Reactive angelic processes

Pedro Ribeiro

Department of Computer Science
University of York, UK

Technical Report

Supervisor: Ana Cavalcanti

February 2014

Revision: ce5092e (2014-02-20)

Abstract

The concept of angelic nondeterminism has traditionally been employed in the refinement calculus. Despite different notions having been proposed in the context of process algebras, namely Communicating Sequential Processes (CSP), the analogous counterpart to the angelic choice operator of the monotonic predicate transformers, has been elusive. In order to consider this concept in the context of reactive processes, we introduce a new theory in the setting of Hoare and He's Unifying Theories of Programming (UTP). Based on a theory of designs with angelic nondeterminism previously developed, we show how these processes can be similarly expressed as reactive designs. Furthermore, a Galois connection is established with the existing theory of reactive processes and a bijection is also found with respect to the subset of non-angelic processes.

Contents

Chapter 1

Reactive angelic processes

1.1 Alphabet and definitions

Definition 1 (Alphabet)

$$
\begin{array}{l}
s : \mathit{State} \\
ac' : \mathbb{P}\, \mathit{State} \\
ok, ok' : \{\mathit{true}, \mathit{false}\} \\
\{tr, \mathit{ref}, \mathit{wait}\} \subseteq \mathrm{dom}\, \mathit{State}
\end{array}
$$

Definition 2 (Trace prefix states)

$$\mathit{States}_{tr \leq tr'}(s) \mathrel{\widehat{=}} \{z : \mathit{State} \mid s.tr \leq z.tr\}$$

1.2 Healthiness conditions

1.2.1 RA1

The healthiness condition **RA1** requires the set of final states ac' not to be empty, and the final value of tr in all final states to be a suffix of the initial trace $s.tr$. It is defined as follows.

Definition 3 (**RA1**)

$$\mathbf{RA1}(P) \mathrel{\widehat{=}} (P \wedge ac' \neq \emptyset)[\mathit{States}_{tr \leq tr'}(s) \cap ac' / ac']$$

This definition can be expressed in two different ways as shown in the following two lemmas.

Lemma 1.2.1

$$\begin{array}{l}\mathbf{RA1}(P)\\ =\\ P[\{z \mid z \in ac' \wedge s.tr \leq z.tr\}/ac'] \wedge \exists\, z \bullet s.tr \leq z.tr \wedge z \in ac'\end{array}$$

Proof.

$$\begin{array}{ll}\mathbf{RA1}(P) & \{\text{Definition of } \mathbf{RA1} \text{ (Definition 3)}\}\\ = (P \wedge ac' \neq \emptyset)[States_{tr \leq tr'}(s) \cap ac'/ac'] & \\ & \{\text{Property of sets and definition of } States_{tr \leq tr'} \text{ (Definition 2)}\}\\ = (P \wedge ac' \neq \emptyset)[\{z \mid z \in ac' \wedge s.tr \leq z.tr\}/ac'] & \{\text{Substitution}\}\\ = P[\{z \mid z \in ac' \wedge s.tr \leq z.tr\}/ac'] \wedge \{z \mid z \in ac' \wedge s.tr \leq z.tr\} \neq \emptyset & \\ & \{\text{Property of sets}\}\\ = P[\{z \mid z \in ac' \wedge s.tr \leq z.tr\}/ac'] \wedge \exists\, z \bullet z \in \{z \mid z \in ac' \wedge s.tr \leq z.tr\} & \\ & \{\text{Property of sets}\}\\ = P[\{z \mid z \in ac' \wedge s.tr \leq z.tr\}/ac'] \wedge \exists\, z \bullet z \in ac' \wedge s.tr \leq z.tr & \end{array}$$

□

Lemma 1.2.2

$$\mathbf{RA1}(P) = (P \wedge ac' \neq \emptyset)[\{z \mid z \in ac' \wedge z \in \{z \mid s.tr \leq z.tr\}\}/ac']$$

Proof.

$$\begin{array}{ll}\mathbf{RA1}(P) & \{\text{Definition of } \mathbf{RA1} \text{ (Definition 3)}\}\\ = (P \wedge ac' \neq \emptyset)[States_{tr \leq tr'}(s) \cap ac'/ac'] & \\ & \{\text{Property of sets and definition of } States_{tr \leq tr'}\}\\ = (P \wedge ac' \neq \emptyset)[\{z \mid z \in ac' \wedge z \in \{z \mid s.tr \leq z.tr\}\}/ac'] & \end{array}$$

□

In what follows we prove properties pertaining to **RA1**.

Properties

Theorem 1.2.1 (**RA1**-disjunction-distribute)

$$\mathbf{RA1}(P \vee Q) = \mathbf{RA1}(P) \vee \mathbf{RA1}(Q)$$

Proof.

$$\begin{array}{ll}
& \mathbf{RA1}(P \vee Q) \qquad \{\text{Definition of } \mathbf{RA1} \text{ (Lemma 1.2.1)}\} \\
& = (P \vee Q)[\{z \mid z \in ac' \wedge s.tr \leq z.tr\}/ac'] \wedge \exists\, z \bullet s.tr \leq z.tr \wedge z \in ac' \\
& \qquad \{\text{Substitution}\} \\
= & \left(\begin{array}{l} (P[\{z \mid z \in ac' \wedge s.tr \leq z.tr\}/ac'] \vee Q[\{z \mid z \in ac' \wedge s.tr \leq z.tr\}/ac']) \\ \wedge \\ \exists\, z \bullet s.tr \leq z.tr \wedge z \in ac' \end{array} \right) \\
& \qquad \{\text{Predicate calculus}\} \\
= & \left(\begin{array}{l} (P[\{z \mid z \in ac' \wedge s.tr \leq z.tr\}/ac'] \wedge \exists\, z \bullet s.tr \leq z.tr \wedge z \in ac') \\ \vee \\ (Q[\{z \mid z \in ac' \wedge s.tr \leq z.tr\}/ac'] \wedge \exists\, z \bullet s.tr \leq z.tr \wedge z \in ac') \end{array} \right) \\
& \qquad \{\text{Definition of } \mathbf{RA1} \text{ (Lemma 1.2.1)}\} \\
& = \mathbf{RA1}(P) \vee \mathbf{RA1}(Q)
\end{array}$$

□

Theorem 1.2.2 (**RA1**-conjunction-distribute)

$$\mathbf{RA1}(P \wedge Q) = \mathbf{RA1}(P) \wedge \mathbf{RA1}(Q)$$

Proof.

$$\begin{array}{ll}
& \mathbf{RA1}(P \wedge Q) \qquad \{\text{Definition of } \mathbf{RA1} \text{ (Lemma 1.2.1)}\} \\
& = (P \wedge Q)[\{z \mid z \in ac' \wedge s.tr \leq z.tr\}/ac'] \wedge \exists\, z \bullet s.tr \leq z.tr \wedge z \in ac' \\
& \qquad \{\text{Substitution}\} \\
= & \left(\begin{array}{l} P[\{z \mid z \in ac' \wedge s.tr \leq z.tr\}/ac'] \\ \wedge \\ Q[\{z \mid z \in ac' \wedge s.tr \leq z.tr\}/ac'] \\ \wedge \\ \exists\, z \bullet s.tr \leq z.tr \wedge z \in ac' \end{array} \right) \qquad \{\text{Predicate calculus}\}
\end{array}$$

$$= \left(\begin{array}{l} (P[\{z \mid z \in ac' \wedge s.tr \leq z.tr\}/ac'] \wedge \exists\, z \bullet s.tr \leq z.tr \wedge z \in ac') \\ \wedge \\ (Q[\{z \mid z \in ac' \wedge s.tr \leq z.tr\}/ac'] \wedge \exists\, z \bullet s.tr \leq z.tr \wedge z \in ac') \end{array} \right)$$

{Definition of **RA1** (Lemma 1.2.1)}

$$= \mathbf{RA1}(P) \wedge \mathbf{RA1}(Q)$$

□

Theorem 1.2.3 (**RA1**-idempotent)

$$\mathbf{RA1} \circ \mathbf{RA1}(P) = \mathbf{RA1}(P)$$

Proof.

