

# Allen's Interval Calculus

Fadoua Ghourabi  
Ochanomizu University, Japan  
fadouaghourabi@gmail.com

May 26, 2024

## Contents

<b>1</b>	<b>Axioms</b>	<b>2</b>
<b>2</b>	<b>Time interval relations</b>	<b>3</b>
<b>3</b>	<b>Basic relations</b>	<b>4</b>
3.1	e-composition . . . . .	4
3.2	r-composition . . . . .	6
3.3	$\alpha$ -composition . . . . .	11
3.4	$\beta$ -composition . . . . .	27
3.5	$\gamma$ -composition . . . . .	39
3.6	$\gamma$ -composition . . . . .	45
3.7	The rest of the composition table . . . . .	51
3.8	Composition rules . . . . .	55
<b>4</b>	<b>PD property</b>	<b>59</b>
4.1	Intersection rules . . . . .	65
<b>5</b>	<b>JE property</b>	<b>66</b>
<b>6</b>	<b>Examples</b>	<b>69</b>
6.1	Compositions of non-basic relations . . . . .	69
6.2	Intersection of non-basic relations . . . . .	73
<b>7</b>	<b>Nests</b>	<b>74</b>
7.1	Definitions . . . . .	74
7.2	Properties of Nests . . . . .	74
7.3	Ordering of nests . . . . .	89

**theory** *xor-cal*

**imports**

*Main*

**begin**

**definition** *xor*::*bool*  $\Rightarrow$  *bool*  $\Rightarrow$  *bool* (**infixl**  $\oplus$  60)

**where** *xor* *A B*  $\equiv$  (*A*  $\wedge$   $\neg$ *B*)  $\vee$  ( $\neg$ *A*  $\wedge$  *B*)

**declare** *xor-def* [*simp*]

**interpretation** *bool*:*semigroup* ( $\oplus$ )

**proof**

{ **fix** *a b c* **show** *a*  $\oplus$  *b*  $\oplus$  *c* = *a*  $\oplus$  (*b*  $\oplus$  *c*) **by** *auto*}

**qed**

**lemma** *xor-distr-L* [*simp*]:*A*  $\oplus$  (*B*  $\oplus$  *C*) = (*A*  $\wedge$   $\neg$ *B*  $\wedge$   $\neg$ *C*)  $\vee$  (*A*  $\wedge$  *B*  $\wedge$  *C*)  $\vee$  ( $\neg$ *A*  $\wedge$  *B*  $\wedge$   $\neg$ *C*)  $\vee$  ( $\neg$ *A*  $\wedge$   $\neg$ *B*  $\wedge$  *C*)  
**by** *auto*

**lemma** *xor-distr-R* [*simp*]:(*A*  $\oplus$  *B*)  $\oplus$  *C* = *A*  $\oplus$  (*B*  $\oplus$  *C*)  
**by** *auto*

**end**

**theory** *axioms*

**imports**

*Main xor-cal*

**begin**

## 1 Axioms

We formalize Allen's definition of theory of time in term of intervals (Allen, 1983). Two relations, namely meets and equality, are defined between intervals. Two interval meets if they are adjacent A set of 5 axioms ((M1)  $\sim$  (M5)) are then defined based on relation meets.

We define a class interval whose assumptions are (i) properties of relations meets and, (ii) axioms (M1)  $\sim$  (M5).

**class** *interval* =

**fixes**

*meets*::'*a*  $\Rightarrow$  '*a*  $\Rightarrow$  *bool* (**infixl**  $\parallel$  60) **and**

*I*::'*a*  $\Rightarrow$  *bool*

**assumes**

*meets-atrans*::[(*p* $\parallel$ *q*);(*q* $\parallel$ *r*)]  $\implies$   $\neg$ (*p* $\parallel$ *r*) **and**

*meets-irrefl*:  $\mathcal{I} p \implies \neg(p\|p)$  **and**  
*meets-asy*:  $(p\|q) \implies \neg(q\|p)$  **and**  
*meets-wd*:  $p\|q \implies \mathcal{I} p \wedge \mathcal{I} q$  **and**

*M1*:  $[(p\|q); (p\|s); (r\|q)] \implies (r\|s)$  **and**  
*M2*:  $[(p\|q); (r\|s)] \implies p\|s \oplus ((\exists t. (p\|t) \wedge (t\|s)) \oplus (\exists t. (r\|t) \wedge (t\|q)))$  **and**  
*M3*:  $\mathcal{I} p \implies (\exists q r. q\|p \wedge p\|r)$  **and**  
*M4*:  $[p\|q; q\|s; p\|r; r\|s] \implies q = r$  **and**  
*M5*:  $exist: p\|q \implies (\exists r s t. r\|p \wedge p\|q \wedge q\|s \wedge r\|t \wedge t\|s)$

**lemma** (*in interval*) *trans2*:  $[p\|t; t\|r; r\|q] \implies \neg p\|q$   
**using** *M1* *meets-asy* **by** *blast*

**lemma** (*in interval*) *nontrans1*:  $u\|r \implies \neg (\exists t. u\|t \wedge t\|r)$   
**using** *meets-atrans* **by** *blast*

**lemma** (*in interval*) *nontrans2*:  $u\|r \implies \neg (\exists t. r\|t \wedge t\|u)$   
**using** *M1* *M5* *exist* *trans2* **by** *blast*

**lemma** (*in interval*) *nonmeets1*:  $\neg (u\|r \wedge r\|u)$   
**using** *meets-asy* **by** *blast*

**lemma** (*in interval*) *nonmeets2*:  $[\mathcal{I} u; \mathcal{I} r] \implies \neg (u\|r \wedge u = r)$   
**using** *meets-irrefl* **by** *blast*

**lemma** (*in interval*) *nonmeets3*:  $\neg (u\|r \wedge (\exists p. u\|p \wedge p\|r))$   
**using** *nontrans1* **by** *blast*

**lemma** (*in interval*) *nonmeets4*:  $\neg (u\|r \wedge (\exists p. r\|p \wedge p\|u))$   
**using** *nontrans2* **by** *blast*

**lemma** (*in interval*) *elimmeets*:  $(p\|s \wedge (\exists t. p\|t \wedge t\|s) \wedge (\exists t. r\|t \wedge t\|q))$   
 $= \text{False}$   
**using** *meets-atrans* **by** *blast*

**lemma** (*in interval*) *M5* *exist* *var*:

**assumes**  $x\|y \ y\|z \ z\|w$

**shows**  $\exists t. x\|t \wedge t\|w$

**proof** –

**from** *assms*(1,3) **have**  $a:x\|w \oplus (\exists t. x\|t \wedge t\|w) \oplus (\exists t. z\|t \wedge t\|y)$  **using** *M2* [*of*  
 $x \ y \ z \ w$ ] **by** *auto*

**from** *assms* **have**  $b1:\neg x\|w$  **using** *trans2* **by** *blast*

**from** *assms*(2) **have**  $\neg (\exists t. z\|t \wedge t\|y)$  **by** (*simp* *add*: *nontrans2*)

**with** *b1* *a* **have**  $(\exists t. x\|t \wedge t\|w)$  **by** *simp*

**thus** *?thesis* **by** *simp*

**qed**

**lemma** (*in interval*) *M5* *exist* *var2*:

**assumes**  $p \parallel q$   
**shows**  $\exists r1\ r2\ r3\ s\ t. r1 \parallel r2 \wedge r2 \parallel r3 \wedge r3 \parallel p \wedge p \parallel q \wedge q \parallel s \wedge r1 \parallel t \wedge t \parallel s$   
**proof** –  
**from** *assms* **obtain**  $r3\ k1\ s$  **where**  $r3p:r3 \parallel p$  **and**  $qs:q \parallel s$  **and**  $r3k1:r3 \parallel k1$   
**and**  $k1s:k1 \parallel s$  **using** *M5exist* **by** *blast*  
**from**  $r3p$  **obtain**  $r2$  **where**  $r2r3:r2 \parallel r3$  **using** *M3[of r3]* *meets-wd* **by** *auto*  
**from**  $r2r3$  **obtain**  $r1$  **where**  $r1r2:r1 \parallel r2$  **using** *M3[of r2]* *meets-wd* **by** *auto*  
**with** *assms*  $r2r3\ r3p\ qs$  **obtain**  $t$  **where**  $r1t1:r1 \parallel t$  **and**  $t1q:t \parallel s$  **using** *M5exist-var* **by** *blast*  
**with** *assms*  $r1r2\ r2r3\ r3p\ qs$  **show** *?thesis* **by** *blast*  
**qed**

**lemma** (in *interval*) *M5exist-var3*:  
**assumes**  $k \parallel l$  **and**  $l \parallel q$  **and**  $q \parallel t$  **and**  $t \parallel r$   
**shows**  $\exists lqt. k \parallel lqt \wedge lqt \parallel r$   
**proof** –  
**from** *assms(1-3)* **obtain**  $lq$  **where**  $k \parallel lq$  **and**  $lq \parallel t$   
**using** *M5exist-var* **by** *blast*  
**with** *assms(4)* **obtain**  $lqt$  **where**  $k \parallel lqt$  **and**  $lqt \parallel r$   
**using** *M5exist-var* **by** *blast*  
**thus** *?thesis* **by** *auto*  
**qed**

end

## 2 Time interval relations

**theory** *allen*

**imports**

*Main axioms*  
*HOL-Eisbach.Eisbach-Tools*

**begin**

## 3 Basic relations

We define 7 binary relations between time intervals. Relations e, m, b, ov, d, s and f stand for equal, meets, before, overlaps, during, starts and finishes, respectively.

**class** *arelations* = *interval* +  
**fixes**  
 $e::('a \times 'a)$  *set* **and**  
 $m::('a \times 'a)$  *set* **and**

$b::('a \times 'a)$  set and  
 $ov::('a \times 'a)$  set and  
 $d::('a \times 'a)$  set and  
 $s::('a \times 'a)$  set and  
 $f::('a \times 'a)$  set  
**assumes**  
 $e:(p,q) \in e = (p = q)$  and  
 $m:(p,q) \in m = p \parallel q$  and  
 $b:(p,q) \in b = (\exists t::'a. p \parallel t \wedge t \parallel q)$  and  
 $ov:(p,q) \in ov = (\exists k \ l \ u \ v t::'a. (k \parallel p \wedge p \parallel u \wedge u \parallel v) \wedge (k \parallel l \wedge l \parallel q \wedge q \parallel v) \wedge (l \parallel t \wedge t \parallel u))$  and  
 $s:(p,q) \in s = (\exists k \ u \ v::'a. k \parallel p \wedge p \parallel u \wedge u \parallel v \wedge k \parallel q \wedge q \parallel v)$  and  
 $f:(p,q) \in f = (\exists k \ l \ u::'a. k \parallel l \wedge l \parallel p \wedge p \parallel u \wedge k \parallel q \wedge q \parallel u)$  and  
 $d:(p,q) \in d = (\exists k \ l \ u \ v::'a. k \parallel l \wedge l \parallel p \wedge p \parallel u \wedge u \parallel v \wedge k \parallel q \wedge q \parallel v)$

### 3.1 e-composition

Relation  $e$  is the identity relation for composition.

**lemma** *cer*:

**assumes**  $r \in \{e, m, b, ov, s, f, d, m^{-1}, b^{-1}, ov^{-1}, s^{-1}, f^{-1}, d^{-1}\}$

**shows**  $e \circ r = r$

**proof** –

**{ fix**  $x \ y$  **assume**  $a:(x,y) \in e \circ r$   
**then obtain**  $z$  **where**  $(x,z) \in e$  **and**  $(z,y) \in r$  **by** *auto*  
**from**  $\langle (x,z) \in e \rangle$  **have**  $x = z$  **using**  $e$  **by** *auto*  
**with**  $\langle (z,y) \in r \rangle$  **have**  $(x,y) \in r$  **by** *simp* **} note**  $c1 = \text{this}$

**{ fix**  $x \ y$  **assume**  $a:(x,y) \in r$   
**have**  $(x,x) \in e$  **using**  $e$  **by** *auto*  
**with**  $a$  **have**  $(x,y) \in e \circ r$  **by** *blast* **} note**  $c2 = \text{this}$

**from**  $c1 \ c2$  **show** *?thesis* **by** *auto*  
**qed**

**lemma** *cre*:

**assumes**  $r \in \{e, m, b, ov, s, f, d, m^{-1}, b^{-1}, ov^{-1}, s^{-1}, f^{-1}, d^{-1}\}$

**shows**  $r \circ e = r$

**proof** –

**{ fix**  $x \ y$  **assume**  $a:(x,y) \in r \circ e$   
**then obtain**  $z$  **where**  $(x,z) \in r$  **and**  $(z,y) \in e$  **by** *auto*  
**from**  $\langle (z,y) \in e \rangle$  **have**  $z = y$  **using**  $e$  **by** *auto*  
**with**  $\langle (x,z) \in r \rangle$  **have**  $(x,y) \in r$  **by** *simp* **} note**  $c1 = \text{this}$

**{ fix**  $x \ y$  **assume**  $a:(x,y) \in r$   
**have**  $(y,y) \in e$  **using**  $e$  **by** *auto*  
**with**  $a$  **have**  $(x,y) \in r \circ e$  **by** *blast* **} note**  $c2 = \text{this}$

**from**  $c1 \ c2$  **show** *?thesis* **by** *auto*  
**qed**

**lemmas**  $ceb = cer[of\ b]$   
**lemmas**  $cebi = cer[of\ b^{\wedge}-1]$   
**lemmas**  $cem = cer[of\ m]$   
**lemmas**  $cemi = cer[of\ m^{\wedge}-1]$   
**lemmas**  $cee = cer[of\ e]$   
**lemmas**  $ces = cer[of\ s]$   
**lemmas**  $cesi = cer[of\ s^{\wedge}-1]$   
**lemmas**  $cef = cer[of\ f]$   
**lemmas**  $cefi = cer[of\ f^{\wedge}-1]$   
**lemmas**  $ceov = cer[of\ ov]$   
**lemmas**  $ceovi = cer[of\ ov^{\wedge}-1]$   
**lemmas**  $ced = cer[of\ d]$   
**lemmas**  $cedi = cer[of\ d^{\wedge}-1]$   
**lemmas**  $cbe = cre[of\ b]$   
**lemmas**  $cbie = cre[of\ b^{\wedge}-1]$   
**lemmas**  $cme = cre[of\ m]$   
**lemmas**  $cmie = cre[of\ m^{\wedge}-1]$   
**lemmas**  $cse = cre[of\ s]$   
**lemmas**  $csie = cre[of\ s^{\wedge}-1]$   
**lemmas**  $cfe = cre[of\ f]$   
**lemmas**  $cfie = cre[of\ f^{\wedge}-1]$   
**lemmas**  $cove = cre[of\ ov]$   
**lemmas**  $covie = cre[of\ ov^{\wedge}-1]$   
**lemmas**  $cde = cre[of\ d]$   
**lemmas**  $cdie = cre[of\ d^{\wedge}-1]$

### 3.2 r-composition

We prove compositions of the form  $r_1 \circ r_2 \subseteq r$ , where  $r$  is a basic relation.

**method** (in *arelations*) *r-compose* **uses**  $r1\ r2\ r3 = ((auto, (subst\ (asm)\ r1\ ), (subst\ (asm)\ r2), (subst\ r3)) , (meson\ M5exist-var))$

**lemma** (in *arelations*)  $cbb:b\ O\ b \subseteq b$   
**by** (*r-compose*  $r1:b\ r2:b\ r3:b$ )

**lemma** (in *arelations*)  $cbm:b\ O\ m \subseteq b$   
**by** (*r-compose*  $r1:b\ r2:m\ r3:b$ )

**lemma**  $cbov:b\ O\ ov \subseteq b$   
**apply** (*auto simp:b ov*)  
**using** *M1 M5exist-var* **by** *blast*

**lemma**  $cbfi:b\ O\ f^{\wedge}-1 \subseteq b$   
**apply** (*auto simp:b f*)  
**by** (*meson M1 M5exist-var*)

**lemma**  $cbdi:b\ O\ d^{\wedge}-1 \subseteq b$

**apply** (*auto simp: b d*)  
**by** (*meson M1 M5exist-var*)

**lemma** *cbs:b O s ⊆ b*  
**apply** (*auto simp: b s*)  
**by** (*meson M1 M5exist-var*)

**lemma** *cbsi:b O s<sup>^-1</sup> ⊆ b*  
**apply** (*auto simp: b s*)  
**by** (*meson M1 M5exist-var*)

**lemma** (*in arelations*) *cmb:m O b ⊆ b*  
**by** (*r-compose r1:m r2:b r3:b*)

**lemma** *cmm:m O m ⊆ b*  
**by** (*auto simp: b m*)

**lemma** *cmov:m O ov ⊆ b*  
**apply** (*auto simp:b m ov*)  
**using** *M1 M5exist-var* **by** *blast*

**lemma** *cmfi:m O f<sup>^-1</sup> ⊆ b*  
**apply** (*r-compose r1:m r2:f r3:b*)  
**by** (*meson M1*)

**lemma** *cmdi:m O d<sup>^-1</sup> ⊆ b*  
**apply** (*auto simp add:m d b*)  
**using** *M1* **by** *blast*

**lemma** *cms:m O s ⊆ m*  
**apply** (*auto simp add:m s*)  
**using** *M1* **by** *auto*

**lemma** *cmsi:m O s<sup>^-1</sup> ⊆ m*  
**apply** (*auto simp add:m s*)  
**using** *M1* **by** *blast*

**lemma** *covb:ov O b ⊆ b*  
**apply** (*auto simp:ov b*)  
**using** *M1 M5exist-var* **by** *blast*

**lemma** *covm:ov O m ⊆ b*  
**apply** (*auto simp:ov m b*)  
**using** *M1* **by** *blast*

**lemma** *covs:ov O s ⊆ ov*  
**proof**  
**fix** *p::'a×'a* **assume** *p ∈ ov O s* **then obtain** *x y z* **where** *p:p = (x,z)* **and**  
*xyov:(x,y) ∈ ov* **and** *yzs:(y,z) ∈ s* **by** *auto*

**from**  $xyov$  **obtain**  $r\ u\ v\ t\ k$  **where**  $rx:r\|x$  **and**  $xu:x\|u$  **and**  $uv:u\|v$  **and**  $rt:r\|t$   
**and**  $tk:t\|k$  **and**  $ty:t\|y$  **and**  $yv:y\|v$  **and**  $ku:k\|u$  **using**  $ov$  **by**  $blast$   
**from**  $yzs$  **obtain**  $l1\ l2$  **where**  $yl1:y\|l1$  **and**  $l1l2:l1\|l2$  **and**  $zl2:z\|l2$  **using**  $s$  **by**  
 $blast$   
**from**  $uv\ yl1\ yv$  **have**  $u\|l1$  **using**  $M1$  **by**  $blast$   
**with**  $xu\ l1l2$  **obtain**  $ul1$  **where**  $xul1:x\|ul1$  **and**  $ul1l2:ul1\|l2$  **using**  $M5exist-var$   
**by**  $blast$   
**from**  $ku\ xu\ xul1\ l1l2$  **have**  $kul1:k\|ul1$  **using**  $M1$  **by**  $blast$   
**from**  $ty\ yzs$  **have**  $t\|z$  **using**  $s\ M1$  **by**  $blast$   
**with**  $rx\ rt\ xul1\ ul1l2\ zl2\ tk\ kul1$  **have**  $(x,z) \in ov$  **using**  $ov$  **by**  $blast$   
**with**  $p$  **show**  $p \in ov$  **by**  $simp$   
**qed**

**lemma**  $cfib:f^{-1}\ O\ b \subseteq b$   
**apply**  $(auto\ simp:f\ b)$   
**using**  $M1$  **by**  $blast$

**lemma**  $cfim:f^{-1}\ O\ m \subseteq m$   
**apply**  $(auto\ simp:f\ m)$   
**using**  $M1$  **by**  $auto$

**lemma**  $cfiov:f^{-1}\ O\ ov \subseteq ov$   
**proof**

**fix**  $p::'a \times 'a$  **assume**  $p \in f^{-1}\ O\ ov$  **then obtain**  $x\ y\ z$  **where**  $p:p = (x,z)$   
**and**  $xyfi:(x,y) \in f^{-1}$  **and**  $yzov:(y,z) \in ov$  **by**  $auto$   
**from**  $xyfi\ yzov$  **obtain**  $t'\ r\ u$  **where**  $tpr:t'\|r$  **and**  $ry:r\|y$  **and**  $yu:y\|u$  **and**  
 $tpx:t'\|x$  **and**  $xu:x\|u$  **using**  $f$  **by**  $blast$   
**from**  $yzov\ ry$  **obtain**  $v\ k\ t\ u'$  **where**  $yup:y\|u'$  **and**  $upv:u'\|v$  **and**  $rk:r\|k$  **and**  
 $kz:k\|z$  **and**  $zv:z\|v$  **and**  $kt:k\|t$  **and**  $tup:t\|u'$   
**using**  $ov$  **using**  $M1$  **by**  $blast$   
**from**  $yu\ xu\ yup$  **have**  $xup:x\|u'$  **using**  $M1$  **by**  $blast$   
**from**  $tpr\ rk\ kt$  **obtain**  $r'$  **where**  $tprp:t'\|r'$  **and**  $rpt:r'\|t$  **using**  $M5exist-var$  **by**  
 $blast$   
**from**  $kt\ rpt\ kz$  **have**  $rpz:r'\|z$  **using**  $M1$  **by**  $blast$   
**from**  $tprp\ rpz\ rpt\ tpx\ xup\ zv\ upv\ tup$  **have**  $(x,z) \in ov$  **using**  $ov$  **by**  $blast$   
**with**  $p$  **show**  $p \in ov$  **by**  $simp$   
**qed**

**lemma**  $cfifi:f^{-1}\ O\ f^{-1} \subseteq f^{-1}$   
**proof**

**fix**  $x::'a \times 'a$  **assume**  $x \in f^{-1}\ O\ f^{-1}$  **then obtain**  $p\ q\ z$  **where**  $x:x = (p, q)$   
**and**  $(p,z) \in f^{-1}$  **and**  $(z,q) \in f^{-1}$  **by**  $auto$   
**from**  $\langle(p,z) \in f^{-1}\rangle$  **obtain**  $k\ l\ u$  **where**  $kp:k\|p$  **and**  $kl:k\|l$  **and**  $lz:l\|z$  **and**  
 $pu:p\|u$  **and**  $zu:z\|u$  **using**  $f$  **by**  $blast$   
**from**  $\langle(z,q) \in f^{-1}\rangle$  **obtain**  $k'\ u'\ l'$  **where**  $kpz:k'\|z$  **and**  $kplp:k'\|l'$  **and**  $lpq:l'\|q$   
**and**  $gup:q\|u'$  **and**  $zup:z\|u'$  **using**  $f$  **by**  $blast$   
**from**  $zu\ zup\ pu$  **have**  $p\|u'$  **using**  $M1$  **by**  $blast$   
**from**  $lz\ kpz\ kplp$  **have**  $l\|l'$  **using**  $M1$  **by**  $blast$   
**with**  $kl\ lpq$  **obtain**  $ll$  **where**  $k\|ll$  **and**  $ll\|q$  **using**  $M5exist-var$  **by**  $blast$



with  $kp \langle p \parallel u' \rangle$   $qup$  show  $x \in f^{-1}$  using  $x f$  by *blast*  
qed

lemma *cfidi*:  $f^{-1} O d^{-1} \subseteq d^{-1}$

proof

fix  $x::'a \times 'a$  assume  $x : f^{-1} O d^{-1}$  then obtain  $p q z$  where  $x:x = (p,q)$   
and  $(p,z) \in f^{-1}$  and  $(z,q) \in d^{-1}$  by *auto*

then obtain  $k l u$  where  $kp:k \parallel p$  and  $kl:k \parallel l$  and  $lz:l \parallel z$  and  $pu:p \parallel u$  and  $zu:z \parallel u$  using  $f$  by *blast*

obtain  $k' l' u' v'$  where  $kpz:k' \parallel z$  and  $kplp:k' \parallel l'$  and  $lpq:l' \parallel q$  and  $qup:q \parallel u'$   
and  $upvp:u' \parallel v'$  and  $zvp:z \parallel v'$  using  $d \langle (z,q) \in d^{-1} \rangle$  by *blast*

from  $lz kpz kplp$  have  $l \parallel l'$  using  $M1$  by *blast*

with  $kl lpq$  obtain  $ll$  where  $k \parallel ll$  and  $ll \parallel q$  using  $M5exist-var$  by *blast*

moreover from  $zu zvp upvp$  have  $u' \parallel u$  using  $M1$  by *blast*

ultimately show  $x \in d^{-1}$  using  $x kp pu qup d$  by *blast*

qed

lemma *cfis*:  $f^{-1} O s \subseteq ov$

proof

fix  $x::'a \times 'a$  assume  $x \in f^{-1} O s$  then obtain  $p q z$  where  $x:x = (p,q)$  and  $(p,z) \in f^{-1}$  and  $(z,q) \in s$  by *auto*

from  $\langle (p,z) \in f^{-1} \rangle$  obtain  $k l u$  where  $kp:k \parallel p$  and  $kl:k \parallel l$  and  $lz:l \parallel z$  and  $pu:p \parallel u$  and  $zu:z \parallel u$  using  $f$  by *blast*

from  $\langle (z,q) \in s \rangle$  obtain  $k' u' v'$  where  $kpz:k' \parallel z$  and  $kpq:k' \parallel q$  and  $zup:z \parallel u'$   
and  $upvp:u' \parallel v'$  and  $qvp:q \parallel v'$  using  $s M1$  by *blast*

from  $pu zu zup$  have  $pup:p \parallel u'$  using  $M1$  by *blast*

moreover from  $lz kpz kpq$  have  $lq:l \parallel q$  using  $M1$  by *blast*

ultimately show  $x \in ov$  using  $x lz zup kp kl upvp upvp ov qvp$  by *blast*

qed

lemma *cfisi*:  $f^{-1} O s^{-1} \subseteq d^{-1}$

proof

fix  $x::'a \times 'a$  assume  $x \in f^{-1} O s^{-1}$  then obtain  $p q z$  where  $x:x = (p,q)$   
and  $(p,z) \in f^{-1}$  and  $(z,q) \in s^{-1}$  by *auto*

then obtain  $k l u$  where  $kp:k \parallel p$  and  $kl:k \parallel l$  and  $lz:l \parallel z$  and  $pu:p \parallel u$  and  $zu:z \parallel u$  using  $f$  by *blast*

obtain  $k' u' v'$  where  $kpz:k' \parallel z$  and  $kpq:k' \parallel q$  and  $qup:q \parallel u'$  and  $upvp:u' \parallel v'$   
and  $zvp:z \parallel v'$  using  $s \langle (z,q) : s^{-1} \rangle$  by *blast*

from  $zu zvp upvp$  have  $u' \parallel u$  using  $M1$  by *blast*

moreover from  $lz kpz kpq$  have  $l \parallel q$  using  $M1$  by *blast*

ultimately show  $x \in d^{-1}$  using  $x d kl kp qup pu$  by *blast*

qed

lemma *cdifi*:  $d^{-1} O f^{-1} \subseteq d^{-1}$

proof

fix  $x::'a \times 'a$  assume  $x : d^{-1} O f^{-1}$  then obtain  $p q z$  where  $x:x = (p,q)$   
and  $(p,z) \in d^{-1}$  and  $(z,q) \in f^{-1}$  by *auto*

then obtain  $k l u v$  where  $kp:k \parallel p$  and  $kl:k \parallel l$  and  $lz:l \parallel z$  and  $zu:z \parallel u$  and  $uv:u \parallel v$  and  $pv:p \parallel v$  using  $d$  by *blast*

**obtain**  $k' l' u'$  **where**  $kpz:k' \parallel z$  **and**  $kplp:k' \parallel l'$  **and**  $lpq:l' \parallel q$  **and**  $qup:q \parallel u'$   
**and**  $zup:z \parallel u'$  **using**  $f \langle (z,q): \widehat{f^{-1}} \rangle$  **by** *blast*  
**from**  $lz\ kpz\ kplp$  **have**  $l \parallel l'$  **using** *M1* **by** *blast*  
**with**  $kl\ lpq$  **obtain**  $ll$  **where**  $k \parallel ll$  **and**  $ll \parallel q$  **using** *M5exist-var* **by** *blast*  
**moreover from**  $zu\ qup\ zup$  **have**  $q \parallel u$  **using** *M1* **by** *blast*  
**ultimately show**  $x \in \widehat{d^{-1}}$  **using**  $x\ d\ kp\ uv\ pv$  **by** *blast*  
**qed**

**lemma** *cdidi*:  $\widehat{d^{-1}}\ O\ \widehat{d^{-1}} \subseteq \widehat{d^{-1}}$

**proof**

**fix**  $x::'a \times 'a$  **assume**  $x : \widehat{d^{-1}}\ O\ \widehat{d^{-1}}$  **then obtain**  $p\ q\ z$  **where**  $x:x = (p,q)$   
**and**  $(p,z) \in \widehat{d^{-1}}$  **and**  $(z,q) \in \widehat{d^{-1}}$  **by** *auto*  
**then obtain**  $k\ l\ u\ v$  **where**  $kp:k \parallel p$  **and**  $kl:k \parallel l$  **and**  $lz:l \parallel z$  **and**  $zu:z \parallel u$  **and**  
 $uv:u \parallel v$  **and**  $pv:p \parallel v$  **using**  $d$  **by** *blast*  
**obtain**  $k' l' u' v'$  **where**  $kpz:k' \parallel z$  **and**  $kplp:k' \parallel l'$  **and**  $lpq:l' \parallel q$  **and**  $qup:q \parallel u'$   
**and**  $upvp:u' \parallel v'$  **and**  $zvp:z \parallel v'$  **using**  $d \langle (z,q): \widehat{d^{-1}} \rangle$  **by** *blast*  
**from**  $lz\ kpz\ kplp$  **have**  $l \parallel l'$  **using** *M1* **by** *blast*  
**with**  $kl\ lpq$  **obtain**  $ll$  **where**  $k \parallel ll$  **and**  $ll \parallel q$  **using** *M5exist-var* **by** *blast*  
**moreover from**  $zvp\ zu\ upvp$  **have**  $u' \parallel u$  **using** *M1* **by** *blast*  
**moreover with**  $qup\ uv$  **obtain**  $uu$  **where**  $q \parallel uu$  **and**  $uu \parallel v$  **using** *M5exist-var*  
**by** *blast*  
**ultimately show**  $x \in \widehat{d^{-1}}$  **using**  $x\ d\ kp\ pv$  **by** *blast*  
**qed**

**lemma** *cdisi*:  $\widehat{d^{-1}}\ O\ \widehat{s^{-1}} \subseteq \widehat{d^{-1}}$

**proof**

**fix**  $x::'a \times 'a$  **assume**  $x : \widehat{d^{-1}}\ O\ \widehat{s^{-1}}$  **then obtain**  $p\ q\ z$  **where**  $x:x = (p,q)$   
**and**  $(p,z) \in \widehat{d^{-1}}$  **and**  $(z,q) \in \widehat{s^{-1}}$  **by** *auto*  
**then obtain**  $k\ l\ u\ v$  **where**  $kp:k \parallel p$  **and**  $kl:k \parallel l$  **and**  $lz:l \parallel z$  **and**  $zu:z \parallel u$  **and**  
 $uv:u \parallel v$  **and**  $pv:p \parallel v$  **using**  $d$  **by** *blast*  
**obtain**  $k' u' v'$  **where**  $kpz:k' \parallel z$  **and**  $kpq:k' \parallel q$  **and**  $qup:q \parallel u'$  **and**  $upvp:u' \parallel v'$   
**and**  $zvp:z \parallel v'$  **using**  $s \langle (z,q): \widehat{s^{-1}} \rangle$  **by** *blast*  
**from**  $upvp\ zvp\ zu$  **have**  $u' \parallel u$  **using** *M1* **by** *blast*  
**with**  $qup\ uv$  **obtain**  $uu$  **where**  $q \parallel uu$  **and**  $uu \parallel v$  **using** *M5exist-var* **by** *blast*  
**moreover from**  $kpz\ lz\ kpq$  **have**  $l \parallel q$  **using** *M1* **by** *blast*  
**ultimately show**  $x \in \widehat{d^{-1}}$  **using**  $x\ d\ kp\ kl\ pv$  **by** *blast*  
**qed**

**lemma** *csb*:  $s\ O\ b \subseteq b$

**apply** (*auto simp:s b*)

**using** *M1 M5exist-var* **by** *blast*

**lemma** *csm*:  $s\ O\ m \subseteq b$

**apply** (*auto simp:s m b*)

**using** *M1* **by** *blast*

**lemma** *css*:  $s\ O\ s \subseteq s$

**proof**

**fix**  $x::'a \times 'a$  **assume**  $x \in s\ O\ s$  **then obtain**  $p\ q\ z$  **where**  $x:x = (p,q)$  **and**  $(p,z)$

$\in s$  and  $(z, q) \in s$  by *auto*  
**from**  $\langle (p, z) \in s \rangle$  **obtain**  $k \ u \ v$  where  $kp:k \parallel p$  and  $kz:k \parallel z$  and  $pu:p \parallel u$  and  $uv:u \parallel v$   
**and**  $zv:z \parallel v$  **using**  $s$  **by** *blast*  
**from**  $\langle (z, q) \in s \rangle$  **obtain**  $k' \ u' \ v'$  where  $kpq:k' \parallel q$  and  $kpz:k' \parallel z$  and  $zup:z \parallel u'$   
**and**  $upvp:u' \parallel v'$  and  $qvp:q \parallel v'$  **using**  $s$  **by** *blast*  
**from**  $kp \ kpz \ kz$  **have**  $k' \parallel p$  **using**  $M1$  **by** *blast*  
**moreover from**  $uv \ zup \ zv$  **have**  $u \parallel u'$  **using**  $M1$  **by** *blast*  
**moreover with**  $pu \ upvp$  **obtain**  $uu$  where  $p \parallel uu$  and  $uu \parallel v'$  **using**  $M5exist-var$   
**by** *blast*  
**ultimately show**  $x \in s$  **using**  $x \ s \ kpq \ qvp$  **by** *blast*  
**qed**

**lemma** *csifi*:  $s^{\wedge-1} \ O \ f^{\wedge-1} \subseteq d^{\wedge-1}$

**proof**

**fix**  $x::'a \times 'a$  **assume**  $x : s^{\wedge-1} \ O \ f^{\wedge-1}$  **then obtain**  $p \ q \ z$  where  $x:x = (p, q)$   
**and**  $(p, z) \in s^{\wedge-1}$  and  $(z, q) \in f^{\wedge-1}$  **by** *auto*  
**then obtain**  $k \ u \ v$  where  $kp:k \parallel p$  and  $kz:k \parallel z$  and  $zu:z \parallel u$  and  $uv:u \parallel v$  and  
 $pv:p \parallel v$  **using**  $s$  **by** *blast*  
**obtain**  $k' \ l' \ u'$  where  $kpz:k' \parallel z$  and  $kplp:k' \parallel l'$  and  $lpq:l' \parallel q$  and  $zup:z \parallel u'$  and  
 $qup:q \parallel u'$  **using**  $f \ \langle (z, q) : f^{\wedge-1} \rangle$  **by** *blast*  
**from**  $kz \ kpz \ kplp$  **have**  $k \parallel l'$  **using**  $M1$  **by** *blast*  
**moreover from**  $qup \ zup \ zu$  **have**  $q \parallel u$  **using**  $M1$  **by** *blast*  
**ultimately show**  $x \in d^{\wedge-1}$  **using**  $x \ d \ kp \ lpq \ pv \ uv$  **by** *blast*  
**qed**

**lemma** *csidi*:  $s^{\wedge-1} \ O \ d^{\wedge-1} \subseteq d^{\wedge-1}$

**proof**

**fix**  $x::'a \times 'a$  **assume**  $x : s^{\wedge-1} \ O \ d^{\wedge-1}$  **then obtain**  $p \ q \ z$  where  $x:x = (p, q)$   
**and**  $(p, z) \in s^{\wedge-1}$  and  $(z, q) \in d^{\wedge-1}$  **by** *auto*  
**then obtain**  $k \ u \ v$  where  $kp:k \parallel p$  and  $kz:k \parallel z$  and  $zu:z \parallel u$  and  $uv:u \parallel v$  and  
 $pv:p \parallel v$  **using**  $s$  **by** *blast*  
**obtain**  $k' \ l' \ u' \ v'$  where  $kpz:k' \parallel z$  and  $kplp:k' \parallel l'$  and  $lpq:l' \parallel q$  and  $qup:q \parallel u'$   
**and**  $upvp:u' \parallel v'$  and  $zvp:z \parallel v'$  **using**  $d \ \langle (z, q) : d^{\wedge-1} \rangle$  **by** *blast*  
**from**  $zvp \ upvp \ zu$  **have**  $u' \parallel u$  **using**  $M1$  **by** *blast*  
**with**  $qup \ uv$  **obtain**  $uu$  where  $q \parallel uu$  and  $uu \parallel v$  **using**  $M5exist-var$  **by** *blast*  
**moreover from**  $kz \ kpz \ kplp$  **have**  $k \parallel l'$  **using**  $M1$  **by** *blast*  
**ultimately show**  $x \in d^{\wedge-1}$  **using**  $x \ d \ kp \ lpq \ pv$  **by** *blast*  
**qed**

**lemma** *cdb*:  $d \ O \ b \subseteq b$

**apply** (*auto simp:d b*)

**using**  $M1 \ M5exist-var$  **by** *blast*

**lemma** *cdm*:  $d \ O \ m \subseteq b$

**apply** (*auto simp:d m b*)

**using**  $M1$  **by** *blast*

**lemma** *cfb*:  $f \ O \ b \subseteq b$

**apply** (*auto simp:f b*)

using  $M1$  by *blast*

lemma  $cfm:f\ O\ m\ \subseteq\ m$

proof

fix  $x::'a\times'a$  assume  $x \in f\ O\ m$  then obtain  $p\ q\ z$  where  $x:x = (p,q)$  and  $1:(p,z) \in f$  and  $2:(z,q) \in m$  by *auto*

from 1 obtain  $u$  where  $pu:p\|u$  and  $zu:z\|u$  using  $f$  by *auto*

with 2 have  $(p,q) \in m$  using  $M1\ m$  by *blast*

thus  $x \in m$  using  $x$  by *auto*

qed

### 3.3 $\alpha$ -composition

We prove compositions of the form  $r_1 \circ r_2 \subseteq s \cup ov \cup d$ .

lemma (in *arelations*)  $cmd:m\ O\ d\ \subseteq\ s\ \cup\ ov\ \cup\ d$

proof

fix  $x::'a\times'a$  assume  $a:x \in m\ O\ d$  then obtain  $p\ q\ z$  where  $x:x = (p,q)$  and  $1:(p,z) \in m$  and  $2:(z,q) \in d$  by *auto*

then obtain  $k\ l\ u\ v$  where  $pz:p\|z$  and  $kq:k\|q$  and  $kl:k\|l$  and  $lz:l\|z$  and  $zu:z\|u$  and  $wv:u\|v$  and  $qv:q\|v$  using  $m\ d$  by *blast*

obtain  $k'$  where  $kpp:k'\|p$  using  $M3\ meets-wd\ pz$  by *blast*

from  $pz\ zu\ uv$  obtain  $zu$  where  $pzu:p\|zu$  and  $zuv:zu\|v$  using  $M5\ exist-var$  by *blast*

from  $kpp\ kq$  have  $k'\|q \oplus ((\exists t. k'\|t \wedge t\|q) \oplus (\exists t. k\|t \wedge t\|p))$  (is  $?A \oplus (?B \oplus ?C)$ ) using  $M2$  by *blast*

then have  $(?A \wedge \neg ?B \wedge \neg ?C) \vee (\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C)$  using *local.meets-atrans xor-distr-L*[of  $?A\ ?B\ ?C$ ] by *blast*

thus  $x \in s \cup ov \cup d$

proof (elim *disjE*)

