $p \{I\} p$
<proof>

lemma *hoare-cons*:

assumes $\text{test } s$
and $r \subseteq p$
and $q \subseteq s$
and $p \{R\} q$
shows $r \{R\} s$
<proof>

lemma *hoare-seq*:

assumes $\text{test } q$
and $\text{test } r$
and $p \{R\} q$
and $q \{S\} r$
shows $p \{R * S\} r$
<proof>

lemma *hoare-if*:

assumes $\text{test } p$
and $\text{test } q$
and $\text{test } r$
and $(p * q) \{R\} r$
and $((\wr p) * q) \{S\} r$
shows $q \{\text{if-then-else } p \ R \ S\} r$
<proof>

lemma *hoare-while*:

assumes $\text{test } p$
and $\text{test } q$
and $(p * q) \{R\} q$
shows $q \{\text{while-do } p \ R\} (q * (\wr p))$
<proof>

lemma *hoare-par*:

assumes $\text{test } q$
and $p \{R\} q$
and $p \{S\} q$
shows $p \{R \cup S\} q$
<proof>

9 Counterexamples

locale *counterexamples*

begin

lemma counter-01:

$\neg ((U::('a,'b) \text{ mrel}) * \neg((U::('b,'c) \text{ mrel}) * (R::('c,'d) \text{ mrel})) \subseteq \neg(U * R))$
<proof>

abbreviation a-1 \equiv *finite-1.a₁*

lemma counter-02:

$\exists R::(\text{Enum.finite-1}, \text{Enum.finite-1}) \text{ mrel} . \exists p . \neg (\text{test } p \longrightarrow (R \cap \neg(U * p)) * U = R * \neg(p * U))$
<proof>

lemma counter-03:

$\exists R::(\text{Enum.finite-1}, \text{Enum.finite-1}) \text{ mrel} . \exists p . \neg (\text{test } p \longrightarrow (R \cap \neg(U * p)) * 1_{\cup\cup} = R * (\neg(p * U) \cap 1_{\cup\cup}))$
<proof>

abbreviation b-1 \equiv *finite-2.a₁*

abbreviation b-2 \equiv *finite-2.a₂*

abbreviation b-1-0 \equiv $(b-1, \{\})$

abbreviation b-1-1 \equiv $(b-1, \{b-1\})$

abbreviation b-1-2 \equiv $(b-1, \{b-2\})$

abbreviation b-1-3 \equiv $(b-1, \{b-1, b-2\})$

abbreviation b-2-0 \equiv $(b-2, \{\})$

abbreviation b-2-1 \equiv $(b-2, \{b-1\})$

abbreviation b-2-2 \equiv $(b-2, \{b-2\})$

abbreviation b-2-3 \equiv $(b-2, \{b-1, b-2\})$

lemma counter-04:

$\exists R::(\text{Enum.finite-2}, \text{Enum.finite-2}) \text{ mrel} . \exists p q . \neg (\text{test } p \longrightarrow \text{test } q \longrightarrow |R * p]q = |R][p]q)$
<proof>

lemma counter-05:

$\neg (\exists f . \forall R p . \text{test } p \longrightarrow |R]p = |f R]p)$
<proof>

lemma counter-06:

$\neg (\exists f . \forall R p . \text{test } p \longrightarrow |R]]p = |f R]p)$
<proof>

lemma counter-07:

$\neg (\exists f . \text{mono } f \wedge (\forall R . \text{fus } R = \text{lfp } (\lambda X . f R X)))$
<proof>

abbreviation c-1 \equiv *finite-3.a₁*

abbreviation c-2 \equiv *finite-3.a₂*

abbreviation c-3 \equiv *finite-3.a₃*

lemma counter-08:

$\neg (\sim(1::(\text{Enum.finite-3}, \text{Enum.finite-3}) \text{ mrel}) * \sim 1 \in \{1, \sim 1\})$
 $\langle \text{proof} \rangle$

lemma counter-09:

$\neg (\sim(1::(\text{Enum.finite-3}, \text{Enum.finite-3}) \text{ mrel}) \odot 1 \in \{1, \sim 1\})$
 $\langle \text{proof} \rangle$

lemma ex-2-cases:

$\exists b. b = b-1 \vee b = b-2$
 $\langle \text{proof} \rangle$

lemma all-2-cases:

