

Inner Structure, Determinism and Modal Algebra of Multirelations

Walter Guttmann and Georg Struth

December 9, 2023

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	16
2.7	Relational box	18
3	Basic Properties of Multirelations	18
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	35
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	55
5.3	Co-composition	56
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
7	Fusion and Fission	88
7.1	Atoms and co-atoms	88
7.2	Inner-functional properties	89
7.3	Fusion	92
7.4	Fission	94
7.5	Co-fusion and co-fission	97
8	Modalities	100
8.1	Tests	100
8.2	Domain and antidomain	106
8.3	Left residual	109
8.4	Modal operations	113
8.5	Goldblatt's axioms without star	118
8.6	Goldblatt's axioms with star	124
9	Counterexamples	126

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** ; 75)

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

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

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

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

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

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

1.1 Univalence, totality, determinism, and related properties

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

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

definition *injective* :: ($'a, 'b$) *rel* \Rightarrow *bool* **where**

injective $R = (R ; R^\smile \subseteq Id)$

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

definition *deterministic* :: ('a,'b) rel \Rightarrow bool **where**
deterministic $R = (univalent\ R \wedge total\ R)$

definition *bijjective* :: ('a,'b) rel \Rightarrow bool **where**
bijjective $R = (injective\ R \wedge surjective\ R)$

lemma *univalent-set*: *univalent* $R = (\forall a\ b\ c. (a,b) \in R \wedge (a,c) \in R \longrightarrow b = c)$
<proof>

Univalent relations feature as single-valued relations in Main.

lemma *univ-single-valued*: *univalent* $R = single\text{-valued}\ R$
<proof>

lemma *total-set*: *total* $R = (\forall a. \exists b. (a,b) \in R)$
<proof>

lemma *total-var*: *total* $R = (R ; top = top)$
<proof>

lemma *deterministic-set*: *deterministic* $R = (\forall a. \exists! B. (a,B) \in R)$
<proof>

lemma *deterministic-var1*: *deterministic* $R = (R ; -Id = -R)$
<proof>

lemma *deterministic-var2*: *deterministic* $R = (\forall S. R ; -S = -(R ; S))$
<proof>

lemma *inj-univ*: *injective* $R = univalent\ (R^\smile)$
<proof>

lemma *injective-set*: *injective* $S = (\forall a\ b\ c. (a,c) \in S \wedge (b,c) \in S \longrightarrow a = b)$
<proof>

lemma *surj-tot*: *surjective* $R = total\ (R^\smile)$
<proof>

lemma *surjective-set*: *surjective* $S = (\forall b. \exists a. (a,b) \in S)$
<proof>

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

lemma *bij-det*: *bijjective* $R = deterministic\ (R^\smile)$

<proof>

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

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

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

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

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

lemma bij-relcomp: *bijjective $R \implies$ bijjective $S \implies$ 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) rel \implies 'b set \implies 'a set* **where**
Invim $R = \text{Image } (R^\smile)$

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

definition $Grph :: ('a \Rightarrow 'b) \Rightarrow ('a, 'b) \text{ rel}$ **where**

$$Grph\ f = \{(x, y). y = f\ x\}$$

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

<proof>

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 $dom :: ('a, 'b) \text{ rel} \Rightarrow ('a, 'a) \text{ rel}$ **where**

$$dom\ R = Id \cap R ; R^\smile$$

definition $cod :: ('a, 'b) \text{ rel} \Rightarrow ('b, 'b) \text{ rel}$ **where**

$$cod\ R = dom\ (R^\smile)$$

definition $rel\text{-}fdia :: ('a, 'b) \text{ rel} \Rightarrow ('b, 'b) \text{ rel} \Rightarrow ('a, 'a) \text{ rel}$ ($([|-])$ [61,81] 82)

where

$$|R\rangle\ Q = dom\ (R ; dom\ Q)$$

definition $rel\text{-}bdia :: ('a, 'b) \text{ rel} \Rightarrow ('a, 'a) \text{ rel} \Rightarrow ('b, 'b) \text{ rel}$ ($((||-))$ [61,81] 82)

where

$$rel\text{-}bdia\ R = rel\text{-}fdia\ (R^\smile)$$

definition $rel\text{-}fbox :: ('a, 'b) \text{ rel} \Rightarrow ('b, 'b) \text{ rel} \Rightarrow ('a, 'a) \text{ rel}$ ($([|-])$ [61,81] 82)

where

$$|R\rangle\ Q = neg\ (dom\ (R ; neg\ (dom\ Q)))$$

definition $rel\text{-}bbox :: ('a, 'b) \text{ rel} \Rightarrow ('a, 'a) \text{ rel} \Rightarrow ('b, 'b) \text{ rel}$ ($((||-))$ [61,81] 82)

where

$$rel\text{-}bbox\ R = rel\text{-}fbox\ (R^\smile)$$

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

<proof>

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

<proof>

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

<proof>

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

<proof>

lemma $cod\text{-}Range$: $cod = \Delta \circ Range$

<proof>

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

<proof>

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

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

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

lemma *bbox-demod*: $(\text{dom } P \subseteq [R \mid Q]) = (R ; \text{dom } P \subseteq \text{dom } Q ; R)$
<proof>

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

lemma *fbox-demod*: $(\text{dom } P \subseteq \mid R \mid Q) = (\text{dom } P ; R \subseteq R ; \text{dom } Q)$
 $\langle \text{proof} \rangle$

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

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

lemma *fdia-bbox-galois*: $(\mid R \mid P \subseteq \text{dom } Q) = (\text{dom } P \subseteq [R \mid Q)$
 $\langle \text{proof} \rangle$

lemma *bdia-fbox-galois*: $(\langle R \mid P \subseteq \text{dom } Q \rangle = (\text{dom } P \subseteq \mid R \mid Q)$
 $\langle \text{proof} \rangle$

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

lemma *bfox-bbox-conjugation*: $(\text{neg } (\text{dom } Q) \subseteq \mid R \mid P) = (\text{neg } (\text{dom } P) \subseteq [R \mid Q)$
 $\langle \text{proof} \rangle$

1.4 Residuation

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

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

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

lemma *lres-galois*: $(R ; S \subseteq T) = (R \subseteq T \parallel S)$
 $\langle \text{proof} \rangle$

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

lemma *lres-compl*: $R \parallel S = -(-R ; S^\smile)$
 $\langle \text{proof} \rangle$

lemma *rres-compl*: $R \setminus S = -(R^\smile ; -S)$
 $\langle \text{proof} \rangle$

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*: $(\text{dom } P \subseteq R \setminus (\text{dom } Q ; \text{top})) = (\text{dom } P ; \text{top} \subseteq R \setminus (\text{dom } Q ; \text{top}))$
<proof>

lemma *dom-rres-top-var*: $(\text{dom } P \subseteq R \setminus (\text{dom } Q ; \text{top})) = (P ; \text{top} \subseteq R \setminus (Q ; \text{top}))$
<proof>

lemma *fdia-rres-top*: $(|R\rangle P \subseteq \text{dom } Q) = (\text{dom } P \subseteq R \setminus (\text{dom } Q ; \text{top}))$
<proof>

lemma *fdia-rres-top-var*: $(|R\rangle P \subseteq \text{dom } Q) = (\text{dom } P \subseteq R \setminus (Q ; \text{top}))$
<proof>

lemma *dom-galois-var2*: $(|R\rangle (Id \cap P) \subseteq Id \cap Q) = (Id \cap P \subseteq R \setminus ((Id \cap Q) ; \text{top}))$
<proof>

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

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

<proof>

lemma *wlp-prop*: $\text{dom } ((R \setminus (\text{dom } Q ; \text{top})) ; \text{top}) = \text{neg } (\text{cod } (\text{neg } (\text{dom } Q); R))$
<proof>

lemma *wlp-prop-var*: $\text{dom } ((R \setminus (\text{dom } Q ; \text{top}))) = \text{neg } (\text{cod } ((\text{neg } (\text{dom } Q)); R))$
<proof>

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

lemma *fdia-bbox-galois-var*: $(\ |R) (Id \cap P) \subseteq Id \cap Q) = (Id \cap P \subseteq Id \cap - \text{cod } ((Id \cap -Q); R))$
<proof>

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

1.5 Symmetric quotient

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

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

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

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

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

lemma *syq-expand1*: $R ; (R \div S) = S \cap (\text{top} ; (R \div S))$
<proof>

lemma *syq-expand2*: $(R \div S) ; S^\smile = R^\smile \cap ((R \div S) ; \text{top})$
<proof>

lemma *syq-comp1*: $(R \div S) ; (S \div T) = (R \div T) \cap (\text{top} ; (S \div T))$
<proof>

lemma *syq-comp2*: $(R \div S) ; (S \div T) = (R \div T) \cap ((R \div S) ; \text{top})$
<proof>

lemma *syq-bij*: *bijective* $T \implies (R \div S) ; T = R \div (S ; T)$

<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) rel \Rightarrow ('a,'b set) rel (Λ) **where**
 $\Lambda R = \{(a,B) \mid a B. B = \{b. (a,b) \in R\}\}$

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

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

definition *alpha* :: ('a,'b set) rel \Rightarrow ('a,'b) rel (α) **where**
 $\alpha R = R ; epsilonoff$

[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*: $epsilonoff = epsilon^\smile$
<proof>

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

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

lemma *Lambda-epsilonoff-up1*: $f = \Lambda R \Longrightarrow R = \alpha f$
<proof>

lemma *Lambda-epsilonoff-up2*: $deterministic f \Longrightarrow R = \alpha f \Longrightarrow f = \Lambda R$
<proof>

lemma *Lambda-epsilonoff-up*:
assumes *deterministic f*
shows $(R = \alpha f) = (f = \Lambda R)$
<proof>

lemma *det-lambda: deterministic* (ΛR)

<proof>

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

<proof>

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

<proof>

lemma *alpha-cancel:*

assumes *deterministic* f

and *deterministic* g

shows $\alpha f = \alpha g \implies f = g$

<proof>

lemma *Lambda-fusion:*

assumes *deterministic* f

shows $\Lambda (f ; R) = f ; \Lambda R$

<proof>

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

<proof>

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

<proof>

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

<proof>

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

<proof>

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

<proof>

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

$= \alpha R \cap \alpha S$

<proof>

2.2 Relational image functor

definition *pow* :: $('a, 'b) \text{rel} \Rightarrow ('a \text{ set}, 'b \text{ set}) \text{rel} (\mathcal{P})$ **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]*: $\mathcal{P} Id = Id$
<proof>

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

lemma *Grph-Image [simp]*: $Grph \circ Image = \mathcal{P}$
<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 (η) **where**
 $\eta = \Lambda Id$

definition *mu* :: ('a set set, 'a set) rel (μ) **where**
 $\mu = pow\ epsilon\ off$

lemma *eta-set*: $\eta = \{(a, \{a\}) \mid a. True\}$
<proof>

lemma *alpha-eta [simp]*: $\alpha \eta = Id$
<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*: $R = \mathcal{P} S \implies \alpha (\eta ; R) = S$

$\langle proof \rangle$

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**
 $\Omega = \text{epsiloff} \setminus \text{epsiloff}$

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

lemma *conv-Omega*: $\Omega^\smile = \text{epsiloff} // \text{epsiloff}$
<proof>

lemma *epsiloff-eta-Omega* [simp]: $\eta ; \Omega = \text{epsiloff}$
<proof>

lemma *epsiloff-eta-Omega* [simp]: $\Omega^\smile ; \eta^\smile = \text{epsiloff}$
<proof>

lemma *epsiloff-Omega* [simp]: $\text{epsiloff} ; \Omega = \text{epsiloff}$
<proof>

lemma *conv-Omega-epsiloff* [simp]: $\Omega^\smile ; \text{epsiloff} = \text{epsiloff}$
<proof>

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

lemma *Lambda-Omega*: $\Lambda R ; \Omega = R^\smile \setminus \text{epsiloff}$
<proof>

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

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

2.5 Complementation relation

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

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

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

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

lemma *converse-Compl* [simp]: $C^\smile = C$
 ⟨proof⟩

lemma *det-Compl*: *deterministic C*
 ⟨proof⟩

lemma *bij-Compl*: *bijjective C*
 ⟨proof⟩

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

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

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

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

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

lemma *Lambda-Compl*: $\Lambda R ; C = \Lambda (-R)$
 ⟨proof⟩

2.6 Kleisli lifting and Kleisli composition

definition *klift* :: ('a, 'b set) rel \Rightarrow ('a set, 'b set) rel (-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** $\cdot_{\mathcal{P}}$ 70) **where**

$$R \cdot_{\mathcal{P}} S = R ; (S)_{\mathcal{P}}$$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2.7 Relational box

definition $rbox :: ('a, 'b) rel \Rightarrow ('b\ set, 'a\ set) rel$ **where**
 $rbox\ R = \Lambda\ (epsilon\ off\ //\ R)$

lemma $rbox\ set$: $rbox\ R = \{(Q, P). P = \{a. \forall b. (a, b) \in R \longrightarrow b \in Q\}\}$
 $\langle proof \rangle$

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

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

lemma $rbox\ semicomm$: $(Q, P) \in rbox\ R ; \Omega^\smile = (\Delta\ P ; R \subseteq R ; \Delta\ Q)$
 $\langle proof \rangle$

lemma $rbox\ semicomm\ var$: $(Q, P) \in rbox\ R ; \Omega^\smile = (\Delta\ P \subseteq (R ; \Delta\ Q) // R)$
 $\langle proof \rangle$

lemma $rbox\ omega$: $rbox\ epsilon\ off = \Lambda\ (\Omega^\smile)$
 $\langle proof \rangle$

lemma $Omega\ rbox$: $\Omega = (\alpha\ (rbox\ epsilon\ off))^\smile$
 $\langle proof \rangle$

lemma $pow\ rbox$: $((Q, P) \in rbox\ R ; \Omega^\smile) = ((P, Q) \in \mathcal{P}\ R ; \Omega)$
 $\langle proof \rangle$

lemma $rbox\ pow\ Compl$: $rbox\ R = \mathcal{C} ; \mathcal{P}\ (R^\smile) ; \mathcal{C}$
 $\langle proof \rangle$

lemma $pow\ rbox\ Compl$: $\mathcal{P}\ R = \mathcal{C} ; rbox\ (R^\smile) ; \mathcal{C}$
 $\langle proof \rangle$

lemma $pow\ conjugation$: $\mathcal{C} ; (\mathcal{P}\ (R^\smile) ; \Omega)^\smile = \mathcal{P}\ R ; \mathcal{C} ; \Omega^\smile$
 $\langle proof \rangle$

lemma $pow\ rbox\ eq$: $rbox\ R ; \Omega^\smile = (\mathcal{P}\ R ; \Omega)^\smile$
 $\langle proof \rangle$