{assume  $(?A \wedge \neg ?B \wedge \neg ?C)$  then have  $?A$  by *simp*

then have  $(p,q) \in s$  using  $s\ qv\ kpp\ pzu\ zuv$  by *blast*

thus  $?thesis$  using  $x$  by *simp* }

next

{assume  $(\neg ?A \wedge ?B \wedge \neg ?C)$  then have  $?B$  by *simp*

then obtain  $t$  where  $kpt:k'\|t$  and  $tq:t\|q$  by *auto*

moreover from  $kq\ kl\ tq$  have  $t\|l$  using  $M1$  by *blast*

moreover from  $lz\ pz\ pzu$  have  $l\|zu$  using  $M1$  by *blast*

ultimately have  $(p,q) \in ov$  using  $ov\ kpp\ qv\ pzu\ zuv$  by *blast*

thus  $?thesis$  using  $x$  by *simp* }

next

{assume  $(\neg ?A \wedge \neg ?B \wedge ?C)$  then have  $?C$  by *simp*

then obtain  $t$  where  $kt:k\|t$  and  $tp:t\|p$  by *auto*

with  $kq\ pzu\ zuv\ qv$  have  $(p,q) \in d$  using  $d$  by *blast*

thus  $?thesis$  using  $x$  by *simp* }

qed

qed

lemma (in *arelations*)  $cmf:m\ O\ f\ \subseteq\ s\ \cup\ ov\ \cup\ d$

proof

**fix**  $x::'a \times 'a$  **assume**  $a:x \in m$   $O f$  **then obtain**  $p q z$  **where**  $x:x=(p,q)$  **and**  
 $1:(p,z) \in m$  **and**  $2:(z,q) \in f$  **by** *auto*  
**then obtain**  $k l u$  **where**  $pz:p||z$  **and**  $kq:k||q$  **and**  $kl:k||l$  **and**  $lz:l||z$  **and**  $zu:z||u$   
**and**  $qu:q||u$  **using**  $m f$  **by** *blast*  
**obtain**  $k'$  **where**  $kpp:k' || p$  **using**  $M3$  *meets-wd*  $pz$  **by** *blast*  
**from**  $kpp kq$  **have**  $k' || q \oplus ((\exists t. k' || t \wedge t || q) \oplus (\exists t. k || t \wedge t || p))$  **(is**  $?A \oplus (?B \oplus$   
 $?C)$  **) using**  $M2$  **by** *blast*  
**then have**  $(?A \wedge \neg ?B \wedge \neg ?C) \vee (\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C)$  **using** *local.meets-atrans*  
*xor-distr-L*[of  $?A ?B ?C$ ] **by** *blast*  
**thus**  $x \in s \cup ov \cup d$   
**proof** (*elim disjE*)  
**{assume**  $(?A \wedge \neg ?B \wedge \neg ?C)$  **then have**  $?A$  **by** *simp*  
**then have**  $(p,q) \in s$  **using**  $s qu kpp pz zu$  **by** *blast*  
**thus** *?thesis* **using**  $x$  **by** *simp* **}**  
**next**  
**{assume**  $(\neg ?A \wedge ?B \wedge \neg ?C)$  **then have**  $?B$  **by** *simp*  
**then obtain**  $t$  **where**  $kpt:k' || t$  **and**  $tq:t || q$  **by** *auto*  
**moreover from**  $kq kl tq$  **have**  $t || l$  **using**  $M1$  **by** *blast*  
**moreover from**  $lz pz pz$  **have**  $l || z$  **using**  $M1$  **by** *blast*  
**ultimately have**  $(p,q) \in ov$  **using**  $ov kpp qu pz zu$  **by** *blast*  
**thus** *?thesis* **using**  $x$  **by** *simp* **}**  
**next**  
**{assume**  $(\neg ?A \wedge \neg ?B \wedge ?C)$  **then have**  $?C$  **by** *simp*  
**then obtain**  $t$  **where**  $kt:k || t$  **and**  $tp:t || p$  **by** *auto*  
**with**  $kq pz zu qu$  **have**  $(p,q) \in d$  **using**  $d$  **by** *blast*  
**thus** *?thesis* **using**  $x$  **by** *simp* **}**  
**qed**  
**qed**

**lemma** *cmovi*:  $m O ov^{\wedge -1} \subseteq s \cup ov \cup d$

**proof**

**fix**  $x::'a \times 'a$  **assume**  $a:x \in m$   $O ov^{\wedge -1}$  **then obtain**  $p q z$  **where**  $x:x=(p,q)$   
**and**  $1:(p,z) \in m$  **and**  $2:(z,q) \in ov^{\wedge -1}$  **by** *auto*  
**then obtain**  $k l c u v$  **where**  $pz:p||z$  **and**  $kq:k||q$  **and**  $kl:k||l$  **and**  $lz:l||z$  **and**  
 $qu:q||u$  **and**  $uv:u||v$  **and**  $zv:z||v$  **and**  $lc:l||c$  **and**  $cu:c||u$  **using**  $m ov$  **by** *blast*  
**obtain**  $k'$  **where**  $kpp:k' || p$  **using**  $M3$  *meets-wd*  $pz$  **by** *blast*  
**from**  $lz lc pz$  **have**  $pc:p || c$  **using**  $M1$  **by** *auto*  
**from**  $kpp kq$  **have**  $k' || q \oplus ((\exists t. k' || t \wedge t || q) \oplus (\exists t. k || t \wedge t || p))$  **(is**  $?A \oplus (?B \oplus$   
 $?C)$  **) using**  $M2$  **by** *blast*  
**then have**  $(?A \wedge \neg ?B \wedge \neg ?C) \vee (\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C)$  **by** (*insert xor-distr-L*[of  
 $?A ?B ?C$ ], *auto simp:elimmeets*)  
**thus**  $x \in s \cup ov \cup d$   
**proof** (*elim disjE*)  
**{assume**  $(?A \wedge \neg ?B \wedge \neg ?C)$  **then have**  $?A$  **by** *simp*  
**then have**  $(p,q) \in s$  **using**  $s kpp qu cu pc$  **by** *blast*  
**thus** *?thesis* **using**  $x$  **by** *simp* **}**  
**next**  
**{assume**  $(\neg ?A \wedge ?B \wedge \neg ?C)$  **then have**  $?B$  **by** *simp*  
**then obtain**  $t$  **where**  $kpt:k' || t$  **and**  $tq:t || q$  **by** *auto*

**moreover from  $kq\ kl\ tq$  have  $t\|l$  using  $M1$  by *auto***  
**ultimately have  $(p,q) \in ov$  using  $ov\ kpp\ qu\ cu\ lc\ pc$  by *blast***  
**thus  $?thesis$  using  $x$  by *simp*}**  
**next**  
**{assume  $(\neg ?A \wedge \neg ?B \wedge ?C)$  then have  $?C$  by *simp***  
**then obtain  $t$  where  $kt:k\|t$  and  $tp:t\|p$  by *auto***  
**then have  $(p,q) \in d$  using  $d\ kq\ cu\ qu\ pc$  by *blast***  
**thus  $?thesis$  using  $x$  by *simp*}**  
**qed**  
**qed**

**lemma  $covd:ov\ O\ d \subseteq s \cup ov \cup d$**   
**proof**  
**fix  $x::'a \times 'a$  assume  $x \in ov\ O\ d$  then obtain  $p\ q\ z$  where  $x:x=(p,q)$  and  $(p,z) \in ov$  and  $(z,q) \in d$  by *auto***  
**from  $\langle(p,z) \in ov\rangle$  obtain  $k\ u\ v\ l\ c$  where  $kp:k\|p$  and  $pu:p\|u$  and  $uv:u\|v$  and  $zv:z\|v$  and  $lc:l\|c$  and  $cu:c\|u$  and  $kl:k\|l$  and  $lz:l\|z$  and  $cu:c\|u$  using  $ov$  by *blast***  
**from  $\langle(z,q) \in d\rangle$  obtain  $k'\ l'\ u'\ v'$  where  $k'p'q:k'\|q$  and  $k'p'l'p:k'\|l'$  and  $lpz:l'\|z$  and  $qvp:q\|v'$  and  $zup:z\|u'$  and  $upvp:u'\|v'$  using  $d$  by *blast***  
**from  $uv\ zv\ zup$  have  $u\|u'$  using  $M1$  by *auto***  
**from  $pu\ upvp$  obtain  $uu$  where  $puu:p\|uu$  and  $uuvp:uu\|v'$  using  $\langle u\|u'\rangle$  using  $M5exist-var$  by *blast***  
**from  $kp\ k'p'q$  have  $k\|q \oplus ((\exists t. k\|t \wedge t\|q) \oplus (\exists t. k'\|t \wedge t\|p))$  (is  $?A \oplus (?B \oplus ?C)$ ) using  $M2$  by *blast***  
**then have  $(?A \wedge \neg ?B \wedge \neg ?C) \vee ((\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C))$  by (*insert xor-distr-L*[of  $?A\ ?B\ ?C$ ], *auto simp:elimmeets*)**  
**thus  $x \in s \cup ov \cup d$**   
**proof (*elim disjE*)**  
**{ assume  $?A \wedge \neg ?B \wedge \neg ?C$  then have  $?A$  by *simp***  
**then have  $(p,q) \in s$  using  $s\ kp\ qvp\ puu\ uuvp$  by *blast***  
**thus  $?thesis$  using  $x$  by *blast*}**  
**next**  
**{ assume  $\neg ?A \wedge ?B \wedge \neg ?C$  then have  $?B$  by *simp***  
**then obtain  $t$  where  $kt:k\|t$  and  $tq:t\|q$  by *auto***  
**from  $cu\ pu\ puu$  have  $c\|uu$  using  $M1$  by *auto***  
**moreover from  $k'p'q\ tq\ k'p'l'p$  have  $t\|l'$  using  $M1$  by *auto***  
**moreover from  $lpz\ lz\ lc$  have  $l'p'c:l'\|c$  using  $M1$  by *auto***  
**ultimately obtain  $lc$  where  $t\|lc$  and  $lc\|uu$  using  $M5exist-var$  by *blast***  
**then have  $(p,q) \in ov$  using  $ov\ kp\ kt\ tq\ puu\ uuvp\ qvp$  by *blast***  
**thus  $?thesis$  using  $x$  by *auto*}**  
**next**  
**{ assume  $\neg ?A \wedge \neg ?B \wedge ?C$  then have  $?C$  by *simp***  
**then obtain  $t$  where  $k'\|t$  and  $t\|p$  by *auto***  
**with  $puu\ uuvp\ qvp\ k'p'q$  have  $(p,q) \in d$  using  $d$  by *blast***  
**thus  $?thesis$  using  $x$  by *auto*}**  
**qed**  
**qed**

**lemma** *covf:ov*  $O f \subseteq s \cup ov \cup d$

**proof**

**fix**  $x::'a \times 'a$  **assume**  $x \in ov$   $O f$  **then obtain**  $p q z$  **where**  $x:x=(p,q)$  **and**  $(p,z) \in ov$  **and**  $(z,q) \in f$  **by** *auto*

**from**  $\langle (p,z) \in ov \rangle$  **obtain**  $k u v l c$  **where**  $kp:k||p$  **and**  $pu:p||u$  **and**  $uv:u||v$  **and**  $zv:z||v$  **and**  $lc:l||c$  **and**  $cu:c||u$  **and**  $kl:k||l$  **and**  $lz:l||z$  **and**  $cu:c||u$  **using** *ov* **by** *blast*

**from**  $\langle (z,q) \in f \rangle$  **obtain**  $k' l' u'$  **where**  $kpq:k'||q$  **and**  $kplp:k'||l'$  **and**  $lpz:l'||z$  **and**  $qup:q||u'$  **and**  $zup:z||u'$  **using** *f* **by** *blast*

**from**  $uv zv zup$  **have**  $uu:u||u'$  **using** *M1* **by** *auto*

**from**  $kp kpq$  **have**  $k||q \oplus ((\exists t. k||t \wedge t||q) \oplus (\exists t. k'||t \wedge t||p))$  **(is**  $?A \oplus (?B \oplus ?C)$  **) using** *M2* **by** *blast*

**then have**  $(?A \wedge \neg ?B \wedge \neg ?C) \vee ((\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C))$  **by** (*insert xor-distr-L[of ?A ?B ?C], auto simp:elimmeets*)

**thus**  $x \in s \cup ov \cup d$

**proof** (*elim disjE*)

{ **assume**  $?A \wedge \neg ?B \wedge \neg ?C$  **then have**  $?A$  **by** *simp*

**then have**  $(p,q) \in s$  **using**  $s kp qup uu pu$  **by** *blast*

**thus**  $?thesis$  **using**  $x$  **by** *blast*}

**next**

{ **assume**  $\neg ?A \wedge ?B \wedge \neg ?C$  **then have**  $?B$  **by** *simp*

**then obtain**  $t$  **where**  $kt:k||t$  **and**  $tq:t||q$  **by** *auto*

**moreover from**  $kpq tq kplp$  **have**  $t||l'$  **using** *M1* **by** *auto*

**moreover from**  $lpz lz lc$  **have**  $lpc:l'||c$  **using** *M1* **by** *auto*

**ultimately obtain**  $lc$  **where**  $t||lc$  **and**  $lc||u$  **using**  $cu M5exist-var$  **by** *blast*

**then have**  $(p,q) \in ov$  **using**  $ov kp kt tq pu uu qup$  **by** *blast*

**thus**  $?thesis$  **using**  $x$  **by** *auto*}

**next**

{ **assume**  $\neg ?A \wedge \neg ?B \wedge ?C$  **then have**  $?C$  **by** *simp*

**then obtain**  $t$  **where**  $k'||t$  **and**  $t||p$  **by** *auto*

**with**  $pu uu qup kpq$  **have**  $(p,q) \in d$  **using**  $d$  **by** *blast*

**thus**  $?thesis$  **using**  $x$  **by** *auto*}

**qed**

**qed**

**lemma** *cfid:f<sup>-1</sup>*  $O d \subseteq s \cup ov \cup d$

**proof**

**fix**  $x::'a \times 'a$  **assume**  $x \in f^{-1} O d$  **then obtain**  $p q z$  **where**  $x:x = (p,q)$  **and**  $(p,z) \in f^{-1}$  **and**  $(z,q) \in d$  **by** *auto*

**from**  $\langle (p,z) \in f^{-1} \rangle$  **obtain**  $k l u$  **where**  $k||l$  **and**  $l||z$  **and**  $kp:k||p$  **and**  $pu:p||u$  **and**  $zu:z||u$  **using** *f* **by** *blast*

**from**  $\langle (z,q) \in d \rangle$  **obtain**  $k' l' u' v$  **where**  $kplp:k'||l'$  **and**  $kpq:k'||q$  **and**  $lpz:l'||z$  **and**  $zup:z||u'$  **and**  $upv:u'||v$  **and**  $qv:q||v$  **using**  $d$  **by** *blast*

**from**  $pu zu zup$  **have**  $pup:p||u'$  **using** *M1* **by** *blast*

**from**  $kp kpq$  **have**  $k||q \oplus ((\exists t. k||t \wedge t||q) \oplus (\exists t. k'||t \wedge t||p))$  **(is**  $?A \oplus (?B \oplus ?C)$  **) using** *M2* **by** *blast*

**then have**  $(?A \wedge \neg ?B \wedge \neg ?C) \vee ((\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C))$  **by** (*insert xor-distr-L[of ?A ?B ?C], auto simp:elimmeets*)

**thus**  $x \in s \cup ov \cup d$

**proof** (*elim disjE*)

```

{ assume  $?A \wedge \neg ?B \wedge \neg ?C$  then have  $?A$  by simp
  with  $pup\ upv\ kp\ qv$  have  $(p,q) \in s$  using  $s$  by blast
  thus  $?thesis$  using  $x$  by auto}
next
{ assume  $\neg ?A \wedge ?B \wedge \neg ?C$  then have  $?B$  by simp
  then obtain  $t$  where  $kt:k||t$  and  $tq:t||q$  by auto
  from  $tq\ kpq\ kplp$  have  $t||l'$  using  $M1$  by blast
  with  $lpz\ zup$  obtain  $lpz$  where  $t||lpz$  and  $lpz||u'$  using  $M5exist-var$  by blast
  with  $kp\ pup\ upv\ kt\ tq\ qv$  have  $(p,q) \in ov$  using  $ov$  by blast
  thus  $?thesis$  using  $x$  by blast}
next
{ assume  $\neg ?A \wedge \neg ?B \wedge ?C$  then have  $?C$  by simp
  then obtain  $t$  where  $k'||t$  and  $t||p$  by auto
  with  $pup\ upv\ kpq\ qv$  have  $(p,q) \in d$  using  $d$  by blast
  thus  $?thesis$  using  $x$  by auto}
qed
qed

lemma cfov:  $f\ O\ ov \subseteq ov \cup s \cup d$ 
proof
  fix  $x::'a \times 'a$  assume  $x \in f\ O\ ov$  then obtain  $p\ q\ z$  where  $x:x = (p,q)$  and
   $(p,z) \in f$  and  $(z,q) \in ov$  by auto
  from  $\langle (p,z) \in f \rangle$  obtain  $k\ l\ u$  where  $k||l$  and  $kz:k||z$  and  $lp:l||p$  and  $pu:p||u$ 
  and  $zu:z||u$  using  $f$  by blast
  from  $\langle (z,q) \in ov \rangle$  obtain  $k'\ l'\ c\ u'\ v$  where  $k'||l'$  and  $kpz:k'||z$  and  $lpq:l'||q$ 
  and  $zup:z||u'$  and  $upv:u'||v$  and  $qv:q||v$  and  $lpc:l'||c$  and  $cup:c||u'$  using  $ov$  by
  blast
  from  $pu\ zu\ zup$  have  $pup:p||u'$  using  $M1$  by blast
  from  $lp\ lpq$  have  $l||q \oplus ((\exists t. l||t \wedge t||q) \oplus (\exists t. l'||t \wedge t||p))$  (is  $?A \oplus (?B \oplus ?C)$ )
  using  $M2$  by blast
  then have  $(?A \wedge \neg ?B \wedge \neg ?C) \vee ((\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C))$  by (insert
  xor-distr-L[of  $?A\ ?B\ ?C$ ], auto simp:elimmeets)
  thus  $x \in ov \cup s \cup d$ 
  proof (elim disjE)
    { assume  $?A \wedge \neg ?B \wedge \neg ?C$  then have  $?A$  by simp
      with  $lp\ pup\ upv\ qv$  have  $(p,q) \in s$  using  $s$  by blast
      thus  $?thesis$  using  $x$  by auto}
    next
    { assume  $\neg ?A \wedge ?B \wedge \neg ?C$  then have  $?B$  by simp
      then obtain  $t$  where  $lt:l||t$  and  $tq:t||q$  by auto
      from  $tq\ lpq\ lpc$  have  $t||c$  using  $M1$  by blast
      with  $lp\ lt\ tq\ pup\ upv\ qv\ cup$  have  $(p,q) \in ov$  using  $ov$  by blast
      thus  $?thesis$  using  $x$  by blast}
    next
    { assume  $\neg ?A \wedge \neg ?B \wedge ?C$  then have  $?C$  by simp
      then obtain  $t$  where  $l'||t$  and  $t||p$  by auto
      with  $lpq\ pup\ upv\ qv$  have  $(p,q) \in d$  using  $d$  by blast
      thus  $?thesis$  using  $x$  by auto}
  qed
qed

```



qed

We prove compositions of the form  $r_1 \circ r_2 \subseteq ov \cup f^{-1} \cup d^{-1}$ .

**lemma** *covsi*:  $ov \circ s^{-1} \subseteq ov \cup f^{-1} \cup d^{-1}$

**proof**

**fix**  $x::'a \times 'a$  **assume**  $x \in ov \circ s^{-1}$  **then obtain**  $p \ q \ z$  **where**  $x:x = (p,q)$  **and**  $(p,z) \in ov$  **and**  $(z,q) \in s^{-1}$  **by** *auto*

**from**  $\langle (p,z) \in ov \rangle$  **obtain**  $k \ l \ c \ u$  **where**  $kp:k||p$  **and**  $pu:p||u$  **and**  $kl:k||l$  **and**  $lz:l||z$  **and**  $lc:l||c$  **and**  $cu:c||u$  **using** *ov* **by** *blast*

**from**  $\langle (z,q) \in s^{-1} \rangle$  **obtain**  $k' \ u' \ v'$  **where**  $kpz:k'||z$  **and**  $kpq:k'||q$  **and**  $kpz:k'||z$  **and**  $zup:z||u'$  **and**  $qvp:q||v'$  **using** *s* **by** *blast*

**from**  $lz \ kpz \ kpq$  **have**  $lq:l||q$  **using** *M1* **by** *blast*

**from**  $pu \ qvp$  **have**  $p||v' \oplus ((\exists t. p||t \wedge t||v') \oplus (\exists t. q||t \wedge t||u))$  **(is**  $?A \oplus (?B \oplus ?C)$  **) using** *M2* **by** *blast*

**then have**  $(?A \wedge \neg ?B \wedge \neg ?C) \vee ((\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C))$  **by** (*insert xor-distr-L*[of  $?A \ ?B \ ?C$ ], *auto simp:elimmeets*)

**thus**  $x \in ov \cup f^{-1} \cup d^{-1}$

**proof** (*elim disjE*)

{ **assume**  $?A \wedge \neg ?B \wedge \neg ?C$  **then have**  $?A$  **by** *simp*

**with**  $qvp \ kp \ kl \ lq$  **have**  $(p,q) \in f^{-1}$  **using** *f* **by** *blast*

**thus**  $?thesis$  **using**  $x$  **by** *auto*}

**next**

{ **assume**  $\neg ?A \wedge ?B \wedge \neg ?C$  **then have**  $?B$  **by** *simp*

**then obtain**  $t$  **where**  $ptp:p||t$  **and**  $t||v'$  **by** *auto*

**moreover with**  $pu \ cu$  **have**  $c||t$  **using** *M1* **by** *blast*

**ultimately have**  $(p,q) \in ov$  **using**  $kp \ kl \ lc \ cu \ lq \ qvp \ ov$  **by** *blast*

**thus**  $?thesis$  **using**  $x$  **by** *auto*}

**next**

{ **assume**  $\neg ?A \wedge \neg ?B \wedge ?C$  **then have**  $?C$  **by** *simp*

**then obtain**  $t$  **where**  $qt:q||t$  **and**  $t||u$  **by** *auto*

**with**  $kp \ kl \ lq \ pu$  **have**  $(p,q) \in d^{-1}$  **using** *d* **by** *blast*

**thus**  $?thesis$  **using**  $x$  **by** *auto*}

qed

qed

**lemma** *cdim*:  $d^{-1} \circ m \subseteq ov \cup d^{-1} \cup f^{-1}$

**proof**

**fix**  $x::'a \times 'a$  **assume**  $x \in d^{-1} \circ m$  **then obtain**  $p \ q \ z$  **where**  $x:x = (p,q)$  **and**  $(p,z) \in d^{-1}$  **and**  $(z,q) \in m$  **by** *auto*

**from**  $\langle (p,z) \in d^{-1} \rangle$  **obtain**  $k \ l \ u \ v$  **where**  $kp:k||p$  **and**  $pv:p||v$  **and**  $kl:k||l$  **and**  $lz:l||z$  **and**  $zu:z||u$  **and**  $wv:u||v$  **using** *d* **by** *blast*

**from**  $\langle (z,q) \in m \rangle$  **have**  $zq:z||q$  **using** *m* **by** *blast*

**obtain**  $v'$  **where**  $qvp:q||v'$  **using** *M3 meets-wd zq* **by** *blast*

**from**  $kl \ lz \ zq$  **obtain**  $lz$  **where**  $klz:k||lz$  **and**  $lzq:lz||q$  **using** *M5 exist-var* **by** *blast*

**from**  $pv \ qvp$  **have**  $p||v' \oplus ((\exists t. p||t \wedge t||v') \oplus (\exists t. q||t \wedge t||v))$  **(is**  $?A \oplus (?B \oplus ?C)$  **) using** *M2* **by** *blast*

**then have**  $(?A \wedge \neg ?B \wedge \neg ?C) \vee ((\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C))$  **by** (*insert*

*xor-distr-L*[of  $?A \ ?B \ ?C$ ], *auto simp:elimmeets*)  
**thus**  $x \in ov \cup d^{\wedge-1} \cup f^{\wedge-1}$   
**proof** (*elim disjE*)  
 { **assume**  $?A \wedge \neg ?B \wedge \neg ?C$  **then have**  $?A$  **by** *simp*  
 with  $qvp \ kp \ klz \ lzq \langle ?A \rangle$  **have**  $(p,q) \in f^{\wedge-1}$  **using**  $f$  **by** *blast*  
**thus** *?thesis* **using**  $x$  **by** *auto* }  
**next**  
 { **assume**  $\neg ?A \wedge ?B \wedge \neg ?C$  **then have**  $?B$  **by** *simp*  
**then obtain**  $t$  **where**  $pt:p||t$  **and**  $tpv:t||v'$  **by** *auto*  
**from**  $zq \ lzq \ zu$  **have**  $lz||u$  **using**  $M1$  **by** *auto*  
**moreover from**  $pt \ pv \ uv$  **have**  $u||t$  **using**  $M1$  **by** *auto*  
**ultimately have**  $(p,q) \in ov$  **using**  $kp \ klz \ lzq \ pt \ tpv \ qvp \ ov$  **by** *blast*  
**thus** *?thesis* **using**  $x$  **by** *auto* }  
**next**  
 { **assume**  $\neg ?A \wedge \neg ?B \wedge ?C$  **then have**  $?C$  **by** *simp*  
**then obtain**  $t$  **where**  $qt:q||t$  **and**  $t||v$  **by** *auto*  
**with**  $kp \ klz \ lzq \ pv$  **have**  $(p,q) \in d^{\wedge-1}$  **using**  $d$  **by** *blast*  
**thus** *?thesis* **using**  $x$  **by** *auto* }  
**qed**  
**qed**

**lemma** *cdiov*:  $d^{\wedge-1} \ O \ ov \subseteq ov \cup f^{\wedge-1} \cup d^{\wedge-1}$

**proof**

**fix**  $x::'a \times 'a$  **assume**  $x \in d^{\wedge-1} \ O \ ov$  **then obtain**  $p \ q \ r$  **where**  $x:x = (p,r)$   
**and**  $(p,q) \in d^{\wedge-1}$  **and**  $(q,r) \in ov$  **by** *auto*  
**from**  $\langle (p,q) \in d^{\wedge-1} \rangle$  **obtain**  $u \ v \ k \ l$  **where**  $kp:k||p$  **and**  $pv:p||v$  **and**  $kl:k||l$   
**and**  $lq:l||q$  **and**  $qu:q||u$  **and**  $uv:u||v$  **using**  $d$  **by** *blast*  
**from**  $\langle (q,r) \in ov \rangle$  **obtain**  $k' \ l' \ t \ u' \ v'$  **where**  $lpr:l'||r$  **and**  $kpq:k'||q$  **and**  $kplp:k'||l'$   
**and**  $qvp:q||u'$  **and**  $u'||v'$  **and**  $rvp:r||v'$  **and**  $lpt:l'||t$  **and**  $tup:t||u'$  **using**  $ov$  **by** *blast*  
**from**  $lq \ kplp \ kpq$  **have**  $l||l'$  **using**  $M1$  **by** *blast*  
**with**  $kl \ lpr$  **obtain**  $ll$  **where**  $kll:k||ll$  **and**  $llr:ll||r$  **using**  $M5exist-var$  **by** *blast*  
**from**  $pv \ rvp$  **have**  $p||v' \oplus ((\exists t'. p||t' \wedge t'||v')) \oplus ((\exists t'. r||t' \wedge t'||v'))$  **(is**  $?A \oplus$   
 $(?B \oplus ?C))$  **using**  $M2$  **by** *blast*  
**then have**  $(?A \wedge \neg ?B \wedge \neg ?C) \vee ((\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C))$  **by** (*insert*  
*xor-distr-L*[of  $?A \ ?B \ ?C$ ], *auto simp:elimmeets*)  
**thus**  $x \in ov \cup f^{\wedge-1} \cup d^{\wedge-1}$   
**proof** (*elim disjE*)  
 { **assume**  $?A \wedge \neg ?B \wedge \neg ?C$  **then have**  $?A$  **by** *simp*  
 with  $rvp \ llr \ kp \ kll$  **have**  $(p,r) \in f^{\wedge-1}$  **using**  $f$  **by** *blast*  
**thus** *?thesis* **using**  $x$  **by** *auto* }  
**next**  
 { **assume**  $\neg ?A \wedge ?B \wedge \neg ?C$  **then have**  $?B$  **by** *simp*  
**then obtain**  $t'$  **where**  $ptp:p||t'$  **and**  $tpvp:t'||v'$  **by** *auto*  
**moreover from**  $lpt \ lpr \ llr$  **have**  $llt:ll||t$  **using**  $M1$  **by** *blast*  
**moreover from**  $ptp \ uv \ pv$  **have**  $utp:u||t'$  **using**  $M1$  **by** *blast*  
**moreover from**  $qu \ tup \ qvp$  **have**  $t||u$  **using**  $M1$  **by** *blast*  
**moreover with**  $utp \ llt$  **obtain**  $tu$  **where**  $ll||tu$  **and**  $tu||t'$  **using**  $M5exist-var$   
**by** *blast*  
**with**  $kp \ ptp \ tpvp \ kll \ llr \ rvp$  **have**  $(p,r) \in ov$  **using**  $ov$  **by** *blast*

thus *?thesis* using *x* by *auto*}  
 next  
 { assume  $\neg ?A \wedge \neg ?B \wedge ?C$  then have *?C* by *simp*  
 then obtain *t'* where *rtp:r||t'* and *t'v* by *auto*  
 with *kl llr kp pv* have  $(p,r) \in d^{\wedge-1}$  using *d* by *blast*  
 thus *?thesis* using *x* by *auto*}  
 qed  
 qed

lemma *cdis*:  $d^{\wedge-1} O s \subseteq ov \cup f^{\wedge-1} \cup d^{\wedge-1}$

proof

fix *x::'a × 'a* assume  $x \in d^{\wedge-1} O s$  then obtain *p q z* where  $x:x = (p,q)$  and  $(p,z) \in d^{\wedge-1}$  and  $(z,q) \in s$  by *auto*

from  $\langle (p,z) \in d^{\wedge-1} \rangle$  obtain *k l u v* where *kl:k||l* and *lz:l||z* and *kp:k||p* and *zu:z||u* and *uv:u||v* and *pv:p||v* using *d* by *blast*

from  $\langle (z,q) \in s \rangle$  obtain *l' v'* where *lpz:l'||z* and *lpq:l'||q* and *qvp:q||v'* using *s* by *blast*

from *lz lpz lpq* have *lq:l||q* using *M1* by *blast*

from *pv qvp* have  $p||v' \oplus ((\exists t. p||t \wedge t||v') \oplus (\exists t. q||t \wedge t||v))$  (is  $?A \oplus (?B \oplus ?C)$ ) using *M2* by *blast*

then have  $(?A \wedge \neg ?B \wedge \neg ?C) \vee ((\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C))$  by (*insert xor-distr-L*[of *?A ?B ?C*], *auto simp:elimmeets*)

thus  $x \in ov \cup f^{\wedge-1} \cup d^{\wedge-1}$

proof (*elim disjE*)

{ assume  $?A \wedge \neg ?B \wedge \neg ?C$  then have *?A* by *simp*

with *kl lq qvp kp* have  $(p,q) \in f^{\wedge-1}$  using *f* by *blast*

thus *?thesis* using *x* by *auto*}

next

{ assume  $\neg ?A \wedge ?B \wedge \neg ?C$  then have *?B* by *simp*

then obtain *t* where *pt:p||t* and *tvp:t||v'* by *auto*

from *pt pv uv* have *u||t* using *M1* by *blast*

with *lz zu* obtain *zu* where *l||zu* and *zu||t* using *M5exist-var* by *blast*

with *kp pt tvp kl lq qvp* have  $(p,q) \in ov$  using *ov* by *blast*

thus *?thesis* using *x* by *auto*}

next

{ assume  $\neg ?A \wedge \neg ?B \wedge ?C$  then have *?C* by *simp*

then obtain *t* where *q||t* and *t||v* by *auto*

with *kl lq kp pv* have  $(p,q) \in d^{\wedge-1}$  using *d* by *blast*

thus *?thesis* using *x* by *auto*}

qed

qed

lemma *csim*:  $s^{\wedge-1} O m \subseteq ov \cup f^{\wedge-1} \cup d^{\wedge-1}$

proof

fix *x::'a × 'a* assume  $x \in s^{\wedge-1} O m$  then obtain *p q z* where  $x:x = (p,q)$  and  $(p,z) \in s^{\wedge-1}$  and  $(z,q) \in m$  by *auto*

from  $\langle (p,z) \in s^{\wedge-1} \rangle$  obtain *k u v* where *kp:k||p* and *kz:k||z* and *zu:z||u* and *uv:u||v* and *pv:p||v* using *s* by *blast*

from  $\langle (z,q) \in m \rangle$  have *zq:z||q* using *m* by *auto*

**obtain**  $v'$  **where**  $qvp:q||v'$  **using**  $M3$  *meets-wd*  $zq$  **by** *blast*  
**from**  $pv$   $qvp$  **have**  $p||v' \oplus ((\exists t. p||t \wedge t||v') \oplus (\exists t. q||t \wedge t||v))$  **(is**  $?A \oplus (?B \oplus ?C)$  **) using**  $M2$  **by** *blast*  
**then have**  $(?A \wedge \neg ?B \wedge \neg ?C) \vee ((\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C))$  **by** (*insert xor-distr-L*[of  $?A ?B ?C$ ], *auto simp:elimmeets*)  
**thus**  $x \in ov \cup f^{\wedge-1} \cup d^{\wedge-1}$   
**proof** (*elim disjE*)  
{ **assume**  $?A \wedge \neg ?B \wedge \neg ?C$  **then have**  $?A$  **by** *simp*  
**with**  $kp$   $kz$   $zq$   $qvp$  **have**  $(p,q) \in f^{\wedge-1}$  **using**  $f$  **by** *blast*  
**thus** *?thesis* **using**  $x$  **by** *auto* }  
**next**  
{ **assume**  $\neg ?A \wedge ?B \wedge \neg ?C$  **then have**  $?B$  **by** *simp*  
**then obtain**  $t$  **where**  $pt:p||t$  **and**  $tpv:t||v'$  **by** *auto*  
**from**  $pt$   $pv$   $uv$  **have**  $u||t$  **using**  $M1$  **by** *blast*  
**with**  $kp$   $pt$   $tpv$   $kz$   $zq$   $qvp$   $zu$  **have**  $(p,q) \in ov$  **using**  $ov$  **by** *blast*  
**thus** *?thesis* **using**  $x$  **by** *auto* }  
**next**  
{ **assume**  $\neg ?A \wedge \neg ?B \wedge ?C$  **then have**  $?C$  **by** *simp*  
**then obtain**  $t$  **where**  $q||t$  **and**  $t||v$  **by** *auto*  
**with**  $kp$   $kz$   $zq$   $pv$  **have**  $(p,q) \in d^{\wedge-1}$  **using**  $d$  **by** *blast*  
**thus** *?thesis* **using**  $x$  **by** *auto* }  
**qed**  
**qed**

**lemma**  $csiov:s^{\wedge-1} O ov \subseteq ov \cup f^{\wedge-1} \cup d^{\wedge-1}$

**proof**

**fix**  $x::'a \times 'a$  **assume**  $x \in s^{\wedge-1} O ov$  **then obtain**  $p$   $q$   $z$  **where**  $x:x = (p,q)$  **and**  $(p,z) \in s^{\wedge-1}$  **and**  $(z,q) \in ov$  **by** *auto*  
**from**  $\langle (p,z) \in s^{\wedge-1} \rangle$  **obtain**  $k$   $u$   $v$  **where**  $kp:k||p$  **and**  $kz:k||z$  **and**  $zu:z||u$  **and**  $uv:u||v$  **and**  $pv:p||v$  **using**  $s$  **by** *blast*  
**from**  $\langle (z,q) \in ov \rangle$  **obtain**  $k'$   $l'$   $u'$   $v'$   $c$  **where**  $kpz:k'||z$  **and**  $zup:z||u'$  **and**  $upvp:u'||v'$  **and**  $kplp:k'||l'$  **and**  $lpq:l'||q$  **and**  $qvp:q||v'$  **and**  $lpc:l'||c$  **and**  $cup:c||u'$  **using**  $ov$  **by** *blast*  
**from**  $kz$   $kpz$   $kplp$  **have**  $klp:k||l'$  **using**  $M1$  **by** *auto*  
**from**  $pv$   $qvp$  **have**  $p||v' \oplus ((\exists t. p||t \wedge t||v') \oplus (\exists t. q||t \wedge t||v))$  **(is**  $?A \oplus (?B \oplus ?C)$  **) using**  $M2$  **by** *blast*  
**then have**  $(?A \wedge \neg ?B \wedge \neg ?C) \vee ((\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C))$  **by** (*insert xor-distr-L*[of  $?A ?B ?C$ ], *auto simp:elimmeets*)  
**thus**  $x \in ov \cup f^{\wedge-1} \cup d^{\wedge-1}$   
**proof** (*elim disjE*)  
{ **assume**  $?A \wedge \neg ?B \wedge \neg ?C$  **then have**  $?A$  **by** *simp*  
**with**  $kp$   $kplp$   $lpq$   $qvp$   $klp$  **have**  $(p,q) \in f^{\wedge-1}$  **using**  $f$  **by** *blast*  
**thus** *?thesis* **using**  $x$  **by** *auto* }  
**next**  
{ **assume**  $\neg ?A \wedge ?B \wedge \neg ?C$  **then have**  $?B$  **by** *simp*  
**then obtain**  $t$  **where**  $pt:p||t$  **and**  $tpv:t||v'$  **by** *auto*  
**from**  $pt$   $pv$   $uv$  **have**  $u||t$  **using**  $M1$  **by** *blast*  
**moreover from**  $cup$   $zup$   $zu$  **have**  $cu:c||u$  **using**  $M1$  **by** *auto*  
**ultimately obtain**  $cu$  **where**  $l'||cu$  **and**  $cu||t$  **using**  $lpc$   $M5$  *exist-var* **by**

**blast**  
**with**  $kp\ pt\ tvp\ klp\ lpq\ qvp$  **have**  $(p,q) \in ov$  **using**  $ov$  **by** *blast*  
**thus** *?thesis* **using**  $x$  **by** *auto*  
**next**  
**{ assume**  $\neg ?A \wedge \neg ?B \wedge ?C$  **then have**  $?C$  **by** *simp*  
**then obtain**  $t$  **where**  $q||t$  **and**  $t||v$  **by** *auto*  
**with**  $kp\ klp\ lpq\ pv$  **have**  $(p,q) \in d^{\wedge-1}$  **using**  $d$  **by** *blast*  
**thus** *?thesis* **using**  $x$  **by** *auto*  
**qed**  
**qed**

**lemma**  $covim:ov^{\wedge-1} O m \subseteq ov \cup f^{\wedge-1} \cup d^{\wedge-1}$   
**proof**  
**fix**  $x::'a \times 'a$  **assume**  $x \in ov^{\wedge-1} O m$  **then obtain**  $p\ q\ z$  **where**  $x:x = (p,q)$   
**and**  $(p,z) \in ov^{\wedge-1}$  **and**  $(z,q) \in m$  **by** *auto*  
**from**  $\langle (p,z) \in ov^{\wedge-1} \rangle$  **obtain**  $k\ l\ c\ u\ v$  **where**  $kz:k||z$  **and**  $zu:z||u$  **and**  $kl:k||l$   
**and**  $lp:l||p$  **and**  $lc:l||c$  **and**  $cu:c||u$  **and**  $pv:p||v$  **and**  $wv:u||v$  **using**  $ov$  **by** *blast*  
**from**  $\langle (z,q) \in m \rangle$  **have**  $zq:z||q$  **using**  $m$  **by** *auto*  
**obtain**  $v'$  **where**  $qvp:q||v'$  **using**  $M3$  *meets-wd*  $zq$  **by** *blast*  
**from**  $zu\ zq\ cu$  **have**  $cq:c||q$  **using**  $M1$  **by** *blast*  
**from**  $pv\ qvp$  **have**  $p||v' \oplus ((\exists t. p||t \wedge t||v') \oplus (\exists t. q||t \wedge t||v))$  **(is**  $?A \oplus (?B$   
 $\oplus ?C)$  **) using**  $M2$  **by** *blast*  
**then have**  $(?A \wedge \neg ?B \wedge \neg ?C) \vee ((\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C))$  **by** (*insert*  
*xor-distr-L*[of  $?A\ ?B\ ?C$ ], *auto simp:elimmeets*)  
**thus**  $x \in ov \cup f^{\wedge-1} \cup d^{\wedge-1}$   
**proof** (*elim disjE*)  
**{ assume**  $?A \wedge \neg ?B \wedge \neg ?C$  **then have**  $?A$  **by** *simp*  
**with**  $lp\ lc\ cq\ qvp$  **have**  $(p,q) \in f^{\wedge-1}$  **using**  $f$  **by** *blast*  
**thus** *?thesis* **using**  $x$  **by** *auto*  
**next**  
**{ assume**  $\neg ?A \wedge ?B \wedge \neg ?C$  **then have**  $?B$  **by** *simp*  
**then obtain**  $t$  **where**  $ptp:p||t$  **and**  $t||v'$  **by** *auto*  
**moreover with**  $pv\ wv$  **have**  $u||t$  **using**  $M1$  **by** *blast*  
**ultimately have**  $(p,q) \in ov$  **using**  $lp\ lc\ cq\ qvp\ cu\ ov$  **by** *blast*  
**thus** *?thesis* **using**  $x$  **by** *auto*  
**next**  
**{ assume**  $\neg ?A \wedge \neg ?B \wedge ?C$  **then have**  $?C$  **by** *simp*  
**then obtain**  $t$  **where**  $qt:q||t$  **and**  $t||v$  **by** *auto*  
**with**  $lp\ lc\ cq\ pv$  **have**  $(p,q) \in d^{\wedge-1}$  **using**  $d$  **by** *blast*  
**thus** *?thesis* **using**  $x$  **by** *auto*  
**qed**  
**qed**

We prove compositions of the form  $r_1 \circ r_2 \subseteq b \cup m \cup ov$ .