$\mathbf{RA1} \circ \mathbf{RA1}(P)$ {Definition of **RA1** (Lemma 1.2.1)}

$$= \mathbf{RA1}(P)[\{z \mid z \in ac' \wedge s.tr \leq z.tr\}/ac'] \wedge \exists\, z \bullet z \in ac' \wedge s.tr \leq z.tr$$

{Definition of **RA1** (Lemma 1.2.1)}

$$= \left(\begin{array}{l} \left(\begin{array}{l} P[\{z \mid z \in ac' \wedge s.tr \leq z.tr\}/ac'] \\ \wedge \\ \exists\, z \bullet z \in ac' \wedge s.tr \leq z.tr \end{array} \right) [\{z \mid z \in ac' \wedge s.tr \leq z.tr\}/ac'] \\ \wedge \exists\, z \bullet z \in ac' \wedge s.tr \leq z.tr \end{array} \right)$$

{Substitution}

$$= \left(\begin{array}{l} \left(\begin{array}{l} P[\{z \mid z \in \{z \mid z \in ac' \wedge s.tr \leq z.tr\} \wedge s.tr \leq z.tr\}/ac'] \\ \wedge \\ \exists\, z \bullet z \in \{z \mid z \in ac' \wedge s.tr \leq z.tr\} \wedge s.tr \leq z.tr \end{array} \right) \\ \wedge \exists\, z \bullet z \in ac' \wedge s.tr \leq z.tr \end{array} \right)$$

{Variable renaming}

$$= \left(\begin{array}{l} \left(\begin{array}{l} P[\{z \mid z \in \{y \mid y \in ac' \wedge s.tr \leq y.tr\} \wedge s.tr \leq z.tr\}/ac'] \\ \wedge \\ \exists\, z \bullet z \in \{y \mid y \in ac' \wedge s.tr \leq y.tr\} \wedge s.tr \leq z.tr \end{array} \right) \\ \wedge \exists\, z \bullet z \in ac' \wedge s.tr \leq z.tr \end{array} \right)$$

{Property of sets}

$$= \left(\begin{array}{l} P[\{z \mid z \in ac' \wedge s.tr \leq z.tr \wedge s.tr \leq z.tr\}/ac'] \\ \wedge \\ \exists\, z \bullet z \in ac' \wedge s.tr \leq z.tr \wedge s.tr \leq z.tr \\ \wedge \\ \exists\, z \bullet z \in ac' \wedge s.tr \leq z.tr \end{array} \right)$$

{Predicate calculus}

$$= \left(\begin{array}{l} P[\{z \mid z \in ac' \land s.tr \leq z.tr\}/ac'] \\ \land \\ \exists\, z \bullet z \in ac' \land s.tr \leq z.tr \end{array} \right)$$

{Definition of **RA1** (Lemma 1.2.1)}

$$= \mathbf{RA1}(P)$$

□

Theorem 1.2.4 (**RA1**-monotonic)

$$P \sqsubseteq Q \Rightarrow \mathbf{RA1}(P) \sqsubseteq \mathbf{RA1}(Q)$$

Proof.

$\mathbf{RA1}(Q)$ {Assumption: $P \sqsubseteq Q = [Q \Rightarrow P]$}
$= \mathbf{RA1}(Q \land P)$ {Theorem 1.2.2}
$= \mathbf{RA1}(Q) \land \mathbf{RA1}(P)$ {Predicate calculus}
$\Rightarrow \mathbf{RA1}(P)$

□

Theorem 1.2.5

$$\mathbf{PBMH} \circ \mathbf{RA1} \circ \mathbf{PBMH}(P) = \mathbf{RA1} \circ \mathbf{PBMH}(P)$$

Proof.

$\mathbf{PBMH} \circ \mathbf{RA1} \circ \mathbf{PBMH}(P)$ {Lemma 1.2.1}

$$= \mathbf{PBMH} \left(\begin{array}{l} \mathbf{PBMH}(P)[\{z \mid z \in ac' \land s.tr \leq z.tr\}/ac'] \\ \land \\ \exists\, z \bullet s.tr \leq z.tr \land z \in ac' \end{array} \right)$$

{Lemma E.1.1}

$$= \mathbf{PBMH} \left(\begin{array}{l} (\exists\, ac_0 \bullet P[ac_0/ac'] \land ac_0 \subseteq ac')[\{z \mid z \in ac' \land s.tr \leq z.tr\}/ac'] \\ \land \\ \exists\, z \bullet s.tr \leq z.tr \land z \in ac' \end{array} \right)$$

{Substitution}

$$= \mathbf{PBMH} \left(\begin{array}{l} (\exists\, ac_0 \bullet P[ac_0/ac'] \land ac_0 \subseteq \{z \mid z \in ac' \land s.tr \leq z.tr\}) \\ \land \\ \exists\, z \bullet s.tr \leq z.tr \land z \in ac' \end{array} \right)$$

{Property of sets}

$$= \mathbf{PBMH} \left(\begin{array}{l} (\exists\, ac_0 \bullet P[ac_0/ac'] \land \forall\, x \bullet x \in ac_0 \Rightarrow (x \in ac' \land s.tr \leq x.tr)) \\ \land \\ \exists\, z \bullet s.tr \leq z.tr \land z \in ac' \end{array} \right)$$

{Predicate calculus}

$$= \mathbf{PBMH} \left(\begin{array}{l} \exists\, ac_0 \bullet \left(\begin{array}{l} P[ac_0/ac'] \land (\forall\, x \bullet x \in ac_0 \Rightarrow x \in ac') \\ \land \\ (\forall\, x \bullet x \in ac_0 \Rightarrow s.tr \leq x.tr) \end{array} \right) \\ \land \\ \exists\, z \bullet s.tr \leq z.tr \land z \in ac' \end{array} \right)$$

{Lemma E.1.1}

$$= \exists\, ac_1 \bullet \left(\begin{array}{l} \exists\, ac_0 \bullet \left(\begin{array}{l} P[ac_0/ac'] \land (\forall\, x \bullet x \in ac_0 \Rightarrow x \in ac') \\ \land \\ (\forall\, x \bullet x \in ac_0 \Rightarrow s.tr \leq x.tr) \end{array} \right) \\ \land \\ \exists\, z \bullet s.tr \leq z.tr \land z \in ac' \end{array} \right) [ac_1/ac'] \land ac_1 \subseteq ac'$$

{Substitution}

$$= \exists\, ac_1 \bullet \left(\begin{array}{l} \exists\, ac_0 \bullet \left(\begin{array}{l} P[ac_0/ac'] \land (\forall\, x \bullet x \in ac_0 \Rightarrow x \in ac_1) \\ \land \\ (\forall\, x \bullet x \in ac_0 \Rightarrow s.tr \leq x.tr) \end{array} \right) \\ \land \\ \exists\, z \bullet s.tr \leq z.tr \land z \in ac_1 \end{array} \right) \land ac_1 \subseteq ac'$$

{Predicate calculus}

$$= \left(\begin{array}{l} \exists\, ac_0 \bullet \left(\begin{array}{l} P[ac_0/ac'] \land (\forall\, x \bullet x \in ac_0 \Rightarrow x \in ac') \\ \land \\ (\forall\, x \bullet x \in ac_0 \Rightarrow s.tr \leq x.tr) \end{array} \right) \\ \land \\ \exists\, z \bullet s.tr \leq z.tr \land z \in ac' \end{array} \right)$$

{Predicate calculus}

$$= \left(\begin{array}{l} \exists\, ac_0 \bullet P[ac_0/ac'] \land (\forall\, x \bullet x \in ac_0 \Rightarrow (x \in ac' \land s.tr \leq x.tr)) \\ \land \\ \exists\, z \bullet s.tr \leq z.tr \land z \in ac' \end{array} \right)$$

{Property of sets}

$$= \left(\begin{array}{l} \exists\, ac_0 \bullet P[ac_0/ac'] \land ac_0 \subseteq \{z \mid z \in ac' \land s.tr \leq z.tr\} \\ \land \\ \exists\, z \bullet s.tr \leq z.tr \land z \in ac' \end{array} \right)$$

{Substitution}

$$= \left(\begin{array}{l} (\exists\, ac_0 \bullet P[ac_0/ac'] \land ac_0 \subseteq ac')[\{z \mid z \in ac' \land s.tr \leq z.tr\}/ac'] \\ \land \\ \exists\, z \bullet s.tr \leq z.tr \land z \in ac' \end{array} \right)$$

{Lemma E.1.1}

$= \mathbf{PBMH}(P)[\{z \mid z \in ac' \land s.tr \leq z.tr\}/ac'] \land \exists\, z \bullet s.tr \leq z.tr \land z \in ac'$

{Lemma 1.2.1}

$= \mathbf{RA1} \circ \mathbf{PBMH}(P)$

□

The functions **PBMH** and **RA1** do not necessarily commute. We consider the following example for a predicate that is not **PBMH**-healthy.

Example 1

$\mathbf{RA1} \circ \mathbf{PBMH}(ac' = \emptyset)$ {Definition of **PBMH** (Lemma E.1.1)}
$= \mathbf{RA1}(\exists\, ac_0 \bullet ac_0 = \emptyset \land ac_0 \subseteq ac')$ {One-point rule}
$= \mathbf{RA1}(\emptyset \subseteq ac')$ {Property of sets}
$= \mathbf{RA1}(\mathit{true})$ {Lemma B.1.6}
$= \mathit{States}_{tr \leq tr'}(s) \cap ac' \neq \emptyset$

$\mathbf{PBMH} \circ \mathbf{RA1}(ac' = \emptyset)$ {Definition of **RA1**}
$= \mathbf{PBMH}((ac' = \emptyset \land ac' \neq \emptyset)[\mathit{States}_{tr \leq tr'}(s) \cap ac'/ac'])$
{Predicate calculus}
$= \mathbf{PBMH}(\mathit{false})$ {Lemma E.4.2}
$= \mathit{false}$

Theorem 1.2.6

$$\mathbf{RA1} \circ \mathbf{A0}(P) = \mathbf{RA1}(P)$$

Proof.