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 $(\prime a, \prime b) \text{ mrel} = (\prime a, \prime b \text{ set}) \text{ rel}$

definition $s\text{-prod} :: (\prime a, \prime b) \text{ mrel} \Rightarrow (\prime b, \prime c) \text{ mrel} \Rightarrow (\prime a, \prime c) \text{ mrel}$ (**infixl** \cdot 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 $s\text{-id} :: (\prime a, \prime a) \text{ mrel}$ (1_σ) **where**

$1_\sigma = (\bigcup a. \{(a, \{a\})\})$

definition $p\text{-prod} :: (\prime a, \prime b) \text{ mrel} \Rightarrow (\prime a, \prime b) \text{ mrel} \Rightarrow (\prime a, \prime b) \text{ mrel}$ (**infixl** \parallel 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 $p\text{-id} :: (\prime a, \prime b) \text{ mrel}$ (1_π) **where**

$1_\pi = (\bigcup a. \{(a, \{\})\})$

definition $U :: (\prime a, \prime b) \text{ mrel}$ **where**

$U = \{(a, A) \mid a \ A. \text{True}\}$

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

named-theorems $mr\text{-simp}$

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

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

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

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

lemma $c\text{-prod-idr}$ [$simp$]: $R \parallel 1_\pi = R$
 $\langle \text{proof} \rangle$

lemma $cl7$ [$simp$]: $1_\sigma \parallel 1_\sigma = 1_\sigma$
 $\langle \text{proof} \rangle$

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*: $R \cdot 1_\pi = \{(a, \{\}) \mid a. \exists B. (a, B) \in R\}$
<proof>

lemma *c6*: $R \cdot 1_\pi \subseteq 1_\pi$
<proof>

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

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

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

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

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

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

lemma *U-U [simp]*: $U \cdot U = U$
 ⟨proof⟩

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

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

lemma *NC-NC [simp]*: $NC \cdot NC = NC$
 ⟨proof⟩

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

lemma *cl4*:
assumes $T \parallel T \subseteq T$
shows $R \cdot T \parallel S \cdot T \subseteq (R \parallel S) \cdot T$
 ⟨proof⟩

lemma *cl3*: $R \cdot (S \parallel T) \subseteq R \cdot S \parallel R \cdot T$
 ⟨proof⟩

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

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-subdistrl*: $(P \cap 1_\sigma) \cdot (S \parallel T) = ((P \cap 1_\sigma) \cdot S) \parallel ((P \cap 1_\sigma) \cdot T)$
 ⟨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*: $(T::('a, 'b) \text{ mrel}) \cdot 1_\pi \subseteq (R::('a, 'b) \text{ mrel}) \cdot 1_\pi \implies T \cdot 1_\pi \subseteq (S::('a, 'b) \text{ mrel}) \cdot 1_\pi \implies T \cdot 1_\pi \subseteq (R \cdot 1_\pi) \parallel (S \cdot 1_\pi)$
 ⟨*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*: $(T::('a, 'b) \text{ mrel}) \cdot 1_\pi \subseteq (R::('a, 'b) \text{ mrel}) \cdot 1_\pi \wedge T \cdot 1_\pi \subseteq$

$$(S::('a,'b) \text{ mrel}) \cdot 1_\pi \longleftrightarrow T \cdot 1_\pi \subseteq (R \cdot 1_\pi) \parallel (S \cdot 1_\pi)$$

$\langle \text{proof} \rangle$

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

$\langle \text{proof} \rangle$

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

$\langle \text{proof} \rangle$

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

$\langle \text{proof} \rangle$

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

$\langle \text{proof} \rangle$

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

$\langle \text{proof} \rangle$

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

$\langle \text{proof} \rangle$

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

$\langle \text{proof} \rangle$

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

$\langle \text{proof} \rangle$

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

$\langle \text{proof} \rangle$

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

$\langle \text{proof} \rangle$

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

$\langle \text{proof} \rangle$

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

$\langle \text{proof} \rangle$

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

$\langle \text{proof} \rangle$

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

$\langle \text{proof} \rangle$

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

$\langle \text{proof} \rangle$

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* :: $('a, 'b) \text{ mrel} \Rightarrow ('a, 'a) \text{ mrel}$ **where**
 $Dom R = \{(a, \{a\}) \mid a. \exists B. (a, B) \in R\}$

named-theorems *mrd-simp*

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

lemma *d-def-expl*: $Dom R = R \cdot 1_\pi \parallel 1_\sigma$
<proof>

lemma *s-subid-iff2*: $(R \cap 1_\sigma = R) = (Dom R = R)$
<proof>

lemma *cl8-var*: $Dom R \cdot S = R \cdot 1_\pi \parallel S$
<proof>

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

lemma *cl10-var*: $Dom (R - 1_\pi) = 1_\sigma \cap ((R - 1_\pi) \cdot NC)$
<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*]: $Dom (R \cap 1_\sigma) = R \cap 1_\sigma$
<proof>

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

lemma *d-s-id-ax*: $Dom R \subseteq 1_\sigma$
<proof>

lemma *d-assoc1*: $Dom R \cdot (S \cdot T) = (Dom R \cdot S) \cdot T$
<proof>

lemma *d-meet-distr-var*: $(Dom R \cap Dom S) \cdot T = Dom R \cdot T \cap Dom S \cdot T$
<proof>

lemma *d-idem* [*simp*]: $Dom (Dom R) = Dom R$
<proof>

lemma *cd-2-var*: $Dom (R \cdot 1_\pi) \cdot S = R \cdot 1_\pi \parallel S$
<proof>

lemma *dc-prop1* [*simp*]: $Dom R \cdot 1_\pi = R \cdot 1_\pi$
<proof>

lemma *dc-prop2* [*simp*]: $Dom (R \cdot 1_\pi) = Dom R$
<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 $(R \parallel S) \cdot \text{Dom } T = R \cdot \text{Dom } T \parallel S \cdot \text{Dom } T$

shows $\text{Dom } ((R \parallel S) \cdot T) = \text{Dom } (R \cdot T) \cdot \text{Dom } (S \cdot T)$

<proof>

lemma *d-lb1*: $\text{Dom } R \cdot \text{Dom } S \subseteq \text{Dom } R$

<proof>

lemma *d-lb2*: $\text{Dom } R \cdot \text{Dom } S \subseteq \text{Dom } S$

<proof>

lemma *d-glb*: $\text{Dom } T \subseteq \text{Dom } R \wedge \text{Dom } T \subseteq \text{Dom } S \implies \text{Dom } T \subseteq \text{Dom } R \cdot \text{Dom } S$

<proof>

lemma *d-glb-iff*: $\text{Dom } T \subseteq \text{Dom } R \wedge \text{Dom } T \subseteq \text{Dom } S \iff \text{Dom } T \subseteq \text{Dom } R \cdot \text{Dom } S$

<proof>

lemma *d-interr*: $R \cdot \text{Dom } P \parallel S \cdot \text{Dom } P = (R \parallel S) \cdot \text{Dom } P$

<proof>

lemma *cl10-d*: $\text{Dom } (R \cap NC) = 1_\sigma \cap (R \cap NC) \cdot NC$

<proof>

lemma *cl11-d [simp]*: $\text{Dom } (R \cap NC) \cdot NC = (R \cap NC) \cdot NC$

<proof>

lemma *cl10-d-var1*: $\text{Dom } (R \cap NC) = 1_\sigma \cap R \cdot NC$

<proof>

lemma *cl10-d-var2*: $\text{Dom } (R \cap NC) = 1_\sigma \cap (R \cap NC) \cdot U$

<proof>

lemma *cl10-d-var3*: $\text{Dom } (R \cap NC) = 1_\sigma \cap R \cdot U$

<proof>

lemma *d-U [simp]*: $\text{Dom } U = 1_\sigma$

<proof>

lemma *d-nc [simp]*: $\text{Dom } NC = 1_\sigma$

<proof>

lemma *alt-d-def-nc-nc*: $\text{Dom } (R \cap NC) = 1_\sigma \cap (((R \cap NC) \cdot 1_\pi) \parallel NC)$

<proof>

lemma *alt-d-def-nc-U*: $\text{Dom } (R \cap NC) = 1_\sigma \cap (((R \cap NC) \cdot 1_\pi) \parallel U)$

<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*]: $Dom (R \cdot U) = Dom R$
<proof>

lemma *d-llp1*: $Dom R \subseteq Dom S \implies R \subseteq Dom S \cdot R$
<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** \otimes 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* :: $('a, 'b) \text{ mrel} \Rightarrow ('a, 'b) \text{ mrel}(\tau)$ **where**
 $\tau R = R \cdot \{\}$

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

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

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

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

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

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

lemma *tarski-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-prod-aux* [*simp*]: $(\nu R \cdot NC) \cdot NC = \nu R \cdot NC$
 ⟨*proof*⟩

lemma *nc-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-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-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-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-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-sharp* [*simp*]: $(\nu R \cdot 1_\pi \parallel NC) \cdot 1_\pi = \nu R \cdot 1_\pi$
 ⟨*proof*⟩

lemma *iso6-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 *nsv-hom-meet*: $Dom (\nu R \cdot NC \cap \nu S \cdot NC) = Dom (\nu R \cdot NC) \cap Dom (\nu S \cdot NC)$

$(\nu S \cdot NC)$
 $\langle proof \rangle$

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

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

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

lemma *tau-int*: $\tau R \leq R$
 $\langle proof \rangle$

lemma *nu-int*: $\nu R \leq R$
 $\langle proof \rangle$

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

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

lemma *tau-iso*: $R \leq S \implies \tau R \leq \tau S$
 $\langle proof \rangle$

lemma *nu-iso*: $R \leq S \implies \nu R \leq \nu S$
 $\langle proof \rangle$

lemma *tau-zero [simp]*: $\tau \{\} = \{\}$
 $\langle proof \rangle$

lemma *nu-zero [simp]*: $\nu \{\} = \{\}$
 $\langle proof \rangle$

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

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

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

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

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

<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-precong1: $\tau R \leq \tau S \implies \tau (T \cdot R) \leq \tau (T \cdot S)$
<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-seq1*: $\tau\ R = \tau\ S \implies \tau\ (T \cdot R) = \tau\ (T \cdot S)$

<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-power $R\ 0 = 1_\sigma \mid$

p-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 $R\ 0 = \{\} \mid$

power-rd $R\ (Suc\ n) = 1_\sigma \cup R \cdot power\text{-rd}\ R\ n$

primrec *power-sq* :: $('a, 'a)\ mrel \Rightarrow nat \Rightarrow ('a, 'a)\ mrel$ **where**

power-sq $R\ 0 = 1_\sigma \mid$

$$\text{power-sq } R \text{ (Suc } n) = 1_\sigma \cup R \cdot \text{power-sq } R \ n$$

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

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

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

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

lemma *power-rd-le-sq*: $\text{power-rd } R \ n \leq \text{power-sq } R \ n$
<proof>

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

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

3.9 Star

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

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

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

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*]: $\omega NC = U$
<proof>

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

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

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

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

lemma *om-nu-tau*: $\omega (\nu R) \cup \text{star } (\nu R) \cdot \tau R \leq \omega R$
<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* :: $('a, 'b) \text{ mrel} \Rightarrow ('a \text{ set}, 'b \text{ set}) \text{ rel}$ (*-** [1000] 999) **where**
 $R_* = \{(A, B). \exists f. (\forall a \in A. (a, f(a)) \in R) \wedge B = \bigcup (f ' A)\}$

lemma *pcomp-plift*: $R \cdot S = R ; S_*$
<proof>

lemma *det-plift-klift*: $\text{deterministic } R \Longrightarrow R_* = (R)_\mathcal{P}$

<proof>

lemma *plift-ext2* [*simp*]: $\eta ; R_* = R$
<proof>

lemma *plift-ext-3* [*simp*]: $\eta_* = Id$
<proof>

lemma *d-dom-pltift*: $(Dom R)_* = dom (R_*)$
<proof>

lemma *d-pid-pltift*: $(Dom R)_* \subseteq Id$
<proof>

lemma *d-pltift-sub*: $A \subseteq B \implies (B, B) \in (Dom R)_* \implies (A, A) \in (Dom R)_*$
<proof>

lemma *pltift-empty*: $(\{\}, A) \in R_* \iff A = \{\}$
<proof>

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

lemma *pltift-ext1*:
 assumes *univalent f*
 shows $(R ; f_*)_* = R_* ; f_*$
<proof>

lemma *pltift-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**
 $\text{fus } R = \Lambda (\alpha R)$

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

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

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

lemma *fis-det-comp*: $\text{deterministic } R \Longrightarrow \text{deterministic } S \Longrightarrow \text{fis } (R \cdot S) = \text{fis } R \cdot \text{fis } S$
 ⟨proof⟩

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

4.3 Galois connections for multirelations

lemma *sub-subh*: $R \subseteq S \Longrightarrow R \subseteq S ; (\text{epsiloff} \parallel \text{epsiloff})$
 ⟨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*: $R \subseteq S \Longrightarrow \Lambda R \subseteq \Lambda S ; (\text{epsiloff} \parallel \text{epsiloff})$
 ⟨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]*: $\alpha (R ; \Omega^\sim) = \alpha R$
 ⟨proof⟩