**lemma**  $covov:ov O ov \subseteq b \cup m \cup ov$

**proof**

**fix**  $x::'a \times 'a$  **assume**  $x \in ov O ov$  **then obtain**  $p\ q\ z$  **where**  $x:x = (p,q)$  **and**  
 $(p,z) \in ov$  **and**  $(z,q) \in ov$  **by** *auto*  
**from**  $\langle (p,z) \in ov \rangle$  **obtain**  $k\ u\ l\ t\ v$  **where**  $kp:k||p$  **and**  $pu:p||u$  **and**  $kl:k||l$  **and**

$lz:l||z$  and  $l||t$  and  $t||u$  and  $uv:u||v$  and  $zv:z||v$  using *ov* by *blast*  
**from**  $\langle (z,q) \in ov \rangle$  **obtain**  $k' l' y u' v'$  **where**  $kplp:k'||l'$  and  $kpz:k'||z$  and  $lpq:l'||q$  and  $lpy:l'||y$  and  $y||u'$  and  $zup:z||u'$  and  $upvp:u'||v'$  and  $qvp:q||v'$  using *ov* by *blast*  
**from**  $lz kplp kpz$  **have**  $llp:l||l'$  using *M1* by *blast*  
**from**  $uv zv zup$  **have**  $u||u'$  using *M1* by *blast*  
**with**  $pu upvp$  **obtain**  $uu$  **where**  $puu:p||uu$  and  $uuv:uu||v'$  using *M5exist-var* by *blast*  
**from**  $puu lpq$  **have**  $p||q \oplus ((\exists t'. p||t' \wedge t' || q) \oplus (\exists t'. l' || t' \wedge t' || uu))$  (**is**  $?A \oplus (?B \oplus ?C)$ ) using *M2* by *blast*  
**then have**  $(?A \wedge \neg ?B \wedge \neg ?C) \vee ((\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C))$  by (*insert xor-distr-L*[of  $?A ?B ?C$ ], *auto simp:elimmeets*)  
**thus**  $x \in b \cup m \cup ov$   
**proof** (*elim disjE*)  
{ **assume**  $?A \wedge \neg ?B \wedge \neg ?C$  **then have**  $?A$  by *simp*  
**then have**  $(p,q) \in m$  using *m* by *auto*  
**thus** *?thesis* using *x* by *auto* }  
**next**  
{ **assume**  $\neg ?A \wedge ?B \wedge \neg ?C$  **then have**  $?B$  by *simp*  
**then have**  $(p,q) \in b$  using *b* by *auto*  
**thus** *?thesis* using *x* by *auto* }  
**next**  
{ **assume**  $\neg ?A \wedge \neg ?B \wedge ?C$  **then have**  $?C$  by *simp*  
**then obtain**  $t'$  **where**  $lptp:l'||t'$  and  $t' || uu$  by *auto*  
**from**  $kl lp lpq$  **obtain**  $ll$  **where**  $kl:k||ll$  and  $llq:ll||q$  using *M5exist-var* by *blast*  
**with**  $lpq lptp$  **have**  $ll||t'$  using *M1* by *blast*  
**with**  $kp puu uuv kll llq qvp \langle t' || uu \rangle$  **have**  $(p,q) \in ov$  using *ov* by *blast*  
**thus** *?thesis* using *x* by *auto* }  
**qed**  
**qed**

**lemma** *covfi:ov*  $O f^{-1} \subseteq b \cup m \cup ov$

**proof**

**fix**  $x::'a \times 'a$  **assume**  $x \in ov O f^{-1}$  **then obtain**  $p q z$  **where**  $x:x = (p,q)$  and  $(p,z) \in ov$  and  $(z,q) \in f^{-1}$  by *auto*  
**from**  $\langle (p,z) \in ov \rangle$  **obtain**  $k u l c v$  **where**  $kp:k||p$  and  $pu:p||u$  and  $kl:k||l$  and  $lz:l||z$  and  $l||c$  and  $c||u$  and  $uv:u||v$  and  $zv:z||v$  using *ov* by *blast*  
**from**  $\langle (z,q) \in f^{-1} \rangle$  **obtain**  $k' l' v'$  **where**  $kplp:k'||l'$  and  $kpz:k'||z$  and  $lpq:l'||q$  and  $qvp:q||v'$  and  $zvp:z||v'$  using *f* by *blast*  
**from**  $lz kplp kpz$  **have**  $llp:l||l'$  using *M1* by *blast*  
**from**  $zv qvp zvp$  **have**  $qv:q||v$  using *M1* by *blast*  
**from**  $pu lpq$  **have**  $p||q \oplus ((\exists t. p||t \wedge t || q) \oplus (\exists t. l' || t \wedge t || u))$  (**is**  $?A \oplus (?B \oplus ?C)$ ) using *M2* by *blast*  
**then have**  $(?A \wedge \neg ?B \wedge \neg ?C) \vee ((\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C))$  by (*insert xor-distr-L*[of  $?A ?B ?C$ ], *auto simp:elimmeets*)  
**thus**  $x \in b \cup m \cup ov$   
**proof** (*elim disjE*)  
{ **assume**  $?A \wedge \neg ?B \wedge \neg ?C$  **then have**  $?A$  by *simp*

then have  $(p,q) \in m$  using  $m$  by *auto*  
 thus *?thesis* using  $x$  by *auto*  
 next  
 { assume  $\neg ?A \wedge ?B \wedge \neg ?C$  then have  $?B$  by *simp*  
 then have  $(p,q) \in b$  using  $b$  by *auto*  
 thus *?thesis* using  $x$  by *auto*  
 next  
 { assume  $\neg ?A \wedge \neg ?B \wedge ?C$  then have  $?C$  by *simp*  
 then obtain  $t$  where  $lptp:l'||t$  and  $t||u$  by *auto*  
 from  $kl\ lpq$  obtain  $ll$  where  $kll:k||ll$  and  $llr:ll||q$  using *M5exist-var*  
 by *blast*  
 with  $lpq\ lptp$  have  $ll||t$  using *M1* by *blast*  
 with  $kp\ pu\ uv\ kll\ llr\ qv\ \langle t||u \rangle$  have  $(p,q) \in ov$  using  $ov$  by *blast*  
 thus *?thesis* using  $x$  by *auto*  
 qed  
 qed

lemma *csov*:  $s\ O\ ov \subseteq b \cup m \cup ov$

proof

fix  $x::'a \times 'a$  assume  $x \in s\ O\ ov$  then obtain  $p\ q\ z$  where  $x:x = (p,q)$  and  
 $(p,z) \in s$  and  $(z,q) \in ov$  by *auto*  
 from  $\langle (p,z) \in s \rangle$  obtain  $k\ u\ v$  where  $kp:k||p$  and  $kz:k||z$  and  $pu:p||u$  and  
 $uv:u||v$  and  $zv:z||v$  using  $s$  by *blast*  
 from  $\langle (z,q) \in ov \rangle$  obtain  $k'\ l'\ u'\ v'$  where  $kpz:k'||z$  and  $kplp:k'||l'$  and  
 $lpq:l'||q$  and  $zup:z||u'$  and  $qvp:q||v'$  and  $upvp:u'||v'$  using  $ov$  by *blast*  
 from  $kz\ kpz\ kplp$  have  $klp:k||l'$  using *M1* by *blast*  
 from  $uv\ zv\ zup$  have  $uup:u||u'$  using *M1* by *blast*  
 with  $pu\ upvp$  obtain  $uu$  where  $puu:p||uu$  and  $uuvp:uu||v'$  using *M5exist-var*  
 by *blast*  
 from  $pu\ lpq$  have  $p||q \oplus ((\exists t. p||t \wedge t||q) \oplus (\exists t. l'||t \wedge t||u))$  (is  $?A \oplus (?B \oplus ?C)$ ) using *M2* by *blast*  
 then have  $(?A \wedge \neg ?B \wedge \neg ?C) \vee ((\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C))$  by (*insert xor-distr-L*[of  $?A\ ?B\ ?C$ ], *auto simp:elimmeets*)  
 thus  $x \in b \cup m \cup ov$   
 proof (*elim disjE*)  
 { assume  $?A \wedge \neg ?B \wedge \neg ?C$  then have  $?A$  by *simp*  
 then have  $(p,q) \in m$  using  $m$  by *auto*  
 thus *?thesis* using  $x$  by *auto*  
 next  
 { assume  $\neg ?A \wedge ?B \wedge \neg ?C$  then have  $?B$  by *simp*  
 then have  $(p,q) \in b$  using  $b$  by *auto*  
 thus *?thesis* using  $x$  by *auto*  
 next  
 { assume  $\neg ?A \wedge \neg ?B \wedge ?C$  then have  $?C$  by *simp*  
 then obtain  $t$  where  $lpt:l'||t$  and  $t||u$  by *auto*  
 with  $pu\ puu$  have  $t||uu$  using *M1* by *blast*  
 with  $lpt\ kp\ puu\ uuvp\ klp\ lpq\ qvp$  have  $(p,q) \in ov$  using  $ov$  by *blast*  
 thus *?thesis* using  $x$  by *auto*  
 }

qed  
qed

**lemma** *csfi*:  $s \circ f^{-1} \subseteq b \cup m \cup ov$

**proof**

**fix**  $x::'a \times 'a$  **assume**  $x \in s \circ f^{-1}$  **then obtain**  $p \ q \ r$  **where**  $x:x = (p,r)$  **and**  $(p,q) \in s$  **and**  $(q,r) \in f^{-1}$  **by** *auto*

**from**  $\langle (p,q) \in s \rangle$  **obtain**  $k \ u \ v$  **where**  $kp:k||p$  **and**  $kq:k||q$  **and**  $pu:p||u$  **and**  $uv:u||v$  **and**  $qv:q||v$  **using**  $s$  **by** *blast*

**from**  $\langle (q,r) \in f^{-1} \rangle$  **obtain**  $k' \ l \ v'$  **where**  $kpq:k'||q$  **and**  $kpl:k'||l$  **and**  $lr:l||r$  **and**  $rvp:r||v'$  **and**  $qvp:q||v'$  **using**  $f$  **by** *blast*

**from**  $kpq \ kpl \ kq$  **have**  $kl:k||l$  **using**  $M1$  **by** *blast*

**from**  $qvp \ qv \ uv$  **have**  $uwp:u||v'$  **using**  $M1$  **by** *blast*

**from**  $pu \ lr$  **have**  $p||r \oplus ((\exists t'. p||t' \wedge t'||r)) \oplus (\exists t'. l||t' \wedge t'||u)$  **(is**  $?A \oplus (?B \oplus ?C)$  **) using**  $M2$  **by** *blast*

**then have**  $(?A \wedge \neg ?B \wedge \neg ?C) \vee ((\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C))$  **by** (*insert xor-distr-L[of ?A ?B ?C], auto simp:elimmeets*)

**thus**  $x \in b \cup m \cup ov$

**proof** (*elim disjE*)

{ **assume**  $?A \wedge \neg ?B \wedge \neg ?C$  **then have**  $?A$  **by** *simp*

**then have**  $(p,r) \in m$  **using**  $m$  **by** *auto*

**thus**  $?thesis$  **using**  $x$  **by** *auto*}

**next**

{ **assume**  $\neg ?A \wedge ?B \wedge \neg ?C$  **then have**  $?B$  **by** *simp*

**then have**  $(p,r) \in b$  **using**  $b$  **by** *auto*

**thus**  $?thesis$  **using**  $x$  **by** *auto*}

**next**

{ **assume**  $\neg ?A \wedge \neg ?B \wedge ?C$  **then have**  $?C$  **by** *simp*

**then obtain**  $t'$  **where**  $ltp:l||t'$  **and**  $t'||u$  **by** *auto*

**with**  $kp \ pu \ uwp \ kl \ lr \ rvp$  **have**  $(p,r) \in ov$  **using**  $ov$  **by** *blast*

**thus**  $?thesis$  **using**  $x$  **by** *auto*}

qed

qed

We prove compositions of the form  $r_1 \circ r_2 \subseteq f \cup f^{-1} \cup e$ .

**lemma** *cmmi*:  $m \circ m^{-1} \subseteq f \cup f^{-1} \cup e$

**proof**

**fix**  $x::'a \times 'a$  **assume**  $x \in m \circ m^{-1}$  **then obtain**  $p \ q \ z$  **where**  $x:x = (p,q)$  **and**  $1:(p,z) \in m$  **and**  $2:(z,q) \in m^{-1}$  **by** *auto*

**then have**  $pz:p||z$  **and**  $qz:q||z$  **using**  $m$  **by** *auto*

**obtain**  $k \ k'$  **where**  $kp:k||p$  **and**  $kpq:k'||q$  **using**  $M3$  *meets-ud*  $qz \ pz$  **by** *blast*

**from**  $kp \ kpq$  **have**  $k||q \oplus ((\exists t. k||t \wedge t||q)) \oplus (\exists t. k'||t \wedge t||p)$  **(is**  $?A \oplus (?B \oplus ?C)$  **) using**  $M2$  **by** *blast*

**then have**  $(?A \wedge \neg ?B \wedge \neg ?C) \vee (\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C)$  **by** (*insert xor-distr-L[of ?A ?B ?C], auto simp:elimmeets*)

**thus**  $x \in f \cup f^{-1} \cup e$

**proof** (*elim disjE*)

{ **assume**  $(?A \wedge \neg ?B \wedge \neg ?C)$  **then have**  $?A$  **by** *simp*



**then have**  $p = q$  **using**  $M_4$   $kp$   $pz$   $qz$  **by** *blast*  
**then have**  $(p, q) \in e$  **using**  $e$  **by** *auto*  
**thus** *?thesis* **using**  $x$  **by** *simp* }  
**next**  
{**assume**  $(\neg ?A \wedge ?B \wedge \neg ?C)$  **then have**  $?B$  **by** *simp*  
**then obtain**  $t$  **where**  $kt:k||t$  **and**  $tq:t||q$  **by** *auto*  
**then have**  $(p, q) \in f^{-1}$  **using**  $f$   $qz$   $pz$   $kp$  **by** *blast*  
**thus** *?thesis* **using**  $x$  **by** *simp*}  
**next**  
{**assume**  $(\neg ?A \wedge \neg ?B \wedge ?C)$  **then have**  $?C$  **by** *simp*  
**then obtain**  $t$  **where**  $kt:k'||t$  **and**  $tp:t||p$  **by** *auto*  
**with**  $kpq$   $pz$   $qz$  **have**  $(p, q) \in f$  **using**  $f$  **by** *blast*  
**thus** *?thesis* **using**  $x$  **by** *simp*}  
**qed**  
**qed**

**lemma**  $cfif:f^{-1} \circ f \subseteq e \cup f^{-1} \cup f$

**proof**

**fix**  $x::'a \times 'a$  **assume**  $a:x \in f^{-1} \circ f$  **then obtain**  $p$   $q$   $z$  **where**  $x:x = (p, q)$  **and**  
 $1:(p, z) \in f^{-1}$  **and**  $2:(z, q) \in f$  **by** *auto*

**from**  $1$  **obtain**  $k$   $l$   $u$  **where**  $kp:k||p$  **and**  $kl:k||l$  **and**  $lz:l||z$  **and**  $zu:z||u$  **and**  $pu:p||u$   
**using**  $f$  **by** *blast*

**from**  $2$  **obtain**  $k'$   $l'$   $u'$  **where**  $kpq:k'||q$  **and**  $kplp:k'||l'$  **and**  $lpz:l'||z$  **and**  $zup:z||u'$   
**and**  $qup:q||u'$  **using**  $f$  **by** *blast*

**from**  $zu$   $zup$   $qup$  **have**  $qu:q||u$  **using**  $M1$  **by** *auto*

**from**  $kp$   $kpq$  **have**  $k||q \oplus ((\exists t. k||t \wedge t||q) \oplus (\exists t. k'||t \wedge t||p))$  **(is**  $?A \oplus (?B \oplus$   
 $?C)$  **using**  $M2$  **by** *blast*

**then have**  $(?A \wedge \neg ?B \wedge \neg ?C) \vee (\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C)$  **by** (*insert xor-distr-L*[of  
 $?A$   $?B$   $?C$ ], *auto simp:elimmeets*)

**thus**  $x \in e \cup f^{-1} \cup f$

**proof** (*elim disjE*)

{**assume**  $(?A \wedge \neg ?B \wedge \neg ?C)$  **then have**  $?A$  **by** *simp*

**then have**  $p = q$  **using**  $M_4$   $kp$   $pu$   $qu$  **by** *blast*

**then have**  $(p, q) \in e$  **using**  $e$  **by** *auto*

**thus** *?thesis* **using**  $x$  **by** *simp* }

**next**

{**assume**  $(\neg ?A \wedge ?B \wedge \neg ?C)$  **then have**  $?B$  **by** *simp*

**then obtain**  $t$  **where**  $kt:k||t$  **and**  $tq:t||q$  **by** *auto*

**then have**  $(p, q) \in f^{-1}$  **using**  $f$   $qu$   $pu$   $kp$  **by** *blast*

**thus** *?thesis* **using**  $x$  **by** *simp*}

**next**

{**assume**  $(\neg ?A \wedge \neg ?B \wedge ?C)$  **then have**  $?C$  **by** *simp*

**then obtain**  $t$  **where**  $kt:k'||t$  **and**  $tp:t||p$  **by** *auto*

**with**  $kpq$   $pu$   $qu$  **have**  $(p, q) \in f$  **using**  $f$  **by** *blast*

**thus** *?thesis* **using**  $x$  **by** *simp*}

**qed**

**qed**

**lemma** *cff*:  $f \circ f^{-1} \subseteq e \cup f \cup f^{-1}$

**proof**

**fix**  $x::'a \times 'a$  **assume**  $x \in f \circ f^{-1}$  **then obtain**  $p \ q \ r$  **where**  $x = (p, r)$  **and**  $(p, q) \in f$  **and**  $(q, r) \in f^{-1}$  **by** *auto*

**from**  $\langle (p, q) \in f \rangle \langle (q, r) \in f^{-1} \rangle$  **obtain**  $k \ k'$  **where**  $kp:k \parallel p$  **and**  $kpr:k' \parallel r$  **using** *f* **by** *blast*

**from**  $\langle (p, q) \in f \rangle \langle (q, r) \in f^{-1} \rangle$  **obtain**  $u$  **where**  $pu:p \parallel u$  **and**  $qu:q \parallel u$  **and**  $ru:r \parallel u$  **using** *f M1* **by** *blast*

**from**  $kp \ kpr$  **have**  $k \parallel r \oplus ((\exists t. k \parallel t \wedge t \parallel r) \oplus (\exists t. k' \parallel t \wedge t \parallel p))$  **(is**  $?A \oplus (?B \oplus ?C)$ **) using** *M2* **by** *blast*

**then have**  $(?A \wedge \neg ?B \wedge \neg ?C) \vee ((\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C))$  **by** (*insert xor-distr-L*[of  $?A \ ?B \ ?C$ ], *auto simp:elimmeets*)

**thus**  $x \in e \cup f \cup f^{-1}$

**proof** (*elim disjE*)

{ **assume**  $?A \wedge \neg ?B \wedge \neg ?C$  **then have**  $?A$  **by** *simp*  
**with**  $pu \ ru \ kp$  **have**  $p = r$  **using** *M4* **by** *auto*  
**thus** *?thesis* **using**  $x \ e$  **by** *auto* }

**next**

{ **assume**  $\neg ?A \wedge ?B \wedge \neg ?C$  **then have**  $?B$  **by** *simp*  
**then obtain**  $t$  **where**  $kt:k \parallel t$  **and**  $tr:t \parallel r$  **by** *auto*  
**with**  $ru \ kp \ pu$  **show** *?thesis* **using**  $x \ f$  **by** *blast* }

**next**

{ **assume**  $\neg ?A \wedge \neg ?B \wedge ?C$  **then have**  $?C$  **by** *simp*  
**then obtain**  $t$  **where**  $rtp:k' \parallel t$  **and**  $t \parallel p$  **by** *auto*  
**with**  $kpr \ ru \ pu$  **show** *?thesis* **using**  $x \ f$  **by** *blast* }

**qed**

**qed**

We prove compositions of the form  $r_1 \circ r_2 \subseteq e \cup s \cup s^{-1}$ .

**lemma** *css*:  $s \circ s^{-1} \subseteq e \cup s \cup s^{-1}$

**proof**

**fix**  $x::'a \times 'a$  **assume**  $x \in s \circ s^{-1}$  **then obtain**  $p \ q \ r$  **where**  $x = (p, r)$  **and**  $(p, q) \in s$  **and**  $(q, r) \in s^{-1}$  **by** *auto*

**from**  $\langle (p, q) \in s \rangle \langle (q, r) \in s^{-1} \rangle$  **obtain**  $k$  **where**  $kp:k \parallel p$  **and**  $kr:k \parallel r$  **and**  $kq:k \parallel q$  **using** *s M1* **by** *blast*

**from**  $\langle (p, q) \in s \rangle \langle (q, r) \in s^{-1} \rangle$  **obtain**  $u \ u'$  **where**  $pu:p \parallel u$  **and**  $rup:r \parallel u'$  **using** *s* **by** *blast*

**then have**  $p \parallel u' \oplus ((\exists t. p \parallel t \wedge t \parallel u') \oplus (\exists t. r \parallel t \wedge t \parallel u))$  **(is**  $?A \oplus (?B \oplus ?C)$ **) using** *M2* **by** *blast*

**then have**  $(?A \wedge \neg ?B \wedge \neg ?C) \vee ((\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C))$  **by** (*insert xor-distr-L*[of  $?A \ ?B \ ?C$ ], *auto simp:elimmeets*)

**thus**  $x \in e \cup s \cup s^{-1}$

**proof** (*elim disjE*)

{ **assume**  $?A \wedge \neg ?B \wedge \neg ?C$  **then have**  $?A$  **by** *simp*  
**with**  $rup \ kp \ kr$  **have**  $p = r$  **using** *M4* **by** *auto*  
**thus** *?thesis* **using**  $x \ e$  **by** *auto* }

**next**

{ **assume**  $\neg ?A \wedge ?B \wedge \neg ?C$  **then have**  $?B$  **by** *simp*  
**then obtain**  $t$  **where**  $kt:p \parallel t$  **and**  $tr:t \parallel u'$  **by** *auto* }

with  $rup\ kp\ kr$  show  $?thesis$  using  $x\ s$  by  $blast$ }  
 next  
 { assume  $\neg ?A \wedge \neg ?B \wedge ?C$  then have  $?C$  by  $simp$   
 then obtain  $t$  where  $rtp:r||t$  and  $t||u$  by  $auto$   
 with  $pu\ kp\ kr$  show  $?thesis$  using  $x\ s$  by  $blast$ }  
 qed  
 qed

lemma  $csis:s^{\wedge-1}\ O\ s \subseteq e \cup s \cup s^{\wedge-1}$

proof

fix  $x::'a \times 'a$  assume  $x \in s^{\wedge-1}\ O\ s$  then obtain  $p\ q\ r$  where  $x:x = (p,r)$  and  $(p,q) \in s^{\wedge-1}$  and  $(q,r) \in s$  by  $auto$

from  $\langle (p,q) \in s^{\wedge-1} \rangle \langle (q,r) \in s \rangle$  obtain  $k$  where  $kp:k||p$  and  $kr:k||r$  and  $kq:k||q$  using  $s\ M1$  by  $blast$

from  $\langle (p,q) \in s^{\wedge-1} \rangle \langle (q,r) \in s \rangle$  obtain  $u\ u'$  where  $pu:p||u$  and  $rup:r||u'$  using  $s$  by  $blast$

then have  $p||u' \oplus ((\exists t. p||t \wedge t||u') \oplus (\exists t. r||t \wedge t||u))$  (is  $?A \oplus (?B \oplus ?C)$ ) using  $M2$  by  $blast$

then have  $(?A \wedge \neg ?B \wedge \neg ?C) \vee ((\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C))$  by ( $insert\ xor\ distr\ L$ [of  $?A\ ?B\ ?C$ ],  $auto\ simp:elimmeets$ )

thus  $x \in e \cup s \cup s^{\wedge-1}$

proof ( $elim\ disjE$ )

{ assume  $?A \wedge \neg ?B \wedge \neg ?C$  then have  $?A$  by  $simp$   
 with  $rup\ kp\ kr$  have  $p = r$  using  $M4$  by  $auto$   
 thus  $?thesis$  using  $x\ e$  by  $auto$ }

next

{ assume  $\neg ?A \wedge ?B \wedge \neg ?C$  then have  $?B$  by  $simp$   
 then obtain  $t$  where  $kt:p||t$  and  $tr:t||u'$  by  $auto$   
 with  $rup\ kp\ kr$  show  $?thesis$  using  $x\ s$  by  $blast$ }

next

{ assume  $\neg ?A \wedge \neg ?B \wedge ?C$  then have  $?C$  by  $simp$   
 then obtain  $t$  where  $rtp:r||t$  and  $t||u$  by  $auto$   
 with  $pu\ kp\ kr$  show  $?thesis$  using  $x\ s$  by  $blast$ }

qed

qed

lemma  $cmim:m^{\wedge-1}\ O\ m \subseteq s \cup s^{\wedge-1} \cup e$

proof

fix  $x::'a \times 'a$  assume  $x \in m^{\wedge-1}\ O\ m$  then obtain  $p\ q\ r$  where  $x:x = (p,r)$  and  $(p,q) \in m^{\wedge-1}$  and  $(q,r) \in m$  by  $auto$

from  $\langle (p,q) \in m^{\wedge-1} \rangle \langle (q,r) \in m \rangle$  have  $qp:q||p$  and  $qr:q||r$  using  $m$  by  $auto$

obtain  $u\ u'$  where  $pu:p||u$  and  $rup:r||u'$  using  $M3\ meets\ wd\ qp\ qr$  by  $fastforce$

then have  $p||u' \oplus ((\exists t. p||t \wedge t||u') \oplus (\exists t. r||t \wedge t||u))$  (is  $?A \oplus (?B \oplus ?C)$ ) using  $M2$  by  $blast$

then have  $(?A \wedge \neg ?B \wedge \neg ?C) \vee ((\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C))$  by ( $insert\ xor\ distr\ L$ [of  $?A\ ?B\ ?C$ ],  $auto\ simp:elimmeets$ )

thus  $x \in s \cup s^{\wedge-1} \cup e$

proof ( $elim\ disjE$ )

{ assume  $?A \wedge \neg ?B \wedge \neg ?C$  then have  $?A$  by  $simp$

**with**  $rup\ qp\ qr$  **have**  $p = r$  **using**  $M4$  **by** *auto*  
**thus**  $?thesis$  **using**  $x\ e$  **by** *auto*  
**next**  
**{** **assume**  $\neg ?A \wedge ?B \wedge \neg ?C$  **then** **have**  $?B$  **by** *simp*  
**then** **obtain**  $t$  **where**  $kt:p||t$  **and**  $tr:t||u'$  **by** *auto*  
**with**  $rup\ qp\ qr$  **show**  $?thesis$  **using**  $x\ s$  **by** *blast*  
**next**  
**{** **assume**  $\neg ?A \wedge \neg ?B \wedge ?C$  **then** **have**  $?C$  **by** *simp*  
**then** **obtain**  $t$  **where**  $rtp:r||t$  **and**  $t||u$  **by** *auto*  
**with**  $pu\ qp\ qr$  **show**  $?thesis$  **using**  $x\ s$  **by** *blast*  
**qed**  
**qed**

### 3.4 $\beta$ -composition

We prove compositions of the form  $r_1 \circ r_2 \subseteq b \cup m \cup ov \cup s \cup d$ .

**lemma**  $cbd:b\ O\ d \subseteq b \cup m \cup ov \cup s \cup d$

**proof**

**fix**  $x::'a \times 'a$  **assume**  $x \in b\ O\ d$  **then** **obtain**  $p\ q\ z$  **where**  $x:x = (p,q)$  **and**  $(p,z) \in b$  **and**  $(z,q) \in d$  **by** *auto*

**from**  $\langle (p,q) \in b \rangle$  **obtain**  $c$  **where**  $pc:p||c$  **and**  $cz:c||z$  **using**  $b$  **by** *auto*

**obtain**  $a$  **where**  $ap:a||p$  **using**  $M3$  *meets-ud*  $pc$  **by** *blast*

**from**  $\langle (z,q) \in d \rangle$  **obtain**  $k\ l\ u\ v$  **where**  $k||l$  **and**  $l||z$  **and**  $kq:k||q$  **and**  $zu:z||u$  **and**  $uv:u||v$  **and**  $qv:q||v$  **using**  $d$  **by** *blast*

**from**  $pc\ cz\ zu$  **obtain**  $cz$  **where**  $pcz:p||cz$  **and**  $czu:cz||u$  **using**  $M5$  *exist-var* **by** *blast*

**with**  $uv$  **obtain**  $czu$  **where**  $pczu:p||czu$  **and**  $czuv:czu||v$  **using**  $M5$  *exist-var* **by** *blast*

**from**  $ap\ kq$  **have**  $a||q \oplus ((\exists t. a||t \wedge t||q) \oplus (\exists t. k||t \wedge t||p))$  **(is**  $?A \oplus (?B \oplus ?C)$  **) using**  $M2$  **by** *blast*

**then** **have**  $(?A \wedge \neg ?B \wedge \neg ?C) \vee ((\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C))$  **by** (*insert xor-distr-L*[of  $?A\ ?B\ ?C$ ], *auto simp:elimmeets*)

**thus**  $x \in b \cup m \cup ov \cup s \cup d$

**proof** (*elim disjE*)

**{** **assume**  $?A \wedge \neg ?B \wedge \neg ?C$  **then** **have**  $?A$  **by** *simp*

**with**  $ap\ pczu\ czuv\ uv\ qv$  **have**  $(p,q) \in s$  **using**  $s$  **by** *blast*

**thus**  $?thesis$  **using**  $x$  **by** *auto*  
**next**

**{** **assume**  $\neg ?A \wedge ?B \wedge \neg ?C$  **then** **have**  $?B$  **by** *simp*

**then** **obtain**  $t$  **where**  $at:a||t$  **and**  $tq:t||q$  **by** *auto*

**from**  $pc\ tq$  **have**  $p||q \oplus ((\exists t'. p||t' \wedge t'||q) \oplus (\exists t'. t||t' \wedge t'||c))$  **(is**  $?A \oplus (?B \oplus ?C)$  **) using**  $M2$  **by** *blast*

**then** **have**  $(?A \wedge \neg ?B \wedge \neg ?C) \vee ((\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C))$  **by** (*insert xor-distr-L*[of  $?A\ ?B\ ?C$ ], *auto simp:elimmeets*)

**thus**  $x \in b \cup m \cup ov \cup s \cup d$

**proof** (*elim disjE*)

**{** **assume**  $?A \wedge \neg ?B \wedge \neg ?C$  **then** **have**  $?A$  **by** *simp*

**thus**  $?thesis$  **using**  $x\ m$  **by** *auto*  
**next**

**next**

```

    { assume  $\neg ?A \wedge ?B \wedge \neg ?C$  then have  $?B$  by simp
      thus ?thesis using  $x b$  by auto }
  next
  { assume  $\neg ?A \wedge \neg ?B \wedge ?C$  then have  $?C$  by simp
    then obtain  $t'$  where  $t \parallel t'$  and  $t' \parallel c$  by auto
    with  $pc$   $pczu$  have  $t' \parallel czu$  using  $M1$  by auto
    with  $at$   $tq$   $ap$   $pczu$   $czuv$   $qv$   $\langle t \parallel t' \rangle$  have  $(p,q) \in ov$  using  $ov$  by blast
    thus ?thesis using  $x$  by auto }
  qed
}
next
{ assume  $\neg ?A \wedge \neg ?B \wedge ?C$  then have  $?C$  by simp
  then obtain  $t$  where  $k \parallel t$  and  $t \parallel p$  by auto
  with  $kq$   $pczu$   $czuv$   $wv$   $qv$  have  $(p,q) \in d$  using  $d$  by blast
  thus ?thesis using  $x$  by auto }
qed

lemma cbf:  $b \ O \ f \subseteq b \cup m \cup ov \cup s \cup d$ 
proof
  fix  $x::'a \times 'a$  assume  $x \in b \ O \ f$  then obtain  $p \ q \ z$  where  $x:x = (p,q)$  and  $(p,z) \in b$  and  $(z,q) \in f$  by auto
  from  $\langle (p,z) \in b \rangle$  obtain  $c$  where  $pc:p \parallel c$  and  $cz:c \parallel z$  using  $b$  by auto
  obtain  $a$  where  $ap:a \parallel p$  using  $M3$  meets-wd  $pc$  by blast
  from  $\langle (z,q) \in f \rangle$  obtain  $k \ l \ u$  where  $k \parallel l$  and  $l \parallel z$  and  $kq:k \parallel q$  and  $zu:z \parallel u$  and  $qu:q \parallel u$  using  $f$  by blast
  from  $pc$   $cz$   $zu$  obtain  $cz$  where  $pcz:p \parallel cz$  and  $czu:cz \parallel u$  using  $M5$  exist-var by blast
  from  $ap$   $kq$  have  $a \parallel q \oplus ((\exists t. a \parallel t \wedge t \parallel q) \oplus (\exists t. k \parallel t \wedge t \parallel p))$  (is  $?A \oplus (?B \oplus ?C)$ ) using  $M2$  by blast
  then have  $(?A \wedge \neg ?B \wedge \neg ?C) \vee ((\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C))$  by (insert xor-distr-L[of  $?A \ ?B \ ?C$ ], auto simp:elimmeets)
  thus  $x \in b \cup m \cup ov \cup s \cup d$ 
  proof (elim disjE)
    { assume  $?A \wedge \neg ?B \wedge \neg ?C$  then have  $?A$  by simp
      with  $ap$   $pcz$   $czu$   $qu$  have  $(p,q) \in s$  using  $s$  by blast
      thus ?thesis using  $x$  by auto }
  next
  { assume  $\neg ?A \wedge ?B \wedge \neg ?C$  then have  $?B$  by simp
    then obtain  $t$  where  $at:a \parallel t$  and  $tq:t \parallel q$  by auto
    from  $pc$   $tq$  have  $p \parallel q \oplus ((\exists t'. p \parallel t' \wedge t' \parallel q) \oplus (\exists t'. t \parallel t' \wedge t' \parallel c))$  (is  $?A \oplus (?B \oplus ?C)$ ) using  $M2$  by blast
    then have  $(?A \wedge \neg ?B \wedge \neg ?C) \vee ((\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C))$  by (insert xor-distr-L[of  $?A \ ?B \ ?C$ ], auto simp:elimmeets)
    thus  $x \in b \cup m \cup ov \cup s \cup d$ 
    proof (elim disjE)
      { assume  $?A \wedge \neg ?B \wedge \neg ?C$  then have  $?A$  by simp
        thus ?thesis using  $x m$  by auto }
    next

```

```

    { assume  $\neg ?A \wedge ?B \wedge \neg ?C$  then have  $?B$  by simp
      thus ?thesis using  $x b$  by auto }
  next
  { assume  $\neg ?A \wedge \neg ?B \wedge ?C$  then have  $?C$  by simp
    then obtain  $t'$  where  $t \parallel t'$  and  $t' \parallel c$  by auto
    with  $pc\ pcz$  have  $t' \parallel cz$  using M1 by auto
    with  $at\ tq\ ap\ pcz\ czu\ qu\ \langle t \parallel t' \rangle$  have  $(p,q) \in ov$  using ov by blast
    thus ?thesis using  $x$  by auto }
  qed
}
next
{ assume  $\neg ?A \wedge \neg ?B \wedge ?C$  then have  $?C$  by simp
  then obtain  $t$  where  $k \parallel t$  and  $t \parallel p$  by auto
  with  $kq\ pcz\ czu\ qu$  have  $(p,q) \in d$  using d by blast
  thus ?thesis using  $x$  by auto }
qed

lemma cbovi:  $b \cap O \overset{\wedge}{-} 1 \subseteq b \cup m \cup ov \cup s \cup d$ 
proof
  fix  $x :: 'a \times 'a$  assume  $x \in b \cap O \overset{\wedge}{-} 1$  then obtain  $p\ q\ z$  where  $x : x = (p,q)$  and
   $(p,z) \in b$  and  $(z,q) \in O \overset{\wedge}{-} 1$  by auto
  from  $\langle (p,z) \in b \rangle$  obtain  $c$  where  $pc : p \parallel c$  and  $cz : c \parallel z$  using b by auto
  obtain  $a$  where  $ap : a \parallel p$  using M3 meets-wd pc by blast
  from  $\langle (z,q) \in O \overset{\wedge}{-} 1 \rangle$  obtain  $k\ l\ u\ v\ w$  where  $k \parallel l$  and  $lz : l \parallel z$  and  $kq : k \parallel q$  and
   $zv : z \parallel v$  and  $qu : q \parallel u$  and  $wv : u \parallel v$  and  $lw : l \parallel w$  and  $wu : w \parallel u$  using ov by blast
  from  $cz\ lz\ lw$  have  $c \parallel w$  using M1 by auto
  with  $pc\ wu$  obtain  $cw$  where  $pcw : p \parallel cw$  and  $cwu : cw \parallel u$  using M5 exist-var by
  blast
  from  $ap\ kq$  have  $a \parallel q \oplus ((\exists t. a \parallel t \wedge t \parallel q) \oplus (\exists t. k \parallel t \wedge t \parallel p))$  (is  $?A \oplus (?B \oplus$ 
   $?C)$ ) using M2 by blast
  then have  $(?A \wedge \neg ?B \wedge \neg ?C) \vee ((\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C))$  by (insert
  xor-distr-L[of  $?A\ ?B\ ?C$ ], auto simp:elimmeets)
  thus  $x \in b \cup m \cup ov \cup s \cup d$ 
  proof (elim disjE)
    { assume  $?A \wedge \neg ?B \wedge \neg ?C$  then have  $?A$  by simp
      with  $ap\ qu\ pcw\ cwu$  have  $(p,q) \in s$  using s by blast
      thus ?thesis using  $x$  by auto }
  next
  { assume  $\neg ?A \wedge ?B \wedge \neg ?C$  then have  $?B$  by simp
    then obtain  $t$  where  $at : a \parallel t$  and  $tq : t \parallel q$  by auto
    from  $pc\ tq$  have  $p \parallel q \oplus ((\exists t'. p \parallel t' \wedge t' \parallel q) \oplus (\exists t'. t \parallel t' \wedge t' \parallel c))$  (is  $?A \oplus$ 
     $(?B \oplus ?C)$ ) using M2 by blast
    then have  $(?A \wedge \neg ?B \wedge \neg ?C) \vee ((\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C))$  by
    (insert xor-distr-L[of  $?A\ ?B\ ?C$ ], auto simp:elimmeets)
    thus  $x \in b \cup m \cup ov \cup s \cup d$ 
    proof (elim disjE)
      { assume  $?A \wedge \neg ?B \wedge \neg ?C$  then have  $?A$  by simp
        thus ?thesis using  $x\ m$  by auto }
    }
  }

```

```

next
{ assume  $\neg ?A \wedge ?B \wedge \neg ?C$  then have  $?B$  by simp
  thus ?thesis using  $x$   $b$  by auto }
next
{ assume  $\neg ?A \wedge \neg ?B \wedge ?C$  then have  $?C$  by simp
  then obtain  $t'$  where  $t \parallel t'$  and  $t' \parallel c$  by auto
  with  $pc$   $pcw$  have  $t' \parallel cw$  using  $M1$  by auto
  with  $at$   $tq$   $ap$   $pcw$   $cwu$   $qu$   $\langle t \parallel t' \rangle$  have  $(p,q) \in ov$  using  $ov$  by blast
  thus ?thesis using  $x$  by auto }
qed
}
next
{ assume  $\neg ?A \wedge \neg ?B \wedge ?C$  then have  $?C$  by simp
  then obtain  $t$  where  $k \parallel t$  and  $t \parallel p$  by auto
  with  $kq$   $pcw$   $cwu$   $qu$  have  $(p,q) \in d$  using  $d$  by blast
  thus ?thesis using  $x$  by auto }
qed
qed

lemma cbmi:  $b \cap m^{-1} \subseteq b \cup m \cup ov \cup s \cup d$ 
proof
  fix  $x::'a \times 'a$  assume  $x \in b \cap m^{-1}$  then obtain  $p$   $q$   $z$  where  $x = (p,q)$  and
   $(p,z) \in b$  and  $(z,q) \in m^{-1}$  by auto
  from  $\langle (p,z) \in b \rangle$  obtain  $c$  where  $pc:p \parallel c$  and  $cz:c \parallel z$  using  $b$  by auto
  obtain  $k$  where  $kp:k \parallel p$  using  $M3$  meets-wd  $pc$  by blast
  from  $\langle (z,q) \in m^{-1} \rangle$  have  $qz:q \parallel z$  using  $m$  by auto
  obtain  $k'$  where  $kpq:k' \parallel q$  using  $M3$  meets-wd  $qz$  by blast
  from  $kp$   $kpq$  have  $k \parallel q \oplus ((\exists t. k \parallel t \wedge t \parallel q) \oplus (\exists t. k' \parallel t \wedge t \parallel p))$  (is  $?A \oplus (?B \oplus ?C)$ ) using  $M2$  by blast
  then have  $(?A \wedge \neg ?B \wedge \neg ?C) \vee ((\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C))$  by (insert xor-distr-L[of  $?A$   $?B$   $?C$ ], auto simp:elimmeets)
  thus  $x \in b \cup m \cup ov \cup s \cup d$ 
  proof (elim disjE)
    { assume  $?A \wedge \neg ?B \wedge \neg ?C$  then have  $?A$  by simp
      with  $kp$   $pc$   $cz$   $qz$  have  $(p,q) \in s$  using  $s$  by blast
      thus ?thesis using  $x$  by auto }
    next
    { assume  $\neg ?A \wedge ?B \wedge \neg ?C$  then have  $?B$  by simp
      then obtain  $t$  where  $kt:k \parallel t$  and  $tq:t \parallel q$  by auto
      from  $pc$   $tq$  have  $p \parallel q \oplus ((\exists t'. p \parallel t' \wedge t' \parallel q) \oplus (\exists t'. t \parallel t' \wedge t' \parallel c))$  (is  $?A \oplus (?B \oplus ?C)$ ) using  $M2$  by blast
      then have  $(?A \wedge \neg ?B \wedge \neg ?C) \vee ((\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C))$  by
      (insert xor-distr-L[of  $?A$   $?B$   $?C$ ], auto simp:elimmeets)
      thus  $x \in b \cup m \cup ov \cup s \cup d$ 
      proof (elim disjE)
        { assume  $?A \wedge \neg ?B \wedge \neg ?C$  then have  $?A$  by simp
          thus ?thesis using  $x$   $m$  by auto }
        next
        { assume  $\neg ?A \wedge ?B \wedge \neg ?C$  then have  $?B$  by simp