$\mathbf{RA1} \circ \mathbf{A0}(P)$ {Lemma 1.2.1}
$= \mathbf{A0}(P)[\{z \mid z \in ac' \land s.tr \leq z.tr\}/ac'] \land \exists\, z \bullet s.tr \leq z.tr \land z \in ac'$
{Definition of **A0**}

$$= \left(\begin{array}{l} (P \wedge ((ok \wedge \neg\, P^f) \Rightarrow (ok' \Rightarrow ac' \neq \emptyset)))[\{z \mid z \in ac' \wedge s.tr \leq z.tr\}/ac'] \\ \wedge \\ \exists\, z \bullet s.tr \leq z.tr \wedge z \in ac' \end{array} \right)$$

{Substitution}

$$= \left(\begin{array}{l} P[\{z \mid z \in ac' \wedge s.tr \leq z.tr\}/ac'] \\ \wedge \\ \left(\begin{array}{l} (ok \wedge \neg\, P^f[\{z \mid z \in ac' \wedge s.tr \leq z.tr\}/ac']) \\ \Rightarrow \\ (ok' \Rightarrow \{z \mid z \in ac' \wedge s.tr \leq z.tr\} \neq \emptyset) \end{array} \right) \\ \wedge \\ \exists\, z \bullet s.tr \leq z.tr \wedge z \in ac' \end{array} \right)$$

{Property of sets}

$$= \left(\begin{array}{l} P[\{z \mid z \in ac' \wedge s.tr \leq z.tr\}/ac'] \\ \wedge \\ \left(\begin{array}{l} (ok \wedge \neg\, P^f[\{z \mid z \in ac' \wedge s.tr \leq z.tr\}/ac']) \\ \Rightarrow \\ (ok' \Rightarrow (\exists\, z \bullet z \in ac' \wedge s.tr \leq z.tr)) \end{array} \right) \\ \wedge \\ \exists\, z \bullet s.tr \leq z.tr \wedge z \in ac' \end{array} \right)$$

{Predicate calculus}

$$= \left(\begin{array}{l} P[\{z \mid z \in ac' \wedge s.tr \leq z.tr\}/ac'] \\ \wedge \\ \left(\begin{array}{l} (\neg\, ok \vee P^f[\{z \mid z \in ac' \wedge s.tr \leq z.tr\}/ac']) \\ \vee \\ (\neg\, ok' \vee (\exists\, z \bullet z \in ac' \wedge s.tr \leq z.tr)) \end{array} \right) \\ \wedge \\ \exists\, z \bullet s.tr \leq z.tr \wedge z \in ac' \end{array} \right)$$

{Predicate calculus: absorption law}

$$= \left(\begin{array}{l} P[\{z \mid z \in ac' \wedge s.tr \leq z.tr\}/ac'] \\ \wedge \\ \exists\, z \bullet s.tr \leq z.tr \wedge z \in ac' \end{array} \right)$$

{Lemma 1.2.1}

$$= \mathbf{RA1}(P)$$

□

1.2.2 RA2

The healthiness condition **RA2** requires processes to be insensitive to the initial value of $s.tr$.

Definition 4 (**RA2**)

$$\mathbf{RA2}(P) \mathrel{\widehat{=}} P[s \oplus \{tr \mapsto \langle\rangle\}, \{z \mid z \in ac' \land s.tr \leq z.tr \bullet z \oplus \{tr \mapsto z.tr - s.tr\}\}/s, ac']$$

Properties regarding **RA2** are proved in what follows. Namely we prove that it is an idempotent and monotonic function.

Properties

Theorem 1.2.7 (**RA2**-idempotent)

$$\mathbf{RA2} \circ \mathbf{RA2}(P) = \mathbf{RA2}(P)$$

Proof.

$$\begin{aligned}
&\mathbf{RA2} \circ \mathbf{RA2}(P) && \{\text{Definition of } \mathbf{RA2} \text{ twice}\}\\
&= P\left[\begin{array}{l} (s \oplus \{tr \mapsto \langle\rangle\}) \oplus \{tr \mapsto \langle\rangle\} \\ \left\{ z \;\middle|\; \begin{array}{l} z \in \{z \mid z \in ac' \land s.tr \leq z.tr \bullet z \oplus \{tr \mapsto z.tr - s.tr\}\} \\ \land\ (s \oplus \{tr \mapsto \langle\rangle\}).tr \leq z.tr \\ \bullet\ z \oplus \{tr \mapsto z.tr - (s \oplus \{tr \mapsto \langle\rangle\}).tr\} \end{array} \right\} \Big/ \end{array} \begin{array}{r} s \\ \\ ac' \end{array}\right] \\
&\qquad\qquad \{\text{Property of } \oplus \text{ and value of } tr \text{ component}\}\\
&= P\left[\begin{array}{l} s \oplus \{tr \mapsto \langle\rangle\} \\ \left\{ z \;\middle|\; \begin{array}{l} z \in \{z \mid z \in ac' \land s.tr \leq z.tr \bullet z \oplus \{tr \mapsto z.tr - s.tr\}\} \\ \bullet\ z \oplus \{tr \mapsto z.tr - \langle\rangle\} \end{array} \right\} \Big/ \end{array} \begin{array}{r} s \\ \\ ac' \end{array}\right] \\
&\qquad\qquad \{\text{Property of sequence difference}\}\\
&= P\left[\begin{array}{l} s \oplus \{tr \mapsto \langle\rangle\} \\ \left\{ z \;\middle|\; \begin{array}{l} z \in \{z \mid z \in ac' \land s.tr \leq z.tr \bullet z \oplus \{tr \mapsto z.tr - s.tr\}\} \\ \bullet\ z \oplus \{tr \mapsto z.tr\} \end{array} \right\} \Big/ \end{array} \begin{array}{r} s \\ \\ ac' \end{array}\right] \\
&\qquad\qquad \{\text{Property of } \oplus\}\\
&= P\left[\begin{array}{l} s \oplus \{tr \mapsto \langle\rangle\} \\ \{z \mid z \in \{z \mid z \in ac' \land s.tr \leq z.tr \bullet z \oplus \{tr \mapsto z.tr - s.tr\}\}\} \Big/ \end{array} \begin{array}{r} s \\ ac' \end{array}\right] \\
&\qquad\qquad \{\text{Property of sets}\}
\end{aligned}$$

$$= P[s \oplus \{tr \mapsto \langle\rangle\}, \{z \mid z \in ac' \wedge s.tr \leq z.tr \bullet z \oplus \{tr \mapsto z.tr - s.tr\}\}/s, ac']$$
{Definition of **RA2**}

$$= \mathbf{RA2}(P)$$

□

Theorem 1.2.8 (**RA2**-monotonic)

$$P \sqsubseteq Q \Rightarrow \mathbf{RA2}(P) \sqsubseteq \mathbf{RA2}(Q)$$

Proof.

$\mathbf{RA2}(Q)$ {Assumption: $P \sqsubseteq Q = [Q \Rightarrow P]$}
$= \mathbf{RA2}(Q \wedge P)$ {Definition of **RA2** and property of substitution}
$= \mathbf{RA2}(Q) \wedge \mathbf{RA2}(P)$ {Predicate calculus}
$\Rightarrow \mathbf{RA2}(P)$

□

Theorem 1.2.9 (**RA2**-conjunction-distribute)

$$\mathbf{RA2}(P \wedge Q) = \mathbf{RA2}(P) \wedge \mathbf{RA2}(Q)$$

Proof.

$\mathbf{RA2}(P \wedge Q)$ {Definition of **RA2**}

$$= (P \wedge Q) \left[\begin{array}{l} s \oplus \{tr \mapsto \langle\rangle\} \\ \{z \mid z \in ac' \wedge s.tr \leq z.tr \bullet z \oplus \{tr \mapsto z.tr - s.tr\}\} \end{array} \middle/ \begin{array}{r} s \\ ac' \end{array} \right]$$
{Property of substitution}

$$= \left(\begin{array}{l} P \left[\begin{array}{l} s \oplus \{tr \mapsto \langle\rangle\} \\ \{z \mid z \in ac' \wedge s.tr \leq z.tr \bullet z \oplus \{tr \mapsto z.tr - s.tr\}\} \end{array} \middle/ \begin{array}{r} s \\ ac' \end{array} \right] \\ \wedge \\ Q \left[\begin{array}{l} s \oplus \{tr \mapsto \langle\rangle\} \\ \{z \mid z \in ac' \wedge s.tr \leq z.tr \bullet z \oplus \{tr \mapsto z.tr - s.tr\}\} \end{array} \middle/ \begin{array}{r} s \\ ac' \end{array} \right] \end{array} \right)$$
{Definition of **RA2**}

$$= \mathbf{RA2}(P) \wedge \mathbf{RA2}(Q)$$

□

Theorem 1.2.10 (**RA2**-disjunction-distribute)

$$\mathbf{RA2}(P \vee Q) = \mathbf{RA2}(P) \vee \mathbf{RA2}(Q)$$

Proof.