$(\forall b. b = b-2 \wedge b = b-1) = \text{False}$
 $\langle \text{proof} \rangle$

lemma impl-2-cases:

$\bigcup \{ X . \exists b. (b = b-1 \longrightarrow X = Y) \wedge (b = b-2 \longrightarrow X = Z) \} = Y \cup Z$
 $\langle \text{proof} \rangle$

lemma ex-2-set-cases:

$(\exists B::\text{Enum.finite-2 set} . P B) \longleftrightarrow P \{\} \vee P \{b-1\} \vee P \{b-2\} \vee P \{b-1, b-2\}$
 $\langle \text{proof} \rangle$

abbreviation B-0 $\equiv \{\}::\text{Enum.finite-2 set}$

abbreviation B-1 $\equiv \{b-1\}$

abbreviation B-2 $\equiv \{b-2\}$

abbreviation B-3 $\equiv \{b-1, b-2\}$

abbreviation mkf x y $\equiv \lambda z . \text{if } z = b-1 \text{ then } x \text{ else } y$

lemma mkf:

$f = \text{mkf } (f \ b-1) \ (f \ b-2)$
 $\langle \text{proof} \rangle$

lemma mkf2:

$f \ b-1 = X \wedge f \ b-2 = Y \implies f = \text{mkf } X \ Y$
 $\langle \text{proof} \rangle$

lemma ex-2-mrel-cases:

$(\exists f::\text{Enum.finite-2} \implies \text{Enum.finite-2 set} . P f) \longleftrightarrow$
 $P (\text{mkf } B-0 \ B-0) \vee P (\text{mkf } B-0 \ B-1) \vee P (\text{mkf } B-0 \ B-2) \vee P (\text{mkf } B-0 \ B-3) \vee$
 $P (\text{mkf } B-1 \ B-0) \vee P (\text{mkf } B-1 \ B-1) \vee P (\text{mkf } B-1 \ B-2) \vee P (\text{mkf } B-1 \ B-3) \vee$
 $P (\text{mkf } B-2 \ B-0) \vee P (\text{mkf } B-2 \ B-1) \vee P (\text{mkf } B-2 \ B-2) \vee P (\text{mkf } B-2 \ B-3) \vee$
 $P (\text{mkf } B-3 \ B-0) \vee P (\text{mkf } B-3 \ B-1) \vee P (\text{mkf } B-3 \ B-2) \vee P (\text{mkf } B-3 \ B-3)$
 $\langle \text{proof} \rangle$

lemma counter-10:

$\exists R::(\text{Enum.finite-2}, \text{Enum.finite-2}) \text{ mrel} . \neg (U::(\text{Enum.finite-2}, \text{Enum.finite-2}))$

$mrel) * (U * R) \subseteq U * R$
<proof>

lemma *counter-11*:

$\exists (R::(Enum.finite-2, Enum.finite-2) mrel) (s::(Enum.finite-2, Enum.finite-2) mrel) (t::(Enum.finite-2, Enum.finite-2) mrel) . \neg (inner-univalent s \wedge inner-univalent t \longrightarrow R * (s * t) = (R * s) * t)$
<proof>

lemma *counter-12*:

$\neg(\exists S . 1_{UU} \odot S = 1_{UU})$
<proof>

lemma *counter-13*:

$\neg(\exists S . \forall R . R \odot S = R)$
<proof>

end

end

References

- [1] H. Furusawa, W. Guttman, and G. Struth. Determinism of multirelations. *arXiv*, 2305.11344, 2023. <https://arxiv.org/abs/2305.11344>.
- [2] H. Furusawa, W. Guttman, and G. Struth. Modal algebra of multirelations. *arXiv*, 2305.11346, 2023. <https://arxiv.org/abs/2305.11346>.
- [3] H. Furusawa, W. Guttman, and G. Struth. On the inner structure of multirelations. *arXiv*, 2305.11342, 2023. <https://arxiv.org/abs/2305.11342>.
- [4] H. Furusawa and G. Struth. Binary multirelations. *Archive of Formal Proofs*, 2015. Formal proof development, <https://isa-afp.org/entries/Multirelations.html>.
- [5] W. Guttman. Algebras for iteration, infinite executions and correctness of sequential computations. *Archive of Formal Proofs*, 2021. Formal proof development, https://isa-afp.org/entries/Correctness_Algebras.html.