```

```

      thus ?thesis using x b by auto}
    next
    { assume  $\neg ?A \wedge \neg ?B \wedge ?C$  then have  $?C$  by simp
      then obtain  $t'$  where  $t \parallel t'$  and  $t' \parallel c$  by auto
      with  $pc \ cz \ qz \ kt \ tq \ kp$  have  $(p,q) \in ov$  using  $ov$  by blast
      thus ?thesis using x b by auto}
  qed
}
next
{ assume  $\neg ?A \wedge \neg ?B \wedge ?C$  then have  $?C$  by simp
  then obtain  $t$  where  $k' \parallel t$  and  $t \parallel p$  by auto
  with  $kpq \ pc \ cz \ qz$  have  $(p,q) \in d$  using  $d$  by blast
  thus ?thesis using x b by auto}
qed
qed

```

lemma  $cdov:d \ O \ ov \subseteq b \cup m \cup ov \cup s \cup d$

proof

fix  $x::'a \times 'a$  assume  $x \in d \ O \ ov$  then obtain  $p \ q \ z$  where  $x:x = (p,q)$  and  $(p,z) \in d$  and  $(z,q) \in ov$  by auto

from  $\langle (p,z) \in d \rangle$  obtain  $k \ l \ u \ v$  where  $kl:k \parallel l$  and  $lp:l \parallel p$  and  $kz:k \parallel z$  and  $pu:p \parallel u$  and  $wv:u \parallel v$  and  $zv:z \parallel v$  using  $d$  by blast

from  $\langle (z,q) \in ov \rangle$  obtain  $k' \ l' \ u' \ v' \ c$  where  $kplp:k' \parallel l'$  and  $kpz:k' \parallel z$  and  $lpq:l' \parallel q$  and  $zup:z \parallel u'$  and  $upvp:u' \parallel v'$  and  $qvp:q \parallel v'$  and  $l' \parallel c$  and  $c \parallel u'$  using  $ov$  by blast

from  $zup \ zv \ uv$  have  $u \parallel u'$  using  $M1$  by auto

with  $pu \ upvp$  obtain  $uu$  where  $puu:p \parallel uu$  and  $uuvp:uu \parallel v'$  using  $M5exist-var$  by blast

from  $lp \ lpq$  have  $l \parallel q \oplus ((\exists t. l \parallel t \wedge t \parallel q) \oplus (\exists t. l' \parallel t \wedge t \parallel p))$  (is  $?A \oplus (?B \oplus ?C)$ ) using  $M2$  by blast

then have  $(?A \wedge \neg ?B \wedge \neg ?C) \vee ((\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C))$  by (insert  $xor-distr-L$ [of  $?A \ ?B \ ?C$ ], auto simp:elimmeets)

thus  $x \in b \cup m \cup ov \cup s \cup d$

proof (elim disjE)

{ assume  $?A \wedge \neg ?B \wedge \neg ?C$  then have  $?A$  by simp

with  $lp \ puu \ uuvp \ qvp$  have  $(p,q) \in s$  using  $s$  by blast

thus ?thesis using x b by auto}

next

{ assume  $\neg ?A \wedge ?B \wedge \neg ?C$  then have  $?B$  by simp

then obtain  $t$  where  $lt:l \parallel t$  and  $tq:t \parallel q$  by auto

from  $pu \ tq$  have  $p \parallel q \oplus ((\exists t'. p \parallel t' \wedge t' \parallel q) \oplus (\exists t'. t \parallel t' \wedge t' \parallel u))$  (is  $?A \oplus (?B \oplus ?C)$ ) using  $M2$  by blast

then have  $(?A \wedge \neg ?B \wedge \neg ?C) \vee ((\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C))$  by (insert  $xor-distr-L$ [of  $?A \ ?B \ ?C$ ], auto simp:elimmeets)

thus  $x \in b \cup m \cup ov \cup s \cup d$

proof (elim disjE)

{ assume  $?A \wedge \neg ?B \wedge \neg ?C$  then have  $?A$  by simp

thus ?thesis using x m by auto}

next

{ assume  $\neg ?A \wedge ?B \wedge \neg ?C$  then have  $?B$  by simp



```

      thus ?thesis using x b by auto}
    next
    { assume  $\neg ?A \wedge \neg ?B \wedge ?C$  then have ?C by simp
      then obtain t' where  $ttp:t||t'$  and  $t'||u$  by auto
      with pu puu have  $t'||uu$  using M1 by auto
      with lp puu qvp uwp lt tq ttp have  $(p,q) \in ov$  using ov by blast
      thus ?thesis using x by auto}
  qed
}
next
{ assume  $\neg ?A \wedge \neg ?B \wedge ?C$  then have ?C by simp
  then obtain t where  $l'||t$  and  $t||p$  by auto
  with lpq puu uwp qvp have  $(p,q) \in d$  using d by blast
  thus ?thesis using x by auto}
qed

lemma cdfi:d O f-1  $\subseteq b \cup m \cup ov \cup s \cup d$ 
proof
  fix x::'a  $\times$  'a assume  $x \in d$  O f-1 then obtain p q z where  $x:x = (p,q)$  and
   $(p,z) \in d$  and  $(z,q) \in f^{-1}$  by auto
  from  $\langle (p,z) \in d \rangle$  obtain k l u v where  $kl:k||l$  and  $lp:l||p$  and  $kz:k||z$  and  $pu:p||u$ 
  and  $wv:u||v$  and  $zv:z||v$  using d by blast
  from  $\langle (z,q) \in f^{-1} \rangle$  obtain k' l' u' where  $kpz:k'||z$  and  $kplp:k'||l'$  and  $lpq:l'||q$ 
  and  $zup:z||u'$  and  $qup:q||u'$  using f by blast
  from  $zup zv uv$  have  $uup:u||u'$  using M1 by auto
  from lp lpq have  $l||q \oplus ((\exists t. l||t \wedge t||q) \oplus (\exists t. l'||t \wedge t||p))$  (is ?A  $\oplus$  (?B  $\oplus$ 
  ?C)) using M2 by blast
  then have  $(?A \wedge \neg ?B \wedge \neg ?C) \vee ((\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C))$  by (insert
  xor-distr-L[of ?A ?B ?C], auto simp:elimmeets)
  thus  $x \in b \cup m \cup ov \cup s \cup d$ 
  proof (elim disjE)
    { assume  $?A \wedge \neg ?B \wedge \neg ?C$  then have ?A by simp
      with lp pu uwp qup have  $(p,q) \in s$  using s by blast
      thus ?thesis using x by auto}
  next
  { assume  $\neg ?A \wedge ?B \wedge \neg ?C$  then have ?B by simp
    then obtain t where  $lt:l||t$  and  $tq:t||q$  by auto
    from pu tq have  $p||q \oplus ((\exists t'. p||t' \wedge t'||q) \oplus (\exists t'. t||t' \wedge t'||u))$  (is ?A  $\oplus$ 
    (?B  $\oplus$  ?C)) using M2 by blast
    then have  $(?A \wedge \neg ?B \wedge \neg ?C) \vee ((\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C))$  by
    (insert xor-distr-L[of ?A ?B ?C], auto simp:elimmeets)
    thus  $x \in b \cup m \cup ov \cup s \cup d$ 
    proof (elim disjE)
      { assume  $?A \wedge \neg ?B \wedge \neg ?C$  then have ?A by simp
        thus ?thesis using x m by auto}
    next
    { assume  $\neg ?A \wedge ?B \wedge \neg ?C$  then have ?B by simp
      thus ?thesis using x b by auto}
  }
}

```

```

next
{ assume  $\neg ?A \wedge \neg ?B \wedge ?C$  then have  $?C$  by simp
  then obtain  $t'$  where  $ttp:t||t'$  and  $tpu:t'||u$  by auto
  with  $lt\ tq\ lp\ pu\ uup\ qup$  have  $(p,q) \in ov$  using ov by blast
  thus ?thesis using  $x$  by auto }
qed
}
next
{ assume  $\neg ?A \wedge \neg ?B \wedge ?C$  then have  $?C$  by simp
  then obtain  $t$  where  $l'||t$  and  $t||p$  by auto
  with  $lpq\ pu\ uup\ qup$  have  $(p,q) \in d$  using d by blast
  thus ?thesis using  $x$  by auto }
qed
qed

```

We prove compositions of the form  $r_1 \circ r_2 \subseteq b \cup m \cup ov \cup f^{-1} \cup d^{-1}$ .

**lemma** *covdi*:  $ov \ O \ d^{-1} \subseteq b \cup m \cup ov \cup f^{-1} \cup d^{-1}$

**proof**

fix  $x::'a \times 'a$  assume  $x \in ov \ O \ d^{-1}$  then obtain  $p\ q\ z$  where  $(p,z) : ov$  and  $(z,q) : d^{-1}$  and  $x:x = (p,q)$  by *auto*

from  $\langle (p,z) : ov \rangle$  obtain  $k\ l\ u\ v\ c$  where  $kp:k||p$  and  $kl:k||l$  and  $lz:l||z$  and  $pu:p||u$  and  $uv:u||v$  and  $zv:z||v$  and  $lc:l||c$  and  $cu:c||u$  using *ov* by *blast*

from  $\langle (z,q) : d^{-1} \rangle$  obtain  $l'\ k'\ u'\ v'$  where  $lpq:l'||q$  and  $kplp:k'||l'$  and  $kpz:k'||z$  and  $qup:q||u'$  and  $upvp:u'||v'$  and  $zvp:z||v'$  using *d* by *blast*

from  $lz\ kpz\ kplp$  have  $l||l'$  using *M1* by *auto*

with  $kl\ lpq$  obtain  $ll$  where  $kl:k||ll$  and  $llq:ll||q$  using *M5exist-var* by *blast*

from  $pu\ qup$  have  $p||u' \oplus ((\exists t. p||t \wedge t||u) \oplus (\exists t. q||t \wedge t||u))$  (is  $?A \oplus (?B \oplus ?C)$ ) using *M2* by *blast*

then have  $(?A \wedge \neg ?B \wedge \neg ?C) \vee ((\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C))$  by (*insert xor-distr-L*[of  $?A\ ?B\ ?C$ ], *auto simp:elimmeets*)

thus  $x \in b \cup m \cup ov \cup f^{-1} \cup d^{-1}$

**proof** (*elim disjE*)

{ assume  $?A \wedge \neg ?B \wedge \neg ?C$  then have  $?A$  by *simp*

with  $qup\ kll\ llq\ kp$  have  $(p,q) \in f^{-1}$  using *f* by *blast*

thus *?thesis* using  $x$  by *auto* }

**next**

{ assume  $\neg ?A \wedge ?B \wedge \neg ?C$  then have  $?B$  by *simp*

then obtain  $t$  where  $pt:p||t$  and  $tup:t||u'$  by *auto*

from  $pt\ lpq$  have  $p||q \oplus ((\exists t'. p||t' \wedge t'||q) \oplus (\exists t'. l'||t' \wedge t'||t))$  (is  $?A \oplus (?B \oplus ?C)$ ) using *M2* by *blast*

then have  $(?A \wedge \neg ?B \wedge \neg ?C) \vee ((\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C))$  by (*insert xor-distr-L*[of  $?A\ ?B\ ?C$ ], *auto simp:elimmeets*)

thus  $x \in b \cup m \cup ov \cup f^{-1} \cup d^{-1}$

**proof** (*elim disjE*)

{ assume  $?A \wedge \neg ?B \wedge \neg ?C$  then have  $?A$  by *simp*

thus *?thesis* using  $x\ m$  by *auto* }

**next**

{ assume  $\neg ?A \wedge ?B \wedge \neg ?C$  then have  $?B$  by *simp*

thus *?thesis* using  $x\ b$  by *auto* }

```

next
{ assume  $\neg ?A \wedge \neg ?B \wedge ?C$  then have  $?C$  by simp
  then obtain  $t'$  where  $lptp:l'||t'$  and  $tpt:t'||t$  by auto
  from  $lpq\ lptp\ llq$  have  $ll||t'$  using M1 by auto
  with  $kp\ kll\ llq\ pt\ tup\ qup\ tpt$  have  $(p,q) \in ov$  using ov by blast
  thus ?thesis using  $x$  by auto }
qed
}
next
{ assume  $\neg ?A \wedge \neg ?B \wedge ?C$  then have  $?C$  by simp
  then obtain  $t$  where  $q||t$  and  $t||u$  by auto
  with  $pu\ kll\ llq\ kp$  have  $(p,q) \in d^{\wedge-1}$  using d by blast
  thus ?thesis using  $x$  by auto }
qed
qed

lemma cdib:  $d^{\wedge-1} O b \subseteq b \cup m \cup ov \cup f^{\wedge-1} \cup d^{\wedge-1}$ 
proof
  fix  $x::'a \times 'a$  assume  $x \in d^{\wedge-1} O b$  then obtain  $p\ q\ z$  where  $(p,z) : d^{\wedge-1}$  and
   $(z,q) : b$  and  $x:x = (p,q)$  by auto
  from  $\langle (p,z) : d^{\wedge-1} \rangle$  obtain  $k\ l\ u\ v$  where  $kp:k||p$  and  $kl:k||l$  and  $lz:l||z$  and
   $pv:p||v$  and  $uv:u||v$  and  $zu:z||u$  using d by blast
  from  $\langle (z,q) : b \rangle$  obtain  $c$  where  $zc:z||c$  and  $cq:c||q$  using b by blast
  with  $kl\ lz$  obtain  $lzc$  where  $klzc:k||lzc$  and  $lzcq:lzc||q$  using M5exist-var by
  blast
  obtain  $v'$  where  $qvp:q||v'$  using M3 meets-wd cq by blast
  from  $pv\ qvp$  have  $p||v' \oplus ((\exists t. p||t \wedge t||v') \oplus (\exists t. q||t \wedge t||v))$  (is  $?A \oplus (?B \oplus ?C)$ ) using M2 by blast
  then have  $(?A \wedge \neg ?B \wedge \neg ?C) \vee ((\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C))$  by (insert xor-distr-L[of ?A ?B ?C], auto simp:elimmeets)
  thus  $x \in b \cup m \cup ov \cup f^{\wedge-1} \cup d^{\wedge-1}$ 
  proof (elim disjE)
    { assume  $?A \wedge \neg ?B \wedge \neg ?C$  then have  $?A$  by simp
      with  $qvp\ kp\ klzc\ lzcq$  have  $(p,q) \in f^{\wedge-1}$  using f by blast
      thus ?thesis using  $x$  by auto }
    next
    { assume  $\neg ?A \wedge ?B \wedge \neg ?C$  then have  $?B$  by simp
      then obtain  $t$  where  $pt:p||t$  and  $tvp:t||v'$  by auto
      from  $pt\ cq$  have  $p||q \oplus ((\exists t'. p||t' \wedge t'||q) \oplus (\exists t'. c||t' \wedge t'||t))$  (is  $?A \oplus (?B \oplus ?C)$ ) using M2 by blast
      then have  $(?A \wedge \neg ?B \wedge \neg ?C) \vee ((\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C))$  by
      (insert xor-distr-L[of ?A ?B ?C], auto simp:elimmeets)
      thus  $x \in b \cup m \cup ov \cup f^{\wedge-1} \cup d^{\wedge-1}$ 
      proof (elim disjE)
        { assume  $?A \wedge \neg ?B \wedge \neg ?C$  then have  $?A$  by simp
          thus ?thesis using  $x\ m$  by auto }
        next
        { assume  $\neg ?A \wedge ?B \wedge \neg ?C$  then have  $?B$  by simp
          thus ?thesis using  $x\ b$  by auto }
      }
  }

```

```

next
{ assume  $\neg ?A \wedge \neg ?B \wedge ?C$  then have  $?C$  by simp
  then obtain  $t'$  where  $ctp:c||t'$  and  $tpt:t'||t$  by auto
  from  $lzcq\ cq\ ctp$  have  $lzc||t'$  using  $M1$  by auto
  with  $pt\ tvp\ qvp\ kp\ klzc\ lzcq\ tpt$  have  $(p,q) \in ov$  using  $ov$  by blast
  thus  $?thesis$  using  $x$  by auto }
qed
}
next
{ assume  $\neg ?A \wedge \neg ?B \wedge ?C$  then have  $?C$  by simp
  then obtain  $t$  where  $q||t$  and  $t||v$  by auto
  with  $pv\ kp\ klzc\ lzcq$  have  $(p,q) \in d^{\wedge-1}$  using  $d$  by blast
  thus  $?thesis$  using  $x$  by auto }
qed
qed

lemma  $csdi:s\ O\ d^{\wedge-1} \subseteq b \cup m \cup ov \cup f^{\wedge-1} \cup d^{\wedge-1}$ 
proof
  fix  $x::'a \times 'a$  assume  $x \in s\ O\ d^{\wedge-1}$  then obtain  $p\ q\ z$  where  $(p,z) : s$  and
   $(z,q) : d^{\wedge-1}$  and  $x:x = (p,q)$  by auto
  from  $\langle (p,z) : s \rangle$  obtain  $k\ u\ v$  where  $kp:k||p$  and  $kz:k||z$  and  $pu:p||u$  and
   $uv:u||v$  and  $zv:z||v$  using  $s$  by blast
  from  $\langle (z,q) : d^{\wedge-1} \rangle$  obtain  $l'\ k'\ u'\ v'$  where  $lpq:l'||q$  and  $kplp:k'||l'$  and
   $kpz:k'||z$  and  $qvp:q||u'$  and  $upvp:u'||v'$  and  $zvp:z||v'$  using  $d$  by blast
  from  $kp\ kz\ kpz$  have  $kpp:k'||p$  using  $M1$  by auto
  from  $pu\ qvp$  have  $p||u' \oplus ((\exists t. p||t \wedge t||u')) \oplus (\exists t. q||t \wedge t||u)$  (is  $?A \oplus (?B \oplus ?C)$ ) using  $M2$  by blast
  then have  $(?A \wedge \neg ?B \wedge \neg ?C) \vee ((\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C))$  by (insert xor-distr-L[of  $?A\ ?B\ ?C$ ], auto simp:elimmeets)
  thus  $x \in b \cup m \cup ov \cup f^{\wedge-1} \cup d^{\wedge-1}$ 
  proof (elim disjE)
    { assume  $?A \wedge \neg ?B \wedge \neg ?C$  then have  $?A$  by simp
      with  $qvp\ kpp\ kplp\ lpq$  have  $(p,q) \in f^{\wedge-1}$  using  $f$  by blast
      thus  $?thesis$  using  $x$  by auto }
    next
    { assume  $\neg ?A \wedge ?B \wedge \neg ?C$  then have  $?B$  by simp
      then obtain  $t$  where  $pt:p||t$  and  $tup:t||u'$  by auto
      from  $pt\ lpq$  have  $p||q \oplus ((\exists t'. p||t' \wedge t'||q) \oplus (\exists t'. l'||t' \wedge t'||t))$  (is  $?A \oplus (?B \oplus ?C)$ ) using  $M2$  by blast
      then have  $(?A \wedge \neg ?B \wedge \neg ?C) \vee ((\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C))$  by
      (insert xor-distr-L[of  $?A\ ?B\ ?C$ ], auto simp:elimmeets)
      thus  $x \in b \cup m \cup ov \cup f^{\wedge-1} \cup d^{\wedge-1}$ 
      proof (elim disjE)
        { assume  $?A \wedge \neg ?B \wedge \neg ?C$  then have  $?A$  by simp
          thus  $?thesis$  using  $x\ m$  by auto }
        next
        { assume  $\neg ?A \wedge ?B \wedge \neg ?C$  then have  $?B$  by simp
          thus  $?thesis$  using  $x\ b$  by auto }
        next
        { assume  $\neg ?A \wedge \neg ?B \wedge ?C$  then have  $?C$  by simp
          thus  $?thesis$  using  $x$  by auto }
      }
  }

```

```

      { assume  $\neg ?A \wedge \neg ?B \wedge ?C$  then have  $?C$  by simp
        then obtain  $t'$  where  $lpt:l'\|t'$  and  $tpt:t'\|t$  by auto
        with  $pt\ tup\ qup\ kpp\ kplp\ lpq$  have  $(p,q) \in ov$  using ov by blast
        thus ?thesis using  $x$  by auto }
    qed
  }
next
{ assume  $\neg ?A \wedge \neg ?B \wedge ?C$  then have  $?C$  by simp
  then obtain  $t$  where  $q\|t$  and  $t\|u$  by auto
  with  $pu\ kpp\ kplp\ lpq$  have  $(p,q) \in d^{\wedge-1}$  using  $d$  by blast
  thus ?thesis using  $x$  by auto }
qed
qed

lemma csib:  $s^{\wedge-1} O b \subseteq b \cup m \cup ov \cup f^{\wedge-1} \cup d^{\wedge-1}$ 
proof
  fix  $x::'a \times 'a$  assume  $x \in s^{\wedge-1} O b$  then obtain  $p\ q\ z$  where  $(p,z) : s^{\wedge-1}$  and
 $(z,q) : b$  and  $x:x = (p,q)$  by auto
  from  $\langle (p,z) : s^{\wedge-1} \rangle$  obtain  $k\ u\ v$  where  $kp:k\|p$  and  $kz:k\|z$  and  $zu:z\|u$  and
 $uv:u\|v$  and  $pv:p\|v$  using  $s$  by blast
  from  $\langle (z,q) : b \rangle$  obtain  $c$  where  $zc:z\|c$  and  $cq:c\|q$  using  $b$  by blast
  from  $kz\ zc\ cq$  obtain  $zc$  where  $kzc:k\|zc$  and  $zcq:zc\|q$  using M5exist-var by
blast
  obtain  $v'$  where  $qvp:q\|v'$  using M3 meets-wd cq by blast
  from  $pv\ qvp$  have  $p\|v' \oplus ((\exists t. p\|t \wedge t\|v') \oplus (\exists t. q\|t \wedge t\|v))$  (is  $?A \oplus (?B \oplus ?C)$ ) using M2 by blast
  then have  $(?A \wedge \neg ?B \wedge \neg ?C) \vee ((\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C))$  by (insert xor-distr-L[of  $?A\ ?B\ ?C$ ], auto simp:elimmeets)
  thus  $x \in b \cup m \cup ov \cup f^{\wedge-1} \cup d^{\wedge-1}$ 
  proof (elim disjE)
    { assume  $?A \wedge \neg ?B \wedge \neg ?C$  then have  $?A$  by simp
      with  $qvp\ kp\ kzc\ zcq$  have  $(p,q) \in f^{\wedge-1}$  using  $f$  by blast
      thus ?thesis using  $x$  by auto }
  next
  { assume  $\neg ?A \wedge ?B \wedge \neg ?C$  then have  $?B$  by simp
    then obtain  $t$  where  $pt:p\|t$  and  $tvp:t\|v'$  by auto
    from  $pt\ cq$  have  $p\|q \oplus ((\exists t'. p\|t' \wedge t'\|q) \oplus (\exists t'. c\|t' \wedge t'\|t))$  (is  $?A \oplus (?B \oplus ?C)$ ) using M2 by blast
    then have  $(?A \wedge \neg ?B \wedge \neg ?C) \vee ((\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C))$  by
    (insert xor-distr-L[of  $?A\ ?B\ ?C$ ], auto simp:elimmeets)
    thus  $x \in b \cup m \cup ov \cup f^{\wedge-1} \cup d^{\wedge-1}$ 
    proof (elim disjE)
      { assume  $?A \wedge \neg ?B \wedge \neg ?C$  then have  $?A$  by simp
        thus ?thesis using  $x\ m$  by auto }
    next
      { assume  $\neg ?A \wedge ?B \wedge \neg ?C$  then have  $?B$  by simp
        thus ?thesis using  $x\ b$  by auto }
    next
      { assume  $\neg ?A \wedge \neg ?B \wedge ?C$  then have  $?C$  by simp

```

**then obtain  $t'$  where  $ctp:c||t'$  and  $tpt:t'||t$  by *auto***  
**from  $zcq\ cq\ ctp$  have  $zc||t'$  using  $M1$  by *auto***  
**with  $zcq\ pt\ tvp\ qvp\ kzc\ kp\ ctp\ tpt$  have  $(p,q) \in ov$  using  $ov$  by *blast***  
**thus *?thesis* using  $x$  by *auto*}**  
**qed**  
**}**  
**next**  
**{ assume  $\neg ?A \wedge \neg ?B \wedge ?C$  then have  $?C$  by *simp***  
****then obtain  $t$  where  $q||t$  and  $t||v$  by *auto*****  
****with  $pv\ kp\ kzc\ zcq$  have  $(p,q) \in d^{\wedge-1}$  using  $d$  by *blast*****  
****thus *?thesis* using  $x$  by *auto*}****  
**qed**  
**qed**

lemma *covib*:  $ov^{\wedge-1} O\ b \subseteq b \cup m \cup ov \cup f^{\wedge-1} \cup d^{\wedge-1}$

**proof**

**fix  $x::'a \times 'a$  assume  $x \in ov^{\wedge-1} O\ b$  then obtain  $p\ q\ z$  where  $(p,z) : ov^{\wedge-1}$**   
**and  $(z,q) : b$  and  $x:x = (p,q)$  by *auto***

**from  $\langle (p,z) : ov^{\wedge-1} \rangle$  obtain  $k\ l\ u\ v\ c$  where  $kz:k||z$  and  $kl:k||l$  and  $lp:l||p$  and**  
 **$zu:z||u$  and  $wv:u||v$  and  $pv:p||v$  and  $lc:l||c$  and  $cu:c||u$  using  $ov$  by *blast***

**from  $\langle (z,q) : b \rangle$  obtain  $w$  where  $zw:z||w$  and  $wq:w||q$  using  $b$  by *blast***

**from  $cu\ zu\ zw$  have  $cw:c||w$  using  $M1$  by *auto***

**with  $lc\ wq$  obtain  $cw$  where  $lcw:l||cw$  and  $cwq:cw||q$  using  $M5$  *exist-var* by**  
*blast*

**obtain  $v'$  where  $qvp:q||v'$  using  $M3$  *meets-wd*  $wq$  by *blast***

**from  $pv\ qvp$  have  $p||v' \oplus ((\exists t. p||t \wedge t||v') \oplus (\exists t. q||t \wedge t||v))$  (is  $?A \oplus (?B \oplus$   
 $?C)$ ) using  $M2$  by *blast***

**then have  $(?A \wedge \neg ?B \wedge \neg ?C) \vee ((\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C))$  by (*insert***  
*xor-distr-L*[of  $?A\ ?B\ ?C$ ], *auto simp:elimmeets*)

**thus  $x \in b \cup m \cup ov \cup f^{\wedge-1} \cup d^{\wedge-1}$**

**proof (*elim disjE*)**

**{ assume  $?A \wedge \neg ?B \wedge \neg ?C$  then have  $?A$  by *simp***

****with  $qvp\ lp\ lcw\ cwq$  have  $(p,q) \in f^{\wedge-1}$  using  $f$  by *blast*****

****thus *?thesis* using  $x$  by *auto*}****

**next**

**{ assume  $\neg ?A \wedge ?B \wedge \neg ?C$  then have  $?B$  by *simp***

****then obtain  $t$  where  $pt:p||t$  and  $tvp:t||v'$  by *auto*****

****from  $pt\ wq$  have  $p||q \oplus ((\exists t'. p||t' \wedge t'||q) \oplus (\exists t'. w||t' \wedge t'||t))$  (is  $?A \oplus$   
 $(?B \oplus ?C)$ ) using  $M2$  by *blast*****

****then have  $(?A \wedge \neg ?B \wedge \neg ?C) \vee ((\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C))$  by****  
*(insert xor-distr-L*[of  $?A\ ?B\ ?C$ ], *auto simp:elimmeets*)

****thus  $x \in b \cup m \cup ov \cup f^{\wedge-1} \cup d^{\wedge-1}$****

****proof (*elim disjE*)****

****{ assume  $?A \wedge \neg ?B \wedge \neg ?C$  then have  $?A$  by *simp*****

****thus *?thesis* using  $x\ m$  by *auto*}****

****next****

****{ assume  $\neg ?A \wedge ?B \wedge \neg ?C$  then have  $?B$  by *simp*****

****thus *?thesis* using  $x\ b$  by *auto*}****

****next****

```

      { assume  $\neg ?A \wedge \neg ?B \wedge ?C$  then have  $?C$  by simp
        then obtain  $t'$  where  $wtp:w||t'$  and  $tpt:t'||t$  by auto
        moreover with  $wq\ cwq$  have  $cw||t'$  using  $M1$  by auto
        ultimately have  $(p,q) \in ov$  using  $ov\ cwq\ lp\ lcw\ pt\ tvp\ qvp$  by blast
        thus ?thesis using  $x$  by auto }
    qed
  }
next
{ assume  $\neg ?A \wedge \neg ?B \wedge ?C$  then have  $?C$  by simp
  then obtain  $t$  where  $q||t$  and  $t||v$  by auto
  with  $pv\ lp\ lcw\ cwq$  have  $(p,q) \in d^{\wedge-1}$  using  $d$  by blast
  thus ?thesis using  $x$  by auto }
qed
qed

lemma cmib:  $m^{\wedge-1} O b \subseteq b \cup m \cup ov \cup f^{\wedge-1} \cup d^{\wedge-1}$ 
proof
  fix  $x::'a \times 'a$  assume  $x \in m^{\wedge-1} O b$  then obtain  $p\ q\ z$  where  $(p,z) : m^{\wedge-1}$ 
  and  $(z,q) : b$  and  $x:x = (p,q)$  by auto
  from  $\langle (p,z) : m^{\wedge-1} \rangle$  have  $zp:z||p$  using  $m$  by auto
  from  $\langle (z,q) : b \rangle$  obtain  $w$  where  $zw:z||w$  and  $wq:w||q$  using  $b$  by blast
  obtain  $v$  where  $pv:p||v$  using  $M3$  meets-wd  $zp$  by blast
  obtain  $v'$  where  $qvp:q||v'$  using  $M3$  meets-wd  $wq$  by blast

  from  $pv\ qvp$  have  $p||v' \oplus ((\exists t. p||t \wedge t||v') \oplus (\exists t. q||t \wedge t||v))$  (is  $?A \oplus (?B \oplus ?C)$ ) using  $M2$  by blast
  then have  $(?A \wedge \neg ?B \wedge \neg ?C) \vee ((\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C))$  by (insert xor-distr-L[of  $?A\ ?B\ ?C$ ], auto simp:elimmeets)
  thus  $x \in b \cup m \cup ov \cup f^{\wedge-1} \cup d^{\wedge-1}$ 
  proof (elim disjE)
    { assume  $?A \wedge \neg ?B \wedge \neg ?C$  then have  $?A$  by simp
      with  $zp\ zw\ wq\ qvp$  have  $(p,q) \in f^{\wedge-1}$  using  $f$  by blast
      thus ?thesis using  $x$  by auto }
  next
  { assume  $\neg ?A \wedge ?B \wedge \neg ?C$  then have  $?B$  by simp
    then obtain  $t$  where  $pt:p||t$  and  $tvp:t||v'$  by auto
    from  $pt\ wq$  have  $p||q \oplus ((\exists t'. p||t' \wedge t'||q) \oplus (\exists t'. w||t' \wedge t'||t))$  (is  $?A \oplus (?B \oplus ?C)$ ) using  $M2$  by blast
    then have  $(?A \wedge \neg ?B \wedge \neg ?C) \vee ((\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C))$  by (insert xor-distr-L[of  $?A\ ?B\ ?C$ ], auto simp:elimmeets)
    thus  $x \in b \cup m \cup ov \cup f^{\wedge-1} \cup d^{\wedge-1}$ 
    proof (elim disjE)
      { assume  $?A \wedge \neg ?B \wedge \neg ?C$  then have  $?A$  by simp
        thus ?thesis using  $x\ m$  by auto }
    next
      { assume  $\neg ?A \wedge ?B \wedge \neg ?C$  then have  $?B$  by simp
        thus ?thesis using  $x\ b$  by auto }
    next
      { assume  $\neg ?A \wedge \neg ?B \wedge ?C$  then have  $?C$  by simp

```

**then obtain  $t'$  where  $wtp:w||t'$  and  $tpt:t'||t$  by *auto***  
**with  $zp\ zw\ wq\ pt\ tvp\ qvp$  have  $(p,q) \in ov$  using *ov* by *blast***  
**thus *?thesis* using  $x$  by *auto*}**  
**qed**  
**}**  
**next**  
**{ assume  $\neg ?A \wedge \neg ?B \wedge ?C$  then have  $?C$  by *simp***  
**then obtain  $t$  where  $q||t$  and  $t||v$  by *auto***  
**with  $zp\ zw\ wq\ pv$  have  $(p,q) \in d^{-1}$  using *d* by *blast***  
**thus *?thesis* using  $x$  by *auto*}**  
**qed**  
**qed**

### 3.5 $\gamma$ -composition

We prove compositions of the form  $r_1 \circ r_2 \subseteq ov \cup s \cup d \cup f \cup e \cup f^{-1} \cup d^{-1} \cup s^{-1} \cup ov^{-1}$ .

**lemma *covovi*:  $ov \ O\ ov^{-1} \subseteq e \cup ov \cup ov^{-1} \cup d \cup d^{-1} \cup s \cup s^{-1} \cup f \cup f^{-1}$**

**proof**

**fix  $x::'a \times 'a$  assume  $x \in ov \ O\ ov^{-1}$  then obtain  $p\ q\ z$  where  $x:x = (p,q)$  and  $(p,z) \in ov$  and  $(z, q) \in ov^{-1}$  by *auto***

**from  $\langle (p,z) \in ov \rangle$  obtain  $k\ l\ c\ u$  where  $kp:k||p$  and  $kl:k||l$  and  $lz:l||z$  and  $lc:l||c$  and  $pu:p||u$  and  $cu:c||u$  using *ov* by *blast***

**from  $\langle (z,q) \in ov^{-1} \rangle$  obtain  $k'\ l'\ c'\ u'$  where  $kpq:k'||q$  and  $kplp:k'||l'$  and  $lpz:l'||z$  and  $lpcp:l'||c'$  and  $qup:q||u'$  and  $cpup:c'||u'$  using *ov* by *blast***

**from  $kp\ kpq$  have  $k||q \oplus ((\exists t. k||t \wedge t||q) \oplus (\exists t. k'||t \wedge t||p))$  (is  $?A \oplus (?B \oplus ?C)$ ) using *M2* by *blast***

**then have  $(?A \wedge \neg ?B \wedge \neg ?C) \vee ((\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C))$  by (*insert xor-distr-L*[of  $?A\ ?B\ ?C$ ], *auto simp:elimmeets*)**

**thus  $x \in e \cup ov \cup ov^{-1} \cup d \cup d^{-1} \cup s \cup s^{-1} \cup f \cup f^{-1}$**

**proof (*elim disjE*)**

**{ assume  $?A \wedge \neg ?B \wedge \neg ?C$  then have  $kq:?A$  by *simp***

**from  $pu\ qup$  have  $p||u' \oplus ((\exists t'. p||t' \wedge t'||u') \oplus (\exists t'. q||t' \wedge t'||u))$  (is  $?A \oplus (?B \oplus ?C)$ ) using *M2* by *blast***

**then have  $(?A \wedge \neg ?B \wedge \neg ?C) \vee ((\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C))$  by (*insert xor-distr-L*[of  $?A\ ?B\ ?C$ ], *auto simp:elimmeets*)**

**thus *?thesis***

**proof (*elim disjE*)**

**{ assume  $?A \wedge \neg ?B \wedge \neg ?C$  then have  $?A$  by *simp***

**with  $kq\ kp\ qup$  have  $p = q$  using *M4* by *auto***

**thus *?thesis* using  $x\ e$  by *auto*}**

**next**

**{ assume  $\neg ?A \wedge ?B \wedge \neg ?C$  then have  $?B$  by *simp***

**with  $kq\ kp\ qup$  show *?thesis* using  $x\ s$  by *blast*}**

**next**

**{ assume  $\neg ?A \wedge \neg ?B \wedge ?C$  then have  $?C$  by *simp***

**with  $kq\ kp\ pu$  show *?thesis* using  $x\ s$  by *blast*}**



```

qed}
next
{ assume  $\neg ?A \wedge ?B \wedge \neg ?C$  then have  $?B$  by simp
  then obtain  $t$  where  $kt:k||t$  and  $tq:t||q$  by auto
  from  $pu\ qup$  have  $p||u' \oplus ((\exists t'. p||t' \wedge t'||u')) \oplus (\exists t'. q||t' \wedge t'||u)$  (is  $?A$ 
 $\oplus (?B \oplus ?C)$ ) using  $M2$  by blast
  then have  $(?A \wedge \neg ?B \wedge \neg ?C) \vee ((\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C))$  by
(insert xor-distr-L[of  $?A\ ?B\ ?C$ ], auto simp:elimmeets)
  thus  $?thesis$ 
proof (elim disjE)
  { assume  $?A \wedge \neg ?B \wedge \neg ?C$  then have  $?A$  by simp
    with  $qup\ kp\ kt\ tq$  show  $?thesis$  using  $x\ f$  by blast}
  next
  { assume  $\neg ?A \wedge ?B \wedge \neg ?C$  then have  $?B$  by simp
    then obtain  $t'$  where  $ptp:p||t'$  and  $tpup:t'||u'$  by auto
    from  $tq\ kpq\ kplp$  have  $t||l'$  using  $M1$  by auto
    moreover with  $lpz\ lz\ lc$  have  $l||c$  using  $M1$  by auto
    moreover with  $cu\ pu\ ptp$  have  $c||t'$  using  $M1$  by auto
    ultimately obtain  $lc$  where  $t||lc$  and  $lc||t'$  using  $M5exist-var$  by blast
    with  $ptp\ tpup\ kp\ kt\ tq\ qup$  show  $?thesis$  using  $x\ ov$  by blast}
  next
  { assume  $\neg ?A \wedge \neg ?B \wedge ?C$  then have  $?C$  by simp
    with  $pu\ kp\ kt\ tq$  show  $?thesis$  using  $x\ d$  by blast}

qed}
next
{assume  $\neg ?A \wedge \neg ?B \wedge ?C$  then have  $?C$  by auto
  then obtain  $t$  where  $kpt:k'||t$  and  $tp:t||p$  by auto
  from  $pu\ qup$  have  $p||u' \oplus ((\exists t'. p||t' \wedge t'||u')) \oplus (\exists t'. q||t' \wedge t'||u)$  (is  $?A$ 
 $\oplus (?B \oplus ?C)$ ) using  $M2$  by blast
  then have  $(?A \wedge \neg ?B \wedge \neg ?C) \vee ((\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C))$  by
(insert xor-distr-L[of  $?A\ ?B\ ?C$ ], auto simp:elimmeets)
  thus  $?thesis$ 
proof (elim disjE)
  { assume  $?A \wedge \neg ?B \wedge \neg ?C$  then have  $?A$  by simp
    with  $kpq\ kpt\ tp\ qup$  show  $?thesis$  using  $x\ f$  by blast}
  next
  { assume  $\neg ?A \wedge ?B \wedge \neg ?C$  then have  $?B$  by simp
    then obtain  $t'$  where  $p||t'$  and  $t'||u'$  by auto
    with  $kpq\ kpt\ tp\ qup$  show  $?thesis$  using  $x\ d$  by blast}
  next
  { assume  $\neg ?A \wedge \neg ?B \wedge ?C$  then have  $?C$  by simp
    then obtain  $t'$  where  $qtp:q||t'$  and  $tpu:t'||u$  by auto
    from  $tp\ kp\ kl$  have  $t||l$  using  $M1$  by auto
    moreover with  $lpcp\ lpz\ lz$  have  $l||c'$  using  $M1$  by auto
    moreover with  $cpup\ qup\ qtp$  have  $c'||t'$  using  $M1$  by auto
    ultimately obtain  $lc$  where  $t||lc$  and  $lc||t'$  using  $M5exist-var$  by blast
    with  $kpt\ tp\ kpq\ qtp\ tpu\ pu$  show  $?thesis$  using  $x\ ov$  by blast}
qed}

```

qed  
qed

**lemma**  $cdid:d^{-1} O d \subseteq e \cup ov \cup ov^{-1} \cup d \cup d^{-1} \cup s \cup s^{-1} \cup f \cup f^{-1}$   
**proof**

**fix**  $x::'a \times 'a$  **assume**  $x \in d^{-1} O d$  **then obtain**  $p q z$  **where**  $x = (p, q)$  **and**  $(p, z) \in d^{-1}$  **and**  $(z, q) \in d$  **by** *auto*

**from**  $\langle (p, z) \in d^{-1} \rangle$  **obtain**  $k l u v$  **where**  $kp:k||p$  **and**  $kl:k||l$  **and**  $lz:l||z$  **and**  $pv:p||v$  **and**  $zu:z||u$  **and**  $uv:u||v$  **using**  $d$  **by** *blast*

**from**  $\langle (z, q) \in d \rangle$  **obtain**  $k' l' u' v'$  **where**  $kpq:k'||q$  **and**  $kplp:k'||l'$  **and**  $lpz:l'||z$  **and**  $qvp:q||v'$  **and**  $zup:z||u'$  **and**  $upvp:u'||v'$  **using**  $d$  **by** *blast*