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

lemma *fus-fus [simp]*: $\text{fus} \circ \text{fus} = \text{fus}$

$\langle proof \rangle$

lemma *fis-fus* [simp]: $fis \circ fus = fis$
 $\langle proof \rangle$

lemma *fus-fis* [simp]: $fus \circ fis = fus$
 $\langle proof \rangle$

lemma *fis-alpha*: $fis R \cdot S = \alpha R ; S$
 $\langle proof \rangle$

lemma *fis-lax*: $fis (R \cdot S) \subseteq fis R \cdot fis S$
 $\langle proof \rangle$

lemma *klift-fus*: $(R)_{\mathcal{P}} = fus (epsilon\ off ; R)$
 $\langle proof \rangle$

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

lemma *fus-Lambda-mu*: $fus R = \Lambda R ; \mu$
 $\langle proof \rangle$

4.5 Properties of fusion, fission, nu and tau

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

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

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

lemma *nu-fis-var*: $\nu (fis R) = fis (\nu R)$
 $\langle proof \rangle$

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

Properties of tests and domain

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

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

lemma *subid-plift-down*: $U ; (P \cap \eta)_* ; \Omega^{\smile} = U ; (P \cap \eta)_*$
 $\langle proof \rangle$

lemma *nu-subid-plitf*: $\nu (R ; (P \cap \eta)_*) = \nu R ; (P \cap \eta)_*$
 ⟨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 (α R)

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

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

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

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

end

theory *Multirelations*

imports *Power-Allegories-Multirelations*

begin

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

no-notation *one-class.one* (1)

no-notation *times-class.times* (infixl * 70)

no-notation *rel-fdia* ((|-)-) [61,81] 82)
no-notation *rel-bdia* ((<|-) [61,81] 82)
no-notation *rel-fbox* ((|-]-) [61,81] 82)
no-notation *rel-bbox* (([-|-) [61,81] 82)

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

notation *s-prod* (**infixl** * 70)

notation *s-id* (1)

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** $\cup\cup$ 65)

where *inner-union* \equiv *p-prod*

definition *inner-intersection* :: ('a,'b) *mrel* \Rightarrow ('a,'b) *mrel* \Rightarrow ('a,'b) *mrel* (**infixl** $\cap\cap$ 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) *mrel* \Rightarrow ('a,'b) *mrel* (\sim - [80] 80) **where**

$\sim R \equiv \{ (a,B) . (a,-B) \in R \}$

abbreviation *iu-unit* ($1_{\cup\cup}$)

where $1_{\cup\cup} \equiv$ *p-id*

definition *ii-unit* :: ('a,'a) *mrel* ($1_{\cap\cap}$)

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*:

$(R \cup\cup S) \cup\cup T = R \cup\cup (S \cup\cup T)$
 $\langle \text{proof} \rangle$

lemma *iu-commute*:

$R \cup\cup S = S \cup\cup R$
 $\langle \text{proof} \rangle$

lemma *iu-unit*:

$$R \cup \cup 1_{\cup \cup} = R$$

<proof>

lemma *ii-assoc*:

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

<proof>

lemma *ii-commute*:

$$R \cap \cap S = S \cap \cap R$$

<proof>

lemma *ii-unit [simp]*:

$$R \cap \cap 1_{\cap \cap} = R$$

<proof>

lemma *pa-ic*:

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

<proof>

lemma *ic-involutive [simp]*:

$$\sim \sim R = R$$

<proof>

lemma *ic-injective*:

$$\sim R = \sim S \implies R = S$$

<proof>

lemma *ic-antidist-ii*:

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

<proof>

lemma *ic-antidist-ii*:

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

<proof>

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

$$\sim 1_{\cup \cup} = 1_{\cap \cap}$$

<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*:

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

<proof>

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

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

<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*:

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

<proof>

lemma *ii-right-subdist-iu*:

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

<proof>

lemma *ic-isotone*:

$R \subseteq S \implies \sim R \subseteq \sim S$
 ⟨proof⟩

lemma *ic-bot* [*simp*]:
 $\sim\{\} = \{\}$
 ⟨proof⟩

lemma *ic-top* [*simp*]:
 $\sim U = U$
 ⟨proof⟩

lemma *ic-dist-ou*:
 $\sim(R \cup S) = \sim R \cup \sim S$
 ⟨proof⟩

lemma *ic-dist-oi*:
 $\sim(R \cap S) = \sim R \cap \sim S$
 ⟨proof⟩

lemma *ic-dist-oc*:
 $\sim \sim R = \sim(\sim R)$
 ⟨proof⟩

lemma *ii-sub-idempotent*:
 $R \subseteq R \cap \cap R$
 ⟨proof⟩

definition *inner-Union* :: ('i \Rightarrow ('a,'b) mrel) \Rightarrow 'i set \Rightarrow ('a,'b) mrel ($\bigcup \cup$ -|
 [80,80] 80) **where**
 $\bigcup \cup X|I \equiv \{ (a,B) . \exists f . B = (\bigcup i \in I . f i) \wedge (\forall i \in I . (a,f i) \in X i) \}$

definition *inner-Intersection* :: ('i \Rightarrow ('a,'b) mrel) \Rightarrow 'i set \Rightarrow ('a,'b) mrel
 ($\bigcap \cap$ -| [80,80] 80) **where**
 $\bigcap \cap X|I \equiv \{ (a,B) . \exists f . B = (\bigcap i \in I . f i) \wedge (\forall i \in I . (a,f i) \in X i) \}$

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

lemma *iU-empty*:
 $\bigcup \cup X|\{\} = 1_{\bigcup \cup}$
 ⟨proof⟩

lemma *iI-empty*:
 $\bigcap \cap X|\{\} = 1_{\bigcap \cap}$
 ⟨proof⟩

lemma *ic-antidist-iU*:
 $\sim \bigcup \cup X|I = \bigcap \cap (\text{inner-complement o } X)|I$
 ⟨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* :: $('a, 'b) \text{ mrel} \Rightarrow ('a, 'b) \text{ mrel} \ (-^d \ [100] \ 100)$
where $R^d \equiv \sim -R$

lemma *dual*:

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

<proof>

declare *dual* [*mr-simp*]

lemma *dual-antitone*:
 $R \subseteq S \implies S^d \subseteq R^d$
<proof>

lemma *ic-oc-dual*:
 $\sim R = -R^d$
<proof>

lemma *dual-involutive* [*simp*]:
 $R^{dd} = R$
<proof>

lemma *dual-antidist-ou*:
 $(R \cup S)^d = R^d \cap S^d$
<proof>

lemma *dual-antidist-oi*:
 $(R \cap S)^d = R^d \cup S^d$
<proof>

lemma *dual-dist-oc*:
 $(-R)^d = -R^d$
<proof>

lemma *dual-dist-ic*:
 $(\sim R)^d = \sim R^d$
<proof>

lemma *dual-antidist-oU*:
 $(\bigcup X)^d = \bigcap (\text{dual } ' X)$
<proof>

lemma *dual-antidist-oI*:
 $(\bigcap X)^d = \bigcup (\text{dual } ' X)$
<proof>

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 $\forall J :: 'a \text{ set} . J \neq \{\} \longrightarrow (\bigcap \bigcap (\lambda j . R) | J) \subseteq R$

shows $(\bigcup \bigcup X | I) \odot R = \bigcap \bigcap (\lambda i . X i \odot R) | (I :: 'a \text{ set})$

<proof>

5.4 Inner order

definition *inner-order-ii* :: 'a × 'b set ⇒ 'a × 'b set ⇒ bool (**infix** $\preceq_{\cup\cup}$ 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 × 'b set ⇒ 'a × 'b set ⇒ bool (**infix** $\preceq_{\cap\cap}$ 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-ii*: 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) mrel ⇒ ('a,'b) mrel ($-\uparrow$ [100] 100)

where $R\uparrow \equiv R \cup\cup U$

abbreviation *down* :: ('a,'b) mrel ⇒ ('a,'b) mrel ($-\downarrow$ [100] 100)

where $R\downarrow \equiv R \cap\cap U$

abbreviation *convex* :: ('a,'b) mrel ⇒ ('a,'b) mrel ($-\updownarrow$ [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*:

$$\sim(R\uparrow) = (\sim R)\downarrow$$

<proof>

lemma *ic-down*:

$$\sim(R\downarrow) = (\sim R)\uparrow$$

<proof>

lemma *ic-convex*:

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

<proof>

lemma *up-isotone*:

$$R \subseteq S \implies R\uparrow \subseteq S\uparrow$$

<proof>

lemma *up-increasing*:

$$R \subseteq R\uparrow$$

<proof>

lemma *up-idempotent [simp]*:

$$R\uparrow\uparrow = R\uparrow$$

<proof>

lemma *up-dist-ou*:

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

<proof>

lemma *up-dist-iu*:

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

<proof>

lemma *up-dist-ii*:

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

<proof>

lemma *down-isotone*:

$$R \subseteq S \implies R\downarrow \subseteq S\downarrow$$

<proof>

lemma *down-increasing*:

$$R \subseteq R\downarrow$$

<proof>

lemma *down-idempotent [simp]*:

$$R\downarrow\downarrow = R\downarrow$$

<proof>

lemma *down-dist-ou*:

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

<proof>

lemma *down-dist-iu*:

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

<proof>

lemma *down-dist-ii*:

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

<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*:

$$R\downarrow = R * (1 \cup \cup 1)$$

<proof>

lemma *up-cp*:

$$R\uparrow = \sim R \odot (1 \cap \cup \sim 1)$$

<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*:

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

<proof>

lemma *up-dist-iu-oi*:

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

<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:*

$$(\bigcup X)\uparrow = \bigcup (up \text{ ` } X)$$

<proof>

lemma *up-dist-iU:*

assumes $I \neq \{\}$

shows $(\bigcup\bigcup X|I)\uparrow = \bigcup\bigcup (up \text{ o } X)|I$

<proof>

lemma *up-dist-iI:*

$$(\bigcap \bigcap X|I)\uparrow = \bigcap \bigcap (up \circ X)|I$$

<proof>

lemma *down-dist-oU:*

$$(\bigcup X)\downarrow = \bigcup (down \circ X)$$

<proof>

lemma *down-dist-iU:*

$$(\bigcup \bigcup X|I)\downarrow = \bigcup \bigcup (down \circ X)|I$$

<proof>

lemma *down-dist-iI:*

assumes $I \neq \{\}$
 shows $(\bigcap \bigcap X|I)\downarrow = \bigcap \bigcap (down \circ X)|I$

<proof>

lemma *iU-up-oI:*

assumes $I \neq \{\}$
 shows $\bigcup \bigcup (up \circ X)|I = \bigcap (up \circ X \circ I)$

<proof>

lemma *iI-down-oI:*

assumes $I \neq \{\}$
 shows $\bigcap \bigcap (down \circ X)|I = \bigcap (down \circ X \circ I)$

<proof>

lemma *down-dist-iI-oI:*

$$\bigcap (down \circ X \circ I) = (\bigcap \bigcap X|I)\downarrow$$

<proof>

lemma *up-dist-iU-oI:*

$$\bigcap (up \circ X \circ I) = (\bigcup \bigcup X|I)\uparrow$$

<proof>

lemma *iu-up:*

$$(R \cup \cup R)\uparrow = R\uparrow$$

<proof>

lemma *ii-down:*

$$(R \cap \cap R)\downarrow = R\downarrow$$

<proof>

lemma *iU-up:*

assumes $I \neq \{\}$
 shows $(\bigcup \bigcup (\lambda j . R)|I)\uparrow = R\uparrow$

<proof>

lemma *iI-down:*

assumes $I \neq \{\}$
shows $(\bigcap (\lambda j . R)|I)\downarrow = R\downarrow$
<proof>

lemma *iu-unit-up*:
 $1_{UU}\uparrow = U$
<proof>

lemma *iu-unit-down*:
 $1_{UU}\downarrow = 1_{UU}$
<proof>

lemma *iu-unit-convex*:
 $1_{UU}\updownarrow = 1_{UU}$
<proof>

lemma *ii-unit-up*:
 $1_{\cap\cap}\uparrow = 1_{\cap\cap}$
<proof>

lemma *ii-unit-down*:
 $1_{\cap\cap}\downarrow = U$
<proof>

lemma *ii-unit-convex*:
 $1_{\cap\cap}\updownarrow = 1_{\cap\cap}$
<proof>

lemma *sp-unit-down*:
 $1\downarrow = 1 \cup 1_{UU}$
<proof>

lemma *sp-unit-convex*:
 $1\updownarrow = 1$
<proof>

lemma *top-up*:
 $U\uparrow = U$
<proof>

lemma *top-down*:
 $U\downarrow = U$
<proof>

lemma *top-convex*:
 $U\updownarrow = U$
<proof>

lemma *bot-up*:

$$\{\}\uparrow = \{\}$$

<proof>

lemma *bot-down*:

$$\{\}\downarrow = \{\}$$

<proof>

lemma *bot-convex*:

$$\{\}\updownarrow = \{\}$$

<proof>

lemma *down-oi-up-convex*:

$$(R\downarrow \cap S\uparrow)\updownarrow = R\downarrow \cap S\uparrow$$

<proof>

lemma *convex-iff-down-oi-up*:

$$Q = Q\updownarrow \iff (\exists R S . Q = R\downarrow \cap S\uparrow)$$

<proof>

lemma *convex-closed-oI*:

$$(\bigcap_{R \in X} R\updownarrow)\updownarrow = (\bigcap_{R \in X} R\updownarrow)$$

<proof>

lemma *convex-closed-oi*:

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

<proof>

lemma

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

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** $\sqsubseteq\updownarrow$ 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** $\sqsubseteq\updownarrow$ 50) **where**

$$R \sqsubseteq\updownarrow S \equiv R \subseteq S\updownarrow$$

lemma *lower-less-eq*:

$$R \sqsubseteq\downarrow S \iff (\forall a B . (a,B) \in R \implies (\exists C . (a,C) \in S \wedge B \subseteq C))$$

<proof>

lemma *upper-less-eq*:

$$R \sqsubseteq\uparrow S \iff (\forall a C . (a,C) \in S \implies (\exists B . (a,B) \in R \wedge B \subseteq C))$$

<proof>

lemma *Convex-less-eq*:

$$R \sqsubseteq\updownarrow S \iff (\forall a C . (a,C) \in R \implies (\exists B D . (a,B) \in S \wedge (a,D) \in S \wedge B \subseteq C \wedge C \subseteq D))$$