$$\begin{array}{ll}
& \mathbf{RA2}(P \vee Q) \qquad \{\text{Definition of } \mathbf{RA2}\} \\
= & (P \vee Q)\left[\begin{array}{l} s \oplus \{tr \mapsto \langle\rangle\} \\ \{z \mid z \in ac' \wedge s.tr \leq z.tr \bullet z \oplus \{tr \mapsto z.tr - s.tr\}\} \end{array} \middle/ \begin{array}{r} s \\ ac' \end{array}\right] \\
& \qquad \{\text{Property of substitution}\} \\
= & \left(\begin{array}{l} P\left[\begin{array}{l} s \oplus \{tr \mapsto \langle\rangle\} \\ \{z \mid z \in ac' \wedge s.tr \leq z.tr \bullet z \oplus \{tr \mapsto z.tr - s.tr\}\} \end{array} \middle/ \begin{array}{r} s \\ ac' \end{array}\right] \\ \vee \\ Q\left[\begin{array}{l} s \oplus \{tr \mapsto \langle\rangle\} \\ \{z \mid z \in ac' \wedge s.tr \leq z.tr \bullet z \oplus \{tr \mapsto z.tr - s.tr\}\} \end{array} \middle/ \begin{array}{r} s \\ ac' \end{array}\right] \end{array}\right) \\
& \qquad \{\text{Definition of } \mathbf{RA2}\} \\
= & \mathbf{RA2}(P) \vee \mathbf{RA2}(Q)
\end{array}$$

□

Theorem 1.2.11

$$\mathbf{PBMH} \circ \mathbf{RA2} \circ \mathbf{PBMH}(P) = \mathbf{RA2} \circ \mathbf{PBMH}(P)$$

Proof.

$$\begin{array}{ll}
& \mathbf{PBMH} \circ \mathbf{RA2} \circ \mathbf{PBMH}(P) \qquad \{\text{Definition of } \mathbf{PBMH} \text{ (Lemma E.1.1)}\} \\
= & \mathbf{PBMH} \circ \mathbf{RA2}(\exists\, ac_0 \bullet P[ac_0/ac'] \wedge ac_0 \subseteq ac') \qquad \{\text{Definition of } \mathbf{RA2}\} \\
= & \mathbf{PBMH}\left(\begin{array}{l} (\exists\, ac_0 \bullet P[ac_0/ac'] \wedge ac_0 \subseteq ac') \\ \left[\begin{array}{l} s \oplus \{tr \mapsto \langle\rangle\} \\ \{z \mid z \in ac' \wedge s.tr \leq z.tr \bullet z \oplus \{tr \mapsto z.tr - s.tr\}\} \end{array} \middle/ \begin{array}{r} s \\ ac' \end{array}\right] \end{array}\right) \\
& \qquad \{\text{Substitution}\} \\
= & \mathbf{PBMH}\left(\begin{array}{l} \exists\, ac_0 \bullet P[ac_0/ac'][s \oplus \{tr \mapsto \langle\rangle\}/s] \\ \wedge\ ac_0 \subseteq \{z \mid z \in ac' \wedge s.tr \leq z.tr \bullet z \oplus \{tr \mapsto z.tr - s.tr\}\} \end{array}\right) \\
& \qquad \{\text{Definition of } \mathbf{PBMH} \text{ (Lemma E.1.1)}\} \\
= & \left(\begin{array}{l} \exists\, ac_1, ac_0 \bullet P[ac_0/ac'][s \oplus \{tr \mapsto \langle\rangle\}/s] \\ \wedge\ ac_0 \subseteq \{z \mid z \in ac_1 \wedge s.tr \leq z.tr \bullet z \oplus \{tr \mapsto z.tr - s.tr\}\} \\ \wedge\ ac_1 \subseteq ac' \end{array}\right) \\
& \qquad \{\text{Definition of subset inclusion}\}
\end{array}$$

$$= \left(\begin{array}{l} \exists\, ac_1, ac_0 \bullet P[ac_0/ac'][s \oplus \{tr \mapsto \langle\rangle\}/s] \\ \land\, \forall\, x \bullet x \in ac_0 \Rightarrow x \in \{z \mid z \in ac_1 \land s.tr \leq z.tr \bullet z \oplus \{tr \mapsto z.tr - s.tr\}\} \\ \land\, ac_1 \subseteq ac' \end{array} \right)$$

{Property of sets}

$$= \left(\begin{array}{l} \exists\, ac_1, ac_0 \bullet P[ac_0/ac'][s \oplus \{tr \mapsto \langle\rangle\}/s] \\ \land\, \forall\, x \bullet x \in ac_0 \Rightarrow \exists\, z \bullet z \in ac_1 \land s.tr \leq z.tr \land x = z \oplus \{tr \mapsto z.tr - s.tr\} \\ \land\, ac_1 \subseteq ac' \end{array} \right)$$

{Lemma B.1.3}

$$= \left(\begin{array}{l} \exists\, ac_1, ac_0 \bullet P[ac_0/ac'][s \oplus \{tr \mapsto \langle\rangle\}/s] \\ \land\, \forall\, x \bullet x \in ac_0 \Rightarrow x \oplus \{tr \mapsto s.tr \frown x.tr\} \in ac_1 \\ \land\, ac_1 \subseteq ac' \end{array} \right)$$

{Lemma E.4.13}

$$= \left(\begin{array}{l} \exists\, ac_0 \bullet P[ac_0/ac'][s \oplus \{tr \mapsto \langle\rangle\}/s] \\ \land \\ \forall\, x \bullet x \in ac_0 \Rightarrow (x \oplus \{tr \mapsto s.tr \frown x.tr\}) \in ac' \end{array} \right)$$

{Lemma B.1.3}

$$= \left(\begin{array}{l} \exists\, ac_0 \bullet P[ac_0/ac'][s \oplus \{tr \mapsto \langle\rangle\}/s] \\ \land\, \forall\, x \bullet x \in ac_0 \Rightarrow \exists\, z \bullet z \in ac' \land s.tr \leq z.tr \land x = z \oplus \{tr \mapsto z.tr - s.tr\} \end{array} \right)$$

{Property of sets}

$$= \left(\begin{array}{l} \exists\, ac_0 \bullet P[ac_0/ac'][s \oplus \{tr \mapsto \langle\rangle\}/s] \\ \land \\ ac_0 \subseteq \{z \mid z \in ac' \land s.tr \leq z.tr \bullet z \oplus \{tr \mapsto z.tr - s.tr\}\} \end{array} \right)$$

{Substitution}

$$= \left(\begin{array}{l} (\exists\, ac_0 \bullet P[ac_0/ac'] \land ac_0 \subseteq ac') \\ \left[\begin{array}{r} s \oplus \{tr \mapsto \langle\rangle\} \\ \{z \mid z \in ac' \land s.tr \leq z.tr \bullet z \oplus \{tr \mapsto z.tr - s.tr\}\} \end{array} \middle/ \begin{array}{r} s \\ ac' \end{array} \right] \end{array} \right)$$

{Definition of **RA2**}

$$= \mathbf{RA2}(\exists\, ac_0 \bullet P[ac_0/ac'] \land ac_0 \subseteq ac')$$

{Definition of **PBMH** (Lemma E.1.1)}

$$= \mathbf{RA2} \circ \mathbf{PBMH}(P)$$

□

Properties of RA2 with respect to RA1

In the following proof the order of substitution in the array in square brackets is from top to bottom.

Theorem 1.2.12 (**RA2-RA1**-commutativity)

$$\mathbf{RA2} \circ \mathbf{RA1}(P) = \mathbf{RA1} \circ \mathbf{RA2}(P)$$

Proof.