**from**  $kp kpq$  **have**  $k||q \oplus ((\exists t. k||t \wedge t||q) \oplus (\exists t. k'||t \wedge t||p))$  **(is**  $?A \oplus (?B \oplus ?C)$ **) using**  $M2$  **by** *blast*

**then have**  $(?A \wedge \neg ?B \wedge \neg ?C) \vee ((\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C))$  **by** (*insert xor-distr-L[of ?A ?B ?C], auto simp:elimmeets*)

**thus**  $x \in e \cup ov \cup ov^{-1} \cup d \cup d^{-1} \cup s \cup s^{-1} \cup f \cup f^{-1}$

**proof** (*elim disjE*)

{ **assume**  $?A \wedge \neg ?B \wedge \neg ?C$  **then have**  $kq:?A$  **by** *simp*

**from**  $pv qvp$  **have**  $p||v' \oplus ((\exists t'. p||t' \wedge t' ||v') \oplus (\exists t'. q||t' \wedge t' ||v))$  **(is**  $?A \oplus (?B \oplus ?C)$ **) using**  $M2$  **by** *blast*

**then have**  $(?A \wedge \neg ?B \wedge \neg ?C) \vee ((\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C))$  **by** (*insert xor-distr-L[of ?A ?B ?C], auto simp:elimmeets*)

**thus** *?thesis*

**proof** (*elim disjE*)

{ **assume**  $?A \wedge \neg ?B \wedge \neg ?C$  **then have**  $?A$  **by** *simp*

**with**  $kq kp qvp$  **have**  $p = q$  **using**  $M4$  **by** *auto*

**thus** *?thesis* **using**  $x e$  **by** *auto*}

**next**

{ **assume**  $\neg ?A \wedge ?B \wedge \neg ?C$  **then have**  $?B$  **by** *simp*

**with**  $kq kp qvp$  **show** *?thesis* **using**  $x s$  **by** *blast*}

**next**

{ **assume**  $\neg ?A \wedge \neg ?B \wedge ?C$  **then have**  $?C$  **by** *simp*

**with**  $kq kp pv$  **show** *?thesis* **using**  $x s$  **by** *blast*}

**qed**}

**next**

{ **assume**  $\neg ?A \wedge ?B \wedge \neg ?C$  **then have**  $?B$  **by** *simp*

**then obtain**  $t$  **where**  $kt:k||t$  **and**  $tq:t||q$  **by** *auto*

**from**  $pv qvp$  **have**  $p||v' \oplus ((\exists t'. p||t' \wedge t' ||v') \oplus (\exists t'. q||t' \wedge t' ||v))$  **(is**  $?A \oplus (?B \oplus ?C)$ **) using**  $M2$  **by** *blast*

**then have**  $(?A \wedge \neg ?B \wedge \neg ?C) \vee ((\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C))$  **by** (*insert xor-distr-L[of ?A ?B ?C], auto simp:elimmeets*)

**thus** *?thesis*

**proof** (*elim disjE*)

{ **assume**  $?A \wedge \neg ?B \wedge \neg ?C$  **then have**  $?A$  **by** *simp*

**with**  $qvp kp kt tq$  **show** *?thesis* **using**  $x f$  **by** *blast*}

**next**

{ **assume**  $\neg ?A \wedge ?B \wedge \neg ?C$  **then have**  $?B$  **by** *simp*

then obtain  $t'$  where  $ptp:p||t'$  and  $tpvp:t'v'$  by *auto*  
 from  $tq\ kpq\ kplp$  have  $t||l'$  using  $M1$  by *auto*  
 moreover with  $ptp\ pv\ uv$  have  $u||t'$  using  $M1$  by *auto*  
 moreover with  $lpz\ zu\ \langle t||l' \rangle$  obtain  $lzu$  where  $t||lzu$  and  $lzu||t'$  using  
*M5exist-var* by *blast*  
 ultimately show *?thesis* using  $x\ ov\ kt\ tq\ kp\ ptp\ tpvp\ qvp$  by *blast*  
 next  
 { assume  $\neg ?A \wedge \neg ?B \wedge ?C$  then have *?C* by *simp*  
 with  $pv\ kp\ kt\ tq$  show *?thesis* using  $x\ d$  by *blast* }  
 qed }  
 next  
 { assume  $\neg ?A \wedge \neg ?B \wedge ?C$  then have *?C* by *auto*  
 then obtain  $t$  where  $kpt:k' || t$  and  $tp:t || p$  by *auto*  
 from  $pv\ qvp$  have  $p || v' \oplus ((\exists t'. p || t' \wedge t' || v') \oplus (\exists t'. q || t' \wedge t' || v))$  (is  $?A$   
 $\oplus (?B \oplus ?C)$ ) using  $M2$  by *blast*  
 then have  $(?A \wedge \neg ?B \wedge \neg ?C) \vee ((\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C))$  by  
 (*insert xor-distr-L*[of  $?A\ ?B\ ?C$ ], *auto simp: elimmeets*)  
 thus *?thesis*  
 proof (*elim disjE*)  
 { assume  $?A \wedge \neg ?B \wedge \neg ?C$  then have *?A* by *simp*  
 with  $kpq\ kpt\ tp\ qvp$  show *?thesis* using  $x\ f$  by *blast* }  
 next  
 { assume  $\neg ?A \wedge ?B \wedge \neg ?C$  then have *?B* by *simp*  
 then obtain  $t'$  where  $p || t'$  and  $t' || v'$  by *auto*  
 with  $kpq\ kpt\ tp\ qvp$  show *?thesis* using  $x\ d$  by *blast* }  
 next  
 { assume  $\neg ?A \wedge \neg ?B \wedge ?C$  then have *?C* by *simp*  
 then obtain  $t'$  where  $qtp:q || t'$  and  $tpv:t' || v$  by *auto*  
 from  $tp\ kp\ kl$  have  $t || l$  using  $M1$  by *auto*  
 moreover with  $qtp\ qvp\ upvp$  have  $u' || t'$  using  $M1$  by *auto*  
 moreover with  $lz\ zup\ \langle t || l \rangle$  obtain  $lzu$  where  $t || lzu$  and  $lzu || t'$  using  
*M5exist-var* by *blast*  
 ultimately show *?thesis* using  $x\ ov\ kpt\ tp\ kpq\ qtp\ tpv\ pv$  by *blast* }  
 qed }  
 qed  
 qed

**lemma**  $coviov:ov\hat{-1}\ O\ ov \subseteq e \cup ov \cup ov\hat{-1} \cup d \cup d\hat{-1} \cup s \cup s\hat{-1} \cup f \cup f\hat{-1}$

**proof**

fix  $x::'a \times 'a$  assume  $x \in ov\hat{-1}\ O\ ov$  then obtain  $p\ q\ z$  where  $x:x = (p,q)$   
 and  $(p,z) \in ov\hat{-1}$  and  $(z,q) \in ov$  by *auto*  
 from  $\langle (p,z) \in ov\hat{-1} \rangle$  obtain  $k\ l\ c\ u\ v$  where  $kz:k || z$  and  $kl:k || l$  and  $lp:l || p$  and  
 $lc:l || c$  and  $zu:z || u$  and  $pv:p || v$  and  $cu:c || u$  and  $uv:u || v$  using *ov* by *blast*  
 from  $\langle (z,q) \in ov \rangle$  obtain  $k'\ l'\ c'\ u'\ v'$  where  $kpz:k' || z$  and  $kplp:k' || l'$  and  $lpq:l' || q$   
 and  $lpcp:l' || c'$  and  $qvp:q || v'$  and  $zup:z || u'$  and  $cpup:c' || u'$  and  $upvp:u' || v'$  using  
*ov* by *blast*

**from**  $lp\ lpq$  **have**  $l\|q \oplus ((\exists t. l\|t \wedge t\|q) \oplus (\exists t. l'\|t \wedge t\|p))$  **(is**  $?A \oplus (?B \oplus ?C)$  **) using**  $M2$  **by** *blast*  
**then have**  $(?A \wedge \neg ?B \wedge \neg ?C) \vee ((\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C))$  **by** (*insert xor-distr-L[of ?A ?B ?C], auto simp:elimmeets*)  
**thus**  $x \in e \cup ov \cup ov^{\wedge-1} \cup d \cup d^{\wedge-1} \cup s \cup s^{\wedge-1} \cup f \cup f^{\wedge-1}$   
**proof** (*elim disjE*)  
    **{ assume**  $?A \wedge \neg ?B \wedge \neg ?C$  **then have**  $lq: ?A$  **by** *simp*  
      **from**  $pv\ qvp$  **have**  $p\|v' \oplus ((\exists t'. p\|t' \wedge t'\|v') \oplus (\exists t'. q\|t' \wedge t'\|v))$  **(is**  $?A \oplus (?B \oplus ?C)$  **) using**  $M2$  **by** *blast*  
      **then have**  $(?A \wedge \neg ?B \wedge \neg ?C) \vee ((\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C))$  **by** (*insert xor-distr-L[of ?A ?B ?C], auto simp:elimmeets*)  
      **thus** *?thesis*  
      **proof** (*elim disjE*)  
        **{ assume**  $?A \wedge \neg ?B \wedge \neg ?C$  **then have**  $?A$  **by** *simp*  
          **with**  $lq\ lp\ qvp$  **have**  $p = q$  **using**  $M4$  **by** *auto*  
          **thus** *?thesis* **using**  $x\ e$  **by** *auto*  
        **next**  
        **{ assume**  $\neg ?A \wedge ?B \wedge \neg ?C$  **then have**  $?B$  **by** *simp*  
          **with**  $lq\ lp\ qvp$  **show** *?thesis* **using**  $x\ s$  **by** *blast*  
        **next**  
        **{ assume**  $\neg ?A \wedge \neg ?B \wedge ?C$  **then have**  $?C$  **by** *simp*  
          **with**  $lq\ lp\ pv$  **show** *?thesis* **using**  $x\ s$  **by** *blast*  
      **qed**  
    **next**  
    **{ assume**  $\neg ?A \wedge ?B \wedge \neg ?C$  **then have**  $?B$  **by** *simp*  
      **then obtain**  $t$  **where**  $lt:l\|t$  **and**  $tq:t\|q$  **by** *auto*  
      **from**  $pv\ qvp$  **have**  $p\|v' \oplus ((\exists t'. p\|t' \wedge t'\|v') \oplus (\exists t'. q\|t' \wedge t'\|v))$  **(is**  $?A \oplus (?B \oplus ?C)$  **) using**  $M2$  **by** *blast*  
      **then have**  $(?A \wedge \neg ?B \wedge \neg ?C) \vee ((\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C))$  **by** (*insert xor-distr-L[of ?A ?B ?C], auto simp:elimmeets*)  
      **thus** *?thesis*  
      **proof** (*elim disjE*)  
        **{ assume**  $?A \wedge \neg ?B \wedge \neg ?C$  **then have**  $?A$  **by** *simp*  
          **with**  $qvp\ lp\ lt\ tq$  **show** *?thesis* **using**  $x\ f$  **by** *blast*  
        **next**  
        **{ assume**  $\neg ?A \wedge ?B \wedge \neg ?C$  **then have**  $?B$  **by** *simp*  
          **then obtain**  $t'$  **where**  $ptp:p\|t'$  **and**  $tpvp:t'\|v'$  **by** *auto*  
          **from**  $tq\ lpq\ lpcp$  **have**  $t\|c'$  **using**  $M1$  **by** *auto*  
          **moreover with**  $cpup\ zup\ zu$  **have**  $c'\|u$  **using**  $M1$  **by** *auto*  
          **moreover with**  $ptp\ pv\ uv$  **have**  $u\|t'$  **using**  $M1$  **by** *auto*  
          **ultimately obtain**  $cu$  **where**  $t\|cu$  **and**  $cu\|t'$  **using**  $M5$  *exist-var* **by**  
*blast*  
          **with**  $lt\ tq\ lp\ ptp\ tpvp\ qvp$  **show** *?thesis* **using**  $x\ ov$  **by** *blast*  
        **next**  
        **{ assume**  $\neg ?A \wedge \neg ?B \wedge ?C$  **then have**  $?C$  **by** *simp*  
          **with**  $pv\ lp\ lt\ tq$  **show** *?thesis* **using**  $x\ d$  **by** *blast*  
      **qed**  
    **next**

**{assume  $\neg ?A \wedge \neg ?B \wedge ?C$  then have  $?C$  by auto**  
**then obtain  $t$  where  $lpt:l'\|t$  and  $tp:t\|p$  by auto**  
**from  $pv\ qvp$  have  $p\|v' \oplus ((\exists t'. p\|t' \wedge t'\|v') \oplus (\exists t'. q\|t' \wedge t'\|v))$  (is  $?A$**   
 **$\oplus (?B \oplus ?C)$ ) using  $M2$  by blast**  
**then have  $(?A \wedge \neg ?B \wedge \neg ?C) \vee ((\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C))$  by**  
*(insert xor-distr-L[of  $?A\ ?B\ ?C$ ], auto simp:elimmeets)*  
**thus  $?thesis$**   
**proof (elim disjE)**  
**{ assume  $?A \wedge \neg ?B \wedge \neg ?C$  then have  $?A$  by simp**  
**with  $qvp\ lpq\ lpt\ tp$  show  $?thesis$  using  $x\ f$  by blast}**  
**next**  
**{ assume  $\neg ?A \wedge ?B \wedge \neg ?C$  then have  $?B$  by simp**  
**then obtain  $t'$  where  $p\|t'$  and  $t'\|v'$  by auto**  
**with  $qvp\ lpq\ lpt\ tp$  show  $?thesis$  using  $x\ d$  by blast}**  
**next**  
**{ assume  $\neg ?A \wedge \neg ?B \wedge ?C$  then have  $?C$  by simp**  
**then obtain  $t'$  where  $qtp:q\|t'$  and  $tpv:t'\|v$  by auto**  
**from  $tp\ lp\ lc$  have  $t\|c$  using  $M1$  by auto**  
**moreover with  $cu\ zu\ zup$  have  $c\|u'$  using  $M1$  by auto**  
**moreover with  $qtp\ qvp\ upvp$  have  $u'\|t'$  using  $M1$  by auto**  
**ultimately obtain  $cu$  where  $t\|cu$  and  $cu\|t'$  using  $M5$  exist-var by**  
*blast*  
**with  $lpt\ tp\ lpq\ pv\ qtp\ tpv$  show  $?thesis$  using  $x\ ov$  by blast}**  
**qed}**  
**qed**  
**qed**

### 3.6 $\gamma$ -composition

We prove compositions of the form  $r_1 \circ r_2 \subseteq b \cup m \cup ov \cup s \cup d \cup f \cup e \cup f^{-1} \cup d^{-1} \cup s^{-1} \cup ov^{-1} \cup b^{-1} \cup m^{-1}$ .

**lemma  $cbbi:b\ O\ b^{-1} \subseteq b \cup b^{-1} \cup m \cup m^{-1} \cup e \cup ov \cup ov^{-1} \cup s \cup s^{-1} \cup d \cup d^{-1} \cup f \cup f^{-1}$  (is  $b\ O\ b^{-1} \subseteq ?R$ )**

**proof**

**fix  $x::'a \times 'a$  assume  $x \in b\ O\ b^{-1}$  then obtain  $p\ q\ z::'a$  where  $x:x = (p,q)$**   
**and  $(p,z) \in b$  and  $(z,q) \in b^{-1}$  by auto**

**from  $\langle (p,z) \in b \rangle$  obtain  $c$  where  $pc:p\|c$  and  $c\|z$  using  $b$  by blast**

**from  $\langle (z,q) \in b^{-1} \rangle$  obtain  $c'$  where  $qcp:q\|c'$  and  $c'\|z$  using  $b$  by blast**

**obtain  $k\ k'$  where  $kp:k\|p$  and  $kpq:k'\|q$  using  $M3$  meets-wd  $pc\ qcp$  by fastforce**

**then have  $k\|q \oplus ((\exists t. k\|t \wedge t\|q) \oplus (\exists t. k'\|t \wedge t\|p))$  (is  $?A \oplus (?B \oplus ?C)$ )**

**using  $M2$  by blast**

**then have  $(?A \wedge \neg ?B \wedge \neg ?C) \vee ((\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C))$  by (insert xor-distr-L[of  $?A\ ?B\ ?C$ ], auto simp:elimmeets)**

**thus  $x \in ?R$**

**proof (elim disjE)**

**{ assume  $?A \wedge \neg ?B \wedge \neg ?C$  then have  $kq:?A$  by simp**

**from  $pc\ qcp$  have  $p\|c' \oplus ((\exists t'. p\|t' \wedge t'\|c') \oplus (\exists t'. q\|t' \wedge t'\|c))$  (is  $?A$**   
 **$\oplus (?B \oplus ?C)$ ) using  $M2$  by blast**

**then have  $(?A \wedge \neg ?B \wedge \neg ?C) \vee ((\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C))$  by**

```

(insert xor-distr-L[of ?A ?B ?C], auto simp:elimmeets)
  thus ?thesis
  proof (elim disjE)
    {assume (?A $\wedge$  $\neg$ ?B $\wedge$  $\neg$ ?C) then have ?A by simp
      with kp kq qcp have p = q using M4 by auto
      thus ?thesis using x e by auto}
    next
    {assume  $\neg$ ?A $\wedge$ ?B $\wedge$  $\neg$ ?C then have ?B by simp
      with kq kp qcp show ?thesis using x s by blast}
    next
    {assume ( $\neg$ ?A $\wedge$  $\neg$ ?B $\wedge$ ?C) then have ?C by simp
      with kq kp pc show ?thesis using x s by blast}
  qed}
next
{ assume  $\neg$ ?A $\wedge$ ?B $\wedge$  $\neg$ ?C then have ?B by simp
  then obtain t where kt:k||t and tq:t||q by auto
  from pc qcp have p||c'  $\oplus$  (( $\exists$  t'. p||t'  $\wedge$  t'||c')  $\oplus$  ( $\exists$  t'. q||t'  $\wedge$  t'||c)) (is ?A
 $\oplus$  (?B  $\oplus$  ?C)) using M2 by blast
  then have (?A $\wedge$  $\neg$ ?B $\wedge$  $\neg$ ?C)  $\vee$  (( $\neg$ ?A $\wedge$ ?B $\wedge$  $\neg$ ?C)  $\vee$  ( $\neg$ ?A $\wedge$  $\neg$ ?B $\wedge$ ?C)) by
(insert xor-distr-L[of ?A ?B ?C], auto simp:elimmeets)
  thus ?thesis
  proof (elim disjE)
    {assume ?A $\wedge$  $\neg$ ?B $\wedge$  $\neg$ ?C then have ?A by simp
      with kp qcp kt tq show ?thesis using f x by blast}
    next
    {assume  $\neg$ ?A $\wedge$ ?B $\wedge$  $\neg$ ?C then have ?B by simp
      then obtain t' where ptp:p||t' and tpcp:t'||c' by auto
      from pc tq have p||q  $\oplus$  (( $\exists$  t''. p||t''  $\wedge$  t''||q)  $\oplus$  ( $\exists$  t''. t||t''  $\wedge$  t''||c)) (is
?A  $\oplus$  (?B  $\oplus$  ?C)) using M2 by blast
      then have (?A $\wedge$  $\neg$ ?B $\wedge$  $\neg$ ?C)  $\vee$  (( $\neg$ ?A $\wedge$ ?B $\wedge$  $\neg$ ?C)  $\vee$  ( $\neg$ ?A $\wedge$  $\neg$ ?B $\wedge$ ?C)) by
(insert xor-distr-L[of ?A ?B ?C], auto simp:elimmeets)
      thus ?thesis
      proof (elim disjE)
        {assume ?A $\wedge$  $\neg$ ?B $\wedge$  $\neg$ ?C then have ?A by simp
          thus ?thesis using x m by auto}
        next
        {assume  $\neg$ ?A $\wedge$ ?B $\wedge$  $\neg$ ?C then have ?B by simp
          thus ?thesis using x b by auto}
        next
        { assume  $\neg$ ?A $\wedge$  $\neg$ ?B $\wedge$ ?C then have ?C by simp
          then obtain g where t||g and g||c by auto
          moreover with pc ptp have g||t' using M1 by blast
          ultimately show ?thesis using x ov kt tq kp ptp tpcp qcp by blast}
      qed}
    next
    {assume  $\neg$ ?A $\wedge$  $\neg$ ?B $\wedge$ ?C then have ?C by simp
      then obtain t' where q||t' and t'||c by auto
      with kp kt tq pc show ?thesis using d x by blast}
  qed}

```

```

next
{ assume  $\neg ?A \wedge \neg ?B \wedge ?C$  then have  $?C$  by simp
  then obtain  $t$  where  $kpt:k' || t$  and  $tp:t || p$  by auto
  from  $pc\ qcp$  have  $p || c' \oplus ((\exists t'. p || t' \wedge t' || c') \oplus (\exists t'. q || t' \wedge t' || c))$  (is  $?A \oplus (?B \oplus ?C)$ ) using M2 by blast
  then have  $(?A \wedge \neg ?B \wedge \neg ?C) \vee ((\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C))$  by
  (insert xor-distr-L[of  $?A\ ?B\ ?C$ ], auto simp:elimmeets)
  thus  $?thesis$ 
  proof (elim disjE)
    {assume  $?A \wedge \neg ?B \wedge \neg ?C$  then have  $?A$  by simp
      with  $qcp\ kpt\ tp\ kpq$  show  $?thesis$  using  $x\ f$  by blast}
    next
    {assume  $\neg ?A \wedge ?B \wedge \neg ?C$  then have  $?B$  by simp
      with  $qcp\ kpt\ tp\ kpq$  show  $?thesis$  using  $x\ d$  by blast}
    next
    {assume  $\neg ?A \wedge \neg ?B \wedge ?C$  then obtain  $t'$  where  $qt':q || t'$  and  $tpc:t' || c$  by
      auto
      from  $qcp\ tp$  have  $q || p \oplus ((\exists t''. q || t'' \wedge t'' || p) \oplus (\exists t''. t || t'' \wedge t'' || c'))$  (is
       $?A \oplus (?B \oplus ?C)$ ) using M2 by blast
      then have  $(?A \wedge \neg ?B \wedge \neg ?C) \vee ((\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C))$  by
      (insert xor-distr-L[of  $?A\ ?B\ ?C$ ], auto simp:elimmeets)
      thus  $?thesis$ 
      proof (elim disjE)
        {assume  $?A \wedge \neg ?B \wedge \neg ?C$  then have  $?A$  by simp
          thus  $?thesis$  using  $x\ m$  by auto}
        next
        {assume  $\neg ?A \wedge ?B \wedge \neg ?C$  then have  $?B$  by simp
          thus  $?thesis$  using  $x\ b$  by auto}
        next
        { assume  $\neg ?A \wedge \neg ?B \wedge ?C$  then obtain  $g$  where  $tg:t || g$  and  $g || c'$  by
          auto
          with  $qcp\ qt'$  have  $g || t'$  using M1 by blast
          with  $qt'\ tpc\ pc\ kpq\ kpt\ tp\ tg$  show  $?thesis$  using  $x\ ov$  by blast}
      qed}
    qed}
  qed}
  qed}
  qed}
  qed}

```

**lemma**  $cbib:b^{\wedge-1} O b \subseteq b \cup b^{\wedge-1} \cup m \cup m^{\wedge-1} \cup e \cup ov \cup ov^{\wedge-1} \cup s \cup s^{\wedge-1} \cup d \cup d^{\wedge-1} \cup f \cup f^{\wedge-1}$  (is  $b^{\wedge-1} O b \subseteq ?R$ )

**proof**

```

fix  $x::'a \times 'a$  assume  $x \in b^{\wedge-1} O b$  then obtain  $p\ q\ z::'a$  where  $x:x = (p,q)$ 
and  $(p,z) \in b^{\wedge-1}$  and  $(z,q) \in b$  by auto
  from  $\langle (p,z) \in b^{\wedge-1} \rangle$  obtain  $c$  where  $zc:z || c$  and  $cp:c || p$  using  $b$  by blast
  from  $\langle (z,q) \in b \rangle$  obtain  $c'$  where  $zcp:z || c'$  and  $cpq:c' || q$  using  $b$  by blast
  obtain  $u\ u'$  where  $pu:p || u$  and  $qup:q || u'$  using M3 meets-wd  $cp\ cpq$  by fastforce
  from  $cp\ cpq$  have  $c || q \oplus ((\exists t. c || t \wedge t || q) \oplus (\exists t. c' || t \wedge t || p))$  (is  $?A \oplus (?B \oplus$ 

```

$?C$ ) using  $M2$  by *blast*  
**then have**  $(?A \wedge \neg ?B \wedge \neg ?C) \vee ((\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C))$  by (*insert xor-distr-L*[of  $?A ?B ?C$ ], *auto simp:elimmeets*)  
**thus**  $x \in ?R$   
**proof** (*elim disjE*)  
    { **assume**  $?A \wedge \neg ?B \wedge \neg ?C$  **then have**  $cq: ?A$  by *simp*  
      **from**  $pu\ qup$  **have**  $p \parallel u' \oplus ((\exists t'. p \parallel t' \wedge t'' \parallel u') \oplus (\exists t'. q \parallel t' \wedge t'' \parallel u))$  (**is**  $?A \oplus (?B \oplus ?C)$ ) using  $M2$  by *blast*  
      **then have**  $(?A \wedge \neg ?B \wedge \neg ?C) \vee ((\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C))$  by (*insert xor-distr-L*[of  $?A ?B ?C$ ], *auto simp:elimmeets*)  
      **thus**  $?thesis$   
      **proof** (*elim disjE*)  
        { **assume**  $(?A \wedge \neg ?B \wedge \neg ?C)$  **then have**  $?A$  by *simp*  
          **with**  $cq\ cp\ qup$  **have**  $p = q$  using  $M4$  by *auto*  
          **thus**  $?thesis$  using  $x\ e$  by *auto* }  
        **next**  
        { **assume**  $\neg ?A \wedge ?B \wedge \neg ?C$  **then have**  $?B$  by *simp*  
          **with**  $cq\ cp\ qup$  **show**  $?thesis$  using  $x\ s$  by *blast* }  
        **next**  
        { **assume**  $(\neg ?A \wedge \neg ?B \wedge ?C)$  **then have**  $?C$  by *simp*  
          **with**  $pu\ cq\ cp$  **show**  $?thesis$  using  $x\ s$  by *blast* }  
      **qed** }  
    **next**  
    { **assume**  $\neg ?A \wedge ?B \wedge \neg ?C$  **then have**  $?B$  by *simp*  
      **then obtain**  $t$  **where**  $ct:c \parallel t$  **and**  $tq:t \parallel q$  by *auto*  
      **from**  $pu\ qup$  **have**  $p \parallel u' \oplus ((\exists t'. p \parallel t' \wedge t'' \parallel u') \oplus (\exists t'. q \parallel t' \wedge t'' \parallel u))$  (**is**  $?A \oplus (?B \oplus ?C)$ ) using  $M2$  by *blast*  
      **then have**  $(?A \wedge \neg ?B \wedge \neg ?C) \vee ((\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C))$  by (*insert xor-distr-L*[of  $?A ?B ?C$ ], *auto simp:elimmeets*)  
      **thus**  $?thesis$   
      **proof** (*elim disjE*)  
        { **assume**  $?A \wedge \neg ?B \wedge \neg ?C$  **then have**  $?A$  by *simp*  
          **with**  $qup\ ct\ tq\ cp$  **show**  $?thesis$  using  $f\ x$  by *blast* }  
        **next**  
        { **assume**  $\neg ?A \wedge ?B \wedge \neg ?C$  **then have**  $?B$  by *simp*  
          **then obtain**  $t'$  **where**  $ptp:p \parallel t'$  **and**  $tpup:t' \parallel u'$  by *auto*  
          **from**  $pu\ tq$  **have**  $p \parallel q \oplus ((\exists t''. p \parallel t'' \wedge t''' \parallel q) \oplus (\exists t''. t \parallel t'' \wedge t''' \parallel u))$  (**is**  $?A \oplus (?B \oplus ?C)$ ) using  $M2$  by *blast*  
          **then have**  $(?A \wedge \neg ?B \wedge \neg ?C) \vee ((\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C))$  by (*insert xor-distr-L*[of  $?A ?B ?C$ ], *auto simp:elimmeets*)  
          **thus**  $?thesis$   
          **proof** (*elim disjE*)  
            { **assume**  $?A \wedge \neg ?B \wedge \neg ?C$  **then have**  $?A$  by *simp*  
              **thus**  $?thesis$  using  $x\ m$  by *auto* }  
            **next**  
            { **assume**  $\neg ?A \wedge ?B \wedge \neg ?C$  **then have**  $?B$  by *simp*  
              **thus**  $?thesis$  using  $x\ b$  by *auto* }  
            **next**  
            { **assume**  $\neg ?A \wedge \neg ?B \wedge ?C$  **then have**  $?C$  by *simp* }  
          }



then obtain  $g$  where  $t \parallel g$  and  $g \parallel u$  by *auto*  
 moreover with  $pu$   $ptp$  have  $g \parallel t'$  using  $M1$  by *blast*  
 ultimately show  $?thesis$  using  $x$  *ov*  $ct$   $tq$   $cp$   $ptp$   $tpup$   $qup$  by *blast*}  
 qed}  
 next  
 {assume  $\neg ?A \wedge \neg ?B \wedge ?C$  then have  $?C$  by *simp*  
 then obtain  $t'$  where  $q \parallel t'$  and  $t' \parallel u$  by *auto*  
 with  $cp$   $ct$   $tq$   $pu$  show  $?thesis$  using  $d$   $x$  by *blast*}  
 qed}  
 next  
 { assume  $\neg ?A \wedge \neg ?B \wedge ?C$  then have  $?C$  by *simp*  
 then obtain  $t$  where  $cpt:c' \parallel t$  and  $tp:t \parallel p$  by *auto*  
 from  $pu$   $qup$  have  $p \parallel u' \oplus ((\exists t'. p \parallel t' \wedge t' \parallel u') \oplus (\exists t'. q \parallel t' \wedge t' \parallel u))$  (is  $?A$   
 $\oplus (?B \oplus ?C)$ ) using  $M2$  by *blast*  
 then have  $(?A \wedge \neg ?B \wedge \neg ?C) \vee ((\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C))$  by  
 (*insert xor-distr-L*[of  $?A$   $?B$   $?C$ ], *auto simp:elimmeets*)  
 thus  $?thesis$   
 proof (*elim disjE*)  
 {assume  $?A \wedge \neg ?B \wedge \neg ?C$  then have  $?A$  by *simp*  
 with  $qup$   $cpt$   $tp$   $cpq$  show  $?thesis$  using  $x$   $f$  by *blast*}  
 next  
 {assume  $\neg ?A \wedge ?B \wedge \neg ?C$  then have  $?B$  by *simp*  
 with  $qup$   $cpt$   $tp$   $cpq$  show  $?thesis$  using  $x$   $d$  by *blast*}  
 next  
 {assume  $\neg ?A \wedge \neg ?B \wedge ?C$  then obtain  $t'$  where  $qt':q \parallel t'$  and  $tpc:t' \parallel u$  by  
*auto*  
 from  $qup$   $tp$  have  $q \parallel p \oplus ((\exists t''. q \parallel t'' \wedge t'' \parallel p) \oplus (\exists t''. t \parallel t'' \wedge t'' \parallel u))$  (is  
 $?A \oplus (?B \oplus ?C)$ ) using  $M2$  by *blast*  
 then have  $(?A \wedge \neg ?B \wedge \neg ?C) \vee ((\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C))$  by  
 (*insert xor-distr-L*[of  $?A$   $?B$   $?C$ ], *auto simp:elimmeets*)  
 thus  $?thesis$   
 proof (*elim disjE*)  
 {assume  $?A \wedge \neg ?B \wedge \neg ?C$  then have  $?A$  by *simp*  
 thus  $?thesis$  using  $x$   $m$  by *auto*}  
 next  
 {assume  $\neg ?A \wedge ?B \wedge \neg ?C$  then have  $?B$  by *simp*  
 thus  $?thesis$  using  $x$   $b$  by *auto*}  
 next  
 { assume  $\neg ?A \wedge \neg ?B \wedge ?C$  then obtain  $g$  where  $tg:t \parallel g$  and  $g \parallel u'$  by  
*auto*  
 with  $qup$   $qt'$  have  $g \parallel t'$  using  $M1$  by *blast*  
 with  $qt'$   $tpc$   $pu$   $cpq$   $cpt$   $tp$   $tg$  show  $?thesis$  using  $x$  *ov* by *blast*}  
 qed}  
 qed}  
 qed  
 qed

**lemma** *cddi*:  $d \ O \ d^{-1} \subseteq b \cup b^{-1} \cup m \cup m^{-1} \cup e \cup ov \cup ov^{-1} \cup s \cup s^{-1} \cup d \cup d^{-1} \cup f \cup f^{-1}$  (is  $d \ O \ d^{-1} \subseteq ?R$ )

**proof**

**fix**  $x::'a \times 'a$  **assume**  $x \in d \ O \ d^{-1}$  **then obtain**  $p \ q \ z::'a$  **where**  $x:x = (p,q)$   
**and**  $(p,z) \in d$  **and**  $(z,q) \in d^{-1}$  **by auto**  
**from**  $\langle (p,z) \in d \rangle$  **obtain**  $kl:u \ v$  **where**  $lp:l||p$  **and**  $kl:k||l$  **and**  $kz:k||z$  **and**  $pu:p||u$   
**and**  $uv:u||v$  **and**  $zv:z||v$  **using**  $d$  **by blast**  
**from**  $\langle (z,q) \in d^{-1} \rangle$  **obtain**  $k' \ l' \ u' \ v'$  **where**  $lpq:l' || q$  **and**  $kplp:k' || l'$  **and**  
 $kpz:k' || z$  **and**  $gup:q || u'$  **and**  $upvp:u' || v'$  **and**  $zv':z || v'$  **using**  $d$  **by blast**  
**from**  $lp \ lpq$  **have**  $l||q \oplus ((\exists t. l||t \wedge t||q) \oplus (\exists t. l' || t \wedge t||p))$  **(is**  $?A \oplus (?B \oplus ?C)$   
**using**  $M2$  **by blast**  
**then have**  $(?A \wedge \neg ?B \wedge \neg ?C) \vee ((\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C))$  **by**  $(insert \ xor-distr-L[of \ ?A \ ?B \ ?C], \ auto \ simp:elimmeets)$   
**thus**  $x \in ?R$   
**proof**  $(elim \ disjE)$   
**{ assume**  $?A \wedge \neg ?B \wedge \neg ?C$  **then have**  $lq:?A$  **by simp**  
**from**  $pu \ qup$  **have**  $p||u' \oplus ((\exists t'. p||t' \wedge t' || u') \oplus (\exists t'. q||t' \wedge t' || u))$  **(is**  $?A$   
 $\oplus (?B \oplus ?C)$   
**using**  $M2$  **by blast**  
**then have**  $(?A \wedge \neg ?B \wedge \neg ?C) \vee ((\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C))$  **by**  
 $(insert \ xor-distr-L[of \ ?A \ ?B \ ?C], \ auto \ simp:elimmeets)$   
**thus**  $?thesis$   
**proof**  $(elim \ disjE)$   
**{ assume**  $(?A \wedge \neg ?B \wedge \neg ?C)$  **then have**  $?A$  **by simp**  
**with**  $lq \ lp \ qup$  **have**  $p = q$  **using**  $M4$  **by auto**  
**thus**  $?thesis$  **using**  $x \ e$  **by auto**  
**next**  
**{ assume**  $\neg ?A \wedge ?B \wedge \neg ?C$  **then have**  $?B$  **by simp**  
**with**  $lq \ lp \ qup$  **show**  $?thesis$  **using**  $x \ s$  **by blast**  
**next**  
**{ assume**  $(\neg ?A \wedge \neg ?B \wedge ?C)$  **then have**  $?C$  **by simp**  
**with**  $pu \ lq \ lp$  **show**  $?thesis$  **using**  $x \ s$  **by blast**  
**qed**  
**next**  
**{ assume**  $\neg ?A \wedge ?B \wedge \neg ?C$  **then have**  $?B$  **by simp**  
**then obtain**  $t$  **where**  $lt:l||t$  **and**  $tq:t||q$  **by auto**  
**from**  $pu \ qup$  **have**  $p||u' \oplus ((\exists t'. p||t' \wedge t' || u') \oplus (\exists t'. q||t' \wedge t' || u))$  **(is**  $?A$   
 $\oplus (?B \oplus ?C)$   
**using**  $M2$  **by blast**  
**then have**  $(?A \wedge \neg ?B \wedge \neg ?C) \vee ((\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C))$  **by**  
 $(insert \ xor-distr-L[of \ ?A \ ?B \ ?C], \ auto \ simp:elimmeets)$   
**thus**  $?thesis$   
**proof**  $(elim \ disjE)$   
**{ assume**  $?A \wedge \neg ?B \wedge \neg ?C$  **then have**  $?A$  **by simp**  
**with**  $qup \ lt \ tq \ lp$  **show**  $?thesis$  **using**  $f \ x$  **by blast**  
**next**  
**{ assume**  $\neg ?A \wedge ?B \wedge \neg ?C$  **then have**  $?B$  **by simp**  
**then obtain**  $t'$  **where**  $ptp:p||t'$  **and**  $tpup:t' || u'$  **by auto**  
**from**  $pu \ tq$  **have**  $p||q \oplus ((\exists t''. p||t'' \wedge t'' || q) \oplus (\exists t''. t||t'' \wedge t'' || u))$  **(is**  
 $?A \oplus (?B \oplus ?C)$   
**using**  $M2$  **by blast**  
**then have**  $(?A \wedge \neg ?B \wedge \neg ?C) \vee ((\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C))$  **by**  
 $(insert \ xor-distr-L[of \ ?A \ ?B \ ?C], \ auto \ simp:elimmeets)$   
**thus**  $?thesis$

```

proof (elim disjE)
  {assume ?A $\wedge$ ?B $\wedge$ ?C then have ?A by simp
   thus ?thesis using x m by auto}
next
  {assume  $\neg$ ?A $\wedge$ ?B $\wedge$ ?C then have ?B by simp
   thus ?thesis using x b by auto}
next
  {assume  $\neg$ ?A $\wedge$ ?B $\wedge$ ?C then have ?C by simp
   then obtain g where t||g and g||u by auto
   moreover with pu ptp have g||t' using M1 by blast
   ultimately show ?thesis using x ov lt tq lp ptp tpup qup by blast}
qed}
next
  {assume  $\neg$ ?A $\wedge$ ?B $\wedge$ ?C then have ?C by simp
   then obtain t' where q||t' and t'||u by auto
   with lp lt tq pu show ?thesis using d x by blast}
qed}
next
  {assume  $\neg$ ?A $\wedge$ ?B $\wedge$ ?C then have ?C by simp
   then obtain t where lpt:l'||t and tpt:t||p by auto
   from pu qup have p||u'  $\oplus$  (( $\exists$  t'. p||t'  $\wedge$  t'||u')  $\oplus$  ( $\exists$  t'. q||t'  $\wedge$  t'||u)) (is ?A
 $\oplus$  (?B  $\oplus$  ?C)) using M2 by blast
   then have (?A $\wedge$ ?B $\wedge$ ?C)  $\vee$  (( $\neg$ ?A $\wedge$ ?B $\wedge$ ?C)  $\vee$  ( $\neg$ ?A $\wedge$ ?B $\wedge$ ?C)) by
(insert xor-distr-L[of ?A ?B ?C], auto simp:elimmeets)
   thus ?thesis
proof (elim disjE)
  {assume ?A $\wedge$ ?B $\wedge$ ?C then have ?A by simp
   with qup lpt tp lpq show ?thesis using x f by blast}
next
  {assume  $\neg$ ?A $\wedge$ ?B $\wedge$ ?C then have ?B by simp
   with qup lpt tp lpq show ?thesis using x d by blast}
next
  {assume  $\neg$ ?A $\wedge$ ?B $\wedge$ ?C then obtain t' where qt':q||t' and tpc:t'||u by
auto
   from qup tp have q||p  $\oplus$  (( $\exists$  t''. q||t''  $\wedge$  t''||p)  $\oplus$  ( $\exists$  t''. t||t''  $\wedge$  t''||u)) (is
?A  $\oplus$  (?B  $\oplus$  ?C)) using M2 by blast
   then have (?A $\wedge$ ?B $\wedge$ ?C)  $\vee$  (( $\neg$ ?A $\wedge$ ?B $\wedge$ ?C)  $\vee$  ( $\neg$ ?A $\wedge$ ?B $\wedge$ ?C)) by
(insert xor-distr-L[of ?A ?B ?C], auto simp:elimmeets)
   thus ?thesis
proof (elim disjE)
  {assume ?A $\wedge$ ?B $\wedge$ ?C then have ?A by simp
   thus ?thesis using x m by auto}
next
  {assume  $\neg$ ?A $\wedge$ ?B $\wedge$ ?C then have ?B by simp
   thus ?thesis using x b by auto}
next
  {assume  $\neg$ ?A $\wedge$ ?B $\wedge$ ?C then obtain g where tg:t||g and g||u' by
auto
   with qup qt' have g||t' using M1 by blast

```

```

    with qt' tpc pu lpq lpt tp tg show ?thesis using x ov by blast}
  qed}
qed}
qed
qed

```

### 3.7 The rest of the composition table

Because of the symmetry  $(r_1 \circ r_2)^{-1} = r_2^{-1} \circ r_1^{-1}$ , the rest of the compositions is easily deduced.