<proof>

lemma *Convex-lower-upper*:

$$R \sqsubseteq\updownarrow S \iff R \sqsubseteq\downarrow S \wedge S \sqsubseteq\uparrow R$$

<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*:

$$R \sqsubseteq\downarrow S \implies S \sqsubseteq\downarrow T \implies R \sqsubseteq\downarrow T$$

<proof>

lemma *upper-transitive*:

$$R \sqsubseteq\uparrow S \implies S \sqsubseteq\uparrow T \implies R \sqsubseteq\uparrow T$$

<proof>

lemma *convex-transitive*:

$$R \sqsubseteq\updownarrow S \implies S \sqsubseteq\updownarrow T \implies R \sqsubseteq\updownarrow T$$

<proof>

lemma *Convex-transitive*:

$$R \sqsubseteq\updownarrow S \implies S \sqsubseteq\updownarrow T \implies R \sqsubseteq\updownarrow T$$

<proof>

lemma *bot-lower-least*:

$$\{\} \sqsubseteq\downarrow R$$

<proof>

lemma *top-upper-least*:

$$U \sqsubseteq\uparrow R$$

<proof>

lemma *bot-Convex-least*:

$$\{\} \sqsubseteq\updownarrow R$$

<proof>

lemma *top-lower-greatest*:

$$R \sqsubseteq\downarrow U$$

<proof>

lemma *bot-upper-greatest*:

$$R \sqsubseteq\uparrow \{\}$$

<proof>

lemma *top-Convex-greatest*:

$$R \sqsubseteq\updownarrow U$$

<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*:

$$R \sqsubseteq\updownarrow R \cup\cup R$$

<proof>

lemma *Convex-ii-increasing*:

$$R \sqsubseteq\updownarrow R \cup\cup R$$

<proof>

lemma *lower-ii-decreasing*:

$$R \cap\cap S \sqsubseteq\downarrow R$$

<proof>

lemma *upper-ii-decreasing*:

$$R \cap\cap R \sqsubseteq\uparrow R$$

<proof>

lemma *convex-ii-decreasing*:

$$R \cap R \sqsubseteq\uparrow R$$

<proof>

lemma *Convex-ii-increasing*:

$$R \sqsubseteq\uparrow R \cap R$$

<proof>

lemma *iu-lower-left-isotone*:

$$R \sqsubseteq\downarrow S \implies R \cup T \sqsubseteq\downarrow S \cup T$$

<proof>

lemma *iu-upper-left-isotone*:

$$R \sqsubseteq\uparrow S \implies R \cup T \sqsubseteq\uparrow S \cup T$$

<proof>

lemma *iu-convex-left-isotone*:

$$R \sqsubseteq\uparrow S \implies R \cup T \sqsubseteq\uparrow S \cup T$$

<proof>

lemma *iu-Convex-left-isotone*:

$$R \sqsubseteq\uparrow S \implies R \cup T \sqsubseteq\uparrow S \cup T$$

<proof>

lemma *iu-lower-right-isotone*:

$$R \sqsubseteq\downarrow S \implies T \cup R \sqsubseteq\downarrow T \cup S$$

<proof>

lemma *iu-upper-right-isotone*:

$$R \sqsubseteq\uparrow S \implies T \cup R \sqsubseteq\uparrow T \cup S$$

<proof>

lemma *iu-convex-right-isotone*:

$$R \sqsubseteq\uparrow S \implies T \cup R \sqsubseteq\uparrow T \cup S$$

<proof>

lemma *iu-Convex-right-isotone*:

$$R \sqsubseteq\uparrow S \implies T \cup R \sqsubseteq\uparrow T \cup S$$

<proof>

lemma *iu-lower-isotone*:

$$R \sqsubseteq\downarrow S \implies P \sqsubseteq\downarrow Q \implies R \cup P \sqsubseteq\downarrow S \cup Q$$

<proof>

lemma *iu-upper-isotone*:

$$R \sqsubseteq\uparrow S \implies P \sqsubseteq\uparrow Q \implies R \cup P \sqsubseteq\uparrow S \cup Q$$

<proof>

lemma *iu-convex-isotone*:

$$R \sqsubseteq\uparrow S \implies P \sqsubseteq\uparrow Q \implies R \cup\cup P \sqsubseteq\uparrow S \cup\cup Q$$

<proof>

lemma *iu-Convex-isotone:*

$$R \sqsubseteq\uparrow S \implies P \sqsubseteq\uparrow Q \implies R \cup\cup P \sqsubseteq\uparrow S \cup\cup Q$$

<proof>

lemma *ii-lower-left-isotone:*

$$R \sqsubseteq\downarrow S \implies R \cap\cap T \sqsubseteq\downarrow S \cap\cap T$$

<proof>

lemma *ii-upper-left-isotone:*

$$R \sqsubseteq\uparrow S \implies R \cap\cap T \sqsubseteq\uparrow S \cap\cap T$$

<proof>

lemma *ii-convex-left-isotone:*

$$R \sqsubseteq\uparrow S \implies R \cap\cap T \sqsubseteq\uparrow S \cap\cap T$$

<proof>

lemma *ii-Convex-left-isotone:*

$$R \sqsubseteq\uparrow S \implies R \cap\cap T \sqsubseteq\uparrow S \cap\cap T$$

<proof>

lemma *ii-lower-right-isotone:*

$$R \sqsubseteq\downarrow S \implies T \cap\cap R \sqsubseteq\downarrow T \cap\cap S$$

<proof>

lemma *ii-upper-right-isotone:*

$$R \sqsubseteq\uparrow S \implies T \cap\cap R \sqsubseteq\uparrow T \cap\cap S$$

<proof>

lemma *ii-convex-right-isotone:*

$$R \sqsubseteq\uparrow S \implies T \cap\cap R \sqsubseteq\uparrow T \cap\cap S$$

<proof>

lemma *ii-Convex-right-isotone:*

$$R \sqsubseteq\uparrow S \implies T \cap\cap R \sqsubseteq\uparrow T \cap\cap S$$

<proof>

lemma *ii-lower-isotone:*

$$R \sqsubseteq\downarrow S \implies P \sqsubseteq\downarrow Q \implies R \cap\cap P \sqsubseteq\downarrow S \cap\cap Q$$

<proof>

lemma *ii-upper-isotone:*

$$R \sqsubseteq\uparrow S \implies P \sqsubseteq\uparrow Q \implies R \cap\cap P \sqsubseteq\uparrow S \cap\cap Q$$

<proof>

lemma *ii-convex-isotone:*

$$R \sqsubseteq\uparrow S \implies P \sqsubseteq\uparrow Q \implies R \cap\cap P \sqsubseteq\uparrow S \cap\cap Q$$

<proof>

lemma *ii-Convex-isotone:*

$$R \sqsubseteq\Downarrow S \implies P \sqsubseteq\Downarrow Q \implies R \sqcap P \sqsubseteq\Downarrow S \sqcap Q$$

<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:*

$$R \sqsubseteq\Downarrow S \implies R \cup T \sqsubseteq\Downarrow S \cup T$$

<proof>

lemma *ou-Convex-left-isotone:*

$$R \sqsubseteq\Downarrow S \implies R \cup T \sqsubseteq\Downarrow S \cup T$$

<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:*

$$R \sqsubseteq\Downarrow S \implies T \cup R \sqsubseteq\Downarrow T \cup S$$

<proof>

lemma *ou-Convex-right-isotone:*

$$R \sqsubseteq\Downarrow S \implies T \cup R \sqsubseteq\Downarrow T \cup S$$

<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:*

$$R \sqsubseteq\Downarrow S \implies P \sqsubseteq\Downarrow Q \implies R \cup P \sqsubseteq\Downarrow S \cup Q$$

<proof>

lemma *ou-Convex-isotone*:

$$R \sqsubseteq\Downarrow S \implies P \sqsubseteq\Downarrow Q \implies R \cup P \sqsubseteq\Downarrow S \cup Q$$

<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*:

$$R \sqsubseteq\Downarrow S \implies T * R \sqsubseteq\Downarrow T * S$$

<proof>

lemma *sp-Convex-left-isotone*:

$$R \sqsubseteq\Downarrow S \implies T * R \sqsubseteq\Downarrow T * S$$

<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*:

$$R \sqsubseteq\Downarrow S \implies T \odot R \sqsubseteq\Downarrow T \odot S$$

<proof>

lemma *cp-Convex-left-isotone*:

$$R \sqsubseteq\Downarrow S \implies T \odot R \sqsubseteq\Downarrow T \odot S$$

<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:*

$$R \sqsubseteq \Downarrow S \implies R \Downarrow \sqsubseteq \Downarrow S \Downarrow$$

<proof>

lemma *convex-Convex-isotone:*

$$R \sqsubseteq\Downarrow S \implies R\Downarrow \sqsubseteq\Downarrow S\Downarrow$$

<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:
 $R \subseteq S \implies R \sqsubseteq\Downarrow S$
<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:
 $R \subseteq S \implies R \cap T \sqsubseteq\Downarrow S \cap T$
<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:
 $R \subseteq S \implies T \cap R \sqsubseteq\Downarrow T \cap S$
<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:
 $R \subseteq S \implies P \subseteq Q \implies R \cap P \sqsubseteq\Downarrow S \cap Q$

$\langle proof \rangle$

lemma *sp-ii-unit-lower*:

$$R * 1_{\cup\cup} \sqsubseteq\downarrow R$$

$\langle proof \rangle$

lemma *cp-ii-unit-upper*:

$$R \sqsubseteq\uparrow R \odot 1_{\cap\cap}$$

$\langle proof \rangle$

lemma *lower-ii-down*:

$$R \sqsubseteq\downarrow S \longleftrightarrow R\downarrow = (R \cap\cap S)\downarrow$$

$\langle proof \rangle$

lemma *lower-ii-lower-bound*:

$$R \sqsubseteq\downarrow S \longleftrightarrow R \subseteq R \cap\cap S$$

$\langle proof \rangle$

lemma *upper-ii-up*:

$$R \sqsubseteq\uparrow S \longleftrightarrow S\uparrow = (R \cup\cup S)\uparrow$$

$\langle proof \rangle$

lemma *upper-ii-upper-bound*:

$$R \sqsubseteq\uparrow S \longleftrightarrow S \subseteq R \cup\cup S$$

$\langle proof \rangle$

lemma

$$R \sqsubseteq\downarrow S \longleftrightarrow R = R \cap\cap S$$

nitpick[*expect=genuine,card=1*]

$\langle proof \rangle$

lemma

$$R \sqsubseteq\uparrow S \longleftrightarrow S = R \cup\cup S$$

nitpick[*expect=genuine,card=1*]

$\langle proof \rangle$

lemma *convex-oi-Convex-ii*:

$$R\downarrow \cap S\downarrow \sqsubseteq\downarrow R \cup\cup S$$

$\langle proof \rangle$

lemma *convex-oi-Convex-ii*:

$$R\downarrow \cap S\downarrow \sqsubseteq\downarrow R \cap\cap S$$

$\langle proof \rangle$

lemma *convex-oi-ii-ii*:

$$R\downarrow \cap S\downarrow = (R \cup\cup S)\uparrow \cap (R \cap\cap S)\downarrow$$

$\langle proof \rangle$

lemma *ii-lower-ii*:

$R \cap S \sqsubseteq \downarrow R \cup S$
 ⟨proof⟩

lemma *ii-upper-ii*:
 $R \cap S \sqsubseteq \uparrow R \cup S$
 ⟨proof⟩

lemma *ii-convex-ii*:
 $R \cap S \sqsubseteq \updownarrow R \cup S$
 ⟨proof⟩

lemma *convex-oi-ii-ii-convex*:
 $R \updownarrow \cap S \updownarrow = (R \cup S) \updownarrow \cap (R \cap S) \updownarrow$
 ⟨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*:
 $total R \longleftrightarrow 1_{UU} = R * 1_{UU}$
 ⟨proof⟩

lemma *domain-pointwise*:
 $x \in R * 1_{UU} \longleftrightarrow (\exists a B . (a,B) \in R \wedge x = (a,\{ \}))$
 ⟨proof⟩

card only works for finite sets

lemma *univalent-2*:
 $univalent R \longleftrightarrow (\forall a . finite \{ B . (a,B) \in R \} \wedge card \{ B . (a,B) \in R \} \leq one-class.one)$
 ⟨proof⟩

lemma *univalent-3*:
 $univalent R \longleftrightarrow (\forall S . R * 1_{UU} = S * 1_{UU} \wedge S \subseteq R \longrightarrow S = R)$
 ⟨proof⟩

lemma total-2:

$total\ R \longleftrightarrow (\forall a . \{ B . (a,B) \in R \} \neq \{\})$
<proof>

lemma total-3:

$total\ R \longleftrightarrow (\forall a . finite\ \{ B . (a,B) \in R \} \longrightarrow card\ \{ B . (a,B) \in R \} \geq one-class.one)$
<proof>

lemma total-4: $total\ R \longleftrightarrow 1_{\cup\cup} \subseteq R * 1_{\cup\cup}$

<proof>

lemma deterministic-2:

$deterministic\ R \longleftrightarrow (\forall a . card\ \{ B . (a,B) \in R \} = one-class.one)$
<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 $S = S\downarrow \cup\cup S$