$$\begin{array}{ll}
& \mathbf{RA2} \circ \mathbf{RA1}(P) \\
& \qquad \{\text{Definition of } \mathbf{RA2}\} \\
= & \mathbf{RA1}(P)[s \oplus \{tr \mapsto \langle\rangle\}, \{z \mid z \in ac' \wedge s.tr \leq z.tr \bullet z \oplus \{tr \mapsto z.tr - s.tr\}\}/s, ac'] \\
& \qquad \{\text{Definition of } \mathbf{RA1}\} \\
= & \left(P \wedge ac' \neq \emptyset \right) [\{z \mid z \in ac' \wedge s.tr \leq z.tr\}/ac'] \\
& [s \oplus \{tr \mapsto \langle\rangle\}, \{z \mid z \in ac' \wedge s.tr \leq z.tr \bullet z \oplus \{tr \mapsto z.tr - s.tr\}\}/s, ac'] \\
& \qquad \{\text{Substitution of } s\} \\
= & \left(\begin{array}{l} P[s \oplus \{tr \mapsto \langle\rangle\}/s] \\ \wedge \\ ac' \neq \emptyset \end{array} \right) [\{z \mid z \in ac' \wedge (s \oplus \{tr \mapsto \langle\rangle\}).tr \leq z.tr\}/ac'] \\
& [\{z \mid z \in ac' \wedge s.tr \leq z.tr \bullet z \oplus \{tr \mapsto z.tr - s.tr\}\}/ac'] \\
& \qquad \{\text{Value of state component } tr\} \\
= & \left(\begin{array}{l} P[s \oplus \{tr \mapsto \langle\rangle\}/s] \\ \wedge \\ ac' \neq \emptyset \end{array} \right) [\{z \mid z \in ac' \wedge \langle\rangle \leq z.tr\}/ac'] \\
& [\{z \mid z \in ac' \wedge s.tr \leq z.tr \bullet z \oplus \{tr \mapsto z.tr - s.tr\}\}/ac'] \\
& \qquad \{\text{Property of sequence prefixing}\} \\
= & \left(\begin{array}{l} P[s \oplus \{tr \mapsto \langle\rangle\}/s] \\ \wedge \\ ac' \neq \emptyset \end{array} \right) [\{z \mid z \in ac'\}/ac'] \\
& [\{z \mid z \in ac' \wedge s.tr \leq z.tr \bullet z \oplus \{tr \mapsto z.tr - s.tr\}\}/ac'] \\
& \qquad \{\text{Property of sets}\} \\
= & \left(\begin{array}{l} P[s \oplus \{tr \mapsto \langle\rangle\}/s] \\ \wedge \\ ac' \neq \emptyset \end{array} \right) [ac'/ac'] \\
& [\{z \mid z \in ac' \wedge s.tr \leq z.tr \bullet z \oplus \{tr \mapsto z.tr - s.tr\}\}/ac'] \\
& \qquad \{\text{Property of substitution}\} \\
= & \left(\begin{array}{l} P[s \oplus \{tr \mapsto \langle\rangle\}/s] \\ \wedge \\ ac' \neq \emptyset \end{array} \right) [\{z \mid z \in ac' \wedge s.tr \leq z.tr \bullet z \oplus \{tr \mapsto z.tr - s.tr\}\}/ac'] \\
& \qquad \{\text{Substitution}\} \\
= & \left(\begin{array}{l} P[s \oplus \{tr \mapsto \langle\rangle\}/s][\{z \mid z \in ac' \wedge s.tr \leq z.tr \bullet z \oplus \{tr \mapsto z.tr - s.tr\}\}/ac'] \\ \wedge \\ \{z \mid z \in ac' \wedge s.tr \leq z.tr \bullet z \oplus \{tr \mapsto z.tr - s.tr\}\} \neq \emptyset \end{array} \right) \\
& \qquad \{\text{Property of sets}\}
\end{array}$$

$$
= \left(\begin{array}{l} P[s \oplus \{tr \mapsto \langle\rangle\}/s][\{z \mid z \in ac' \land s.tr \leq z.tr \bullet z \oplus \{tr \mapsto z.tr - s.tr\}\}/ac'] \\ \land \\ \exists\, y, z \bullet z \in ac' \land s.tr \leq z.tr \land y = z \oplus \{tr \mapsto z.tr - s.tr\} \end{array} \right)
$$

{One-point rule}

$$
= \left(\begin{array}{l} P[s \oplus \{tr \mapsto \langle\rangle\}/s][\{z \mid z \in ac' \land s.tr \leq z.tr \bullet z \oplus \{tr \mapsto z.tr - s.tr\}\}/ac'] \\ \land \\ \exists\, z \bullet z \in ac' \land s.tr \leq z.tr \end{array} \right)
$$

{Property of sets}

$$
= \left(\begin{array}{l} P[s \oplus \{tr \mapsto \langle\rangle\}/s] \left[\left\{ \; z \;\middle|\; \begin{array}{l} z \in \{z \mid z \in ac' \land s.tr \leq z.tr\} \\ \land\ s.tr \leq z.tr \bullet z \oplus \{tr \mapsto z.tr - s.tr\} \end{array} \right\} / ac' \right] \\ \land \\ \exists\, z \bullet z \in ac' \land s.tr \leq z.tr \end{array} \right)
$$

{Property of substitution}

$$
= \left(\begin{array}{l} P[s \oplus \{tr \mapsto \langle\rangle\}/s] \left[\left\{ \; z \;\middle|\; \begin{array}{l} z \in ac' \\ \land\ s.tr \leq z.tr \bullet z \oplus \{tr \mapsto z.tr - s.tr\} \end{array} \right\} / ac' \right] \\ \qquad\qquad [\{z \mid z \in ac' \land s.tr \leq z.tr\}/ac'] \\ \land \\ \exists\, z \bullet z \in ac' \land s.tr \leq z.tr \end{array} \right)
$$

{Definition of **RA2**}

$$
= \left(\begin{array}{l} \mathbf{RA2}(P)[\{z \mid z \in ac' \land s.tr \leq z.tr\}/ac'] \\ \land \\ \exists\, z \bullet z \in ac' \land s.tr \leq z.tr \end{array} \right)
$$

{Lemma 1.2.1}

$$
= \mathbf{RA1} \circ \mathbf{RA2}(P)
$$

□

1.2.3 $\mathit{II}_{\mathcal{R}ac}$

The identity of the theory, $\mathit{II}_{\mathcal{R}ac}$ is defined as follows.

Definition 5 ($\mathit{II}_{\mathcal{R}ac}$)

$$
\mathit{II}_{\mathcal{R}ac} \mathrel{\widehat{=}} (\mathbf{RA1}(\neg\ ok) \lor (ok' \land s \in ac'))
$$

If the process has not been started or, the previous process has diverged, then the only guarantee is that the final traces are a suffix of the initial trace $s.tr$ as required by **RA1**. Otherwise, it terminates and the initial state s

must be in the set of final states. This definition can be rewritten as shown in the following lemma.

Lemma 1.2.3 ($\Pi_{\mathcal{R}ac}$-alternative-1)

$$\Pi_{\mathcal{R}ac} = (\neg\ ok \wedge \exists\, z \bullet s.tr \leq z.tr \wedge z \in ac') \vee (ok' \wedge s \in ac')$$

Proof.

$$\begin{array}{ll}
\Pi_{\mathcal{R}ac} & \{\text{Definition of } \Pi_{\mathcal{R}ac}\} \\
= \mathbf{RA1}(\neg\ ok) \vee (ok' \wedge s \in ac') & \{\text{Definition of } \mathbf{RA1} \text{ (Lemma 1.2.1)}\} \\
= \left(\begin{array}{l} ((\neg\ ok)[\{z \mid z \in ac' \wedge s.tr \leq z.tr\}/ac'] \wedge \exists\, z \bullet s.tr \leq z.tr \wedge z \in ac') \\ \vee \\ (ok' \wedge s \in ac') \end{array} \right) & \{\text{Substitution}\} \\
= (\neg\ ok \wedge \exists\, z \bullet s.tr \leq z.tr \wedge z \in ac') \vee (ok' \wedge s \in ac') &
\end{array}$$

□

Properties of $\Pi_{\mathcal{R}ac}$

Theorem 1.2.13 ($\Pi_{\mathcal{R}ac}$-**RA1**-healthy)

$$\mathbf{RA1}(\Pi_{\mathcal{R}ac}) = \Pi_{\mathcal{R}ac}$$

Proof.

$$\begin{array}{ll}
\mathbf{RA1}(\Pi_{\mathcal{R}ac}) & \{\text{Definition of } \Pi_{\mathcal{R}ac}\} \\
= \mathbf{RA1}(\mathbf{RA1}(\neg\ ok) \vee (ok' \wedge s \in ac')) & \\
& \{\text{Distributivity of } \mathbf{RA1} \text{ (Theorem 1.2.1)}\} \\
= \mathbf{RA1} \circ \mathbf{RA1}(\neg\ ok) \vee \mathbf{RA1}(ok' \wedge s \in ac') & \{\text{Lemma B.1.11}\} \\
= \mathbf{RA1} \circ \mathbf{RA1}(\neg\ ok) \vee (ok' \wedge \mathbf{RA1}(s \in ac')) & \{\text{Lemma B.1.9}\} \\
= \mathbf{RA1} \circ \mathbf{RA1}(\neg\ ok) \vee (ok' \wedge s \in ac') & \\
& \{\mathbf{RA1}\text{-idempotent (Theorem 1.2.3)}\} \\
= \mathbf{RA1}(\neg\ ok) \vee (ok' \wedge s \in ac') & \{\text{Definition of } \Pi_{\mathcal{R}ac}\} \\
= \Pi_{\mathcal{R}ac} &
\end{array}$$

□

Theorem 1.2.14 ($\mathbb{I}_{\mathcal{R}ac}$-**RA2**-healthy)

$$\mathbf{RA2}(\mathbb{I}_{\mathcal{R}ac}) = \mathbb{I}_{\mathcal{R}ac}$$

Proof.