**lemma** *cmibi*:  $m \circ b^{-1} \subseteq b^{-1} \cup m^{-1} \cup s^{-1} \cup ov^{-1} \cup d^{-1}$   
**using** *cmibi* **by** *auto*

**lemma** *covmi*:  $ov \circ m^{-1} \subseteq ov^{-1} \cup d^{-1} \cup s^{-1}$   
**using** *cmovi* **by** *auto*

**lemma** *covbi*:  $ov \circ b^{-1} \subseteq b^{-1} \cup m^{-1} \cup s^{-1} \cup ov^{-1} \cup d^{-1}$   
**using** *cbovi* **by** *auto*

**lemma** *cfiovi*:  $f^{-1} \circ ov^{-1} \subseteq ov^{-1} \cup s^{-1} \cup d^{-1}$   
**using** *covf* **by** *auto*

**lemma** *cfimi*:  $(f^{-1} \circ m^{-1}) \subseteq s^{-1} \cup ov^{-1} \cup d^{-1}$   
**using** *cmf* **by** *auto*

**lemma** *cfibi*:  $f^{-1} \circ b^{-1} \subseteq b^{-1} \cup m^{-1} \cup ov^{-1} \cup s^{-1} \cup d^{-1}$   
**using** *cbf* **by** *auto*

**lemma** *cdif*:  $d^{-1} \circ f \subseteq ov^{-1} \cup s^{-1} \cup d^{-1}$   
**using** *cfid* **by** *auto*

**lemma** *cdiovi*:  $d^{-1} \circ ov^{-1} \subseteq ov^{-1} \cup s^{-1} \cup d^{-1}$   
**using** *covd* **by** *auto*

**lemma** *cdimi*:  $d^{-1} \circ m^{-1} \subseteq s^{-1} \cup ov^{-1} \cup d^{-1}$   
**using** *cmd* **by** *auto*

**lemma** *cdibi*:  $d^{-1} \circ b^{-1} \subseteq b^{-1} \cup m^{-1} \cup ov^{-1} \cup s^{-1} \cup d^{-1}$   
**using** *cbd* **by** *auto*

**lemma** *csd*:  $s \circ d \subseteq d$   
**using** *cdisi* **by** *auto*

**lemma** *csf*:  $s \circ f \subseteq d$   
**using** *cfisi* **by** *auto*

**lemma** *csovi*:  $s \circ ov^{-1} \subseteq ov^{-1} \cup f \cup d$   
**using** *covsi* **by** *auto*

**lemma** *csmi*: $s \ O \ m^{\wedge-1} \subseteq m^{\wedge-1}$   
**using** *cmsi* **by** *auto*

**lemma** *csbi*: $s \ O \ b^{\wedge-1} \subseteq b^{\wedge-1}$   
**using** *cbsi* **by** *auto*

**lemma** *csisi*: $s^{\wedge-1} \ O \ s^{\wedge-1} \subseteq s^{\wedge-1}$   
**using** *css* **by** *auto*

**lemma** *csid*: $s^{\wedge-1} \ O \ d \subseteq ov^{\wedge-1} \cup f \cup d$   
**using** *cdi* **by** *auto*

**lemma** *csif*: $s^{\wedge-1} \ O \ f \subseteq ov^{\wedge-1}$   
**using** *cfis* **by** *auto*

**lemma** *csiovi*: $s^{\wedge-1} \ O \ ov^{\wedge-1} \subseteq ov^{\wedge-1}$   
**using** *covs* **by** *auto*

**lemma** *csimi*: $s^{\wedge-1} \ O \ m^{\wedge-1} \subseteq m^{\wedge-1}$   
**using** *cms* **by** *auto*

**lemma** *csibi*: $s^{\wedge-1} \ O \ b^{\wedge-1} \subseteq b^{\wedge-1}$   
**using** *cbs* **by** *auto*

**lemma** *cds*: $d \ O \ s \subseteq d$   
**using** *csidi* **by** *auto*

**lemma** *cdsi*: $d \ O \ s^{\wedge-1} \subseteq b^{\wedge-1} \cup m^{\wedge-1} \cup ov^{\wedge-1} \cup f \cup d$   
**using** *csdi* **by** *auto*

**lemma** *cdd*: $d \ O \ d \subseteq d$   
**using** *cdidi* **by** *auto*

**lemma** *cdf*: $d \ O \ f \subseteq d$   
**using** *cfidi* **by** *auto*

**lemma** *cdovi*: $d \ O \ ov^{\wedge-1} \subseteq b^{\wedge-1} \cup m^{\wedge-1} \cup ov^{\wedge-1} \cup f \cup d$   
**using** *covdi* **by** *auto*

**lemma** *cdmi*: $d \ O \ m^{\wedge-1} \subseteq b^{\wedge-1}$   
**using** *cmdi* **by** *auto*

**lemma** *cbdi*: $d \ O \ b^{\wedge-1} \subseteq b^{\wedge-1}$   
**using** *cbdi* **by** *auto*

**lemma** *cdfi*: $f \ O \ d^{\wedge-1} \subseteq b^{\wedge-1} \cup m^{\wedge-1} \cup ov^{\wedge-1} \cup s^{\wedge-1} \cup d^{\wedge-1}$   
**using** *cdfi* **by** *auto*

**lemma** *cfs*: $f \ O \ s \subseteq d$   
using *csifi* by *auto*

**lemma** *cfsi*: $f \ O \ s^{\wedge-1} \subseteq b^{\wedge-1} \cup m^{\wedge-1} \cup ov^{\wedge-1}$   
using *csfi* by *auto*

**lemma** *efd*: $f \ O \ d \subseteq d$   
using *cdifi* by *auto*

**lemma** *cff*: $f \ O \ f \subseteq f$   
using *cfifi* by *auto*

**lemma** *cfovi*: $f \ O \ ov^{\wedge-1} \subseteq b^{\wedge-1} \cup m^{\wedge-1} \cup ov^{\wedge-1}$   
using *covfi* by *auto*

**lemma** *cfmi*: $f \ O \ m^{\wedge-1} \subseteq b^{\wedge-1}$   
using *cmfi* by *auto*

**lemma** *cfbi*: $f \ O \ b^{\wedge-1} \subseteq b^{\wedge-1}$   
using *cbfi* by *auto*

**lemma** *covifi*: $ov^{\wedge-1} \ O \ f^{\wedge-1} \subseteq ov^{\wedge-1} \cup s^{\wedge-1} \cup d^{\wedge-1}$   
using *cfov* by *auto*

**lemma** *covidi*: $ov^{\wedge-1} \ O \ d^{\wedge-1} \subseteq b^{\wedge-1} \cup m^{\wedge-1} \cup s^{\wedge-1} \cup ov^{\wedge-1} \cup d^{\wedge-1}$   
using *cdov* by *auto*

**lemma** *covis*: $ov^{\wedge-1} \ O \ s \subseteq ov^{\wedge-1} \cup f \cup d$   
using *csiov* by *auto*

**lemma** *covisi*: $ov^{\wedge-1} \ O \ s^{\wedge-1} \subseteq b^{\wedge-1} \cup m^{\wedge-1} \cup ov^{\wedge-1}$   
using *csov* by *auto*

**lemma** *covid*: $ov^{\wedge-1} \ O \ d \subseteq ov^{\wedge-1} \cup f \cup d$   
using *cdiov* by *auto*

**lemma** *covif*: $ov^{\wedge-1} \ O \ f \subseteq ov^{\wedge-1}$   
using *cfiov* by *auto*

**lemma** *coviovi*: $ov^{\wedge-1} \ O \ ov^{\wedge-1} \subseteq b^{\wedge-1} \cup m^{\wedge-1} \cup ov^{\wedge-1}$   
using *covov* by *auto*

**lemma** *covimi*: $ov^{\wedge-1} \ O \ m^{\wedge-1} \subseteq b^{\wedge-1}$   
using *cmov* by *auto*

**lemma** *covibi*: $ov^{\wedge-1} \ O \ b^{\wedge-1} \subseteq b^{\wedge-1}$   
using *cbov* by *auto*

**lemma** *cmiov*: $m^{\wedge-1} O ov \subseteq ov^{\wedge-1} \cup d \cup f$   
**using** *covim* **by** *auto*

**lemma** *cmifi*: $m^{\wedge-1} O f^{\wedge-1} \subseteq m^{\wedge-1}$   
**using** *cfm* **by** *auto*

**lemma** *cmidi*: $m^{\wedge-1} O d^{\wedge-1} \subseteq b^{\wedge-1}$   
**using** *cdm* **by** *auto*

**lemma** *cmis*: $m^{\wedge-1} O s \subseteq ov^{\wedge-1} \cup d \cup f$   
**using** *csim* **by** *auto*

**lemma** *cmisi*: $m^{\wedge-1} O s^{\wedge-1} \subseteq b^{\wedge-1}$   
**using** *esm* **by** *auto*

**lemma** *cmid*: $m^{\wedge-1} O d \subseteq ov^{\wedge-1} \cup d \cup f$   
**using** *cdim* **by** *auto*

**lemma** *cmif*: $m^{\wedge-1} O f \subseteq m^{\wedge-1}$   
**using** *cfim* **by** *auto*

**lemma** *cmiovi*: $m^{\wedge-1} O ov^{\wedge-1} \subseteq b^{\wedge-1}$   
**using** *covm* **by** *auto*

**lemma** *cmimi*: $m^{\wedge-1} O m^{\wedge-1} \subseteq b^{\wedge-1}$   
**using** *cmm* **by** *auto*

**lemma** *cmibi*: $m^{\wedge-1} O b^{\wedge-1} \subseteq b^{\wedge-1}$   
**using** *cbm* **by** *auto*

**lemma** *cbim*: $b^{\wedge-1} O m \subseteq b^{\wedge-1} \cup m^{\wedge-1} \cup ov^{\wedge-1} \cup f \cup d$   
**using** *cmib* **by** *auto*

**lemma** *cbiov*: $b^{\wedge-1} O ov \subseteq b^{\wedge-1} \cup m^{\wedge-1} \cup ov^{\wedge-1} \cup f \cup d$   
**using** *covib* **by** *auto*

**lemma** *cbifi*: $b^{\wedge-1} O f^{\wedge-1} \subseteq b^{\wedge-1}$   
**using** *cfb* **by** *auto*

**lemma** *cbidi*: $b^{\wedge-1} O d^{\wedge-1} \subseteq b^{\wedge-1}$   
**using** *cdb* **by** *auto*

**lemma** *cbis*: $b^{\wedge-1} O s \subseteq b^{\wedge-1} \cup m^{\wedge-1} \cup ov^{\wedge-1} \cup f \cup d$   
**using** *csib* **by** *auto*

**lemma** *cbisi*: $b^{\wedge-1} O s^{\wedge-1} \subseteq b^{\wedge-1}$   
**using** *csb* **by** *auto*

**lemma** *cbid*: $b^{\wedge-1} O d \subseteq b^{\wedge-1} \cup m^{\wedge-1} \cup ov^{\wedge-1} \cup f \cup d$

using *cdib* by *auto*

**lemma** *cbif*: $b^{\wedge-1} O f \subseteq b^{\wedge-1}$   
using *cfib* by *auto*

**lemma** *cbiovi*: $b^{\wedge-1} O ov^{\wedge-1} \subseteq b^{\wedge-1}$   
using *covb* by *auto*

**lemma** *cbimi*: $b^{\wedge-1} O m^{\wedge-1} \subseteq b^{\wedge-1}$   
using *cmb* by *auto*

**lemma** *cbibi*: $b^{\wedge-1} O b^{\wedge-1} \subseteq b^{\wedge-1}$   
using *ccb* by *auto*

### 3.8 Composition rules

**named-theorems** *ce-rules* **declare** *cem*[*ce-rules*] **and** *ceb*[*ce-rules*] **and** *ceov*[*ce-rules*]  
**and** *ces*[*ce-rules*] **and** *cef*[*ce-rules*] **and** *ced*[*ce-rules*] **and**  
*cemi*[*ce-rules*] **and** *cebi*[*ce-rules*] **and** *ceovi*[*ce-rules*] **and** *cesi*[*ce-rules*] **and** *cefi*[*ce-rules*]  
**and** *cedi*[*ce-rules*]

**named-theorems** *cm-rules* **declare** *cme*[*cm-rules*] **and** *cmb*[*cm-rules*] **and** *cmm*[*cm-rules*]  
**and** *cmov*[*cm-rules*] **and** *cms* [*cm-rules*] **and** *cmd*[*cm-rules*] **and** *cmf*[*cm-rules*]  
**and**  
*cmbi*[*cm-rules*] **and** *cmmi*[*cm-rules*] **and** *cmovi*[*cm-rules*] **and** *cmsi*[*cm-rules*] **and**  
*cmdi*[*cm-rules*] **and** *cmfi*[*cm-rules*]

**named-theorems** *cb-rules* **declare** *cbe*[*cb-rules*] **and** *cbm*[*cb-rules*] **and** *ccb*[*cb-rules*]  
**and** *cbov*[*cb-rules*] **and** *cbs* [*cb-rules*] **and** *cbd*[*cb-rules*] **and** *cbf*[*cb-rules*] **and**  
*cbbi*[*cb-rules*] **and** *cbbi*[*cb-rules*] **and** *cbovi*[*cb-rules*] **and** *cbsi*[*cb-rules*] **and** *cbdi*[*cb-rules*]  
**and** *cbfi*[*cb-rules*]

**named-theorems** *cov-rules* **declare** *cove*[*cov-rules*] **and** *covb*[*cov-rules*] **and** *covb*[*cov-rules*]  
**and** *covov*[*cov-rules*] **and** *covs* [*cov-rules*] **and** *covd*[*cov-rules*] **and** *covf*[*cov-rules*]  
**and**  
*covbi*[*cov-rules*] **and** *covbi*[*cov-rules*] **and** *covovi*[*cov-rules*] **and** *covsi*[*cov-rules*] **and**  
*covdi*[*cov-rules*] **and** *covfi*[*cov-rules*]

**named-theorems** *cs-rules* **declare** *cse*[*cs-rules*] **and** *csb*[*cs-rules*] **and** *csb*[*cs-rules*]  
**and** *csov*[*cs-rules*] **and** *css* [*cs-rules*] **and** *csd*[*cs-rules*] **and** *csf*[*cs-rules*] **and**  
*csbi*[*cs-rules*] **and** *csbi*[*cs-rules*] **and** *csovi*[*cs-rules*] **and** *cssi*[*cs-rules*] **and** *csdi*[*cs-rules*]  
**and** *csfi*[*cs-rules*]

**named-theorems** *cf-rules* **declare** *cfe*[*cf-rules*] **and** *cfb*[*cf-rules*] **and** *cfb*[*cf-rules*]  
**and** *cfov*[*cf-rules*] **and** *cfs* [*cf-rules*] **and** *cfv*[*cf-rules*] **and** *cff*[*cf-rules*] **and**  
*cfbi*[*cf-rules*] **and** *cfbi*[*cf-rules*] **and** *cfovi*[*cf-rules*] **and** *cfvi*[*cf-rules*] **and** *cfdi*[*cf-rules*]  
**and** *cfi*[*cf-rules*]

**named-theorems** *cd-rules* **declare** *cde*[*cd-rules*] **and** *cdb*[*cd-rules*] **and** *cdb*[*cd-rules*]



**and** *cdov*[*cd-rules*] **and** *cds* [*cd-rules*] **and** *cdd*[*cd-rules*] **and** *cdf*[*cd-rules*] **and**  
*cdbi*[*cd-rules*] **and** *cdbi*[*cd-rules*] **and** *cdovi*[*cd-rules*] **and** *cdsi*[*cd-rules*] **and** *cddi*[*cd-rules*]  
**and** *cdfi*[*cd-rules*]

**named-theorems** *cmi-rules* **declare** *cmie*[*cmi-rules*] **and** *cmib*[*cmi-rules*] **and**  
*cmib*[*cmi-rules*] **and** *cmiov*[*cmi-rules*] **and** *cmis* [*cmi-rules*] **and** *cmid*[*cmi-rules*]  
**and** *cmif*[*cmi-rules*] **and**  
*cmibi*[*cmi-rules*] **and** *cmibi*[*cmi-rules*] **and** *cmiovi*[*cmi-rules*] **and** *cmisi*[*cmi-rules*]  
**and** *cmidi*[*cmi-rules*] **and** *cmifi*[*cmi-rules*]

**named-theorems** *cbi-rules* **declare** *cbie*[*cbi-rules*] **and** *cbim*[*cbi-rules*] **and** *cbib*[*cbi-rules*]  
**and** *cbiov*[*cbi-rules*] **and** *cbis* [*cbi-rules*] **and** *cbid*[*cbi-rules*] **and** *cbif*[*cbi-rules*] **and**  
*cbimi*[*cbi-rules*] **and** *cbibi*[*cbi-rules*] **and** *cbiovi*[*cbi-rules*] **and** *cbisi*[*cbi-rules*] **and**  
*cbidi*[*cbi-rules*] **and** *cbifi*[*cbi-rules*]

**named-theorems** *covi-rules* **declare** *covie*[*covi-rules*] **and** *covib*[*covi-rules*] **and**  
*covib*[*covi-rules*] **and** *coviov*[*covi-rules*] **and** *covis* [*covi-rules*] **and** *covid*[*covi-rules*]  
**and** *covif*[*covi-rules*] **and**  
*covibi*[*covi-rules*] **and** *covibi*[*covi-rules*] **and** *coviovi*[*covi-rules*] **and** *covisi*[*covi-rules*]  
**and** *covidi*[*covi-rules*] **and** *covifi*[*covi-rules*]

**named-theorems** *csi-rules* **declare** *csie*[*csi-rules*] **and** *csib*[*csi-rules*] **and** *csib*[*csi-rules*]  
**and** *csiov*[*csi-rules*] **and** *csis* [*csi-rules*] **and** *csid*[*csi-rules*] **and** *csif*[*csi-rules*] **and**  
*csibi*[*csi-rules*] **and** *csibi*[*csi-rules*] **and** *csiovi*[*csi-rules*] **and** *csisi*[*csi-rules*] **and**  
*csidi*[*csi-rules*] **and** *csifi*[*csi-rules*]

**named-theorems** *cfi-rules* **declare** *cfie*[*cfi-rules*] **and** *cfib*[*cfi-rules*] **and** *cfib*[*cfi-rules*]  
**and** *cfiov*[*cfi-rules*] **and** *cfis* [*cfi-rules*] **and** *cfid*[*cfi-rules*] **and** *cfif*[*cfi-rules*] **and**  
*cfibi*[*cfi-rules*] **and** *cfibi*[*cfi-rules*] **and** *cfiovi*[*cfi-rules*] **and** *cfisi*[*cfi-rules*] **and** *cfidi*[*cfi-rules*]  
**and** *cfifi*[*cfi-rules*]

**named-theorems** *cdi-rules* **declare** *cdie*[*cdi-rules*] **and** *cdib*[*cdi-rules*] **and** *cdib*[*cdi-rules*]  
**and** *cdiov*[*cdi-rules*] **and** *cdis* [*cdi-rules*] **and** *cdid*[*cdi-rules*] **and** *cdif*[*cdi-rules*] **and**  
*cdibi*[*cdi-rules*] **and** *cdibi*[*cdi-rules*] **and** *cdiovi*[*cdi-rules*] **and** *cdisi*[*cdi-rules*] **and**  
*cdidi*[*cdi-rules*] **and** *cdifi*[*cdi-rules*]

**named-theorems** *cre-rules* **declare** *cee*[*cre-rules*] **and** *cme*[*cre-rules*] **and** *cbe*[*cre-rules*]  
**and** *cove*[*cre-rules*] **and** *cse*[*cre-rules*] **and** *cfe*[*cre-rules*] **and** *cde*[*cre-rules*] **and**  
*cmie*[*cre-rules*] **and** *cbie*[*cre-rules*] **and** *covie*[*cre-rules*] **and** *csie*[*cre-rules*] **and**  
*cfie*[*cre-rules*] **and** *cdie*[*cre-rules*]

**named-theorems** *crm-rules* **declare** *cem*[*crm-rules*] **and** *cbm*[*crm-rules*] **and**  
*cmm*[*crm-rules*] **and** *covm*[*crm-rules*] **and** *csm*[*crm-rules*] **and** *cfm*[*crm-rules*]  
**and** *cdm*[*crm-rules*] **and**  
*cmim*[*crm-rules*] **and** *cbim*[*crm-rules*] **and** *covim*[*crm-rules*] **and** *csim*[*crm-rules*]  
**and** *cfim*[*crm-rules*] **and** *cdim*[*crm-rules*]

**named-theorems** *crmi-rules* **declare** *cemi*[*crmi-rules*] **and** *cbmi*[*crmi-rules*] **and**  
*cmmi*[*crmi-rules*] **and** *covmi*[*crmi-rules*] **and** *csmi*[*crmi-rules*] **and** *cfmi*[*crmi-rules*]

**and** *cdmi*[*crmi-rules*] **and**  
*cmimi*[*crmi-rules*] **and** *cbimi*[*crmi-rules*] **and** *covimi*[*crmi-rules*] **and** *csimi*[*crmi-rules*]  
**and** *cfimi*[*crmi-rules*] **and** *cdimi*[*crmi-rules*]

**named-theorems** *crs-rules* **declare** *ces*[*crs-rules*] **and** *cbs*[*crs-rules*] **and** *cms*[*crs-rules*]  
**and** *covs*[*crs-rules*] **and** *css*[*crs-rules*] **and** *cfs*[*crs-rules*] **and** *cds*[*crs-rules*] **and**  
*cmis*[*crs-rules*] **and** *cbis*[*crs-rules*] **and** *covis*[*crs-rules*] **and** *csis*[*crs-rules*] **and** *cfis*[*crs-rules*]  
**and** *cdis*[*crs-rules*]

**named-theorems** *crsi-rules* **declare** *cesi*[*crsi-rules*] **and** *cbsi*[*crsi-rules*] **and** *cmsi*[*crsi-rules*]  
**and** *covsi*[*crsi-rules*] **and** *cssi*[*crsi-rules*] **and** *cfsi*[*crsi-rules*] **and** *cdsi*[*crsi-rules*]  
**and**  
*cmisi*[*crsi-rules*] **and** *cbisi*[*crsi-rules*] **and** *covisi*[*crsi-rules*] **and** *csisi*[*crsi-rules*]  
**and** *cfisi*[*crsi-rules*] **and** *cdisi*[*crsi-rules*]

**named-theorems** *crb-rules* **declare** *ceb*[*crb-rules*] **and** *cbb*[*crb-rules*] **and** *cmb*[*crb-rules*]  
**and** *covb*[*crb-rules*] **and** *csb*[*crb-rules*] **and** *cfb*[*crb-rules*] **and** *cdb*[*crb-rules*] **and**  
*cmib*[*crb-rules*] **and** *cbib*[*crb-rules*] **and** *covib*[*crb-rules*] **and** *csib*[*crb-rules*] **and**  
*cfib*[*crb-rules*] **and** *cdib*[*crb-rules*]

**named-theorems** *crbi-rules* **declare** *cebi*[*crbi-rules*] **and** *cbbi*[*crbi-rules*] **and** *cmbi*[*crbi-rules*]  
**and** *covbi*[*crbi-rules*] **and** *csbi*[*crbi-rules*] **and** *cfbi*[*crbi-rules*] **and** *cdbi*[*crbi-rules*]  
**and**  
*cmibi*[*crbi-rules*] **and** *cbibi*[*crbi-rules*] **and** *covibi*[*crbi-rules*] **and** *csibi*[*crbi-rules*]  
**and** *cfibi*[*crbi-rules*] **and** *cdibi*[*crbi-rules*]

**named-theorems** *crov-rules* **declare** *ceov*[*crov-rules*] **and** *cbov*[*crov-rules*] **and**  
*cmov*[*crov-rules*] **and** *covov*[*crov-rules*] **and** *csov*[*crov-rules*] **and** *cfov*[*crov-rules*]  
**and** *cdov*[*crov-rules*] **and**  
*cmiov*[*crov-rules*] **and** *cbiov*[*crov-rules*] **and** *coviov*[*crov-rules*] **and** *csiov*[*crov-rules*]  
**and** *cfiov*[*crov-rules*] **and** *cdiov*[*crov-rules*]

**named-theorems** *crovi-rules* **declare** *ceovi*[*crovi-rules*] **and** *cbovi*[*crovi-rules*] **and**  
*cmovi*[*crovi-rules*] **and** *covovi*[*crovi-rules*] **and** *csovi*[*crovi-rules*] **and** *cfovi*[*crovi-rules*]  
**and** *cdovi*[*crovi-rules*] **and**  
*cmiovi*[*crovi-rules*] **and** *cbiovi*[*crovi-rules*] **and** *coviovi*[*crovi-rules*] **and** *csiovi*[*crovi-rules*]  
**and** *cfiovi*[*crovi-rules*] **and** *cdiovi*[*crovi-rules*]

**named-theorems** *crf-rules* **declare** *cef*[*crf-rules*] **and** *cbf*[*crf-rules*] **and** *cmf*[*crf-rules*]  
**and** *covf*[*crf-rules*] **and** *csf*[*crf-rules*] **and** *cff*[*crf-rules*] **and** *cdf*[*crf-rules*] **and**  
*cmif*[*crf-rules*] **and** *cbif*[*crf-rules*] **and** *covif*[*crf-rules*] **and** *csif*[*crf-rules*] **and** *cfif*[*crf-rules*]  
**and** *cdif*[*crf-rules*]

**named-theorems** *crfi-rules* **declare** *cefi*[*crfi-rules*] **and** *cbfi*[*crfi-rules*] **and** *cmfi*[*crfi-rules*]  
**and** *covfi*[*crfi-rules*] **and** *csfi*[*crfi-rules*] **and** *cff*[*crfi-rules*] **and** *cdf*[*crfi-rules*] **and**

*cmifi*[*crfi-rules*] **and** *cbifi*[*crfi-rules*] **and** *covifi*[*crfi-rules*] **and** *csifi*[*crfi-rules*] **and**  
*cfifi*[*crfi-rules*] **and** *cdifi*[*crfi-rules*]

```

named-theorems crd-rules declare ced[crd-rules] and cbd[crd-rules] and cmd[crd-rules]
and covd[crd-rules] and csd[crd-rules] and cfid[crd-rules] and cdd[crd-rules] and
cmid[crd-rules] and cbid[crd-rules] and covid[crd-rules] and csid[crd-rules] and
cfid[crd-rules] and cdid[crd-rules]

```

```

named-theorems crdi-rules declare cedi[crdi-rules] and cbdi[crdi-rules] and cmdi[crdi-rules]
and covdi[crdi-rules] and csdi[crdi-rules] and cfdi[crdi-rules] and cddi[crdi-rules]
and
cmidi[crdi-rules] and cbidi[crdi-rules] and covidi[crdi-rules] and csidi[crdi-rules]
and cfidi[crdi-rules] and cdidi[crdi-rules]

```

```

end

```

```

theory disjoint-relations

```

```

imports

```

```

  allen

```

```

begin

```

## 4 PD property

The 13 time interval relations (i.e.  $e$ ,  $b$ ,  $m$ ,  $s$ ,  $f$ ,  $d$ ,  $ov$  and their inverse relations) are pairwise disjoint.

```

lemma em :  $e \cap m = \{\}$ 
using e m meets-irrefl
by (metis ComplI disjoint-eq-subset-Compl meets-wd subrelI)

```

```

lemma eb :  $e \cap b = \{\}$ 
using b e meets-asym
by (metis ComplI disjoint-eq-subset-Compl subrelI)

```

```

lemma eov :  $e \cap ov = \{\}$ 
apply (auto simp: e ov)
using elimmeets by blast

```

```

lemma es :  $e \cap s = \{\}$ 
apply (auto simp: e s)
using elimmeets by blast

```

```

lemma ef :  $e \cap f = \{\}$ 
using e f by (metis (no-types, lifting) ComplI disjoint-eq-subset-Compl meets-atrans subrelI)

```

**lemma**  $ed : e \cap d = \{\}$   
**using**  $e d$  **by** (*metis (no-types, lifting) ComplI disjoint-eq-subset-Compl meets-atrans subrelI*)

**lemma**  $emi : e \cap m^{\wedge-1} = \{\}$   
**using**  $converseE em e$   
**by** (*metis disjoint-iff-not-equal*)

**lemma**  $ebi : e \cap b^{\wedge-1} = \{\}$   
**using**  $converseE eb e$   
**by** (*metis disjoint-iff-not-equal*)

**lemma**  $eovi : e \cap ov^{\wedge-1} = \{\}$   
**using**  $converseE eov e$   
**by** (*metis disjoint-iff-not-equal*)

**lemma**  $esi : e \cap s^{\wedge-1} = \{\}$   
**using**  $converseE es e$   
**by** (*metis disjoint-iff-not-equal*)

**lemma**  $efi : e \cap f^{\wedge-1} = \{\}$   
**using**  $converseE ef e$   
**by** (*metis disjoint-iff-not-equal*)

**lemma**  $edi : e \cap d^{\wedge-1} = \{\}$   
**using**  $converseE ed e$   
**by** (*metis disjoint-iff-not-equal*)

**lemma**  $mb : m \cap b = \{\}$   
**using**  $m b$   
**apply**  $auto$   
**using**  $elimmeets$  **by**  $blast$

**lemma**  $mov : m \cap ov = \{\}$   
**apply** ( $auto simp:m ov$ )  
**by** ( $meson M1 elimmeets$ )

**lemma**  $ms : m \cap s = \{\}$   
**apply** ( $auto simp:m s$ )  
**by** ( $meson M1 elimmeets$ )

**lemma**  $mf : m \cap f = \{\}$   
**apply** ( $auto simp:m f$ )  
**using**  $elimmeets$  **by**  $blast$

**lemma**  $md : m \cap d = \{\}$   
**apply** ( $auto simp: m d$ )

**using** *trans2* **by** *blast*

**lemma** *mi* :  $m \cap m^{-1} = \{\}$

**apply** (*auto simp:m*)

**using** *converseE m meets-asm* **by** *blast*

**lemma** *mbi* :  $m \cap b^{-1} = \{\}$

**apply** (*auto simp:mb*)

**apply** (*auto simp: m b*)

**using** *nontrans2* **by** *blast*

**lemma** *movi* :  $m \cap ov^{-1} = \{\}$

**using** *m ov*

**apply** *auto*

**using** *trans2* **by** *blast*

**lemma** *msi* :  $m \cap s^{-1} = \{\}$

**apply** (*auto simp:m s*)

**by** (*meson M1 elimmeets*)

**lemma** *mfi* :  $m \cap f^{-1} = \{\}$

**apply** (*auto simp:m f*)

**by** (*meson M1 elimmeets*)

**lemma** *mdi* :  $m \cap d^{-1} = \{\}$

**apply** (*auto simp:m d*)

**using** *trans2* **by** *blast*

**lemma** *bov* :  $b \cap ov = \{\}$

**apply** (*auto simp:b ov*)

**by** (*meson M1 trans2*)

**lemma** *bs* :  $b \cap s = \{\}$

**apply** (*auto simp:b s*)

**by** (*meson M1 trans2*)

**lemma** *bf* :  $b \cap f = \{\}$

**apply** (*auto simp: b f*)

**by** (*meson M1 trans2*)

**lemma** *bd* :  $b \cap d = \{\}$

**apply** (*auto simp:b d*)

**by** (*meson M1 nonmeets4*)

**lemma** *bmi* :  $b \cap m^{-1} = \{\}$

**using** *mbi* **by** *auto*

**lemma** *bi* :  $b \cap b^{-1} = \{\}$

**apply** (*auto simp:b*)  
**using** *M5exist-var3 trans2* **by** *blast*

**lemma** *bovi* :  $b \cap ov^{-1} = \{\}$   
**apply** (*auto simp:bov*)  
**apply** (*auto simp:b ov*)  
**by** (*meson M1 nontrans2*)

**lemma** *bsi* :  $b \cap s^{-1} = \{\}$   
**using** *bs* **apply** *auto* **using** *b s* **apply** *auto*  
**using** *trans2* **by** *blast*

**lemma** *bfi* :  $b \cap f^{-1} = \{\}$   
**using** *bf* **apply** *auto* **using** *b f* **apply** *auto*  
**using** *trans2* **by** *blast*

**lemma** *bdi* :  $b \cap d^{-1} = \{\}$   
**apply** (*auto simp:bd*)  
**apply** (*auto simp:b d*)  
**using** *trans2*  
**using** *M1 nonmeets4* **by** *blast*

**lemma** *ovs* :  $ov \cap s = \{\}$   
**apply** (*auto simp:ov s*)  
**by** (*meson M1 meets-atrans*)

**lemma** *ovf* :  $ov \cap f = \{\}$   
**apply** (*auto simp:ov f*)  
**by** (*meson M1 meets-atrans*)

**lemma** *ovd* :  $ov \cap d = \{\}$   
**apply** (*auto simp:ov d*)  
**by** (*meson M1 trans2*)

**lemma** *ovmi* :  $ov \cap m^{-1} = \{\}$   
**using** *movi* **by** *auto*

**lemma** *ovbi* :  $ov \cap b^{-1} = \{\}$   
**using** *bovi* **by** *blast*

**lemma** *ovi* :  $ov \cap ov^{-1} = \{\}$   
**apply** (*auto simp:ov*)  
**by** (*meson M1 trans2*)

**lemma** *ovsi* :  $ov \cap s^{-1} = \{\}$   
**apply** (*auto simp:ov s*)  
**by** (*meson M1 elimmeets*)

**lemma** *ovfi* :  $ov \cap f^{-1} = \{\}$   
**apply** (*auto simp:ov f*)  
**by** (*meson M1 elimmeets*)

**lemma** *ovdi* :  $ov \cap d^{-1} = \{\}$   
**apply** (*auto simp:ov d*)  
**by** (*meson M1 trans2*)

**lemma** *sf* :  $s \cap f = \{\}$   
**apply** (*auto simp:s f*)  
**by** (*metis M4 elimmeets*)

**lemma** *sd* :  $s \cap d = \{\}$   
**apply** (*auto simp:s d*)  
**by** (*metis M1 meets-atrans*)

**lemma** *smi* :  $s \cap m^{-1} = \{\}$   
**using** *msi* **by** *auto*

**lemma** *sbi* :  $s \cap b^{-1} = \{\}$   
**using** *bsi* **by** *blast*

**lemma** *sovi* :  $s \cap ov^{-1} = \{\}$   
**using** *ovsi* **by** *auto*

**lemma** *si* :  $s \cap s^{-1} = \{\}$   
**apply** (*auto simp:s*)  
**by** (*meson M1 trans2*)

**lemma** *sfi* :  $s \cap f^{-1} = \{\}$   
**apply** (*auto simp:s f*)  
**by** (*metis M4 elimmeets*)

**lemma** *sdi* :  $s \cap d^{-1} = \{\}$   
**apply** (*auto simp:s d*)  
**by** (*meson M1 meets-atrans*)

**lemma** *fd* :  $f \cap d = \{\}$   
**apply** (*auto simp:f d*)  
**by** (*meson M1 meets-atrans*)

**lemma** *fmi* :  $f \cap m^{-1} = \{\}$   
**using** *mfi* **by** *auto*

**lemma** *fbi* :  $f \cap b^{-1} = \{\}$

**using** *bfi converse-Int* **by** *auto*

**lemma** *fovi* :  $f \cap ov^{-1} = \{\}$   
**using** *ovfi* **by** *auto*

**lemma** *fsi* :  $f \cap s^{-1} = \{\}$   
**using** *sfi* **by** *auto*

**lemma** *fi* :  $f \cap f^{-1} = \{\}$   
**apply** (*auto simp:f*)  
**by** (*meson M1 trans2*)

**lemma** *fdi* :  $f \cap d^{-1} = \{\}$   
**apply** (*auto simp:f d*)  
**by** (*meson M1 trans2*)

**lemma** *dmi* :  $d \cap m^{-1} = \{\}$   
**using** *mdi* **by** *auto*

**lemma** *dbi* :  $d \cap b^{-1} = \{\}$   
**using** *bdi* **by** *blast*

**lemma** *dovi* :  $d \cap ov^{-1} = \{\}$   
**using** *ovdi* **by** *auto*

**lemma** *dsi* :  $d \cap s^{-1} = \{\}$   
**using** *sdi* **by** *auto*

**lemma** *dfi* :  $d \cap f^{-1} = \{\}$   
**apply** (*auto simp:d f*)  
**by** (*meson M1 trans2*)

**lemma** *di* :  $d \cap d^{-1} = \{\}$   
**apply** (*auto simp:d*)  
**by** (*meson M1 trans2*)

**lemma** *mibi* :  $m^{-1} \cap b^{-1} = \{\}$   
**using** *mb* **by** *auto*

**lemma** *miovi* :  $m^{-1} \cap ov^{-1} = \{\}$   
**using** *mov* **by** *auto*

**lemma** *misi* :  $m^{-1} \cap s^{-1} = \{\}$   
**using** *ms* **by** *auto*

**lemma** *mifi* :  $m^{-1} \cap f^{-1} = \{\}$



using *mf* by *auto*

lemma *midi* :  $m^{-1} \cap d^{-1} = \{\}$   
using *md* by *auto*

lemma *bid* :  $b^{-1} \cap d = \{\}$   
by (*simp add: dbi inf-sup-aci(1)*)

lemma *bimi* :  $b^{-1} \cap m^{-1} = \{\}$   
using *mibi* by *auto*

lemma *biovi* :  $b^{-1} \cap ov^{-1} = \{\}$   
using *bov* by *blast*

lemma *bisi* :  $b^{-1} \cap s^{-1} = \{\}$   
using *bs* by *blast*

lemma *bifi* :  $b^{-1} \cap f^{-1} = \{\}$   
using *bf* by *blast*

lemma *bidi* :  $b^{-1} \cap d^{-1} = \{\}$   
using *bd* by *blast*

lemma *ovisi* :  $ov^{-1} \cap s^{-1} = \{\}$   
using *ovs* by *blast*

lemma *ovifi* :  $ov^{-1} \cap f^{-1} = \{\}$   
using *ovf* by *blast*

lemma *ovidi* :  $ov^{-1} \cap d^{-1} = \{\}$   
using *ovd* by *blast*

lemma *sifi* :  $s^{-1} \cap f^{-1} = \{\}$   
using *sf* by *blast*

lemma *sidi* :  $s^{-1} \cap d^{-1} = \{\}$   
using *sd* by *blast*

lemma *fidi* :  $f^{-1} \cap d^{-1} = \{\}$   
using *fd* by *blast*

lemma *eei*[*simp*] :  $e^{-1} = e$   
using *e*

by (*metis converse-iff subrelI subset-antisym*)

**lemma** *rdisj-sym*:  $A \cap B = \{\} \implies B \cap A = \{\}$   
by *auto*

#### 4.1 Intersection rules

**named-theorems** *e-rules* **declare** *em*[*e-rules*] **and** *eb*[*e-rules*] **and** *eov*[*e-rules*]  
**and** *es*[*e-rules*] **and** *ef*[*e-rules*] **and** *ed*[*e-rules*] **and** *emi*[*e-rules*] **and** *ebi*[*e-rules*]  
**and** *eovi*[*e-rules*]  
**and** *esi*[*e-rules*] **and** *efi*[*e-rules*] **and** *edi*[*e-rules*]

**named-theorems** *m-rules* **declare** *em*[*THEN rdisj-sym, m-rules*] **and** *mb* [*m-rules*]  
**and** *ms* [*m-rules*] **and** *mov* [*m-rules*] **and** *mf*[*m-rules*] **and**  
*md*[*m-rules*] **and** *mi* [*m-rules*] **and** *mbi* [*m-rules*] **and** *movi* [*m-rules*] **and** *msi*  
[*m-rules*] **and** *mfi* [*m-rules*] **and** *mdi* [*m-rules*] **and** *emi*[*m-rules*]

**named-theorems** *b-rules* **declare** *eb*[*THEN rdisj-sym, b-rules*] **and** *mb* [*THEN*  
*rdisj-sym, b-rules*] **and** *bs* [*b-rules*] **and** *bov* [*b-rules*] **and** *bf*[*b-rules*] **and**  
*bd*[*b-rules*] **and** *bmi* [*b-rules*] **and** *bi* [*b-rules*] **and** *bovi* [*b-rules*] **and** *bsi* [*b-rules*]  
**and** *bfi* [*b-rules*] **and** *bdi* [*b-rules*] **and** *ebi*[*b-rules*]

**named-theorems** *ov-rules* **declare** *eov*[*THEN rdisj-sym, ov-rules*] **and** *mov* [*THEN*  
*rdisj-sym, ov-rules*] **and** *ovs* [*ov-rules*] **and** *bov* [*THEN rdisj-sym, ov-rules*] **and**  
*ovf*[*ov-rules*] **and**  
*ovd*[*ov-rules*] **and** *ovmi* [*ov-rules*] **and** *ovi* [*ov-rules*] **and** *ovsi* [*ov-rules*] **and** *ovfi*  
[*ov-rules*] **and** *ovdi* [*ov-rules*] **and** *eovi*[*ov-rules*]

**named-theorems** *s-rules* **declare** *es*[*THEN rdisj-sym, s-rules*] **and** *ms* [*THEN*  
*rdisj-sym, s-rules*] **and** *ovs* [*THEN rdisj-sym, s-rules*] **and** *bs* [*THEN rdisj-sym, s-rules*]  
**and** *sf*[*s-rules*] **and**  
*sd*[*s-rules*] **and** *smi* [*s-rules*] **and** *sovi* [*s-rules*] **and** *si* [*s-rules*] **and** *sfi* [*s-rules*]  
**and** *sdi* [*s-rules*]

**named-theorems** *d-rules* **declare** *ed*[*THEN rdisj-sym, d-rules*] **and** *md* [*THEN*  
*rdisj-sym, d-rules*] **and** *sd* [*THEN rdisj-sym, d-rules*] **and** *fd*[*THEN rdisj-sym,*  
*d-rules*] **and**  
*ovd*[*THEN rdisj-sym, d-rules*] **and** *dmi* [*d-rules*] **and** *dovi* [*d-rules*] **and** *dsi* [*d-rules*]  
**and** *dfi* [*d-rules*] **and** *di* [*d-rules*]

**named-theorems** *f-rules* **declare** *ef*[*THEN rdisj-sym, f-rules*] **and** *mf* [*THEN*  
*rdisj-sym, f-rules*] **and** *sf* [*THEN rdisj-sym, f-rules*] **and** *ovf* [*THEN rdisj-sym, f-rules*]  
**and** *fd*[*f-rules*] **and**  
*fmi* [*f-rules*] **and** *fovi* [*f-rules*] **and** *fsi* [*f-rules*] **and** *fi* [*f-rules*] **and** *fdi* [*f-rules*]

**end**

**theory** *jointly-exhaustive*

**imports**

*allen*

**begin**

## 5 JE property

The 13 time interval relations are jointly exhaustive. For any two intervals  $x$  and  $y$ , we can find a basic relation  $r$  such that  $(x, y) \in r$ .