<proof>

lemma univalent-convex-ii-idempotent:

assumes *univalent S*

shows $S = S \Downarrow \cap \cap S$
<proof>

lemma *univalent-iu-closed*:
 $univalent R \implies univalent S \implies univalent (R \cup \cup S)$
<proof>

lemma *univalent-ii-closed*:
 $univalent R \implies univalent S \implies univalent (R \cap \cap S)$
<proof>

lemma *total-lower*:
 $total R \iff 1 \cup \cup \sqsubseteq \downarrow R$
<proof>

lemma *total-upper*:
 $total R \iff R \sqsubseteq \uparrow 1 \cap \cap$
<proof>

lemma *total-lower-iu*:
assumes *total T*
shows $R \sqsubseteq \downarrow R \cup \cup T$
<proof>

lemma *total-upper-ii*:
assumes *total T*
shows $R \cap \cap T \sqsubseteq \uparrow R$
<proof>

lemma *total-univalent-lower-iu*:
assumes *total T*
and *univalent S*
and $T \sqsubseteq \downarrow S$
shows $T \cup \cup S = S$
<proof>

lemma *total-iu-closed*:
 $total R \implies total S \implies total (R \cup \cup S)$
<proof>

lemma *total-ii-closed*:
 $total R \implies total S \implies total (R \cap \cap S)$
<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 $V \sqsubseteq\uparrow R \longleftrightarrow (\forall a B C . (a,B) \in R \wedge (a,C) \in V \longrightarrow C \subseteq B)$
<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 $S \sqsubseteq\downarrow T \longleftrightarrow S \sqsubseteq\uparrow T$
 ⟨*proof*⟩

lemma *deterministic-upper-conver*:
assumes *deterministic T*
and *deterministic S*
shows $S \sqsubseteq\uparrow T \longleftrightarrow S \sqsubseteq\downarrow T$
 ⟨*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 $(R \sqsubseteq\uparrow S) \longleftrightarrow (R \cup\cup S = S)$
 ⟨*proof*⟩

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** $=\downarrow$ 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** $=\uparrow$ 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** $=\Downarrow$ 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*:
 $R =\uparrow S \longleftrightarrow (\forall a C . (\exists B . (a, B) \in R \wedge B \subseteq C) \longleftrightarrow (\exists B . (a, B) \in S \wedge B \subseteq C))$
 $\langle proof \rangle$

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*:

$$R =\Downarrow S \implies P =\Downarrow Q \implies R \cap\cap P =\Downarrow S \cap\cap Q$$

<proof>

lemma *sp-lower-eq-left-congruence*:

$$R =\downarrow S \implies T * R =\downarrow T * S$$

<proof>

lemma *sp-upper-eq-left-congruence*:

$$R =\uparrow S \implies T * R =\uparrow T * S$$

\langle proof \rangle

lemma *sp-convex-eq-left-congruence*:

$$R =\Downarrow S \implies T * R =\Downarrow T * S$$

\langle proof \rangle

lemma *cp-lower-eq-left-congruence*:

$$R =\downarrow S \implies T \odot R =\downarrow T \odot S$$

\langle proof \rangle

lemma *cp-upper-eq-left-congruence*:

$$R =\uparrow S \implies T \odot R =\uparrow T \odot S$$

\langle proof \rangle

lemma *cp-convex-eq-left-congruence*:

$$R =\Downarrow S \implies T \odot R =\Downarrow T \odot S$$

\langle proof \rangle

lemma *lower-eq-ic-upper*:

$$R =\downarrow S \longleftrightarrow \sim R =\uparrow \sim S$$

\langle proof \rangle

lemma *upper-eq-ic-lower*:

$$R =\uparrow S \longleftrightarrow \sim R =\downarrow \sim S$$

\langle proof \rangle

lemma *convex-eq-ic-lower*:

$$R =\Downarrow S \longleftrightarrow \sim R =\Downarrow \sim S$$

\langle proof \rangle

lemma *up-lower-eq-congruence*:

$$R =\downarrow S \implies R\uparrow =\downarrow S\uparrow$$

\langle proof \rangle

lemma *up-upper-eq-congruence*:

$$R =\uparrow S \implies R\uparrow =\uparrow S\uparrow$$

\langle proof \rangle

lemma *up-convex-eq-congruence*:

$$R =\Downarrow S \implies R\uparrow =\Downarrow S\uparrow$$

\langle proof \rangle

lemma *down-lower-eq-congruence*:

$$R =\downarrow S \implies R\downarrow =\downarrow S\downarrow$$

\langle proof \rangle

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:*

$R =\downarrow S \implies R\Downarrow =\downarrow S\Downarrow$
<proof>

lemma *convex-upper-eq-congruence:*

$R =\uparrow S \implies R\Downarrow =\uparrow S\Downarrow$
<proof>

lemma *convex-convex-eq-congruence:*

$R =\Downarrow S \implies R\Downarrow =\Downarrow S\Downarrow$
<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 $(R =\downarrow S) \longleftrightarrow (R = S)$

<proof>

lemma *univalent-upper-eq-subset:*

assumes *univalent* S

and $S =\uparrow R$

shows $S \subseteq R$

<proof>

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*:

$(\forall P . Q \sqsubseteq \uparrow P \longleftrightarrow R \sqsubseteq \uparrow P \wedge S \sqsubseteq \uparrow P) \longleftrightarrow Q = \uparrow R \cup \cup S$

$\langle proof \rangle$

lemma *upper-meet*:

$(\forall P . P \sqsubseteq \uparrow Q \longleftrightarrow P \sqsubseteq \uparrow R \wedge P \sqsubseteq \uparrow S) \longleftrightarrow Q = \uparrow R \cup S$

$\langle proof \rangle$

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*:

$$(\cap i \in I . X i \downarrow) = \downarrow \cap \cap X|I$$

<proof>

lemma *oU-up-upper-eq-oU*:

$(\bigcup R \in X . R \uparrow) = \uparrow \bigcup X$
 ⟨proof⟩

lemma *oI-up-upper-eq-iI*:
 $(\bigcap i \in I . X i \uparrow) = \uparrow \bigcup \bigcup X | I$
 ⟨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⟩

7 Fusion and Fission

7.1 Atoms and co-atoms

definition *atoms* :: ('a,'b) mrel ($A_{\cup\cup}$)
 where $A_{\cup\cup} \equiv \{ (a, \{b\}) \mid a \ b . \text{True} \}$

definition *co-atoms* :: ('a,'b) mrel ($A_{\cap\cap}$)
 where $A_{\cap\cap} \equiv \{ (a, \text{UNIV} - \{b\}) \mid a \ b . \text{True} \}$

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**

inner-univalent $R \equiv R \subseteq 1_{\cup\cup} \cup A_{\cup\cup}$

abbreviation *inner-total* :: ('a,'b) mrel \Rightarrow bool **where**

inner-total $R \equiv R \subseteq -1_{\cup\cup}$

abbreviation *inner-deterministic* :: ('a,'b) mrel \Rightarrow bool **where**

inner-deterministic $R \equiv \text{inner-total } R \wedge \text{inner-univalent } R$

lemma *inner-deterministic-atoms*:

inner-deterministic $R \longleftrightarrow R \subseteq A_{\cup\cup}$
<proof>

lemma *inner-univalent*:

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*:

inner-univalent $R \longleftrightarrow (\forall a B . (a,B) \in R \longrightarrow \text{finite } B \wedge \text{card } B \leq$

one-class.one)
⟨proof⟩

lemma *inner-total*:

inner-total $R \iff (\forall a B . (a,B) \in R \implies (\exists b . b \in B))$
⟨proof⟩

lemma *inner-total-2*:

inner-total $R \iff (\forall a B . (a,B) \in R \implies B \neq \{\})$
⟨proof⟩

lemma *inner-total-3*:

inner-total $R \iff (\forall a B . (a,B) \in R \wedge \text{finite } B \implies \text{card } B \geq \text{one-class.one})$
⟨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 O converse 1 O 1 = R)

<proof>

lemma *inner-deterministic-s-id-conv-epsiloff*:

inner-deterministic R \implies R O converse s-id = R O 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 $(R =\downarrow\uparrow S) \longleftrightarrow (R = S)$

<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* $(R \cap S)$
 \langle *proof* \rangle

lemma *inner-total-iu-closed*:
inner-total $R \implies$ *inner-total* $S \implies$ *inner-total* $(R \cup S)$
 \langle *proof* \rangle

lemma
inner-total $R \implies$ *inner-total* $S \implies$ *inner-total* $(R \cap S)$
nitpick[*expect=genuine,card=1,2*]
 \langle *proof* \rangle

7.3 Fusion

lemma *fusion-set*:
 $fus\ R \equiv \{ (a,B) . B = \bigcup \{ C . (a,C) \in R \} \}$
 \langle *proof* \rangle

declare *fusion-set* [*mr-simp*]

lemma *fusion-lower-increasing*:
 $R \sqsubseteq\downarrow fus\ R$
 \langle *proof* \rangle

lemma *fusion-deterministic*:
deterministic $(fus\ R)$
 \langle *proof* \rangle

lemma *fusion-least*:
assumes $R \sqsubseteq\downarrow S$
and *deterministic* S
shows $fus\ R \sqsubseteq\downarrow S$
 \langle *proof* \rangle

lemma *fusion-unique*:
assumes $\forall R . R \sqsubseteq\downarrow f\ R$
and $\forall R .$ *deterministic* $(f\ R)$
and $\forall R\ S . R \sqsubseteq\downarrow S \wedge$ *deterministic* $S \longrightarrow f\ R \sqsubseteq\downarrow S$
shows $f\ T = fus\ T$
 \langle *proof* \rangle

lemma *fusion-down-char*:
 $(fus\ R)\downarrow = -((-(R\downarrow) \cap A_{\cup\cup})\uparrow)$
 \langle *proof* \rangle

lemma *fusion-up-char*:
 $(fus\ R)\uparrow = -((\sim(R\downarrow) \cap A_{\cap\cap})\downarrow)$

<proof>

lemma *fusion-up-char-2:*

$$(fus R)\uparrow = -(((R\downarrow \cap A_{UU}) * \sim I)\downarrow)$$

<proof>

lemma *fusion-char:*

$$fus R = -((-(R\downarrow) \cap A_{UU})\uparrow) \cap -((\sim(R\downarrow) \cap A_{\cap\cap})\downarrow)$$

<proof>

lemma *fusion-char-2:*

$$fus R = -((-(R\downarrow) \cap A_{UU})\uparrow) \cap -(((R\downarrow \cap A_{UU}) * \sim I)\downarrow)$$

<proof>

lemma *fusion-lower-isotone:*

$$R \sqsubseteq\downarrow S \implies fus R \sqsubseteq\downarrow fus S$$

<proof>

lemma *fusion-iu-idempotent:*

$$fus R \cup\cup fus R = fus R$$

<proof>

lemma *fusion-down:*

$$fus R = fus (R\downarrow)$$

<proof>

lemma *fusion-iu-total:*

$$total T \implies T \cup\cup fus T = fus T$$

<proof>

lemma *fusion-deterministic-fixpoint:*

$$deterministic R \longleftrightarrow R = fus R$$

<proof>

abbreviation *non-empty* :: ('a,'b) mrel \Rightarrow ('a,'b) mrel (ne - [100] 100)

where $ne R \equiv R \cap -1_{UU}$

lemma *non-empty:*

$$ne R = \{ (a,B) \mid a B . (a,B) \in R \wedge B \neq \{\} \}$$

<proof>

lemma *ne-equality:*

$$ne R = R \longleftrightarrow R \subseteq -1_{UU}$$

<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*:

$$total T \implies ne ((R * T)\downarrow) = ne (R\downarrow) * ne (T\downarrow)$$

<proof>

lemma *inner-univalent-char*:

$$inner-univalent S \iff (\forall R . fus R = fus S \wedge R \sqsubseteq\downarrow S \longrightarrow ne R = ne S)$$

<proof>

lemma *ne-dist-oU*:

$$ne (\bigcup X) = \bigcup (non-empty \text{ ' } X)$$

<proof>

7.4 Fission

lemma *fission-set*:

$$fis R = \{ (a, \{b\}) \mid a b . \exists B . (a, B) \in R \wedge b \in B \}$$

<proof>

declare *fission-set* [*mr-simp*]

lemma *fission-var*:

$$fis R = R\downarrow \cap A_{\cup\cup}$$

<proof>

lemma *fission-lower-decreasing*:

$$fis R \sqsubseteq\downarrow R$$

<proof>

lemma *fission-inner-deterministic*:

$$inner-deterministic (fis R)$$

<proof>

lemma *fission-greatest*:

assumes $S \sqsubseteq\downarrow R$

and *inner-deterministic* S

shows $S \sqsubseteq\downarrow fis R$

<proof>

lemma *fission-unique*:

assumes $\forall R . f R \sqsubseteq\downarrow R$

and $\forall R . \text{inner-deterministic } (f R)$

and $\forall R S . S \sqsubseteq\downarrow R \wedge \text{inner-deterministic } S \longrightarrow S \sqsubseteq\downarrow f R$

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 *fusion-fission-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*:

$$\text{fis } (\cup X) = \cup (\text{fis } ' X)$$

<proof>

7.5 Co-fusion and co-fission

definition *co-fusion* $:: ('a, 'b) \text{ mrel} \Rightarrow ('a, 'b) \text{ mrel} (\Box\Box - [80] 80)$ where
 $\Box\Box R \equiv \{ (a, B) . B = \bigcap \{ C . (a, C) \in R \} \}$

declare *co-fusion-def* [*mr-simp*]

lemma *co-fusion-upper-decreasing*:

$\Box\Box R \sqsubseteq\uparrow R$
 $\langle \text{proof} \rangle$

lemma *co-fusion-deterministic*:

deterministic $(\Box\Box R)$
 $\langle \text{proof} \rangle$

lemma *co-fusion-greatest*:

assumes $S \sqsubseteq\uparrow R$
and *deterministic* S
shows $S \sqsubseteq\uparrow \Box\Box R$
 $\langle \text{proof} \rangle$

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 $f T = \Box\Box T$
 $\langle \text{proof} \rangle$

lemma *co-fusion-up-char*:

$(\Box\Box R)\uparrow = -((-(R\uparrow) \cap A_{\cap\cap})\downarrow)$
 $\langle \text{proof} \rangle$

lemma *co-fusion-down-char*:

$(\Box\Box R)\downarrow = -((\sim(R\uparrow) \cap A_{\cup\cup})\uparrow)$
 $\langle \text{proof} \rangle$

lemma *co-fusion-down-char-2*:

$(\Box\Box R)\downarrow = -(((R\uparrow) \cap A_{\cap\cap}) \odot \sim 1)\uparrow)$
 $\langle \text{proof} \rangle$

lemma *co-fusion-char*:

$\Box\Box R = -((-(R\uparrow) \cap A_{\cap\cap})\downarrow) \cap -((\sim(R\uparrow) \cap A_{\cup\cup})\uparrow)$
 $\langle \text{proof} \rangle$

lemma *co-fusion-char-2*:

$\Box\Box R = -((-(R\uparrow) \cap A_{\cap\cap})\downarrow) \cap -(((R\uparrow) \cap A_{\cap\cap}) \odot \sim 1)\uparrow)$
 $\langle \text{proof} \rangle$

lemma *co-fusion-upper-isotone*:

$R \sqsubseteq\uparrow S \Longrightarrow \Box\Box R \sqsubseteq\uparrow \Box\Box S$

<proof>

lemma *co-fusion-ii-idempotent*:

$$\sqcap \sqcap R \sqcap \sqcap \sqcap R = \sqcap \sqcap R$$

<proof>

lemma *co-fusion-up*:

$$\sqcap \sqcap R = \sqcap \sqcap (R\uparrow)$$

<proof>

lemma *co-fusion-ii-total*:

$$\text{total } T \implies T \sqcap \sqcap \sqcap T = \sqcap \sqcap T$$

<proof>

lemma *co-fusion-deterministic-fixpoint*:

$$\text{deterministic } R \longleftrightarrow R = \sqcap \sqcap R$$

<proof>

abbreviation *co-fission* :: ('a,'b) mrel \implies ('a,'b) mrel (*at_{sqcap}* - [80] 80) **where**

$$\text{at}_{\sqcap} R \equiv R\uparrow \sqcap A_{\sqcap}$$

lemma *co-fission*:

$$\text{at}_{\sqcap} R = \{ (a,B) \mid a B . (\exists b . \neg B = \{b\}) \wedge (\exists C . (a,C) \in R \wedge C \subseteq B) \}$$

<proof>

declare *co-fission* [*mr-simp*]

lemma *co-fission-upper-increasing*:

$$R \sqsubseteq \uparrow \text{at}_{\sqcap} R$$

<proof>

lemma *co-fission-ic-inner-deterministic*:

$$\text{inner-deterministic } (\sim \text{at}_{\sqcap} R)$$

<proof>

lemma *co-fission-least*:

$$\text{assumes } R \sqsubseteq \uparrow S$$

and *inner-deterministic* ($\sim S$)

$$\text{shows } \text{at}_{\sqcap} R \sqsubseteq \uparrow S$$

<proof>

lemma *co-fission-unique*:

$$\text{assumes } \forall R . R \sqsubseteq \uparrow f R$$

and $\forall R . \text{inner-deterministic } (\sim f R)$

$$\text{and } \forall R S . R \sqsubseteq \uparrow S \wedge \text{inner-deterministic } (\sim S) \longrightarrow f R \sqsubseteq \uparrow S$$

$$\text{shows } f T = \text{at}_{\sqcap} T$$

<proof>

lemma *co-fission-upper-isotone*:

$R \sqsubseteq \uparrow S \implies at_{\cap\cap} R \sqsubseteq \uparrow at_{\cap\cap} S$
 ⟨proof⟩

lemma *co-fission-idempotent*:

$at_{\cap\cap} (at_{\cap\cap} R) = at_{\cap\cap} R$
 ⟨proof⟩

lemma *co-fission-top*:

$at_{\cap\cap} U = A_{\cap\cap}$
 ⟨proof⟩

lemma *co-fission-up*:

$at_{\cap\cap} R = at_{\cap\cap} (R \uparrow)$
 ⟨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*:

$\Box\Box (at_{\cap\cap} R) \sqsubseteq \uparrow R$
 ⟨proof⟩

lemma *co-fusion-co-fusion-upper-increasing*:

$R \sqsubseteq \uparrow at_{\cap\cap} (\Box\Box R)$
 ⟨proof⟩

lemma *co-fusion-co-fission-galois*:

$\Box\Box R \sqsubseteq \uparrow S \longleftrightarrow R \sqsubseteq \uparrow at_{\cap\cap} S$
 ⟨proof⟩

lemma *co-fusion-co-fusion*:

$at_{\cap\cap} (\Box\Box R) = at_{\cap\cap} R$
 ⟨proof⟩

lemma *co-fusion-co-fission*:

$\Box\Box (at_{\cap\cap} R) = \Box\Box R$
 ⟨proof⟩

lemma *same-co-fusion-co-fission-upper*:

$\Box\Box R = \Box\Box S \implies S \sqsubseteq \uparrow at_{\cap\cap} R$
 ⟨proof⟩

lemma *co-fusion-idempotent*:

$\Box\Box (\Box\Box R) = \Box\Box R$
 ⟨proof⟩

8 Modalities

8.1 Tests

abbreviation $test :: ('a, 'a) mrel \Rightarrow bool$ **where**
 $test\ R \equiv R \subseteq 1$

lemma *test*:
 $test\ R \longleftrightarrow (\forall a\ B . (a, B) \in R \longrightarrow B = \{a\})$
<proof>

lemma *test-fix*: $test\ R \equiv R \cap 1_\sigma = R$
<proof>

lemma *test-ou-closed*:
 $test\ p \Longrightarrow test\ q \Longrightarrow test\ (p \cup q)$
<proof>

lemma *test-oi-closed*:
 $test\ p \Longrightarrow test\ (p \cap q)$
<proof>

abbreviation *test-complement* $:: ('a, 'a) mrel \Rightarrow ('a, 'a) mrel$ (λ - [80] 80) **where**
 $\lambda\ R \equiv -R \cap 1$

lemma *test-complement-closed*:
 $test\ (\lambda\ p)$
<proof>

lemma *test-double-complement*:
 $test\ p \longleftrightarrow p = \lambda\ \lambda\ p$
<proof>

lemma *test-complement*:
 $(a, \{a\}) \in \lambda\ p \longleftrightarrow \neg (a, \{a\}) \in p$
<proof>

declare *test-complement* [*mr-simp*]

lemma *test-complement-antitone*:
assumes $test\ p$
shows $p \subseteq q \longleftrightarrow \lambda\ q \subseteq \lambda\ p$
<proof>

lemma *test-complement-huntington*:
 $test\ p \Longrightarrow p = \lambda\ (\lambda\ p \cup \lambda\ q) \cup \lambda\ (\lambda\ p \cup q)$
<proof>

abbreviation *test-implication* $:: ('a, 'a) mrel \Rightarrow ('a, 'a) mrel \Rightarrow ('a, 'a) mrel$
(**infixl** \rightarrow 65) **where**

$$p \rightarrow q \equiv \lambda p \cup q$$

lemma *test-implication-closed*:

$$\text{test } q \implies \text{test } (p \rightarrow q)$$

<proof>

lemma *test-implication*:

$$(a, \{a\}) \in p \rightarrow q \iff ((a, \{a\}) \in p \implies (a, \{a\}) \in q)$$

<proof>

declare *test-implication* [*mr-simp*]

lemma *test-implication-left-antitone*:

$$\text{assumes } \text{test } p$$

$$\text{shows } p \subseteq r \implies r \rightarrow q \subseteq p \rightarrow q$$

<proof>

lemma *test-implication-right-isotone*:

$$\text{assumes } \text{test } p$$

$$\text{shows } q \subseteq r \implies p \rightarrow q \subseteq p \rightarrow r$$

<proof>

lemma *test-sp-idempotent*:

$$\text{test } p \implies p * p = p$$

<proof>

lemma *test-sp*:

$$\text{assumes } \text{test } p$$

$$\text{shows } p * R = (p * U) \cap R$$

<proof>

lemma *sp-test*:

$$\text{test } p \implies R * p = R \cap (U * p)$$

<proof>

lemma *sp-test-dist-oi*:

$$\text{test } p \implies (R \cap S) * p = (R * p) \cap (S * p)$$

<proof>

lemma *sp-test-dist-oi-left*:

$$\text{test } p \implies (R \cap S) * p = (R * p) \cap S$$

<proof>

lemma *sp-test-dist-oi-right*:

$$\text{test } p \implies (R \cap S) * p = R \cap (S * p)$$

<proof>

lemma *sp-test-sp-oi-left*:

$$\text{test } p \implies (R \cap (U * p)) * T = R * p * T$$

$\langle \text{proof} \rangle$

lemma *sp-test-sp-oi-right*:

$\text{test } p \implies R * ((p * U) \cap T) = R * p * T$

$\langle \text{proof} \rangle$

lemma *test-sp-ne*:

$\text{test } p \implies p * \text{ne } R = \text{ne } (p * R)$

$\langle \text{proof} \rangle$

lemma *ne-sp-test*:

$\text{test } p \implies \text{ne } R * p = \text{ne } (R * p)$

$\langle \text{proof} \rangle$

lemma *top-sp-test-down-closed*:

assumes *test p*

shows $U * p = (U * p)\downarrow$

$\langle \text{proof} \rangle$

lemma *oc-top-sp-test-up-closed*:

$\text{test } p \implies -(U * p) = (-(U * p))\uparrow$

$\langle \text{proof} \rangle$

lemma *top-sp-test*:

$\text{test } p \implies (a, B) \in U * p \longleftrightarrow (\forall b \in B . (b, \{b\}) \in p)$

$\langle \text{proof} \rangle$

lemma *oc-top-sp-test*:

$\text{test } p \implies (a, B) \in -(U * p) \longleftrightarrow (\exists b \in B . (b, \{b\}) \notin p)$

$\langle \text{proof} \rangle$

declare *top-sp-test* [*mr-simp*] *oc-top-sp-test* [*mr-simp*]

lemma *oc-top-sp-test-0*:

$-1_{\cup\cup} * \wr p = \text{ne } (U * \wr p)$

$\langle \text{proof} \rangle$

lemma *oc-top-sp-test-1*:

assumes *test p*

shows $-(U * p) = (\text{ne } (U * \wr p))\uparrow$

$\langle \text{proof} \rangle$

lemma *oc-top-sp-test-2*:

$\text{test } p \implies -(U * p) = (-1_{\cup\cup} * \wr p)\uparrow$

$\langle \text{proof} \rangle$

lemma *split-sp-test*:

assumes *test p*

shows $R = (R * p) \cup (\text{ne } R \cap (\text{ne } (R\downarrow * \wr p))\uparrow)$

<proof>

lemma *top-sp-test-down-iff-1:*

assumes *test p*

shows $R \subseteq U * p \longleftrightarrow R \downarrow \subseteq U * p$

<proof>

lemma *test-ne:*

$test\ p \implies ne\ p = p$

<proof>

lemma *ne-test-up:*

$test\ p \implies ne\ (p \uparrow) = p \uparrow$

<proof>

lemma *ne-sp-test-up:*

$test\ p \implies (ne\ (R * p)) \uparrow = ne\ R * p \uparrow$

<proof>

lemma *ne-down-sp-test-up:*

$test\ p \implies ne\ (R \downarrow * p \uparrow) = ne\ (R \downarrow) * p \uparrow$

<proof>

lemma *test-up-sp:*

$test\ p \implies p \uparrow = p * 1 \uparrow$

<proof>

lemma *top-test-oi-top-complement:*

$test\ p \implies (U * p) \cap (U * \imath p) = 1 \cup \cup$

<proof>

lemma *sp-test-oi-complement:*

$test\ p \implies (R * p) \cap (R * \imath p) = R \cap 1 \cup \cup$

<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 $R\downarrow \subseteq U * p \longleftrightarrow R\downarrow * \wr p \subseteq 1_{UU}$
<proof>

lemma *top-sp-test-down-iff-3*:
 $R\downarrow * \wr p \subseteq 1_{UU} \longleftrightarrow ne (R\downarrow) * \wr p \subseteq \{\}$
<proof>

lemma *top-sp-test-down-iff-4*:
assumes *test p*
shows $R\downarrow \cap (U * \wr p) \subseteq 1_{UU} \longleftrightarrow R\downarrow \subseteq 1_{UU} \cup (U * p)$
<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*:
 $t \subseteq 1 \cup 1_{UU} \Longrightarrow t * (R * S) = (t * R) * S$
<proof>

lemma *test-iu-test-sp-assoc-2*:
 $t \subseteq 1_{UU} \Longrightarrow R * (t * S) = (R * t) * S$
<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*:
 $t \subseteq 1_{UU} \Longrightarrow R * (S * t) = (R * S) * t$
<proof>

lemma *test-iu-test-sp-assoc-5*:
assumes $t \subseteq 1 \cup 1_{UU}$
shows $R * (S * t) = (R * S) * t$

$\langle proof \rangle$

lemma *inner-deterministic-sp-assoc:*

assumes *inner-univalent t*

shows $t * (R * S) = (t * R) * S$

$\langle proof \rangle$

lemma *iu-unit-below-top-sp-test:*

$1_{\cup\cup} \subseteq U * R$

$\langle proof \rangle$

lemma *ne-oi-complement-top-sp-test-1:*

ne $(R \cap -(U * S)) = R \cap -(U * S)$

$\langle proof \rangle$

lemma *ne-oi-complement-top-sp-test-2:*

ne $R \cap -(U * S) = R \cap -(U * S)$

$\langle proof \rangle$

lemma *schroeder-test:*

assumes *test p*

shows $R * p \subseteq S \longleftrightarrow -S * p \subseteq -R$

$\langle proof \rangle$

lemma *complement-test-sp-test:*

test p $\implies -p * p \subseteq -1$

$\langle proof \rangle$

lemma *test-sp-commute:*

test p \implies *test q* $\implies p * q = q * p$

$\langle proof \rangle$

lemma *test-shunting:*

assumes *test p*

and *test q*

and *test r*

shows $p * q \subseteq r \longleftrightarrow p \subseteq r \cup \wr q$

$\langle proof \rangle$

lemma *test-sp-is-iu:*

test p \implies *test q* $\implies p * q = p \cup\cup q$

$\langle proof \rangle$

lemma *test-set:*

test p $\implies p = \{ (a, \{a\}) \mid a . (a, \{a\}) \in p \}$

$\langle proof \rangle$

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 $p * q \subseteq r \iff q \subseteq p \rightarrow r$
<proof>

lemma *test-sp-shunting*:
assumes *test* p
shows $\wr p * R \subseteq \{\}$ $\iff R \subseteq p * R$
<proof>

lemma *test-oU-closed*:
 $\forall p \in X . \text{test } p \implies \text{test } (\bigcup X)$
<proof>

lemma *test-oI-closed*:
 $\exists p \in X . \text{test } p \implies \text{test } (\bigcap X)$
<proof>

lemma *sp-test-dist-oI*:
assumes *test* p
and $X \neq \{\}$
shows $(\bigcap X) * p = (\bigcap R \in X . R * p)$
<proof>

lemma *test-iU-is-iI*:
assumes $\forall i \in I . \text{test } (X \ i)$
and $I \neq \{\}$
shows $\bigcup \bigcup X | I = \bigcap \bigcap X | I$
<proof>

lemma *test-iU-is-oI*:
assumes $\forall i \in I . \text{test } (X \ i)$
and $I \neq \{\}$
shows $\bigcup \bigcup X | I = \bigcap (X \ ' I)$
<proof>