$$\begin{array}{ll}
\mathbf{RA2}(\mathbb{I}_{\mathcal{R}ac}) & \{\text{Definition of } \mathbb{I}_{\mathcal{R}ac}\} \\
= \mathbf{RA2}((\neg\ ok \wedge \mathbf{RA1}(true)) \vee (ok' \wedge s \in ac')) & \\
& \{\text{Distributivity of } \mathbf{RA2} \text{ (Theorem 1.2.10)}\} \\
= \mathbf{RA2}(\neg\ ok \wedge \mathbf{RA1}(true)) \vee \mathbf{RA2}(ok' \wedge s \in ac') & \\
& \{\text{Distributivity of } \mathbf{RA2} \text{ (Theorem 1.2.9)}\} \\
= (\mathbf{RA2}(\neg\ ok) \wedge \mathbf{RA2} \circ \mathbf{RA1}(true)) \vee (\mathbf{RA2}(ok') \wedge \mathbf{RA2}(s \in ac')) & \\
& \{\text{Lemma B.2.4}\} \\
= (\neg\ ok \wedge \mathbf{RA2} \circ \mathbf{RA1}(true)) \vee (ok' \wedge \mathbf{RA2}(s \in ac')) & \{\text{Lemma B.2.3}\} \\
= (\neg\ ok \wedge \mathbf{RA2} \circ \mathbf{RA1}(true)) \vee (ok' \wedge s \in ac') & \{\text{Theorem 1.2.12}\} \\
= (\neg\ ok \wedge \mathbf{RA1} \circ \mathbf{RA2}(true)) \vee (ok' \wedge s \in ac') & \{\text{Lemma B.2.2}\} \\
= (\neg\ ok \wedge \mathbf{RA1}(true)) \vee (ok' \wedge s \in ac') & \{\text{Definition of } \mathbb{I}_{\mathcal{R}ac}\} \\
= \mathbb{I}_{\mathcal{R}ac} &
\end{array}$$

□

Theorem 1.2.15 ($\mathbb{I}_{\mathcal{R}ac}$-**PBMH**-healthy)

$$\mathbf{PBMH}(\mathbb{I}_{\mathcal{R}ac}) = \mathbb{I}_{\mathcal{R}ac}$$

Proof.

$$\begin{array}{ll}
\mathbf{PBMH}(\mathbb{I}_{\mathcal{R}ac}) & \{\text{Definition of } \mathbb{I}_{\mathcal{R}ac}\} \\
= \mathbf{PBMH}((\neg\ ok \wedge \exists\, z \bullet s.tr \leq z.tr \wedge z \in ac') \vee (ok' \wedge s \in ac')) & \\
& \{\text{Distributivity of } \mathbf{PBMH}\} \\
= \left(\begin{array}{l} \mathbf{PBMH}(\neg\ ok \wedge \exists\, z \bullet s.tr \leq z.tr \wedge z \in ac') \\ \vee \\ \mathbf{PBMH}(ok' \wedge s \in ac') \end{array}\right) & \{\text{Lemma E.4.8}\} \\
= \left(\begin{array}{l} (\neg\ ok \wedge \mathbf{PBMH}(\exists\, z \bullet s.tr \leq z.tr \wedge z \in ac')) \\ \vee \\ (ok' \wedge \mathbf{PBMH}(s \in ac')) \end{array}\right) & \{\text{Lemma E.4.7}\}
\end{array}$$

$$= \left(\begin{array}{l} (\neg\ ok \wedge \exists\, z \bullet s.tr \leq z.tr \wedge z \in ac') \\ \vee \\ (ok' \wedge s \in ac') \end{array} \right) \qquad \{\text{Definition of } \mathit{II}_{\mathcal{R}ac}\}$$

$$= \mathit{II}_{\mathcal{R}ac}$$

□

1.2.4 RA3

The healthiness condition **RA3** ensures that a process cannot start interacting with the environment before its predecessor has terminated in a stable state, that is, *s.wait* is *false*. Otherwise the behaviour is given by the identity of the theory $\mathit{II}_{\mathcal{R}ac}$.

Definition 6 (**RA3**)

$$\mathbf{RA3}(P) \mathrel{\widehat{=}} \mathit{II}_{\mathcal{R}ac} \lhd s.wait \rhd P$$

Properties of RA3

In this section we prove that **RA3** is idempotent and monotonic and also that it distributes through both disjunction and conjunction.

Theorem 1.2.16 (**RA3**-idempotent)

$$\mathbf{RA3} \circ \mathbf{RA3}(P) = \mathbf{RA3}(P)$$

Proof.

$\mathbf{RA3} \circ \mathbf{RA3}(P)$ {Definition of **RA3**}

$= \mathit{II}_{\mathcal{R}ac} \lhd s.wait \rhd \mathbf{RA3}(P)$ {Definition of **RA3**}

$= \mathit{II}_{\mathcal{R}ac} \lhd s.wait \rhd (\mathit{II}_{\mathcal{R}ac} \lhd s.wait \rhd P)$ {Defiition of conditional}

$= (s.wait \wedge \mathit{II}_{\mathcal{R}ac}) \vee (\neg\ s.wait \wedge (\mathit{II}_{\mathcal{R}ac} \lhd s.wait \rhd P))$ {Property of conditional}

$= (s.wait \wedge \mathit{II}_{\mathcal{R}ac}) \vee (\neg\ s.wait \wedge P)$ {Defiition of conditional}

$= \mathit{II}_{\mathcal{R}ac} \lhd s.wait \rhd P$ {Definition of **RA3**}

$= \mathbf{RA3}(P)$

□

Theorem 1.2.17 (**RA3**-monotonic)

$$P \sqsubseteq Q \Rightarrow \mathbf{RA3}(P) \sqsubseteq \mathbf{RA3}(Q)$$

Proof.

$$\begin{aligned}
&\mathbf{RA3}(Q) && \{\text{Assumption: } P \sqsubseteq Q = [Q \Rightarrow P]\}\\
&= \mathbf{RA3}(Q \wedge P) && \{\text{Theorem 1.2.18}\}\\
&= \mathbf{RA3}(Q) \wedge \mathbf{RA3}(P) && \{\text{Predicate calculus}\}\\
&\sqsupseteq \mathbf{RA3}(P)
\end{aligned}$$

□

Theorem 1.2.18 (**RA3**-conjunction-distribute)

$$\mathbf{RA3}(P \wedge Q) = \mathbf{RA3}(P) \wedge \mathbf{RA3}(Q)$$

Proof.

$$\begin{aligned}
&\mathbf{RA3}(P \wedge Q) && \{\text{Definition of } \mathbf{RA3}\}\\
&= I\!I_{\mathcal{R}ac} \lhd s.wait \rhd (P \wedge Q) && \{\text{Definition of conditional}\}\\
&= (s.wait \wedge I\!I_{\mathcal{R}ac}) \vee (\neg\, s.wait \wedge P \wedge Q) && \{\text{Predicate calculus}\}\\
&= (s.wait \wedge I\!I_{\mathcal{R}ac}) \vee ((\neg\, s.wait \wedge P) \wedge (\neg\, s.wait \wedge Q)) && \{\text{Predicate calculus}\}\\
&= ((s.wait \wedge I\!I_{\mathcal{R}ac}) \vee (\neg\, s.wait \wedge P)) \wedge ((s.wait \wedge I\!I_{\mathcal{R}ac}) \vee (\neg\, s.wait \wedge Q)) && \{\text{Definition of conditional}\}\\
&= (I\!I_{\mathcal{R}ac} \lhd s.wait \rhd P) \wedge (I\!I_{\mathcal{R}ac} \lhd s.wait \rhd Q) && \{\text{Definition of } \mathbf{RA3}\}\\
&= \mathbf{RA3}(P) \wedge \mathbf{RA3}(Q)
\end{aligned}$$

□

Theorem 1.2.19 (**RA3**-disjunction-distribute)

$$\mathbf{RA3}(P \vee Q) = \mathbf{RA3}(P) \vee \mathbf{RA3}(Q)$$

Proof.

$$\begin{aligned}
&\mathbf{RA3}(P \vee Q) && \{\text{Definition of } \mathbf{RA3}\}
\end{aligned}$$

$= \mathbb{I}_{\mathcal{R}ac} \lhd s.wait \rhd (P \vee Q)$ {Definition of conditional}
$= (s.wait \wedge \mathbb{I}_{\mathcal{R}ac}) \vee (\neg\, s.wait \wedge (P \vee Q))$ {Predicate calculus}
$= (s.wait \wedge \mathbb{I}_{\mathcal{R}ac}) \vee (\neg\, s.wait \wedge P) \vee (\neg\, s.wait \wedge Q)$ {Predicate calculus}
$= (s.wait \wedge \mathbb{I}_{\mathcal{R}ac}) \vee (\neg\, s.wait \wedge P) \vee (s.wait \wedge \mathbb{I}_{\mathcal{R}ac}) \vee (\neg\, s.wait \wedge Q)$ {Definition of conditional}
$= (\mathbb{I}_{\mathcal{R}ac} \lhd s.wait \rhd P) \vee (\mathbb{I}_{\mathcal{R}ac} \lhd s.wait \rhd Q)$ {Definition of **RA3**}
$= \mathbf{RA3}(P) \vee \mathbf{RA3}(Q)$

□

Properties with respect to $\mathbb{I}_{\mathcal{R}ac}$

Theorem 1.2.20 ($\mathbb{I}_{\mathcal{R}ac}$-**RA3**-healthy)

$$\mathbf{RA3}(\mathbb{I}_{\mathcal{R}ac}) = \mathbb{I}_{\mathcal{R}ac}$$

Proof.