**lemma** (in *arelations*) *jointly-exhaustive*:

**assumes**  $\mathcal{I} p \mathcal{I} q$

**shows**  $(p::'a, q::'a) \in b \vee (p, q) \in m \vee (p, q) \in ov \vee (p, q) \in s \vee (p, q) \in d \vee (p, q) \in f^{\wedge-1} \vee (p, q) \in e \vee$

$(p, q) \in f \vee (p, q) \in s^{\wedge-1} \vee (p, q) \in d^{\wedge-1} \vee (p, q) \in ov^{\wedge-1} \vee (p, q) \in m^{\wedge-1} \vee (p, q) \in b^{\wedge-1}$  (is  $?R$ )

**proof** –

**obtain**  $k k' u u'::'a$  **where**  $kp:k\|p$  **and**  $kpq:k'\|q$  **and**  $pu:p\|u$  **and**  $qup:q\|u'$  **using**  $M3$  *meets-wd assms(1,2)* **by** *fastforce*

**from**  $kp kpq$  **have**  $k\|q \oplus ((\exists t. k\|t \wedge t\|q) \oplus (\exists t. k'\|t \wedge t\|p))$  (is  $?A \oplus (?B \oplus ?C)$ ) **using**  $M2$  **by** *blast*

**then have**  $(?A \wedge \neg ?B \wedge \neg ?C) \vee ((\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C))$  **by** (*insert xor-distr-L[of ?A ?B ?C], auto simp:elimmeets*)

**thus**  $?thesis$

**proof** (*elim disjE*)

{ **assume**  $?A \wedge \neg ?B \wedge \neg ?C$  **then have**  $kq:?A$  **by** *simp*

**from**  $pu qup$  **have**  $p\|u' \oplus ((\exists t'::'a. p\|t' \wedge t'\|u') \oplus (\exists t'. q\|t' \wedge t'\|u))$  (is  $?A \oplus (?B \oplus ?C)$ ) **using**  $M2$  **by** *blast*

**then have**  $(?A \wedge \neg ?B \wedge \neg ?C) \vee ((\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C))$  **by** (*insert xor-distr-L[of ?A ?B ?C], auto simp:elimmeets*)

**thus**  $?thesis$

**proof** (*elim disjE*)

{**assume**  $(?A \wedge \neg ?B \wedge \neg ?C)$  **then have**  $?A$  **by** *simp*

**with**  $kp kq qup$  **have**  $p = q$  **using**  $M4$  **by** *auto*

**thus**  $?thesis$  **using**  $e$  **by** *auto*}

**next**

{**assume**  $\neg ?A \wedge ?B \wedge \neg ?C$  **then have**  $?B$  **by** *simp*

**with**  $kq kp qup$  **show**  $?thesis$  **using**  $s$  **by** *blast*}

**next**

{**assume**  $(\neg ?A \wedge \neg ?B \wedge ?C)$  **then have**  $?C$  **by** *simp*

**then obtain**  $t'$  **where**  $q\|t'$  **and**  $t'\|u$  **by** *blast*

**with**  $kq kp pu$  **show**  $?thesis$  **using**  $s$  **by** *blast* }

**qed**}

**next**

{ **assume**  $\neg ?A \wedge ?B \wedge \neg ?C$  **then have**  $?B$  **by** *simp*

**then obtain  $t$  where  $kt:k||t$  and  $tq:t||q$  by *auto***  
**from  $pu\ qup$  have  $p||u' \oplus ((\exists t'. p||t' \wedge t''||u')) \oplus (\exists t'. q||t' \wedge t''||u)$  (is  $?A \oplus (?B \oplus ?C)$ ) using  $M2$  by *blast***  
**then have  $(?A \wedge \neg ?B \wedge \neg ?C) \vee ((\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C))$  by**  
*(insert xor-distr-L[of ?A ?B ?C], auto simp:elimmeets)*  
**thus  $?thesis$**   
**proof (elim disjE)**  
**{assume  $?A \wedge \neg ?B \wedge \neg ?C$  then have  $?A$  by *simp***  
**with  $kp\ qup\ kt\ tq$  show  $?thesis$  using  $f$  by *blast*}**  
**next**  
**{assume  $\neg ?A \wedge ?B \wedge \neg ?C$  then have  $?B$  by *simp***  
**then obtain  $t'$  where  $ptp:p||t'$  and  $tpup:t''||u'$  by *auto***  
**from  $pu\ tq$  have  $p||q \oplus ((\exists t''. p||t'' \wedge t'''||q) \oplus (\exists t''. t||t'' \wedge t'''||u))$  (is**  
 $?A \oplus (?B \oplus ?C)$ **) using  $M2$  by *blast***  
**then have  $(?A \wedge \neg ?B \wedge \neg ?C) \vee ((\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C))$  by**  
*(insert xor-distr-L[of ?A ?B ?C], auto simp:elimmeets)*  
**thus  $?thesis$**   
**proof (elim disjE)**  
**{assume  $?A \wedge \neg ?B \wedge \neg ?C$  then have  $?A$  by *simp***  
**thus  $?thesis$  using  $m$  by *auto*}**  
**next**  
**{assume  $\neg ?A \wedge ?B \wedge \neg ?C$  then have  $?B$  by *simp***  
**thus  $?thesis$  using  $b$  by *auto*}**  
**next**  
**{assume  $\neg ?A \wedge \neg ?B \wedge ?C$  then have  $?C$  by *simp***  
**then obtain  $g$  where  $t||g$  and  $g||u$  by *auto***  
**moreover with  $pu\ ptp$  have  $g||t'$  using  $M1$  by *blast***  
**ultimately show  $?thesis$  using  $ov\ kt\ tq\ kp\ ptp\ tpup\ qup$  by *blast*}**  
**qed}**  
**next**  
**{assume  $\neg ?A \wedge \neg ?B \wedge ?C$  then have  $?C$  by *simp***  
**then obtain  $t'$  where  $q||t'$  and  $t''||u$  by *auto***  
**with  $kp\ kt\ tq\ pu$  show  $?thesis$  using  $d$  by *blast*}**  
**qed}**  
**next**  
**{assume  $\neg ?A \wedge \neg ?B \wedge ?C$  then have  $?C$  by *simp***  
**then obtain  $t$  where  $kpt:k'||t$  and  $tp:t||p$  by *auto***  
**from  $pu\ qup$  have  $p||u' \oplus ((\exists t'. p||t' \wedge t''||u')) \oplus (\exists t'. q||t' \wedge t''||u)$  (is  $?A \oplus (?B \oplus ?C)$ ) using  $M2$  by *blast***  
**then have  $(?A \wedge \neg ?B \wedge \neg ?C) \vee ((\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C))$  by**  
*(insert xor-distr-L[of ?A ?B ?C], auto simp:elimmeets)*  
**thus  $?thesis$**   
**proof (elim disjE)**  
**{assume  $?A \wedge \neg ?B \wedge \neg ?C$  then have  $?A$  by *simp***  
**with  $qup\ kpt\ tp\ kpq$  show  $?thesis$  using  $f$  by *blast*}**  
**next**  
**{assume  $\neg ?A \wedge ?B \wedge \neg ?C$  then have  $?B$  by *simp***  
**with  $qup\ kpt\ tp\ kpq$  show  $?thesis$  using  $d$  by *blast*}**  
**next**

```

    {assume  $\neg ?A \wedge \neg ?B \wedge ?C$  then obtain  $t'$  where  $qt':q||t'$  and  $tpc:t'||u$  by
  auto
    from  $qup\ tp$  have  $q||p \oplus ((\exists t''. q||t'' \wedge t''||p) \oplus (\exists t''. t||t'' \wedge t''||u'))$  (is
   $?A \oplus (?B \oplus ?C)$ ) using  $M2$  by blast
    then have  $(?A \wedge \neg ?B \wedge \neg ?C) \vee ((\neg ?A \wedge ?B \wedge \neg ?C) \vee (\neg ?A \wedge \neg ?B \wedge ?C))$  by
  (insert xor-distr-L[of  $?A\ ?B\ ?C$ ], auto simp:elimmeets)
    thus ?thesis
    proof (elim disjE)
      {assume  $?A \wedge \neg ?B \wedge \neg ?C$  then have  $?A$  by simp
      thus ?thesis using  $m$  by auto}
    next
      {assume  $\neg ?A \wedge ?B \wedge \neg ?C$  then have  $?B$  by simp
      thus ?thesis using  $b$  by auto}
    next
      {assume  $\neg ?A \wedge \neg ?B \wedge ?C$  then obtain  $g$  where  $tg:t||g$  and  $g||u'$  by
  auto
        with  $qup\ qt'$  have  $g||t'$  using  $M1$  by blast
        with  $qt'\ tpc\ pu\ kpq\ kpt\ tp\ tg$  show ?thesis using  $ov$  by blast}
    qed}
  qed}
qed
qed

```

**lemma** (in *arelations*) *JE*:  
**assumes**  $\mathcal{I}\ p\ \mathcal{I}\ q$   
**shows**  $(p::'a,q::'a) \in b \cup m \cup ov \cup s \cup d \cup f^{-1} \cup e \cup f \cup s^{-1} \cup d^{-1} \cup$   
 $ov^{-1} \cup m^{-1} \cup b^{-1}$   
**using** *jointly-exhaustive UnCI assms(1,2)* by blast

**end**

**theory** *examples*

**imports**

*disjoint-relations*

**begin**

## 6 Examples

### 6.1 Compositions of non-basic relations

Basic relations are the 13 time interval relations. The unions of basic relations are also relations and their compositions is the union of compositions.

We prove few of these compositions that are required in theory nest.thy.

**method** (in *arelations*) *e-compose* = (match **conclusion** in  $e \ O \ b \subseteq - \Rightarrow \langle \text{insert } \text{ceb}, \text{blast} \rangle$   
 $| - \Rightarrow \langle \text{match conclusion in } e \ O \ m \subseteq - \Rightarrow \langle \text{insert } \text{cem}, \text{blast} \rangle | - \Rightarrow \langle \text{fail} \rangle \rangle$ )

**declare** [[*simp-trace-depth-limit=4*]]

**lemma** *eovisidifmifiOm*: $(e \cup \text{ov}^{-1} \cup s^{-1} \cup d^{-1} \cup f \cup m^{-1} \cup \widehat{f^{-1}}) \ O \ m \subseteq m \cup \text{ov} \cup \widehat{f^{-1}} \cup \widehat{d^{-1}} \cup s \cup s^{-1} \cup e$

**apply** (*simp*, *intro conjI*)  
**using** *cem* **apply** *blast*  
**using** *crm-rules* **by** *auto*

**lemma** *ovsmfidiesiOmi*: $(\text{ov} \cup s \cup m \cup \widehat{f^{-1}} \cup \widehat{d^{-1}} \cup e \cup \widehat{s^{-1}}) \ O \ m \widehat{-1} \subseteq \widehat{d^{-1}} \cup \widehat{s^{-1}} \cup \widehat{\text{ov}^{-1}} \cup \widehat{m^{-1}} \cup \widehat{f^{-1}} \cup f \cup e$

**apply** (*simp*, *intro conjI*)  
**using** *crmi-rules* **by** *auto*

**lemma** *ovsmfidiesiOm*: $(\text{ov} \cup s \cup m \cup f^{-1} \cup d^{-1} \cup e \cup s^{-1}) \ O \ m \subseteq b \cup \text{ov} \cup \widehat{f^{-1}} \cup \widehat{d^{-1}} \cup m$

**apply** (*simp*, *intro conjI*)  
**using** *crm-rules* **by** *auto*

**lemma** *ovsmfidiesiOssie*: $(\text{ov} \cup s \cup m \cup f^{-1} \cup d^{-1} \cup e \cup s^{-1}) \ O \ (s \cup \widehat{s^{-1}} \cup e) \subseteq \text{ov} \cup \widehat{f^{-1}} \cup \widehat{d^{-1}} \cup s \cup e \cup \widehat{s^{-1}} \cup m$

**apply** (*simp*, *intro conjI*)  
**using** *crs-rules* **apply** *auto*[7]  
**using** *crsi-rules* **apply** *auto*[7]  
**using** *cre-rules* **by** *auto*[7]

**lemma**  $(b \cup m \cup \text{ov} \cup s \cup d) \ O \ (b \cup m \cup \text{ov} \cup s \cup d) \subseteq b \cup m \cup \text{ov} \cup s \cup d$

**apply** (*simp*, *intro conjI*)  
**using** *crb-rules* **apply** *auto*[5]  
**using** *crm-rules* **apply** *auto*[5]  
**using** *crov-rules* **apply** *auto*[5]  
**using** *crs-rules* **apply** *auto*[5]  
**using** *crd-rules* **by** *auto*[5]

**lemma** *ebmovovissifsiddib*: $(e \cup b \cup m \cup \text{ov} \cup \text{ov}^{-1} \cup s \cup s^{-1} \cup f \cup f^{-1} \cup d \cup d^{-1}) \ O \ b \subseteq b \cup m \cup \text{ov} \cup \widehat{f^{-1}} \cup \widehat{d^{-1}}$

**apply** (*simp*, *intro conjI*)  
**using** *crb-rules* **by** *auto*

**lemma** *ebmovovissiffiddibmovsd*: $(e \cup b \cup m \cup \text{ov} \cup \text{ov}^{-1} \cup s \cup s^{-1} \cup f \cup f^{-1} \cup$

$d \cup d^{-1} \cup O ( b \cup m \cup ov \cup s \cup d ) \subseteq ( b \cup m \cup ov \cup s \cup d \cup f^{-1} \cup d^{-1} \cup ov^{-1} \cup s^{-1} \cup f \cup e )$

**apply** (*simp*, *intro conjI*)  
**using** *crb-rules* **apply** *auto*[11]  
**using** *crm-rules* **apply** *auto*[11]  
**using** *crov-rules* **apply** *auto*[11]  
**using** *crs-rules* **apply** *auto*[11]  
**using** *crd-rules* **by** *auto*

**lemma** *difimov*: $(d^{-1} \cup f^{-1} \cup ov \cup e \cup f \cup m \cup b \cup s^{-1} \cup s) \cup O ( m \cup ov \cup s \cup d \cup b \cup f^{-1} \cup f \cup e ) \subseteq ( e \cup b \cup m \cup ov \cup ov^{-1} \cup s \cup s^{-1} \cup f \cup f^{-1} \cup d \cup d^{-1} )$

**apply** (*simp*, *intro conjI*)  
**using** *crm-rules* **apply** *auto*[9]  
**using** *crov-rules* **apply** *auto*[9]  
**using** *crs-rules* **apply** *auto*[9]  
**using** *crd-rules* **apply** *auto*[9]  
**using** *crb-rules* **apply** *auto*[9]  
**using** *crfi-rules* **apply** *auto*[9]  
**using** *crf-rules* **apply** *auto*[9]  
**using** *cre-rules* **by** *auto*

**lemma** *difibs*: $(d^{-1} \cup f^{-1} \cup ov \cup e \cup f \cup m \cup b \cup s^{-1} \cup s) \cup O ( b \cup s \cup m ) \subseteq ( b \cup m \cup ov \cup f^{-1} \cup d^{-1} \cup d \cup e \cup s \cup s^{-1} )$

**apply** (*simp*, *intro conjI*)  
**using** *crb-rules* **apply** *auto*[9]  
**using** *crs-rules* **apply** *auto*[9]  
**using** *crm-rules* **by** *auto*

**lemma** *bebmovovissiffiddi*: $b \cup O ( e \cup b \cup m \cup ov \cup ov^{-1} \cup s \cup s^{-1} \cup f \cup f^{-1} \cup d \cup d^{-1} ) \subseteq ( b \cup m \cup ov \cup s \cup d )$

**apply** (*simp*, *intro conjI*)  
**using** *cb-rules* **by** *auto*[11]

**lemma** *ovsmfidiesi*: $((ov \cup s \cup m \cup f^{-1} \cup d^{-1} \cup e \cup s^{-1}) \cup O ( ov^{-1} \cup s^{-1} \cup m^{-1} \cup f \cup d \cup e \cup s )) \subseteq ( s \cup s^{-1} \cup f \cup f^{-1} \cup d \cup d^{-1} \cup e \cup ov \cup ov^{-1} \cup m \cup m^{-1} )$

**apply** (*simp*, *intro conjI*)  
**using** *crovi-rules* **apply** *auto*[7]  
**using** *crsi-rules* **apply** *auto*[7]  
**using** *crmi-rules* **apply** *auto*[7]  
**using** *crf-rules* **apply** *auto*[7]  
**using** *crd-rules* **apply** *auto*[7]  
**using** *cre-rules* **apply** *auto*[7]  
**using** *crs-rules* **by** *auto*

**lemma** *pii* $q:(p,i) \in ov \cup s \cup m \cup f^{-1} \cup d^{-1} \cup e \cup s^{-1} \implies (i,q) \in ov^{-1} \cup s^{-1} \cup m^{-1} \cup f \cup d \cup e \cup s \implies (p,q) \in s \cup s^{-1} \cup f \cup f^{-1} \cup d \cup d^{-1} \cup e \cup ov \cup ov^{-1} \cup m \cup m^{-1}$

**using** *ovsmfidiesi relcomp.relcompI subsetCE* **by** *blast*

**lemma** *ceovisidiffimi-ffie*:  $(e \cup ov^{-1} \cup s^{-1} \cup d^{-1} \cup f \cup f^{-1} \cup m^{-1}) \ O \ (f \cup f^{-1} \cup e) \subseteq e \cup ov^{-1} \cup s^{-1} \cup d^{-1} \cup f \cup f^{-1} \cup m^{-1}$   
**apply** (*simp, intro conjI*)  
**using** *crf-rules* **apply** *auto*[7]  
**using** *crfi-rules* **apply** *auto*[7]  
**using** *cre-rules* **by** *auto*

**lemma** *ceovisidiffimi-ffie-simp*:  $(p, i) \in (e \cup ov^{-1} \cup s^{-1} \cup d^{-1} \cup f \cup f^{-1} \cup m^{-1}) \implies (i, q) \in (f \cup f^{-1} \cup e) \implies (p, q) \in e \cup ov^{-1} \cup s^{-1} \cup d^{-1} \cup f \cup f^{-1} \cup m^{-1}$

**using** *ceovisidiffimi-ffie relcomp.relcompI subsetCE* **by** *blast*

**lemma** *ceovisidiffimi-fife*:  $(e \cup ov^{-1} \cup s^{-1} \cup d^{-1} \cup f \cup f^{-1} \cup m^{-1}) \ O \ (f^{-1} \cup f \cup e) \subseteq e \cup ov^{-1} \cup s^{-1} \cup d^{-1} \cup f \cup f^{-1} \cup m^{-1}$   
**apply** (*simp, intro conjI*)  
**using** *cefi covifi csifi cdifi cffi cfifi cmifi covifi csifi cdifi* **apply** *auto*[7]  
**using** *cef covif csif cdif cff cfif cmif* **apply** *auto*[7]  
**using** *cee covie csie cdie cfe cfie cmie* **by** *auto*[7]

**lemma**  $(x, j) \in e \cup ov^{-1} \cup s^{-1} \cup d^{-1} \cup f \cup f^{-1} \cup m^{-1} \implies (j, i) \in f^{-1} \cup f \cup e \implies (x, i) \in e \cup ov^{-1} \cup s^{-1} \cup d^{-1} \cup f \cup f^{-1} \cup m^{-1}$   
**using** *ceovisidiffimi-ffie-simp* **by** *blast*

**lemma** *m-ovsmfidiesi:m*  $O \ (ov \cup s \cup m \cup f^{-1} \cup d^{-1} \cup e \cup s^{-1}) \subseteq b \cup s \cup m$   
**apply** (*simp, intro conjI*)  
**using** *cm-rules* **by** *auto*

**lemma** *ovsmfidiesi-d*:  $(ov \cup s \cup m \cup f^{-1} \cup d^{-1} \cup e \cup s^{-1}) \ O \ d \subseteq e \cup s \cup d \cup ov \cup ov^{-1} \cup s^{-1} \cup f \cup f^{-1} \cup d^{-1}$   
**apply** (*simp, intro conjI*)  
**using** *crd-rules* **by** *auto*[7]

**lemma** *cbi-esdovovisiffidi*:  $b^{-1} \ O \ (e \cup s \cup d \cup ov \cup ov^{-1} \cup s^{-1} \cup f \cup f^{-1} \cup d^{-1}) \subseteq b^{-1} \cup m^{-1} \cup ov^{-1} \cup f \cup d$   
**apply** (*simp, intro conjI*)  
**using** *cbi-rules* **by** *auto*[9]

**lemma** *cm-alpha1alpha4mi:m*  $O \ (e \cup ov^{-1} \cup s^{-1} \cup d^{-1} \cup f \cup f^{-1} \cup m^{-1}) \subseteq m \cup ov \cup s \cup d \cup b \cup f^{-1} \cup f \cup e$   
**apply** (*simp, intro conjI*)  
**using** *cm-rules* **by** *auto*

**lemma** *cbi-alpha1alpha4mi*:  $b^{-1} \ O \ (e \cup ov^{-1} \cup s^{-1} \cup d^{-1} \cup f \cup f^{-1} \cup m^{-1}) \subseteq b^{-1}$



**apply** (*simp*, *intro conjI*)  
**using** *cbi-rules* **by** *auto*

**lemma** *cbeta2-beta2*: $(b \cup m \cup ov \cup f^{-1} \cup d^{-1}) \cap O (b \cup m \cup ov \cup f^{-1} \cup d^{-1}) \subseteq b \cup m \cup ov \cup f^{-1} \cup d^{-1}$

**apply** (*simp*, *intro conjI*)  
**using** *crb-rules* **apply** *auto*[5]  
**using** *crm-rules* **apply** *auto*[5]  
**using** *crov-rules* **apply** *auto*[5]  
**using** *crfi-rules* **apply** *auto*[5]  
**using** *crdi-rules* **by** *auto*

**lemma** *cbeta2-gammabm*: $(b \cup m \cup ov \cup f^{-1} \cup d^{-1}) \cap O (e \cup b \cup m \cup ov \cup ov^{-1} \cup s \cup s^{-1} \cup f \cup f^{-1} \cup d \cup d^{-1}) \subseteq (e \cup b \cup m \cup ov \cup ov^{-1} \cup s \cup s^{-1} \cup f \cup f^{-1} \cup d \cup d^{-1})$

**apply** (*simp*, *intro conjI*)  
**using** *cre-rules* **apply** *auto*[5]  
**using** *crb-rules* **apply** *auto*[5]  
**using** *crm-rules* **apply** *auto*[5]  
**using** *crov-rules* **apply** *auto*[5]  
**using** *crovi-rules* **apply** *auto*[5]  
**using** *crs-rules* **apply** *auto*[5]  
**using** *crsi-rules* **apply** *auto*[5]  
**using** *crf-rules* **apply** *auto*[5]  
**using** *crfi-rules* **apply** *auto*[5]  
**using** *crd-rules* **apply** *auto*[5]  
**using** *crdi-rules* **by** *auto*

**lemma** *calpha1-alpha1*: $(b \cup m \cup ov \cup s \cup d) \cap O (b \cup m \cup ov \cup s \cup d) \subseteq (b \cup m \cup ov \cup s \cup d)$

**apply** (*simp*, *intro conjI*)  
**using** *crb-rules* **apply** *auto*[5]  
**using** *crm-rules* **apply** *auto*[5]  
**using** *crov-rules* **apply** *auto*[5]  
**using** *crs-rules* **apply** *auto*[5]  
**using** *crd-rules* **by** *auto*

## 6.2 Intersection of non-basic relations

**lemma** *inter-ov*:

**assumes**  $(i,j) \in (b \cup m \cup ov \cup f^{-1} \cup d^{-1}) \cap (e \cup b^{-1} \cup m^{-1} \cup ov^{-1} \cup ov \cup s^{-1} \cup s \cup f^{-1} \cup d^{-1} \cup d) \cap (b \cup m \cup ov \cup s \cup d)$

**shows**  $(i,j) \in ov$

**using** *assms* **apply** *auto*  
**using** *b-rules* **apply** *auto*[43]  
**using** *e-rules* **apply** *auto*[9]  
**using** *b-rules* **apply** *auto*[30]  
**using** *m-rules* **apply** *auto*[24]  
**using** *b-rules* **apply** *auto*[6]

```

using m-rules apply auto[20]
using f-rules apply auto[14]
using d-rules by auto

```

```

lemma neg-beta2i-alpha2alpha5m:
assumes  $(q, j) \in b^{-1} \cup d \cup f \cup ov^{-1} \cup m^{-1}$  and  $(q, j) \in ov \cup s \cup m \cup f^{-1}$ 
 $\cup d^{-1} \cup e \cup s^{-1}$ 
shows False
using assms apply auto
  using b-rules apply auto[7]
  using ov-rules apply auto[4]
  using d-rules apply auto[6]
  using s-rules apply auto[3]
  using f-rules apply auto[5]
  using m-rules apply auto[2]
  using ov-rules apply auto[4]
  using m-rules by auto

```

```

lemma neg-bi-alpha1ialpha4mi:
assumes  $(q, i) \in b^{-1}$  and  $(q, i) \in e \cup ov^{-1} \cup s^{-1} \cup d^{-1} \cup f \cup f^{-1} \cup m^{-1}$ 
shows False
using assms apply auto
  using b-rules by auto

```

**end**

**theory** *nest*

**imports**

*Main jointly-exhaustive examples*  
*HOL-Eisbach.Eisbach-Tools*

**begin**

## 7 Nests

Nests are sets of intervals that share a meeting point. We define relation before between nests that give the ordering properties of points.

### 7.1 Definitions

**type-synonym** *'a nest* = *'a set*

**definition** (in *arelations*) *BEGIN* :: *'a*  $\Rightarrow$  *'a nest*

**where** *BEGIN* *i* =  $\{j \mid j. (j, i) \in ov \cup s \cup m \cup f^{-1} \cup d^{-1} \cup e \cup s^{-1}\}$

**definition** (in *arelations*)  $END :: 'a \Rightarrow 'a \text{ nest}$   
**where**  $END\ i = \{j \mid j. (j,i) \in e \cup ov^{-1} \cup s^{-1} \cup d^{-1} \cup f \cup f^{-1} \cup m^{-1}\}$

**definition** (in *arelations*)  $NEST :: 'a \text{ nest} \Rightarrow \text{bool}$   
**where**  $NEST\ S \equiv \exists i. \mathcal{I}\ i \wedge (S = BEGIN\ i \vee S = END\ i)$

**definition** (in *arelations*)  $before :: 'a \text{ nest} \Rightarrow 'a \text{ nest} \Rightarrow \text{bool}$  (**infix**  $\ll 100$ )  
**where**  $before\ N\ M \equiv NEST\ N \wedge NEST\ M \wedge (\exists n\ m. \mathcal{I}\ n \wedge m \in M \wedge (n,m) \in b)$

## 7.2 Properties of Nests

**lemma** *intv1*:  
**assumes**  $\mathcal{I}\ i$   
**shows**  $i \in BEGIN\ i$   
**unfolding** *BEGIN-def*  
**by** (*simp add: e assms*)

**lemma** *intv2*:  
**assumes**  $\mathcal{I}\ i$   
**shows**  $i \in END\ i$   
**unfolding** *END-def*  
**by** (*simp add: e assms*)

**lemma** *NEST-nonempty*:  
**assumes**  $NEST\ S$   
**shows**  $S \neq \{\}$   
**using** *assms* **unfolding** *NEST-def*  
**by** (*insert intv1 intv2, auto*)

**lemma** *NEST-BEGIN*:  
**assumes**  $\mathcal{I}\ i$   
**shows**  $NEST\ (BEGIN\ i)$   
**using** *NEST-def assms* **by** *auto*

**lemma** *NEST-END*:  
**assumes**  $\mathcal{I}\ i$   
**shows**  $NEST\ (END\ i)$   
**using** *NEST-def assms* **by** *auto*

**lemma** *before*:  
**assumes**  $a:\mathcal{I}\ i$   
**shows**  $BEGIN\ i \ll END\ i$   
**proof** –

**obtain**  $p$  **where**  $pi:(p,i) \in m$   
**using** *a M3 m* **by** *blast*  
**then have**  $p:p \in BEGIN\ i$  **using** *BEGIN-def* **by** *auto*

**obtain**  $q$  **where**  $qi:(q,i) \in m^{\wedge-1}$   
**using**  $a$   $M3$   $m$  **by**  $blast$   
**then have**  $q:q \in END$   $i$  **using**  $END-def$  **by**  $auto$

**from**  $pi$   $qi$  **have**  $c1:(p,q) \in b$  **using**  $b$   $m$   
**by**  $blast$

**with**  $c1$   $p$   $q$   $assms$  **show**  $?thesis$  **by**  $(auto$   $simp:NEST-def$   $before-def)$

**qed**

**lemma**  $meets$ :  
**fixes**  $i$   $j$   
**assumes**  $\mathcal{I}$   $i$  **and**  $\mathcal{I}$   $j$   
**shows**  $(i,j) \in m = ((END$   $i) = (BEGIN$   $j))$   
**proof**  
**assume**  $ij:(i,j) \in m$  **then have**  $ibj:i \in (BEGIN$   $j)$  **unfolding**  $BEGIN-def$  **by**  $auto$   
**from**  $ij$  **have**  $ji:(j,i) \in m^{\wedge-1}$  **by**  $simp$   
**then have**  $jeo:j \in (END$   $i)$  **unfolding**  $END-def$  **by**  $simp$   
**show**  $((END$   $i) = (BEGIN$   $j))$   
**proof**  
**{fix**  $x::'a$  **assume**  $a:x \in (END$   $i)$   
**then have**  $asimp:(x,i) \in e \cup ov^{-1} \cup s^{-1} \cup d^{-1} \cup f \cup m^{-1} \cup f^{\wedge-1}$   
**unfolding**  $END-def$  **by**  $auto$   
**then have**  $x \in (BEGIN$   $j)$  **using**  $ij$   $eovisidifmifiOm$   
**by**  $(auto$   $simp:BEGIN-def)$   
**}**  
**thus**  $conc1:END$   $i \subseteq BEGIN$   $j$  **by**  $auto$

**next**  
**{fix**  $x$  **assume**  $b:x \in (BEGIN$   $j)$   
**then have**  $bsimp:(x,j) \in ov \cup s \cup m \cup f^{\wedge-1} \cup d^{\wedge-1} \cup e \cup s^{\wedge-1}$   
**unfolding**  $BEGIN-def$  **by**  $auto$   
**then have**  $x \in (END$   $i)$  **using**  $ij$   $ovsmfidiesiOmi$   
**by**  $(auto$   $simp:END-def)$   
**}thus**  $conc2:BEGIN$   $j \subseteq END$   $i$  **by**  $auto$

**qed**

**next**  
**assume**  $a0:END$   $(i::'a) = BEGIN$   $(j::'a)$  **show**  $(i,j) \in m$   
**proof**  $(rule$   $ccontr)$   
**assume**  $a:(i,j) \notin m$  **then have**  $\neg i||j$  **using**  $m$  **by**  $auto$   
**from**  $a$  **have**  $(i,j) \in b \cup ov \cup s \cup d \cup f^{\wedge-1} \cup e \cup f \cup s^{\wedge-1} \cup d^{\wedge-1} \cup$   
 $ov^{\wedge-1} \cup m^{\wedge-1} \cup b^{\wedge-1}$  **using**  $assms$   $JE$  **by**  $auto$   
**thus**  $False$   
**proof**  $(auto)$   
**{assume**  $ij:(i,j) \in e$   
**obtain**  $p$  **where**  $ip:i||p$  **using**  $M3$   $assms(1)$  **by**  $auto$   
**then have**  $pi:(p,i) \in m^{\wedge-1}$  **using**  $m$  **by**  $auto$

```

then have  $p \in \text{END } i$  using  $\text{END-def}$  by auto
with  $a0$  have  $pj:p \in (\text{BEGIN } j)$  by auto
from  $ij$   $pi$  have  $(p,j) \in m^{\wedge-1}$  by ( $\text{simp add: } e$ )
with  $pj$  show ?thesis
apply (auto simp: $\text{BEGIN-def}$ )
using  $m\text{-rules}$  by auto[7] }
next
{assume  $ij:(j,i) \in m$ 
obtain  $p$  where  $ip:i||p$  using  $M3$   $\text{assms}(1)$  by auto
then have  $pi:(p,i) \in m^{\wedge-1}$  using  $m$  by auto
then have  $p \in \text{END } i$  using  $\text{END-def}$  by auto
with  $a0$  have  $pj:p \in (\text{BEGIN } j)$  by auto
from  $ij$  have  $(i,j) \in m^{\wedge-1}$  by  $\text{simp}$ 
with  $pi$  have  $(p,j) \in b^{\wedge-1}$  using  $\text{cmimi}$  by auto
with  $pj$  show ?thesis
apply (auto simp: $\text{BEGIN-def}$ )
using  $b\text{-rules}$  by auto
}
```

next

```

{assume  $ij:(i,j) \in b$ 
have  $ii:(i,i) \in e$  and  $i \in \text{END } i$  using  $\text{assms}$   $\text{intv2 } e$  by auto
with  $a0$  have  $j:i \in \text{BEGIN } j$  by  $\text{simp}$ 
with  $ij$  show ?thesis
apply (auto simp: $\text{BEGIN-def}$ )
using  $b\text{-rules}$  by auto
}
```

next

```

{ assume  $ji:(j,i) \in b$  then have  $ij:(i,j) \in b^{\wedge-1}$  by  $\text{simp}$ 
have  $ii:(i,i) \in e$  and  $i \in \text{END } i$  using  $\text{assms}$   $\text{intv2 } e$  by auto
with  $a0$  have  $j:i \in \text{BEGIN } j$  by  $\text{simp}$ 
with  $ij$  show ?thesis
apply (auto simp: $\text{BEGIN-def}$ )
using  $b\text{-rules}$  by auto }
```

next

```

{assume  $ij:(i,j) \in \text{ov}$ 
then obtain  $u$   $v::'a$  where  $iu:i||u$  and  $uv:u||v$  and  $uv:u||v$  using  $\text{ov}$  by
blast
from  $iu$  have  $u \in \text{END } i$  using  $m$   $\text{END-def}$  by auto
with  $a0$  have  $u:v \in \text{BEGIN } j$  by  $\text{simp}$ 
from  $iu$  have  $(u,i) \in m^{\wedge-1}$  using  $m$  by auto
with  $ij$  have  $uj:(u,j) \in \text{ov}^{\wedge-1} \cup d \cup f$  using  $\text{covim}$  by auto
show ?thesis using  $u$   $uj$ 
apply (auto simp: $\text{BEGIN-def}$ )
```

```

    using ov-rules eovi apply auto[9]
    using s-rules apply auto[2]
    using d-rules apply auto[5]
    using f-rules by auto[5]
  }

next

{assume  $(j,i) \in ov$  then have  $ij:(i,j) \in ov^{-1}$  by simp let  $?p = i$ 
from  $ij$  have  $pi:(?p, i) \in e$  by (simp add:e)
from  $ij$  have  $pj:(?p,j) \in ov^{-1}$  by simp
from  $pi$  have  $?p \in END\ i$  using END-def by auto
with  $a0$  have  $?p \in (BEGIN\ j)$  by auto
with  $pj$  show ?thesis
apply (auto simp:BEGIN-def)
  using ov-rules by auto
}

next
{assume  $ij:(i,j) \in s$ 
then obtain  $p\ q\ t$  where  $ip:i||p$  and  $pq:p||q$  and  $jq:j||q$  and  $ti:t||i$  and
tj:t||j using  $s$  by blast
from  $ip$  have  $(p,i) \in m^{-1}$  using  $m$  by auto
then have  $p \in END\ i$  using END-def by auto
with  $a0$  have  $p:p \in BEGIN\ j$  by simp
from  $ti\ ip\ pq\ tj\ jq$  have  $(p,j) \in f$  using  $f$  by blast
with  $p$  show ?thesis
apply (auto simp:BEGIN-def)
  using f-rules by auto
}

next
{assume  $(j,i) \in s$  then have  $ij:(i,j) \in s^{-1}$  by simp
then obtain  $u\ v$  where  $ju:j||u$  and  $uv:u||v$  and  $iv:i||v$  using  $s$  by blast
from  $iv$  have  $(v,i) \in m^{-1}$  using  $m$  by blast
then have  $v \in END\ i$  using END-def by auto
with  $a0$  have  $v:v \in BEGIN\ j$  by simp
from  $ju\ uv$  have  $(v,j) \in b^{-1}$  using  $b$  by auto
with  $v$  show ?thesis
apply (auto simp:BEGIN-def)
  using b-rules by auto}

next
{assume  $ij:(i,j) \in f$ 
have  $(i,i) \in e$  and  $i \in END\ i$ 
by (simp add: e) (auto simp: assms intu2 )
with  $a0$  have  $i \in BEGIN\ j$  by simp
with  $ij$  show ?thesis
apply (auto simp:BEGIN-def)
  using f-rules by auto
}

```

```

next
{assume  $(j,i) \in f$  then have  $(i,j) \in f^{-1}$  by simp
then obtain  $u$  where  $ju:j||u$  and  $iu:i||u$  using  $f$  by auto
then have  $ui:(u,i) \in m^{-1}$  and  $u \in \text{END } i$ 
apply (simp add: converse.intros m)
using END-def iu m by auto
with a0 have  $ubj:u \in \text{BEGIN } j$  by simp
from ju have  $(u,j) \in m^{-1}$  by (simp add: converse.intros m)
with ubj show ?thesis
apply (auto simp:BEGIN-def)
using m-rules by auto
}
next
{assume  $ij:(i,j) \in d$  then
have  $(i,i) \in e$  and  $i \in \text{END } i$  using  $assms\ e$  by (blast, simp add: intv2)
with a0 have  $i \in \text{BEGIN } j$  by simp
with ij show ?thesis
apply (auto simp:BEGIN-def)
using d-rules by auto}
next
{assume  $ji:(j,i) \in d$  then have  $(i,j) \in d^{-1}$  using  $d$  by simp
then obtain  $u\ v$  where  $ju:j||u$  and  $uv:u||v$  and  $iv:i||v$  using  $d$  using  $ji$ 
by blast
then have  $(v,i) \in m^{-1}$  and  $v \in \text{END } i$  using  $m\ \text{END-def}$  by auto
with a0 ju uv have  $vj:(v,j) \in b^{-1}$  and  $v \in \text{BEGIN } j$  using  $b$  by auto
with vj show ?thesis
apply (auto simp:BEGIN-def)
using b-rules by auto}

```

qed

qed

qed

lemma starts:

fixes  $i\ j$

assumes  $\mathcal{I}\ i$  and  $\mathcal{I}\ j$

shows  $((i,j) \in s \cup s^{-1} \cup e) = (\text{BEGIN } i = \text{BEGIN } j)$

proof

assume  $a3:(i,j) \in s \cup s^{-1} \cup e$  show  $\text{BEGIN } i = \text{BEGIN } j$

proof -

{ fix  $x$  assume  $x \in \text{BEGIN } i$  then have  $(x,i) \in ov \cup s \cup m \cup f^{-1} \cup d^{-1} \cup e \cup s^{-1}$  unfolding BEGIN-def by auto

hence  $x \in \text{BEGIN } j$  using  $a3\ ovsmfidiesiOssie$

by (auto simp:BEGIN-def)