8.2 Domain and antidomain

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

abbreviation $a\text{Dom} :: ('a, 'b) \text{mrel} \Rightarrow ('a, 'a) \text{mrel}$ **where**
 $a\text{Dom } R \equiv \wr \text{Dom } R$

lemma *ad-set*: $a\text{Dom } R = \{(a, \{a\}) \mid a. \neg(\exists A. (a, A) \in R)\}$

<proof>

lemma *d-test:*

$test (Dom R)$

<proof>

lemma *ad-test:*

$test (aDom R)$

<proof>

lemma *ad-expl:*

$aDom R = -((R * 1_{\cup\cup}) \cup\cup 1) \cap 1$

<proof>

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*:

$$Dom (R\downarrow) = Dom R$$

<proof>

lemma *d-up*:

$$Dom (R\uparrow) = Dom R$$

<proof>

lemma *d-isotone*:

$$R \subseteq S \implies Dom R \subseteq Dom S$$

<proof>

lemma *ad-antitone*:

$$R \subseteq S \implies aDom S \subseteq aDom R$$

<proof>

lemma *d-dist-ou*:

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

<proof>

lemma *d-dist-iu*:

$$Dom (R \cup\cup S) = Dom R * Dom S$$

<proof>

lemma *d-dist-ii*:

$$Dom (R \cap\cap S) = Dom R * Dom S$$

<proof>

lemma *d-loc*:

$$Dom (R * Dom S) = Dom (R * S)$$

<proof>

lemma *ad-loc*:

$aDom (R * Dom S) = aDom (R * S)$
 ⟨proof⟩

lemma *d-ne-down*:
 $Dom (ne (R\downarrow)) = Dom (ne R)$
 ⟨proof⟩

lemma *ne-sp-iu-unit-up*:
 $ne R = R \implies (R * 1_{\cup\cup})\uparrow = R * U$
 ⟨proof⟩

lemma *ne-d-expl*:
 $ne R = R \implies Dom R = R * U \cap 1$
 ⟨proof⟩

lemma *ne-a-expl*:
 $ne R = R \implies aDom R = -(R * U) \cap 1$
 ⟨proof⟩

lemma *d-dist-oU*:
 $Dom (\bigcup X) = \bigcup (Dom \text{ ' } X)$
 ⟨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 $Dom (\bigcup\bigcup X|I) = \bigcap (Dom \text{ ' } X \text{ ' } I)$
 ⟨proof⟩

8.3 Left residual

definition *sp-lres* :: $('a, 'c) \text{ mrel} \Rightarrow ('b, 'c) \text{ mrel} \Rightarrow ('a, 'b) \text{ mrel}$ (**infixl** \circledast 65)

where

$Q \circledast R \equiv \{ (a, B) . \forall f . (\forall b \in B . (b, f b) \in R) \longrightarrow (a, \bigcup \{ f b \mid b . b \in B \}) \in Q \}$

declare *sp-lres-def* [*mr-simp*]

lemma *sp-lres-galois*:
 $S * R \subseteq Q \longleftrightarrow S \subseteq Q \circledast R$
 ⟨proof⟩

lemma *sp-lres-expl*:
 $Q \circledast R = \bigcup \{ S . S * R \subseteq Q \}$
 ⟨proof⟩

lemma *bot-sp-lres-d*:

$$\{\} \circ R = \{\} \circ \text{Dom } R$$

<proof>

lemma *bot-sp-lres-expl*:

$$\{\} \circ R = -(U * \text{Dom } R)$$

<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*:

$$R \downarrow * S = R * (1_{\cup\cup} \cup S)$$

<proof>

lemma *iu-unit-sp-lres-iu-unit-ou*:

$$U * a\text{Dom } (ne \ R) = 1_{\cup\cup} \circ (1_{\cup\cup} \cup R)$$

<proof>

lemma *bot-sl-below-complement-d*:

$$\{\} \circ R \subseteq - \text{Dom } R$$

<proof>

lemma *sp-unit-oi-bot-sp-lres*:

$$1 \cap - \text{Dom } R = 1 \cap (\{\} \circ R)$$

<proof>

lemma *ad-explicit-d*:

$$a\text{Dom } R = -(U * \text{Dom } R) \cap 1$$

<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 $aDom (ne (R \downarrow) * \wr p) = ((U * p) \circ R) \cap 1$
<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 $R * (p \cup q) \subseteq R * p \cup ne (R \downarrow) * q \uparrow$

$\langle proof \rangle$

lemma *split-sp-test-5:*

assumes *test p*

and *test q*

shows $R * (p \cup q) \subseteq R * p \cup R \downarrow * q \uparrow$

$\langle proof \rangle$

lemma *split-sp-test-6:*

assumes *test p*

and *test q*

shows $Dom (R * (p \cup q)) \subseteq Dom (R * p \cup ne (R \downarrow) * q)$

$\langle proof \rangle$

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* :: $('a, 'b) \text{ mrel} \Rightarrow ('b, 'b) \text{ mrel} \Rightarrow ('a, 'a) \text{ mrel} (| -) - [50,90] 95$

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* :: $('a, 'b) \text{ mrel} \Rightarrow ('b, 'b) \text{ mrel} \Rightarrow ('a, 'a) \text{ mrel} (| -] - [50,90] 95$

where

$$|R]p \equiv \{ (a, \{a\}) \mid a . \forall B . (a, B) \in R \longrightarrow (\forall b \in B . (b, \{b\}) \in p) \}$$

definition *edia* :: $('a, 'b) \text{ mrel} \Rightarrow ('b, 'b) \text{ mrel} \Rightarrow ('a, 'a) \text{ mrel} (| - \rangle) - [50,90] 95$

where

$$|R\rangle\rangle p \equiv \{ (a, \{a\}) \mid a . \exists B . (a, B) \in R \wedge (\exists b \in B . (b, \{b\}) \in p) \}$$

definition *ebox* :: $('a, 'b) \text{ mrel} \Rightarrow ('b, 'b) \text{ mrel} \Rightarrow ('a, 'a) \text{ mrel} (| -] - [50,90] 95$

where

$$|R]]p \equiv \{ (a, \{a\}) \mid a . \forall B . (a, B) \in R \longrightarrow (\exists b \in B . (b, \{b\}) \in p) \}$$

declare *adia-def* [*mr-simp*] *abox-def* [*mr-simp*] *edia-def* [*mr-simp*] *ebox-def* [*mr-simp*]

lemma *adia*:

assumes *test p*

shows $|R\rangle p = \text{Dom} (R * p)$

$\langle proof \rangle$

lemma *abox-1*:

assumes *test p*

shows $|R]p = a\text{Dom} (R \cap -(U * p))$

$\langle proof \rangle$

lemma *abox*:

assumes *test p*

shows $|R]p = a\text{Dom} (ne (R\downarrow) * \wr p)$

$\langle proof \rangle$

lemma *edia-1*:

assumes *test p*

shows $|R\rangle\rangle p = \text{Dom} (R \cap -(U * \wr p))$

$\langle proof \rangle$

lemma *edia*:

assumes *test p*

shows $|R\rangle p = \text{Dom} (ne (R\downarrow) * p)$
<proof>

lemma *ebox*:
assumes *test p*
shows $|R]]p = a\text{Dom} (R * \wr p)$
<proof>

lemma *abox-2*:
assumes *test p*
shows $|R]p = -((R \cap -(U * p)) * U) \cap 1$
<proof>

lemma *abox-3*:
assumes *test p*
shows $|R]p = -(ne (R\downarrow) * \wr p * U) \cap 1$
<proof>

lemma *abox-4*:
assumes *test p*
shows $|R]p = ((U * p) \otimes R) \cap 1$
<proof>

lemma *abox-ebox*:
assumes *test p*
shows $|R]p = |ne (R\downarrow)]p$
<proof>

lemma *abox-edia*:
assumes *test p*
shows $|R]p = \wr |R\rangle(\wr p)$
<proof>

lemma *abox-adia*:
assumes *test p*
shows $|R]p = \wr |ne (R\downarrow)\rangle(\wr p)$
<proof>

lemma *edia-adia*:
assumes *test p*
shows $|R\rangle p = |ne (R\downarrow)\rangle p$
<proof>

lemma *edia-abox*:
assumes *test p*
shows $|R\rangle p = \wr |R](\wr p)$
<proof>

lemma *edia-ebox*:

assumes *test p*
shows $|R\rangle p = \iota |ne (R\downarrow)\rangle\rangle(\iota p)$
 $\langle proof \rangle$

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 $|R\rangle\rangle p = |ne (R\downarrow)\rangle\rangle p$
 $\langle proof \rangle$

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 $|R]p = \iota |R]](\iota p)$
 $\langle proof \rangle$

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:*

$test\ p \implies R \subseteq S \implies |R\rangle p \subseteq |S\rangle p$
<proof>

lemma *adia-right-isotone:*

$test\ p \implies test\ q \implies p \subseteq q \implies |R\rangle p \subseteq |R\rangle q$
<proof>

lemma *abox-left-antitone:*

$test\ p \implies R \subseteq S \implies |S]p \subseteq |R]p$
<proof>

lemma *abox-right-isotone:*

$test\ p \implies test\ q \implies p \subseteq q \implies |R]p \subseteq |R]q$
<proof>

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:*

$test\ p \implies test\ q \implies p \subseteq q \implies |R\rangle\rangle p \subseteq |R\rangle\rangle q$
<proof>

lemma *ebox-left-antitone:*

$test\ p \implies R \subseteq S \implies |S]]p \subseteq |R]]p$
<proof>

lemma *ebox-right-isotone:*

$test\ p \implies test\ q \implies p \subseteq q \implies |R]]p \subseteq |R]]q$
<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 $|R\rangle\rangle p = |fis\ R\rangle\rangle p$

$\langle proof \rangle$

lemma *fission-below*:

$fis\ R \subseteq S \iff (\forall a\ b\ B . (a,B) \in R \wedge b \in B \implies (a,\{b\}) \in S)$

$\langle proof \rangle$

lemma *below-fission-up*:

$S \subseteq (fis\ R)\uparrow \iff (\forall a\ B . (a,B) \in S \implies (\exists C . (a,C) \in R \wedge C \cap B \neq \{\}))$

$\langle proof \rangle$

lemma *ebox-below-abox*:

assumes *test p*

and $fis\ R \subseteq S$

shows $|S|]p \subseteq |R]p$

$\langle proof \rangle$

lemma *abox-below-ebox*:

assumes *test p*

and $S \subseteq (fis\ R)\uparrow$

shows $|R]p \subseteq |S|]p$

$\langle proof \rangle$

lemma *abox-eq-ebox*:

assumes *test p*

and $fis\ R \subseteq S$

and $S \subseteq (fis\ R)\uparrow$

shows $|R]p = |S|]p$

$\langle proof \rangle$

lemma *abox-eq-ebox-sufficient*:

$S = fis\ R \vee S = ne\ (R\downarrow) \vee S = (ne\ (R\downarrow))\uparrow \implies fis\ R \subseteq S \wedge S \subseteq (fis\ R)\uparrow$

$\langle proof \rangle$

lemma *ebox-fission-abox*:

$test\ p \implies |R]p = |fis\ R|]p$

$\langle proof \rangle$

lemma *ebox-down-ne-up-abox*:

$test\ p \implies |R]p = |(ne\ (R\downarrow))\uparrow|]p$

$\langle proof \rangle$

lemma *same-fusion*:

assumes $fis\ R \sqsubseteq\downarrow S$

and $S \sqsubseteq\downarrow fus\ R$

shows $fis\ R = fis\ S$

$\langle proof \rangle$

lemma *same-abox*:

assumes $fis\ R \sqsubseteq\downarrow S$

and $S \sqsubseteq \downarrow \text{fus } R$
and $\text{test } p$
shows $|R]p = |S]p$
 $\langle \text{proof} \rangle$

lemma *abox-ebox-inner-deterministic*:
assumes $\text{test } p$
and *inner-deterministic* R
shows $|R]p = |R]]p$
 $\langle \text{proof} \rangle$

lemma *adia-edia-inner-deterministic*:
assumes $\text{test } p$
and *inner-deterministic* R
shows $|R\rangle p = |R\rangle\rangle p$
 $\langle \text{proof} \rangle$

lemma *abox-adia-deterministic*:
assumes $\text{test } p$
and *deterministic* R
shows $|R]p = |R\rangle p$
 $\langle \text{proof} \rangle$

lemma *ebox-edia-deterministic*:
assumes $\text{test } p$
and *deterministic* R
shows $|R]]p = |R\rangle\rangle p$
 $\langle \text{proof} \rangle$

lemma *abox-ebox-fusion*:
assumes $\text{test } p$
shows $|fis R]p = |fis R]]p$
 $\langle \text{proof} \rangle$

lemma *abox-fission-edia-fusion*:
assumes $\text{test } p$
shows $|fis R]p = |fus R\rangle p$
 $\langle \text{proof} \rangle$

lemma *abox-adia-fusion*:
assumes $\text{test } p$
shows $|fus R]p = |fus R\rangle p$
 $\langle \text{proof} \rangle$

8.5 Goldblatt's axioms without star

lemma *abox-sp-unit*:
 $|R]1 = 1$
 $\langle \text{proof} \rangle$

lemma *ou-unit-abox*:

$test\ p \implies |\{\}\rangle p = 1$
 $\langle proof \rangle$

lemma *ou-unit-test-implication*:

$test\ p \implies \{\} \rightarrow p = 1$
 $\langle proof \rangle$

lemma *sp-unit-abox*:

$test\ p \implies |1\rangle p = p$
 $\langle proof \rangle$

lemma *sp-unit-test-implication*:

$test\ p \implies 1 \rightarrow p = p$
 $\langle proof \rangle$

lemma *test-abox-ebox*:

$test\ p \implies test\ q \implies |q\rangle p = |q\rangle p$
 $\langle proof \rangle$

lemma *test-abox*:

$test\ p \implies test\ q \implies |q\rangle p = q \rightarrow p$
 $\langle proof \rangle$

lemma *abox-ou-adia-sp-unit*:

assumes $test\ p$
shows $|R\rangle p \cup |R\rangle 1 = 1$
 $\langle proof \rangle$

lemma *d-test-sp*:

$test\ p \implies Dom\ (p * R) = p * Dom\ R$
 $\langle proof \rangle$

lemma *ad-test-sp*:

$test\ p \implies aDom\ (p * R) = \imath\ p \cup aDom\ R$
 $\langle proof \rangle$

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*:

$test\ p \implies test\ q \implies |p * R\rangle q = \imath\ p \cup |R\rangle q$
 $\langle proof \rangle$

lemma *abox-test-sp*:

assumes $test\ p$
and $test\ q$

shows $|p * R]q = \wr p \cup |R]q$
<proof>

lemma *abox-test-sp-2*:
 $test\ p \implies test\ q \implies p \cup |R]q = |\wr p * R]q$
<proof>

lemma *abox-test-sp-3*:
 $test\ p \implies test\ q \implies p \rightarrow |R]q = |p * R]q$
<proof>

lemma *fission-sp-dist*:
 $fis\ (R * S) = fis\ (R * Dom\ S) * fis\ S$
<proof>

lemma *abox-test*:
 $test\ p \implies test\ (|R]p)$
<proof>

lemma *adia-test*:
 $test\ p \implies test\ (|R\rangle p)$
<proof>

lemma *ebox-test*:
 $test\ p \implies test\ (|R]]p)$
<proof>

lemma *edia-test*:
 $test\ p \implies test\ (|R\rangle\rangle p)$
<proof>

lemma *abox-sp*:
assumes $test\ p$
and $test\ q$
shows $|R](p * q) = |R]p * |R]q$
<proof>

lemma *adia-ou-below-ne-down*:
assumes $test\ p$
shows $|R](p \cup \wr q) \subseteq |R]p \cup |ne\ (R\downarrow)](\wr q)$
<proof>

lemma *abox-adia-mp*:
assumes $test\ p$
and $test\ q$
shows $|R](p \rightarrow q) * |R]p \subseteq |R]q$
<proof>

lemma *adia-abox-mp*:

assumes *test p*
and *test q*
shows $|R\rangle p * |R](p \rightarrow q) \subseteq |R\rangle q$
<proof>

lemma *abox-implication-adia:*
assumes *test p*
and *test q*
shows $|R](p \rightarrow q) \subseteq |R\rangle p \rightarrow |R\rangle q$
<proof>

lemma *abox-adia-implication:*
assumes *test p*
and *test q*
shows $|R]p \subseteq |R\rangle q \rightarrow |R\rangle(p * q)$
<proof>

lemma *abox-mp:*
assumes *test p*
and *test q*
shows $|R]p * |R](p \rightarrow q) \subseteq |R]q$
<proof>

lemma *abox-implication:*
assumes *test p*
and *test q*
shows $|R](p \rightarrow q) \subseteq |R]p \rightarrow |R]q$
<proof>

lemma *ebox-left-dist-ou:*
assumes *test p*
shows $|R \cup S]]p = |R]]p * |S]]p$
<proof>

lemma *abox-left-dist-ou:*
assumes *test p*
shows $|R \cup S]p = |R]p * |S]p$
<proof>

lemma *adia-left-dist-ou:*
assumes *test p*
shows $|R \cup S\rangle p = |R\rangle p \cup |S\rangle p$
<proof>

lemma *edia-left-dist-ou:*
assumes *test p*
shows $|R \cup S\rangle\rangle p = |R\rangle\rangle p \cup |S\rangle\rangle p$
<proof>

lemma *abox-dist-iu-1*:

assumes *test p*

shows $|R \cup S]p = |Dom R * ne (S\downarrow)]p * |Dom S * ne (R\downarrow)]p$
<proof>

lemma *abox-dist-iu-2*:

assumes *test p*

shows $|R \cup S]p = |Dom R * S]p * |Dom S * R]p$
<proof>

lemma *abox-dist-iu-3*:

assumes *test p*

shows $|R \cup S]p = (|R]1 \rightarrow |S]p) * (|S]1 \rightarrow |R]p)$
<proof>

lemma *abox-adia-sp-one-set*:

$|R]|S]1 = \{ (a, \{a\}) \mid a . \forall B . (a, B) \in R \longrightarrow (\forall b \in B . \exists D . (b, D) \in S) \}$
<proof>

lemma *abox-abox-set*:

$|R]|S]p = \{ (a, \{a\}) \mid a . \forall B . (a, B) \in R \longrightarrow (\forall C . (\exists b \in B . (b, C) \in S) \longrightarrow (\forall c \in C . (c, \{c\}) \in p)) \}$
<proof>

lemma *sp-abox-set*:

$|R * S]p = \{ (a, \{a\}) \mid a . \forall B . (a, B) \in R \longrightarrow (\forall C . (\exists f . (\forall b \in B . (b, f b) \in S) \wedge C = \bigcup \{ f b \mid b . b \in B \}) \longrightarrow (\forall c \in C . (c, \{c\}) \in p)) \}$
<proof>

lemma *abox-sp-1*:

assumes *test p*

shows $|R]|S]1 * |R * S]p \subseteq |R]|S]p$
<proof>

lemma *abox-sp-2*:

assumes *test p*

shows $|R]|S]p = |R\downarrow * S]p$
<proof>

lemma *abox-sp-3*:

assumes *test p*

shows $|R]|S]p \subseteq |R * S]p$
<proof>

lemma *abox-sp-4*:

assumes *test p*

shows $|R * S]p \subseteq |R]|S]1 \rightarrow |R]|S]p$
<proof>

lemma *abox-sp-5*:
assumes *test p*
shows $|R||S\rangle 1 * |R * S\rangle p = |R||S\rangle 1 * |R||S\rangle p$
 $\langle proof \rangle$

lemma *abox-sp-6*:
assumes *test p*
shows $|R||S\rangle 1 \rightarrow |R * S\rangle p = |R||S\rangle 1 \rightarrow |R||S\rangle p$
 $\langle proof \rangle$

lemma *abox-sp-7*:
assumes *test p*
and *total S*
shows $|R * S\rangle p = |R||S\rangle p$
 $\langle proof \rangle$

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

no-notation *rtrancl* $((-)^* [1000] 999)$

notation *star* $(-)^* [1000] 999)$

lemma *star-induct-1*:

assumes $1 \subseteq X$

and $R * X \subseteq X$

shows $R^* \subseteq X$

$\langle proof \rangle$

lemma *star-induct*:

assumes $S \subseteq 1 \cup 1_{\cup\cup}$

and $S \subseteq X$

and $R * X \subseteq X$

shows $R^* * S \subseteq X$

$\langle proof \rangle$

lemma *star-total*:

total (R^*)

$\langle proof \rangle$

lemma *star-down*:

$$R^* \downarrow = (R \downarrow)^* \cup 1_{\cup\cup}$$

$\langle proof \rangle$

lemma *ne-star-down*:

$$ne (R^* \downarrow) = ne ((R \downarrow)^*)$$

$\langle proof \rangle$

lemma *ne-down-star*:

$$ne ((R \downarrow)^*) = (ne (R \downarrow))^*$$

$\langle proof \rangle$

lemma *abox-star-unfold*:

$$test p \implies |R^*]p = p * |R]|R^*]p$$

$\langle proof \rangle$

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 $|R\rangle p \subseteq p \longleftrightarrow |R^*\rangle p \subseteq p$
 ⟨*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 $(s-id \cup p-id) * R = R \cup p-id$
 $\langle proof \rangle$

9 Counterexamples

locale *counterexamples*
begin

lemma *counter-01*:
 $\neg ((U::('a,'b) mrel) * \neg((U::('b,'c) mrel) * (R::('c,'d) mrel))) \subseteq \neg(U * R)$
 $\langle proof \rangle$

abbreviation $a-1 \equiv finite-1.a_1$

lemma *counter-02*:
 $\exists R::(Enum.finite-1, Enum.finite-1) mrel . \exists p . \neg (test\ p \longrightarrow (R \cap \neg(U * p))) * U = R * \neg(p * U)$
 $\langle proof \rangle$

lemma *counter-03*:
 $\exists R::(Enum.finite-1, Enum.finite-1) mrel . \exists p . \neg (test\ p \longrightarrow (R \cap \neg(U * p))) * 1_{\cup\cup} = R * (\neg(p * U) \cap 1_{\cup\cup})$
 $\langle proof \rangle$

abbreviation $b-1 \equiv finite-2.a_1$
abbreviation $b-2 \equiv finite-2.a_2$
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*:
 $\exists R::(Enum.finite-2, Enum.finite-2) mrel . \exists p\ q . \neg (test\ p \longrightarrow test\ q \longrightarrow |R * p]q = |R][p]q)$
 $\langle proof \rangle$

lemma *counter-05*:
 $\neg (\exists f . \forall R\ p . test\ p \longrightarrow |R]p = |f\ R]p)$
 $\langle proof \rangle$

lemma *counter-06*:
 $\neg (\exists f . \forall R\ p . test\ p \longrightarrow |R][p] = |f\ R][p])$
 $\langle proof \rangle$

lemma *counter-07*:

$\neg (\exists f . \text{mono } f \wedge (\forall R . \text{fus } R = \text{lfp } (\lambda X . f R X)))$
 ⟨proof⟩

abbreviation $c-1 \equiv \text{finite-3}.a_1$

abbreviation $c-2 \equiv \text{finite-3}.a_2$

abbreviation $c-3 \equiv \text{finite-3}.a_3$

lemma *counter-08*:

$\neg (\sim(1::(\text{Enum}.finite-3, \text{Enum}.finite-3) \text{ mrel}) * \sim 1 \in \{1, \sim 1\})$
 ⟨proof⟩

lemma *counter-09*:

$\neg (\sim(1::(\text{Enum}.finite-3, \text{Enum}.finite-3) \text{ mrel}) \odot 1 \in \{1, \sim 1\})$
 ⟨proof⟩

lemma *ex-2-cases*:

$\exists b. b = b-1 \vee b = b-2$
 ⟨proof⟩

lemma *all-2-cases*:

$(\forall b. b = b-2 \wedge b = b-1) = \text{False}$
 ⟨proof⟩

lemma *impl-2-cases*:

$\bigcup \{ X . \exists b. (b = b-1 \longrightarrow X = Y) \wedge (b = b-2 \longrightarrow X = Z) \} = Y \cup Z$
 ⟨proof⟩

lemma *ex-2-set-cases*:

$(\exists B::\text{Enum}.finite-2 \text{ set} . P B) \longleftrightarrow P \{ \} \vee P \{ b-1 \} \vee P \{ b-2 \} \vee P \{ b-1, b-2 \}$
 ⟨proof⟩

abbreviation $B-0 \equiv \{ \}::\text{Enum}.finite-2 \text{ set}$

abbreviation $B-1 \equiv \{ b-1 \}$

abbreviation $B-2 \equiv \{ b-2 \}$

abbreviation $B-3 \equiv \{ b-1, b-2 \}$

abbreviation $\text{mkf } x \ y \equiv \lambda z . \text{if } z = b-1 \text{ then } x \text{ else } y$

lemma *mkf*:

$f = \text{mkf } (f \ b-1) \ (f \ b-2)$
 ⟨proof⟩

lemma *mkf2*:

$f \ b-1 = X \wedge f \ b-2 = Y \implies f = \text{mkf } X \ Y$
 ⟨proof⟩

lemma *ex-2-mrel-cases*:

$(\exists f::\text{Enum}.finite-2 \implies \text{Enum}.finite-2 \text{ set} . P f) \longleftrightarrow$
 $P (\text{mkf } B-0 \ B-0) \vee P (\text{mkf } B-0 \ B-1) \vee P (\text{mkf } B-0 \ B-2) \vee P (\text{mkf } B-0 \ B-3) \vee$
 $P (\text{mkf } B-1 \ B-0) \vee P (\text{mkf } B-1 \ B-1) \vee P (\text{mkf } B-1 \ B-2) \vee P (\text{mkf } B-1 \ B-3) \vee$

$P (mkf\ B-2\ B-0) \vee P (mkf\ B-2\ B-1) \vee P (mkf\ B-2\ B-2) \vee P (mkf\ B-2\ B-3) \vee$
 $P (mkf\ B-3\ B-0) \vee P (mkf\ B-3\ B-1) \vee P (mkf\ B-3\ B-2) \vee P (mkf\ B-3\ B-3)$
 ⟨proof⟩

lemma counter-10:

$\exists R::(Enum.\text{finite-2}, Enum.\text{finite-2})\ mrel . \neg (U::(Enum.\text{finite-2}, Enum.\text{finite-2})$
 $mrel) * (U * R) \subseteq U * R$
 ⟨proof⟩

lemma counter-11:

$\exists (R::(Enum.\text{finite-2}, Enum.\text{finite-2})\ mrel) (s::(Enum.\text{finite-2}, Enum.\text{finite-2})$
 $mrel) (t::(Enum.\text{finite-2}, Enum.\text{finite-2})\ mrel) . \neg (inner\text{-univalent}\ s \wedge$
 $inner\text{-univalent}\ t \longrightarrow R * (s * t) = (R * s) * t)$
 ⟨proof⟩

lemma counter-12:

$\neg(\exists S . 1_{\cup\cup} \odot S = 1_{\cup\cup})$
 ⟨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.