$\mathbf{RA3}(\mathbb{I}_{\mathcal{R}ac})$ {Definition of **RA3**}
$= \mathbb{I}_{\mathcal{R}ac} \lhd s.wait \rhd \mathbb{I}_{\mathcal{R}ac}$ {Property of conditonal}
$= \mathbb{I}_{\mathcal{R}ac}$

□

Properties of RA3 with respect to RA1

Theorem 1.2.21 (**RA3**-**RA1**-commutativity)

$$\mathbf{RA3} \circ \mathbf{RA1}(P) = \mathbf{RA3} \circ \mathbf{RA1}(P)$$

Proof.

$\mathbf{RA1} \circ \mathbf{RA3}(P)$ {Definition of **RA3**}
$= \mathbf{RA1}(\mathbb{I}_{\mathcal{R}ac} \lhd s.wait \rhd P)$ {Lemma B.1.10}
$= \mathbf{RA1}(\mathbb{I}_{\mathcal{R}ac}) \lhd s.wait \rhd \mathbf{RA1}(P)$ {Theorem 1.2.13}
$= \mathbb{I}_{\mathcal{R}ac} \lhd s.wait \rhd \mathbf{RA1}(P)$ {Definition of **RA3**}
$= \mathbf{RA3} \circ \mathbf{RA1}(P)$

□

Properties of RA3 with respect to RA2

Theorem 1.2.22 (**RA3**-**RA2**-commutative)

$$\mathbf{RA2} \circ \mathbf{RA3}(P) = \mathbf{RA3} \circ \mathbf{RA2}(P)$$

Proof.

$$\begin{aligned}
&\mathbf{RA2} \circ \mathbf{RA3}(P) && \{\text{Definition of } \mathbf{RA3}\}\\
&= \mathbf{RA2}(\mathbb{I}_{\mathcal{R}ac} \lhd s.wait \rhd P) && \{\text{Lemma B.2.6 and } s.wait \text{ is } \mathbf{RA2}\text{-healthy}\}\\
&= \mathbf{RA2}(\mathbb{I}_{\mathcal{R}ac}) \lhd s.wait \rhd \mathbf{RA2}(P) && \{\text{Theorem 1.2.14}\}\\
&= \mathbb{I}_{\mathcal{R}ac} \lhd s.wait \rhd \mathbf{RA2}(P) && \{\text{Definition of } \mathbf{RA3}\}\\
&= \mathbf{RA3} \circ \mathbf{RA2}(P)
\end{aligned}$$

□

Properties with respect to PBMH

Theorem 1.2.23

$$\mathbf{PBMH} \circ \mathbf{RA3} \circ \mathbf{PBMH}(P) = \mathbf{RA3} \circ \mathbf{PBMH}(P)$$

Proof.

$$\begin{aligned}
&\mathbf{PBMH} \circ \mathbf{RA3} \circ \mathbf{PBMH}(P) && \{\text{Definition of } \mathbf{RA3}\}\\
&= \mathbf{PBMH}(\mathbb{I}_{\mathcal{R}ac} \lhd s.wait \rhd \mathbf{PBMH}(P)) && \{\text{Lemma E.4.9}\}\\
&= \mathbf{PBMH}(\mathbb{I}_{\mathcal{R}ac}) \lhd s.wait \rhd \mathbf{PBMH} \circ \mathbf{PBMH}(P) && \{\text{Theorem 1.2.15}\}\\
&= \mathbb{I}_{\mathcal{R}ac} \lhd s.wait \rhd \mathbf{PBMH} \circ \mathbf{PBMH}(P) && \{\text{Theorem E.2.1}\}\\
&= \mathbb{I}_{\mathcal{R}ac} \lhd s.wait \rhd \mathbf{PBMH}(P) && \{\text{Definition of } \mathbf{RA3}\}\\
&= \mathbf{RA3} \circ \mathbf{PBMH}(P)
\end{aligned}$$

□

Theorem New 1.2.1

$$\mathbf{PBMH} \circ \mathbf{RA3}(P) = \mathbf{RA3} \circ \mathbf{PBMH}(P)$$

Proof.

$$
\begin{aligned}
&\mathbf{PBMH} \circ \mathbf{RA3}(P) && \{\text{Definition of } \mathbf{RA3}\}\\
&= \mathbf{PBMH}(\mathbb{I}_{\mathcal{R}ac} \lhd s.wait \rhd P) && \{\text{Lemma E.4.9}\}\\
&= \mathbf{PBMH}(\mathbb{I}_{\mathcal{R}ac}) \lhd s.wait \rhd \mathbf{PBMH}(P) && \{\text{Theorem 1.2.15}\}\\
&= \mathbb{I}_{\mathcal{R}ac} \lhd s.wait \rhd \mathbf{PBMH}(P) && \{\text{Definition of } \mathbf{RA3}\}\\
&= \mathbf{RA3} \circ \mathbf{PBMH}(P)
\end{aligned}
$$

□

1.2.5 RA

Definition 7 (**RA**)

$$\mathbf{RA}(P) \mathrel{\widehat{=}} \mathbf{RA1} \circ \mathbf{RA2} \circ \mathbf{RA3}(P)$$

Lemma 1.2.4

$$\mathbf{RA1} \circ \mathbf{RA2} \circ \mathbf{RA3}(P) = \mathbf{RA3} \circ \mathbf{RA2} \circ \mathbf{RA1}(P)$$

Proof.

$$
\begin{aligned}
&\mathbf{RA1} \circ \mathbf{RA2} \circ \mathbf{RA3}(P) && \{\text{Theorem 1.2.12}\}\\
&= \mathbf{RA2} \circ \mathbf{RA1} \circ \mathbf{RA3}(P) && \{\text{Theorem 1.2.21}\}\\
&= \mathbf{RA2} \circ \mathbf{RA3} \circ \mathbf{RA1}(P) && \{\text{Theorem 1.2.22}\}\\
&= \mathbf{RA3} \circ \mathbf{RA2} \circ \mathbf{RA1}(P)
\end{aligned}
$$

□

Properties

Theorem 1.2.24 (**RA**-conjunction-distribute)

$$\mathbf{RA}(P \wedge Q) = \mathbf{RA}(P) \wedge \mathbf{RA}(Q)$$

Proof.

$$
\begin{aligned}
&\mathbf{RA}(P \wedge Q) && \{\text{Definition of } \mathbf{RA}\}\\
&= \mathbf{RA1} \circ \mathbf{RA2} \circ \mathbf{RA3}(P \wedge Q) && \{\text{Theorem 1.2.18}\}
\end{aligned}
$$

$= \mathbf{RA1} \circ \mathbf{RA2}(\mathbf{RA3}(P) \wedge \mathbf{RA3}(Q))$ {Theorem 1.2.9}
$= \mathbf{RA1}(\mathbf{RA2} \circ \mathbf{RA3}(P) \wedge \mathbf{RA2} \circ \mathbf{RA3}(Q))$ {Theorem 1.2.2}
$= \mathbf{RA1} \circ \mathbf{RA2} \circ \mathbf{RA3}(P) \wedge \mathbf{RA1} \circ \mathbf{RA2} \circ \mathbf{RA3}(Q)$ {Definition of **RA**}
$= \mathbf{RA}(P) \wedge \mathbf{RA}(Q)$

□

Theorem 1.2.25 (**RA**-disjunction-distribute)

$$\mathbf{RA}(P \vee Q) = \mathbf{RA}(P) \vee \mathbf{RA}(Q)$$

Proof.

$\mathbf{RA}(P \vee Q)$ {Definition of **RA**}
$= \mathbf{RA1} \circ \mathbf{RA2} \circ \mathbf{RA3}(P \vee Q)$ {Theorem 1.2.19}
$= \mathbf{RA1} \circ \mathbf{RA2}(\mathbf{RA3}(P) \vee \mathbf{RA3}(Q))$ {Theorem 1.2.10}
$= \mathbf{RA1}(\mathbf{RA2} \circ \mathbf{RA3}(P) \vee \mathbf{RA2} \circ \mathbf{RA3}(Q))$ {Theorem 1.2.1}
$= \mathbf{RA1} \circ \mathbf{RA2} \circ \mathbf{RA3}(P) \vee \mathbf{RA1} \circ \mathbf{RA2} \circ \mathbf{RA3}(Q)$ {Definition of **RA**}
$= \mathbf{RA}(P) \vee \mathbf{RA}(Q)$

□

Theorem 1.2.26 (**RA**-idempotent)

$$\mathbf{RA} \circ \mathbf{RA}(P) = \mathbf{RA}(P)$$

Proof.