} note  $c1 = \text{this}$

{ fix  $x$  assume  $x \in \text{BEGIN } j$  then have  $xj:(x,j) \in ov \cup s \cup m \cup f^{-1} \cup d^{-1} \cup e \cup s^{-1}$  unfolding BEGIN-def by auto

```

then have  $x \in \text{BEGIN } i$ 
apply (insert converseI[OF a3] xj)
apply (subst (asm) converse-Un)+
apply (subst (asm) converse-converse)
using ovsmfidiesiOssie
by (auto simp:BEGIN-def)
} note c2 = this

from c1 have  $\text{BEGIN } i \subseteq \text{BEGIN } j$  by auto
moreover with c2 have  $\text{BEGIN } j \subseteq \text{BEGIN } i$  by auto
ultimately show ?thesis by auto
qed
next
assume a4:  $\text{BEGIN } i = \text{BEGIN } j$ 
with assms have  $i \in \text{BEGIN } j$  and  $j \in \text{BEGIN } i$  using intro1 by auto
then have  $ij:(i,j) \in \text{ov} \cup \text{s} \cup \text{m} \cup \hat{f}^{-1} \cup \hat{d}^{-1} \cup \text{e} \cup \hat{s}^{-1}$  and  $ji:(j,i) \in$ 
 $\text{ov} \cup \text{s} \cup \text{m} \cup \hat{f}^{-1} \cup \hat{d}^{-1} \cup \text{e} \cup \hat{s}^{-1}$ 
unfolding BEGIN-def by auto
then have  $ijov:(i,j) \notin \text{ov}$ 
apply auto
using ov-rules by auto

from ij ji have  $ijm:(i,j) \notin \text{m}$ 
apply (simp-all, elim disjE, simp-all)
using ov-rules apply auto[13]
using s-rules apply auto[11]
using m-rules apply auto[9]
using f-rules apply auto[7]
using d-rules apply auto[5]
using m-rules by auto[4]

from ij ji have  $ijfi:(i,j) \notin \hat{f}^{-1}$ 
apply (simp-all, elim disjE, simp-all)
using ov-rules apply auto[13]
using s-rules apply auto[11]
using m-rules apply auto[9]
using f-rules apply auto[7]
using d-rules apply auto[5]
using f-rules by auto[4]

from ij ji have  $ijdi:(i,j) \notin \hat{d}^{-1}$ 
apply (simp-all, elim disjE, simp-all)
using ov-rules apply auto[13]
using s-rules apply auto[11]
using m-rules apply auto[9]
using f-rules apply auto[7]
using d-rules apply auto[5]
using d-rules by auto[4]

```



**from**  $ij\ ijm\ ijov\ ijfi\ ijdi$  **show**  $(i, j) \in s \cup s^{-1} \cup e$  **by** *auto*

**qed**

**lemma**  $xj\text{-set}: x \in \{a \mid a. (a, j) \in e \cup ov^{-1} \cup s^{-1} \cup d^{-1} \cup f \cup f^{-1} \cup m^{-1}\} =$   
 $((x, j) \in e \cup ov^{-1} \cup s^{-1} \cup d^{-1} \cup f \cup f^{-1} \cup m^{-1})$   
**by** *blast*

**lemma** *ends:*

**fixes**  $i\ j$

**assumes**  $\mathcal{I}\ i$  **and**  $\mathcal{I}\ j$

**shows**  $((i, j) \in f \cup f^{-1} \cup e) = (END\ i = END\ j)$

**proof**

**assume**  $a3: (i, j) \in f \cup f^{-1} \cup e$  **show**  $END\ i = END\ j$

**proof**  $-$

**{ fix**  $x$  **assume**  $x \in END\ i$  **then have**  $(x, i) \in e \cup ov^{-1} \cup s^{-1} \cup d^{-1} \cup f \cup$   
 $f^{-1} \cup m^{-1}$  **unfolding** *END-def* **by** *auto*  
**then have**  $x \in END\ j$  **using**  $a3$  **unfolding** *END-def*  
**apply** (*subst xj-set*)  
**using** *ceovisidiffimi-ffie-simp* **by** *simp*  
**}** **note**  $c1 = this$

**{ fix**  $x$  **assume**  $x \in END\ j$  **then have**  $(x, j) \in e \cup ov^{-1} \cup s^{-1} \cup d^{-1} \cup f \cup$   
 $f^{-1} \cup m^{-1}$  **unfolding** *END-def* **by** *auto*  
**then have**  $x \in END\ i$  **using**  $a3$  **unfolding** *END-def*  
**by** (*metis Un-iff ceovisidiffimi-ffie-simp converse-iff eei mem-Collect-eq*)  
**}** **note**  $c2 = this$

**from**  $c1$  **have**  $END\ i \subseteq END\ j$  **by** *auto*

**moreover with**  $c2$  **have**  $END\ j \subseteq END\ i$  **by** *auto*

**ultimately show** *?thesis* **by** *auto*

**qed**

**next**

**assume**  $a4: END\ i = END\ j$

**with** *assms* **have**  $i \in END\ j$  **and**  $j \in END\ i$  **using** *intv2* **by** *auto*

**then have**  $ij: (i, j) \in e \cup ov^{-1} \cup s^{-1} \cup d^{-1} \cup f \cup f^{-1} \cup m^{-1}$  **and**  $ji: (j, i) \in e$   
 $\cup ov^{-1} \cup s^{-1} \cup d^{-1} \cup f \cup f^{-1} \cup m^{-1}$

**unfolding** *END-def* **by** *auto*

**then have**  $ijov: (i, j) \notin ov^{-1}$

**apply** (*simp-all, elim disjE, simp-all*)

**using** *eov es ed efi ef em eov* **apply** *auto[13]*

**using** *ov-rules* **apply** *auto[11]*

**using** *s-rules* **apply** *auto[9]*

**using** *d-rules* **apply** *auto[7]*

**using** *f-rules* **apply** *auto[8]*

**using** *movi* **by** *auto*

**from**  $ij\ ji$  **have**  $ijm: (i, j) \notin m^{-1}$

**apply** (*simp-all, elim disjE, simp-all*)

```

using m-rules by auto

from ij ji have ijfi:(i,j) ∉ s-1
apply (simp-all, elim disjE, simp-all)
using s-rules by auto

from ij ji have ijdi:(i,j) ∉ d-1
apply (simp-all, elim disjE, simp-all)
using d-rules by auto

from ij ijm ijov ijfi ijdi show  $(i, j) \in f \cup f^{-1} \cup e$  by auto
qed

lemma before-irrefl:
fixes a
shows  $\neg a \ll a$ 
proof (rule ccontr, auto)
  assume a0:a ∥ a
  then have NEST a unfolding before-def by auto
  then obtain i where  $i:a = \text{BEGIN } i \vee a = \text{END } i$  unfolding NEST-def by
auto
  from i show False
  proof
    assume  $a = \text{BEGIN } i$ 
    with a0 have  $\text{BEGIN } i \ll \text{BEGIN } i$  by simp
    then obtain p q where  $p \in \text{BEGIN } i$  and  $q \in \text{BEGIN } i$  and  $b:(p,q) \in b$ 
unfolding before-def by auto
    then have  $a1:(p,i) \in ov \cup s \cup m \cup f^{-1} \cup d^{-1} \cup e \cup s^{-1}$  and  $a2:(i,q) \in$ 
 $ov^{-1} \cup s^{-1} \cup m^{-1} \cup f \cup d \cup e \cup s$  unfolding BEGIN-def
    apply auto
    using eei apply fastforce
    by (simp add: e)+
    with b show False
    using pii[of p i q]
    using b-rules by safe fast+
  next
  assume  $a = \text{END } i$ 
  with a0 have  $\text{END } i \ll \text{END } i$  by simp
  then obtain p q where  $p \in \text{END } i$  and  $q \in \text{END } i$  and  $b:(p,q) \in b$  unfolding
before-def by auto
  then have  $a1:(p,i) \in e \cup ov^{-1} \cup s^{-1} \cup d^{-1} \cup f \cup f^{-1} \cup m^{-1}$  and  $a2:(q,i)$ 
 $\in e \cup ov^{-1} \cup s^{-1} \cup d^{-1} \cup f \cup f^{-1} \cup m^{-1}$  unfolding END-def
  by auto
  with b show False
  apply (subst (asm) converse-iff[THEN sym])
  using cbi-alpha1alpha4mi neq-bi-alpha1alpha4mi relcomp.relcompI subsetCE
by blast
qed
qed

```

**lemma** *BEGIN-before*:

**fixes**  $i\ j$

**assumes**  $\mathcal{I}\ i$  and  $\mathcal{I}\ j$

**shows**  $BEGIN\ i \ll BEGIN\ j = ((i,j) \in b \cup m \cup ov \cup f^{-1} \cup d^{-1})$

**proof**

**assume**  $a3:BEGIN\ i \ll BEGIN\ j$

**from**  $a3$  **obtain**  $p\ q$  **where**  $pa:p \in BEGIN\ i$  **and**  $qc:q \in BEGIN\ j$  **and**  
 $pq:(p,q) \in b$  **unfolding** *before-def* **by** *auto*

**then obtain**  $r$  **where**  $p||r$  **and**  $r||q$  **using**  $b$  **by** *auto*

**then have**  $pr:(p,r) \in m$  **and**  $rq:(r,q) \in m$  **using**  $m$  **by** *auto*

**from**  $pa$  **have**  $pi:(p,i) \in ov \cup s \cup m \cup f^{-1} \cup d^{-1} \cup e \cup s^{-1}$  **unfolding**  
*BEGIN-def* **by** *auto*

**moreover with**  $pr$  **have**  $(r,p) \in m^{\wedge-1}$  **by** *simp*

**ultimately have**  $(r,i) \in d \cup f \cup ov^{\wedge-1} \cup e \cup f^{\wedge-1} \cup m^{\wedge-1} \cup b^{\wedge-1} \cup s \cup s^{\wedge-1}$

**using**  $cmiov\ cmis\ cmim\ cmifi\ cmidi\ cmisi$

**apply** (*simp-all, elim disjE, auto*)

**by** (*simp add: e*)

**then have**  $ir:(i,r) \in d^{\wedge-1} \cup f^{\wedge-1} \cup ov \cup e \cup f \cup m \cup b \cup s^{\wedge-1} \cup s$

**by** (*metis (mono-tags, lifting) converseD converse-Un converse-converse eei*)

**from**  $qc$  **have**  $(q,j) \in ov \cup s \cup m \cup f^{-1} \cup d^{-1} \cup e \cup s^{-1}$  **unfolding**  
*BEGIN-def* **by** *auto*

**with**  $rq$  **have**  $rj:(r,j) \in b \cup s \cup m$

**using**  $m\text{-ovsmfidiesi}$  **using** *contra-subsetD relcomp.relcompI* **by** *blast*

**with**  $ir$  **have**  $c1:(i,j) \in b \cup m \cup ov \cup f^{-1} \cup d^{-1} \cup d \cup e \cup s \cup s^{-1}$

**using** *difibs* **by** *blast*

**{assume**  $(i,j) \in s \vee (i,j) \in s^{\wedge-1} \vee (i,j) \in e$  **then have**  $BEGIN\ i = BEGIN\ j$

**using** *starts Un-iff assms(1) assms(2)* **by** *blast*

**with**  $a3$  **have** *False* **by** (*simp add: before-irrefl*)}

**from**  $c1$  **have**  $c1':(i,j) \in b \cup m \cup ov \cup f^{-1} \cup d^{-1} \cup d$

**using**  $\langle (i,j) \in s \vee (i,j) \in s^{-1} \vee (i,j) \in e \implies False \rangle$  **by** *blast*

**{assume**  $(i,j) \in d$  **with**  $pi$  **have**  $(p,j) \in e \cup s \cup d \cup ov \cup ov^{\wedge-1} \cup s^{\wedge-1} \cup f \cup f^{\wedge-1} \cup d^{\wedge-1}$

**using**  $ovsmfidiesi\text{-}d$  **using** *relcomp.relcompI subsetCE* **by** *blast*

**with**  $pq$  **have**  $(q,j) \in b^{\wedge-1} \cup d \cup f \cup ov^{\wedge-1} \cup m^{\wedge-1}$

**apply** (*subst (asm) converse-iff[THEN sym]*)

**using**  $cbi\text{-}esdovovisiffidi$  **by** *blast*

**with**  $qc$  **have** *False* **unfolding** *BEGIN-def*

**apply** (*subgoal-tac*  $(q,j) \in ov \cup s \cup m \cup f^{-1} \cup d^{-1} \cup e \cup s^{-1}$ )

**prefer** 2

**apply** *simp*

```

    using neq-beta2i-alpha2alpha5m by auto
  }

  with c1' show ((i, j) ∈ b ∪ m ∪ ov ∪ f-1 ∪ d-1) by auto
next
  assume (i, j) ∈ b ∪ m ∪ ov ∪ f-1 ∪ d-1
  then show BEGIN i ≪ END j
  proof (simp-all, elim disjE, simp-all)
    assume (i, j) ∈ b thus ?thesis using intv1 using before-def NEST-BEGIN
  assms by metis
  next
    assume iu:(i, j) ∈ m
    obtain l where li:(l, i) ∈ m using M3 m meets-wd assms by blast
    with iu have (l, j) ∈ b using cmm by auto
    moreover from li have l ∈ (BEGIN i) using BEGIN-def by auto
    ultimately show ?thesis using intv1 before-def NEST-BEGIN assms by
  blast
  next
    assume iu:(i, j) ∈ ov
    obtain l where li:(l, i) ∈ m using M3 m meets-wd assms by blast
    with iu have (l, j) ∈ b using cmov by auto
    moreover from li have l ∈ (BEGIN i) using BEGIN-def by auto
    ultimately show ?thesis using intv1 before-def NEST-BEGIN assms by
  blast
  next
    assume iu:(j, i) ∈ f
    obtain l where li:(l, i) ∈ m using M3 m meets-wd assms by blast
    with iu have (l, j) ∈ b using cmfi by auto
    moreover from li have l ∈ (BEGIN i) using BEGIN-def by auto
    ultimately show ?thesis using intv1 before-def NEST-BEGIN assms by
  blast
  next
    assume iu:(j, i) ∈ d
    obtain l where li:(l, i) ∈ m using M3 m meets-wd assms by blast
    with iu have (l, j) ∈ b using cmdi by auto
    moreover from li have l ∈ (BEGIN i) using BEGIN-def by auto
    ultimately show ?thesis using intv1 before-def NEST-BEGIN assms by
  blast

  qed
qed

lemma BEGIN-END-before:
fixes i j
assumes I i and I j
shows BEGIN i ≪ END j = ((i, j) ∈ e ∪ b ∪ m ∪ ov ∪ ov-1 ∪ s ∪ s-1 ∪ f
∪ f-1 ∪ d ∪ d-1)
proof
  assume a3:BEGIN i ≪ END j

```

**then obtain  $p\ q$  where  $pa:p \in \text{BEGIN } i$  and  $qc:q \in \text{END } j$  and  $pq:(p,q) \in b$  unfolding before-def by auto**  
**then obtain  $r$  where  $p\|r$  and  $r\|q$  using  $b$  by auto**  
**then have  $pr:(p,r) \in m$  and  $rq:(r,q) \in m$  using  $m$  by auto**  
**from  $pa$  have  $pi:(p,i) \in ov \cup s \cup m \cup f^{-1} \cup d^{-1} \cup e \cup s^{-1}$  unfolding BEGIN-def by auto**  
**moreover with  $pr$  have  $(r,p) \in m^{\wedge-1}$  by simp**  
**ultimately have  $(r,i) \in d \cup f \cup ov^{\wedge-1} \cup e \cup f^{\wedge-1} \cup m^{\wedge-1} \cup b^{\wedge-1} \cup s \cup s^{\wedge-1}$  using  $cmiov\ cmis\ cmim\ cmifi\ cmidi\ e\ cmisi$**   
**by ( simp-all, elim disjE, auto simp:e)**

**then have  $ir:(i,r) \in d^{\wedge-1} \cup f^{\wedge-1} \cup ov \cup e \cup f \cup m \cup b \cup s^{\wedge-1} \cup s$**   
**by (metis (mono-tags, lifting) converseD converse-Un converse-converse eei)**

**from  $qc$  have  $(q,j) \in e \cup ov^{-1} \cup s^{-1} \cup d^{-1} \cup f \cup f^{-1} \cup m^{-1}$  unfolding END-def by auto**  
**with  $rq$  have  $rj:(r,j) \in m \cup ov \cup s \cup d \cup b \cup f^{\wedge-1} \cup f \cup e$  using  $cm-alpha1\alpha4mi$  by blast**

**with  $ir$  show  $c1:(i,j) \in e \cup b \cup m \cup ov \cup ov^{\wedge-1} \cup s \cup s^{\wedge-1} \cup f \cup f^{-1} \cup d \cup d^{-1}$**   
**using difmov by blast**  
**next**  
**assume  $a4:(i,j) \in e \cup b \cup m \cup ov \cup ov^{-1} \cup s \cup s^{-1} \cup f \cup f^{-1} \cup d \cup d^{-1}$**   
**then show BEGIN  $i \ll$  END  $j$**   
**proof ( simp-all, elim disjE, simp-all)**  
**assume  $(i,j) \in e$**   
**obtain  $l\ k$  where  $l\|i$  and  $i\|k$  using M3 meets-wd assms by blast**  
**with  $\langle(i,j) \in e\rangle$  have  $k:j\|k$  by (simp add: e)**  
**from  $l\ k$  have  $(l,i) \in m$  and  $(k,j) \in m^{\wedge-1}$  using  $m$  by auto**  
**then have  $l \in \text{BEGIN } i$  and  $k \in \text{END } j$  using BEGIN-def END-def**  
**by auto**  
**moreover from  $l\ \langle i\|k\rangle$  have  $(l,k) \in b$  using  $b$  by auto**  
**ultimately show ?thesis using before-def assms NEST-BEGIN NEST-END**  
**by blast**  
**next**  
**assume  $(i,j) \in b$**   
**then show ?thesis using before-def assms NEST-BEGIN NEST-END**  
**intv1[of i] intv2[of j] by auto**  
**next**  
**assume  $(i,j) \in m$**   
**obtain  $l$  where  $l\|i$  using M3 assms by blast**  
**then have  $l \in \text{BEGIN } i$  using  $m$  BEGIN-def by auto**  
**moreover from  $\langle(i,j) \in m\rangle\ \langle l\|i\rangle$  have  $(l,j) \in b$  using  $b\ m$  by blast**  
**ultimately show ?thesis using intv2[of j] assms NEST-BEGIN**  
**NEST-END before-def by blast**  
**next**  
**assume  $(i,j) \in ov$**   
**then obtain  $l\ k$  where  $li:l\|i$  and  $lk:l\|k$  and  $ku:k\|j$  using  $ov$  by blast**

**from**  $li$  **have**  $l \in \text{BEGIN } i$  **using**  $m$  *BEGIN-def* **by** *auto*  
**moreover from**  $lk \text{ } ku$  **have**  $(l,j) \in b$  **using**  $b$  **by** *auto*  
**ultimately show** *?thesis* **using**  $\text{intv2}[\text{of } j]$  *assms* *NEST-BEGIN*  
*NEST-END before-def by blast*  
**next**  
**assume**  $(j,i) \in ov$   
**then obtain**  $lk \text{ } v$  **where**  $wv:j||v$  **and**  $lk:l||k$  **and**  $kv:k||v$  **and**  $li:l||i$  **using**  
*ov by blast*  
**from**  $li$  **have**  $l \in \text{BEGIN } i$  **using**  $m$  *BEGIN-def* **by** *auto*  
**moreover from**  $wv$  **have**  $v \in \text{END } j$  **using**  $m$  *END-def* **by** *auto*  
**moreover from**  $lk \text{ } kv$  **have**  $(l,v) \in b$  **using**  $b$  **by** *auto*  
**ultimately show** *?thesis* **using** *assms* *NEST-BEGIN NEST-END*  
*before-def by blast*  
**next**  
**assume**  $(i,j) \in s$   
**then obtain**  $v \text{ } v'$  **where**  $iv:i||v$  **and**  $vvp:v||v'$  **and**  $j||v'$  **using**  $s$  **by** *blast*  
**then have**  $v' \in \text{END } j$  **using** *END-def*  $m$  **by** *auto*  
**moreover from**  $iv \text{ } vvp$  **have**  $(i,v') \in b$  **using**  $b$  **by** *auto*  
**ultimately show** *?thesis* **using**  $\text{intv1}[\text{of } i]$  *assms* *NEST-BEGIN*  
*NEST-END before-def by blast*  
**next**  
**assume**  $(j,i) \in s$   
**then obtain**  $l \text{ } v$  **where**  $li:l||i$  **and**  $lu:l||j$  **and**  $j||v$  **using**  $s$  **by** *blast*  
**then have**  $v \in \text{END } j$  **using**  $m$  *END-def* **by** *auto*  
**moreover from**  $li$  **have**  $l \in \text{BEGIN } i$  **using**  $m$  *BEGIN-def* **by** *auto*  
**moreover from**  $lu \text{ } \langle j||v \rangle$  **have**  $(l,v) \in b$  **using**  $b$  **by** *auto*  
**ultimately show** *?thesis* **using** *assms* *NEST-BEGIN NEST-END*  
*before-def by blast*  
**next**  
**assume**  $(i,j) : f$   
**then obtain**  $l \text{ } v$  **where**  $li:l||i$  **and**  $iv:i||v$  **and**  $j||v$  **using**  $f$  **by** *blast*  
**then have**  $v \in \text{END } j$  **using**  $m$  *END-def* **by** *auto*  
**moreover from**  $li$  **have**  $l \in \text{BEGIN } i$  **using**  $m$  *BEGIN-def* **by** *auto*  
**moreover from**  $iv \text{ } li$  **have**  $(l,v) \in b$  **using**  $b$  **by** *auto*  
**ultimately show** *?thesis* **using** *assms* *NEST-BEGIN NEST-END*  
*before-def by blast*  
**next**  
**assume**  $(j,i) \in f$   
**then obtain**  $l \text{ } v$  **where**  $li:l||i$  **and**  $iv:i||v$  **and**  $j||v$  **using**  $f$  **by** *blast*  
**then have**  $v \in \text{END } j$  **using**  $m$  *END-def* **by** *auto*  
**moreover from**  $li$  **have**  $l \in \text{BEGIN } i$  **using**  $m$  *BEGIN-def* **by** *auto*  
**moreover from**  $iv \text{ } li$  **have**  $(l,v) \in b$  **using**  $b$  **by** *auto*  
**ultimately show** *?thesis* **using** *assms* *NEST-BEGIN NEST-END*  
*before-def by blast*  
**next**  
**assume**  $(i,j) : d$   
**then obtain**  $k \text{ } v$  **where**  $ik:i||k$  **and**  $kv:k||v$  **and**  $j||v$  **using**  $d$  **by** *blast*  
**then have**  $v \in \text{END } j$  **using** *END-def*  $m$  **by** *auto*  
**moreover from**  $ik \text{ } kv$  **have**  $(i,v) \in b$  **using**  $b$  **by** *auto*

**ultimately show** *?thesis* **using**  $intv1[of\ i]$  *assms* *NEST-BEGIN*  
*NEST-END* *before-def* **by** *blast*  
**next**  
**assume**  $(j,i) \in d$   
**then obtain**  $l\ k$  **where**  $l||i$  **and**  $lk:l||k$  **and**  $ku:k||j$  **using**  $d$  **by** *blast*  
**then have**  $l \in BEGIN\ i$  **using** *BEGIN-def*  $m$  **by** *auto*  
**moreover from**  $lk\ ku$  **have**  $(l,j) \in b$  **using**  $b$  **by** *auto*  
**ultimately show** *?thesis* **using**  $intv2[of\ j]$  *assms* *NEST-BEGIN*  
*NEST-END* *before-def* **by** *blast*  
**qed**  
**qed**

**lemma** *END-BEGIN-before:*

**fixes**  $i\ j$

**assumes**  $\mathcal{I}\ i$  **and**  $\mathcal{I}\ j$

**shows**  $END\ i \ll BEGIN\ j = ((i,j) \in b)$

**proof**

**assume**  $a3:END\ i \ll BEGIN\ j$

**from**  $a3$  **obtain**  $p\ q$  **where**  $pa:p \in END\ i$  **and**  $qc:q \in BEGIN\ j$  **and**  $pq:(p,q) \in b$  **unfolding** *before-def* **by** *auto*

**then obtain**  $r$  **where**  $p||r$  **and**  $r||q$  **using**  $b$  **by** *auto*

**then have**  $pr:(p,r) \in m$  **and**  $rq:(r,q) \in m$  **using**  $m$  **by** *auto*

**from**  $pa$  **have**  $pi:(p,i) \in e \cup ov^{-1} \cup s^{-1} \cup d^{-1} \cup f \cup f^{-1} \cup m^{-1}$  **unfolding** *END-def* **by** *auto*

**moreover with**  $pr$  **have**  $(r,p) \in m^{-1}$  **by** *simp*

**ultimately have**  $(r,i) \in m^{-1} \cup b^{-1}$  **using**  $e\ cmiovi\ cmisi\ cmidi\ cmif\ cmifi\ cmimi$

**by** (*simp-all, elim disjE, auto simp:e*)

**then have**  $ir:(i,r) \in m \cup b$  **by** *simp*

**from**  $qc$  **have**  $(q,j) \in ov \cup s \cup m \cup f^{-1} \cup d^{-1} \cup e \cup s^{-1}$  **unfolding** *BEGIN-def* **by** *auto*

**with**  $rq$  **have**  $rj:(r,j) \in b \cup m$  **using**  $cmov\ cms\ cmm\ cmfi\ cmdi\ e\ cmsi$

**by** (*simp-all, elim disjE, auto simp:e*)

**with**  $ir$  **show**  $(i,j) \in b$  **using**  $cmb\ cmm\ cbm\ cbb$  **by** *auto*

**next**

**assume**  $(i,j) \in b$  **thus**  $END\ i \ll BEGIN\ j$  **using**  $intv1[of\ j]\ intv2[of\ i]$  *assms* *before-def* *NEST-END* *NEST-BEGIN* **by** *auto*

**qed**

**lemma** *END-END-before:*

**fixes**  $i\ j$

**assumes**  $\mathcal{I}\ i$  **and**  $\mathcal{I}\ j$

**shows**  $END\ i \ll END\ j = ((i,j) \in b \cup m \cup ov \cup s \cup d)$

**proof**

**assume**  $a3:END\ i \ll END\ j$

**from  $a\beta$  obtain  $p\ q$  where  $pa:p \in \text{END } i$  and  $qc:q \in \text{END } j$  and  $pq:(p,q) \in b$  unfolding before-def by auto**  
**then obtain  $r$  where  $p\|r$  and  $r\|q$  using  $b$  by auto**  
**then have  $pr:(p,r) \in m$  and  $rq:(r,q) \in m$  using  $m$  by auto**  
**from  $pa$  have  $pi:(p,i) \in e \cup ov^{-1} \cup s^{-1} \cup d^{-1} \cup f \cup f^{-1} \cup m^{-1}$  unfolding END-def by auto**  
**moreover with  $pr$  have  $(r,p) \in m^{\wedge-1}$  by simp**  
**ultimately have  $(r,i) \in m^{\wedge-1} \cup b^{\wedge-1}$  using  $e$  cmiovi cmisi cmidi cmif cmifi cmimi**  
**by ( simp-all, elim disjE, auto simp:e)**  
  
**then have  $ir:(i,r) \in m \cup b$  by simp**  
  
**from  $qc$  have  $(q,j) \in e \cup ov^{-1} \cup s^{-1} \cup d^{-1} \cup f \cup f^{-1} \cup m^{-1}$  unfolding END-def by auto**  
**with  $rq$  have  $rj:(r,j) \in m \cup ov \cup s \cup d \cup b \cup f^{\wedge-1} \cup e \cup f$  using  $e$  cmovi cmisi cmidi cmf cmfi cmmi**  
**by ( simp-all, elim disjE, auto simp:e)**  
  
**with  $ir$  show  $(i,j) \in b \cup m \cup ov \cup s \cup d$  using  $cmm$  cmov cms cmd cmb cmfi e cmf cbm cbov cbs cbd cbb cbfi cbf**  
**by ( simp-all, elim disjE, auto simp:e)**  
**next**  
**assume  $(i, j) \in b \cup m \cup ov \cup s \cup d$**   
**then show  $\text{END } i \ll \text{END } j$**   
**proof ( simp-all, elim disjE, simp-all)**  
**assume  $(i,j) \in b$  thus ?thesis using intv2[of i] intv2[of j] assms NEST-END before-def by blast**  
**next**  
**assume  $(i,j) \in m$**   
**obtain  $v$  where  $j\|v$  using  $M\beta$  assms by blast**  
**with  $\langle(i,j) \in m\rangle$  have  $(i,v) \in b$  using  $b\ m$  by blast**  
**moreover from  $\langle j\|v\rangle$  have  $v \in \text{END } j$  using  $m$  END-def by auto**  
**ultimately show ?thesis using intv2[of i] assms NEST-END before-def by blast**  
**next**  
**assume  $(i,j) : ov$**   
**then obtain  $v\ v'$  where  $iv:i\|v$  and  $vvp:v\|v'$  and  $j\|v'$  using  $ov$  by blast**  
**then have  $v' \in \text{END } j$  using  $m$  END-def by auto**  
**moreover from  $iv\ vvp$  have  $(i,v') \in b$  using  $b$  by auto**  
**ultimately show ?thesis using intv2[of i] assms NEST-END before-def by blast**  
**next**  
**assume  $(i,j) \in s$**   
**then obtain  $v\ v'$  where  $iv:i\|v$  and  $vvp:v\|v'$  and  $j\|v'$  using  $s$  by blast**  
**then have  $v' \in \text{END } j$  using  $m$  END-def by auto**  
**moreover from  $iv\ vvp$  have  $(i,v') \in b$  using  $b$  by auto**  
**ultimately show ?thesis using intv2[of i] assms NEST-END before-def by blast**



**next**  
**assume**  $(i,j) \in d$   
**then obtain**  $v v'$  **where**  $iv:i||v$  **and**  $vvp:v||v'$  **and**  $j||v'$  **using**  $d$  **by** *blast*  
**then have**  $v' \in \text{END } j$  **using**  $m \text{ END-def}$  **by** *auto*  
**moreover from**  $iv vvp$  **have**  $(i,v') \in b$  **using**  $b$  **by** *auto*  
**ultimately show** *?thesis* **using**  $\text{intv2}[of i]$  *assms NEST-END before-def* **by**  
*blast*  
**qed**  
**qed**

**lemma overlaps:**  
**assumes**  $\mathcal{I} i$  **and**  $\mathcal{I} j$   
**shows**  $(i,j) \in ov = ((\text{BEGIN } i \ll \text{BEGIN } j) \wedge (\text{BEGIN } j \ll \text{END } i) \wedge (\text{END } i \ll \text{END } j))$   
**proof**

**assume**  $a:(i,j) \in ov$   
**then obtain**  $n t q u v$  **where**  $nt:n||t$  **and**  $tj:t||j$  **and**  $tq:t||q$  **and**  $qu:q||u$  **and**  
 $iu:i||u$  **and**  $wv:u||v$  **and**  $qv:j||v$  **and**  $n||i$  **using**  $ov$  **by** *blast*  
**then have**  $ni:(n,i) \in m$  **using**  $m$  **by** *blast*  
**then have**  $n:n \in \text{BEGIN } i$  **unfolding** *BEGIN-def* **by** *auto*  
**from**  $nt tj$  **have**  $nj:(n,j) \in b$  **using**  $b$  **by** *auto*  
**have**  $j \in \text{BEGIN } j$  **using** *assms(2)* **by** (*simp add: intv1*)  
**with** *assms n nj* **have**  $c1:\text{BEGIN } i \ll \text{BEGIN } j$  **unfolding** *before-def* **using**  
*NEST-BEGIN* **by** *blast*

**from**  $tj$  **have**  $a1:(t,j) \in m$  **and**  $a2:t \in \text{BEGIN } j$  **using**  $m \text{ BEGIN-def}$  **by** *auto*  
**from**  $iu$  **have**  $(u,i) \in m^{\wedge-1}$  **and**  $u \in \text{END } i$  **using**  $m \text{ END-def}$  **by** *auto*  
**with** *assms tq qu a2* **have**  $c2:\text{BEGIN } j \ll \text{END } i$  **unfolding** *before-def* **using**  
 $b \text{ NEST-BEGIN NEST-END}$  **by** *blast*

**have**  $i \in \text{END } i$  **by** (*simp add: assms intv2*)  
**moreover with**  $qv$  **have**  $v \in \text{END } j$  **using**  $m \text{ END-def}$  **by** *auto*  
**moreover with**  $iu uv$  **have**  $(i,v) \in b$  **using**  $b$  **by** *auto*  
**ultimately have**  $c3:\text{END } i \ll \text{END } j$  **using** *assms NEST-END before-def* **by**  
*blast*

**show**  $((\text{BEGIN } i \ll \text{BEGIN } j) \wedge (\text{BEGIN } j \ll \text{END } i) \wedge (\text{END } i \ll \text{END } j))$   
**using**  $c1 c2 c3$  **by** *simp*

**next**  
**assume**  $a0:((\text{BEGIN } i \ll \text{BEGIN } j) \wedge (\text{BEGIN } j \ll \text{END } i) \wedge (\text{END } i \ll \text{END } j))$

**then have**  $(i,j) \in b \cup m \cup ov \cup f^{-1} \cup d^{-1} \wedge (i,j) \in e \cup b^{\wedge-1} \cup m^{\wedge-1} \cup$   
 $ov^{\wedge-1} \cup ov \cup s^{\wedge-1} \cup s \cup f^{\wedge-1} \cup f \cup d^{\wedge-1} \cup d$

^

$(i,j) \in b \cup m \cup ov \cup s \cup d$   
**using** *BEGIN-before BEGIN-END-before END-END-before assms*  
**by** (*metis (no-types, lifting) converseD converse-Un converse-converse eei*)  
**then have**  $(i,j) \in (b \cup m \cup ov \cup f^{-1} \cup d^{-1}) \cap (e \cup b^{\wedge-1} \cup m^{\wedge-1} \cup ov^{\wedge-1})$

```

 $\cup ov \cup s^{-1} \cup s \cup f^{-1} \cup f \cup d^{-1} \cup d) \cap (b \cup m \cup ov \cup s \cup d)$ 
  by (auto)
  then show  $(i,j) \in ov$ 
  using inter-ov by blast

```

qed

### 7.3 Ordering of nests

```

class strict-order =
fixes ls::'a nest  $\Rightarrow$  'a nest  $\Rightarrow$  bool
assumes
  irrefl: $\neg$  ls a a and
  trans:ls a c  $\Longrightarrow$  ls c g  $\Longrightarrow$  ls a g and
  asym:ls a c  $\Longrightarrow$   $\neg$  ls c a

```

```

class total-strict-order = strict-order +
assumes trichotomy: a = c  $\Longrightarrow$  ( $\neg$  (ls a c)  $\wedge$   $\neg$  (ls c a))

```

interpretation nest:total-strict-order ( $\ll$ )

proof

```

{ fix a::'a nest
  show  $\neg$  a  $\ll$  a
  by (simp add: before-irrefl) } note irrefl-nest = this

```

```

{ fix a c::'a nest
  assume a = c
  show  $\neg$  a  $\ll$  c  $\wedge$   $\neg$  c  $\ll$  a
  by (simp add:  $\langle$ a = c $\rangle$  irrefl-nest)} note trichotomy-nest = this

```

```

{ fix a c g::'a nest
  assume a:a  $\ll$  c and c: c  $\ll$  g
  show a  $\ll$  g
  proof -

```

from a c have na:NEST a and nc:NEST c and ng:NEST g unfolding before-def by auto

from na obtain i where i:a = BEGIN i  $\vee$  a = END i and wdi: $\mathcal{I}$  i unfolding NEST-def by auto

from nc obtain j where j:c = BEGIN j  $\vee$  c = END j and wdj: $\mathcal{I}$  j unfolding NEST-def by auto

from ng obtain u where u:g = BEGIN u  $\vee$  g = END u and wdu: $\mathcal{I}$  u unfolding NEST-def by auto

from i j u show ?thesis

proof (elim disjE, auto)

assume abi:a = BEGIN i and cbj:c = BEGIN j and gbu:g = BEGIN u

from abi cbj a wdi wdj have  $(i,j) \in b \cup m \cup ov \cup f^{-1} \cup d^{-1}$  using BEGIN-before by auto

moreover from cbj gbu c wdj wdu have  $(j,u) \in b \cup m \cup ov \cup f^{-1} \cup d^{-1}$  using BEGIN-before by auto

ultimately have  $c1:(i,u) \in b \cup m \cup ov \cup f^{-1} \cup d^{-1}$   
using *cbeta2-beta2* by *blast*

then have  $a \ll g$  by (*simp add: BEGIN-before abi gbu wdi wdu*)

thus *BEGIN*  $i \ll$  *BEGIN*  $u$  using *abi gbu* by *auto*

next

assume *abi*: $a =$  *BEGIN*  $i$  and *cbj*: $c =$  *BEGIN*  $j$  and *geu*: $g =$  *END*  $u$   
from *abi* *cbj*  $a$  *wdi* *wdj* have  $(i,j) \in b \cup m \cup ov \cup f^{-1} \cup d^{-1}$  using  
*BEGIN-before* by *auto*

moreover from *cbj* *geu*  $c$  *wdj* *wdu* have  $(j,u) : e \cup b \cup m \cup ov \cup ov^{-1} \cup s$   
 $\cup s^{-1} \cup f \cup f^{-1} \cup d \cup d^{-1}$  using *BEGIN-END-before* by *auto*

ultimately have  $(i,u) \in e \cup b \cup m \cup ov \cup ov^{-1} \cup s \cup s^{-1} \cup f \cup f^{-1} \cup d \cup$   
 $d^{-1}$   
using *cbeta2-gammabm* by *blast*

then have  $a \ll g$   
by (*simp add: BEGIN-END-before abi geu wdi wdj wdu*)

thus *BEGIN*  $i \ll$  *END*  $u$  using *abi geu* by *auto*

next

assume *abi*: $a =$  *BEGIN*  $i$  and *cej*: $c =$  *END*  $j$  and *gbu*: $g =$  *BEGIN*  $u$   
from *abi* *cej*  $a$  *wdi* *wdj* have  $ij:(i,j) : e \cup b \cup m \cup ov \cup ov^{-1} \cup s \cup s^{-1} \cup f$   
 $\cup f^{-1} \cup d \cup d^{-1}$  using *BEGIN-END-before* by *auto*

from *cej* *gbu*  $c$  *wdj* *wdu* have  $(j,u) \in b$  using *END-BEGIN-before* by *auto*  
with *ij* have  $(i,u) \in b \cup m \cup ov \cup f^{-1} \cup d^{-1}$   
using *ebmovovissifsiddib* by (*auto*)

thus *BEGIN*  $i \ll$  *BEGIN*  $u$   
by (*simp add: BEGIN-before abi gbu wdi wdu*)

next

assume *abi*: $a =$  *BEGIN*  $i$  and *cej*: $c =$  *END*  $j$  and *geu*: $g =$  *END*  $u$   
with  $a$  have  $(i,j) \in e \cup b \cup m \cup ov \cup ov^{-1} \cup s \cup s^{-1} \cup f \cup f^{-1} \cup d \cup d^{-1}$   
using *BEGIN-END-before wdi wdj* by *auto*

moreover from *cej* *geu*  $c$  *wdj* *wdu* have  $(j,u) \in b \cup m \cup ov \cup s \cup d$   
using *END-END-before* by *auto*

ultimately have  $(i,u) \in b \cup m \cup ov \cup s \cup d \cup f^{-1} \cup d^{-1} \cup ov^{-1} \cup$   
 $s^{-1} \cup f \cup e$   
using *ebmovovissiffiddibmouvd* by *blast*

thus *BEGIN*  $i \ll$  *END*  $u$  using *BEGIN-END-before wdi wdu* by *auto*

next

assume *aei*: $a =$  *END*  $i$  and *cbj*: $c =$  *BEGIN*  $j$  and *gbu*: $g =$  *BEGIN*  $u$   
from  $a$  *aei* *cbj* *wdi* *wdj* have  $(i,j) \in b$   
using *END-BEGIN-before* by *auto*

moreover from  $c$  *cbj* *gbu* *wdj* *wdu* have  $(j,u) \in b \cup m \cup ov \cup f^{-1} \cup d^{-1}$   
using *BEGIN-before* by *auto*

ultimately have  $(i,u) : b$  using *cbb cbm cbov cbfi cbdi*

```

    by (simp-all, elim disjE, auto)
    thus END i << BEGIN u using END-BEGIN-before wdi wdu by auto
next
    assume aei:a = END i and cbj:c = BEGIN j and geu:g = END u
    from a aei cbj wdi wdj have (i,j) ∈ b
    using END-BEGIN-before by auto
    moreover from c cbj geu wdj wdu have (j,u) ∈ e ∪ b ∪ m ∪ ov ∪ ov-1 ∪ s
    ∪ s-1 ∪ f ∪ f-1 ∪ d ∪ d-1
    using BEGIN-END-before by auto
    ultimately have (i,u) ∈ b ∪ m ∪ ov ∪ s ∪ d
    using bebmovovissiffiddi by blast
    thus END i << END u using END-END-before wdi wdu by auto
next
    assume aei:a = END i and cej:c = END j and gbu:g = BEGIN u
    from aei cej wdi wdj have (i,j) ∈ b ∪ m ∪ ov ∪ s ∪ d using END-END-before
a by auto
    moreover from cej gbu c wdj wdu have (j,u) ∈ b using END-BEGIN-before
by auto
    ultimately have (i,u) ∈ b
    using cbb cmb covb csb cdb
    by (simp-all, elim disjE, auto)
    thus END i << BEGIN u using END-BEGIN-before wdi wdu by auto
next
    assume aei:a = END i and cej:c = END j and geu:g = END u
    from aei cej wdi wdj have (i,j) ∈ b ∪ m ∪ ov ∪ s ∪ d using END-END-before
a by auto
    moreover from cej geu c wdj wdu have (j,u) ∈ b ∪ m ∪ ov ∪ s ∪ d using
END-END-before by auto
    ultimately have (i,u) ∈ b ∪ m ∪ ov ∪ s ∪ d
    using calpha1-alpha1 by auto
    thus END i << END u using END-END-before wdi wdu by auto
qed
qed} note trans-nest = this

{ fix a c::'a nest
  assume a:a << c
  show ¬ c << a
  apply (rule ccontr, auto)
  using a irrefl-nest trans-nest by blast}
qed

end

```