$\mathbf{RA} \circ \mathbf{RA}(P)$ {Definition of **RA**}
$= \mathbf{RA3} \circ \mathbf{RA2} \circ \mathbf{RA1} \circ \mathbf{RA3} \circ \mathbf{RA2} \circ \mathbf{RA1}(P)$ {Theorem 1.2.12}
$= \mathbf{RA3} \circ \mathbf{RA2} \circ \mathbf{RA1} \circ \mathbf{RA3} \circ \mathbf{RA1} \circ \mathbf{RA2}(P)$ {Theorem 1.2.21}
$= \mathbf{RA3} \circ \mathbf{RA2} \circ \mathbf{RA1} \circ \mathbf{RA1} \circ \mathbf{RA3} \circ \mathbf{RA2}(P)$ {Theorem 1.2.3}
$= \mathbf{RA3} \circ \mathbf{RA2} \circ \mathbf{RA1} \circ \mathbf{RA3} \circ \mathbf{RA2}(P)$ {Theorem 1.2.22}
$= \mathbf{RA2} \circ \mathbf{RA3} \circ \mathbf{RA1} \circ \mathbf{RA3} \circ \mathbf{RA2}(P)$ {Theorem 1.2.21}
$= \mathbf{RA2} \circ \mathbf{RA1} \circ \mathbf{RA3} \circ \mathbf{RA3} \circ \mathbf{RA2}(P)$ {Theorem 1.2.16}

$= \mathbf{RA2} \circ \mathbf{RA1} \circ \mathbf{RA3} \circ \mathbf{RA2}(P)$ {Theorem 1.2.21}
$= \mathbf{RA2} \circ \mathbf{RA3} \circ \mathbf{RA1} \circ \mathbf{RA2}(P)$ {Theorem 1.2.22}
$= \mathbf{RA3} \circ \mathbf{RA2} \circ \mathbf{RA1} \circ \mathbf{RA2}(P)$ {Theorem 1.2.12}
$= \mathbf{RA3} \circ \mathbf{RA1} \circ \mathbf{RA2} \circ \mathbf{RA2}(P)$ {Theorem 1.2.7}
$= \mathbf{RA3} \circ \mathbf{RA1} \circ \mathbf{RA2}(P)$ {Theorem 1.2.12}
$= \mathbf{RA3} \circ \mathbf{RA2} \circ \mathbf{RA1}(P)$ {Definition of **RA**}
$= \mathbf{RA}(P)$

□

Properties with respect to A

Theorem 1.2.27

$$\mathbf{RA} \circ \mathbf{A}(P) = \mathbf{RA} \circ \mathbf{PBMH}(P)$$

Proof.

$\mathbf{RA} \circ \mathbf{A}(P)$ {Definition of **RA** and **A**}
$= \mathbf{RA3} \circ \mathbf{RA2} \circ \mathbf{RA1} \circ \mathbf{A0} \circ \mathbf{A1}(P)$ {**A1** is **PBMH**}
$= \mathbf{RA3} \circ \mathbf{RA2} \circ \mathbf{RA1} \circ \mathbf{A0} \circ \mathbf{PBMH}(P)$ {Theorem 1.2.6}
$= \mathbf{RA3} \circ \mathbf{RA2} \circ \mathbf{RA1} \circ \mathbf{PBMH}(P)$ {Definition of **RA**}
$= \mathbf{RA} \circ \mathbf{PBMH}(P)$

□

Properties with respect to PBMH

Theorem 1.2.28 *Provided P is* **PBMH***-healthy.*

$$\mathbf{PBMH} \circ \mathbf{RA}(P) = \mathbf{RA}(P)$$

Proof.

$\mathbf{RA}(P)$ {Definition of **RA**}
$= \mathbf{RA3} \circ \mathbf{RA2} \circ \mathbf{RA1}(P)$
{Assumption: P is **PBMH**-healthy and Theorem 1.2.5}
$= \mathbf{RA3} \circ \mathbf{RA2} \circ \mathbf{PBMH} \circ \mathbf{RA1}(P)$ {Theorem 1.2.11}

$= \mathbf{RA3} \circ \mathbf{PBMH} \circ \mathbf{RA2} \circ \mathbf{PBMH} \circ \mathbf{RA1}(P)$ {Theorem 1.2.23}
$= \mathbf{PBMH} \circ \mathbf{RA3} \circ \mathbf{PBMH} \circ \mathbf{RA2} \circ \mathbf{PBMH} \circ \mathbf{RA1}(P)$
{Theorem 1.2.11}
$= \mathbf{PBMH} \circ \mathbf{RA3} \circ \mathbf{RA2} \circ \mathbf{PBMH} \circ \mathbf{RA1}(P)$
{Assumption: P is **PBMH**-healthy and Theorem 1.2.5}
$= \mathbf{PBMH} \circ \mathbf{RA3} \circ \mathbf{RA2} \circ \mathbf{RA1}(P)$ {Definition of **RA**}
$= \mathbf{PBMH} \circ \mathbf{RA}(P)$

□

Clearly, **PBMH** and **RA** do not commute, because **PBMH** and **RA1** also do not commute.

1.2.6 CSPA1

Definition 8 (**CSPA1**)

$$\mathbf{CSPA1}(P) \mathrel{\widehat{=}} P \vee \mathbf{RA1}(\neg\ ok)$$

This definition can be rewritten as shown in the following lemma.

Lemma 1.2.5 (**CSPA1**-alternative-1)

$$\mathbf{CSPA1}(P) = P \vee (\neg\ ok \wedge \exists\, z \bullet s.tr \leq z.tr \wedge z \in ac')$$

Proof.

$\mathbf{CSPA1}(P)$ {Definition of **CSPA1**}
$= P \vee \mathbf{RA1}(\neg\ ok)$ {Lemma B.1.12}
$= P \vee (\neg\ ok \wedge \mathbf{RA1}(true))$ {Lemma B.1.5}
$= P \vee (\neg\ ok \wedge \exists\, z \bullet s.tr \leq z.tr \wedge z \in ac')$

□

Properties

Theorem 1.2.29 (**CSPA1**-idempotent)

$$\mathbf{CSPA1} \circ \mathbf{CSPA1}(P) = \mathbf{CSPA1}(P)$$

Proof.

$$
\begin{aligned}
&\mathbf{CSPA1} \circ \mathbf{CSPA1}(P) && \{\text{Definition of } \mathbf{CSPA1}\}\\
&= \mathbf{CSPA1}(P \vee (\neg\ ok \wedge \mathbf{RA1}(true))) && \{\text{Definition of } \mathbf{CSPA1}\}\\
&= (P \vee (\neg\ ok \wedge \mathbf{RA1}(true))) \vee (\neg\ ok \wedge \mathbf{RA1}(true)) \\
& && \{\text{Predicate calculus}\}\\
&= P \vee (\neg\ ok \wedge \mathbf{RA1}(true)) && \{\text{Definition of } \mathbf{CSPA1}\}\\
&= \mathbf{CSPA1}(P)
\end{aligned}
$$

□

Theorem 1.2.30 (**CSPA1**-monotonic)

$$P \sqsubseteq Q \Rightarrow \mathbf{CSPA1}(P) \sqsubseteq \mathbf{CSPA1}(Q)$$

Proof.

$$
\begin{aligned}
&\mathbf{CSPA1}(Q) && \{\text{Definition of } \mathbf{CSPA1}\}\\
&= Q \vee (\neg\ ok \wedge \mathbf{RA1}(true)) && \{\text{Assumption: } P \sqsubseteq Q = [Q \Rightarrow P]\}\\
&= (Q \wedge P) \vee (\neg\ ok \wedge \mathbf{RA1}(true)) && \{\text{Predicate calculus}\}\\
&= (Q \vee (\neg\ ok \wedge \mathbf{RA1}(true))) \wedge (P \vee (\neg\ ok \wedge \mathbf{RA1}(true))) \\
& && \{\text{Predicate calculus}\}\\
&\Rightarrow (P \vee (\neg\ ok \wedge \mathbf{RA1}(true))) && \{\text{Definition of } \mathbf{CSPA1}\}\\
&= \mathbf{CSPA1}(P)
\end{aligned}
$$

□

Properties with respect to PBMH

Theorem 1.2.31 *Provided P is* **PBMH***-healthy.*

$$\mathbf{PBMH} \circ \mathbf{CSPA1}(P) = \mathbf{CSPA1}(P)$$

Proof.

$$
\begin{aligned}
&\mathbf{PBMH} \circ \mathbf{CSPA1}(P) && \{\text{Definition of } \mathbf{CSPA1}\}\\
&= \mathbf{PBMH}(P \vee (\mathbf{RA1}(\neg\ ok))) && \{\text{Distributivity of } \mathbf{PBMH}\}\\
&= \mathbf{PBMH}(P) \vee \mathbf{PBMH} \circ \mathbf{RA1}(\neg\ ok) && \{\text{Lemma E.4.6}\}
\end{aligned}
$$

$= \mathbf{PBMH}(P) \vee \mathbf{PBMH} \circ \mathbf{RA1} \circ \mathbf{PBMH}(\neg\ ok)$
$\{\neg\ ok$ is **PBMH**-healthy and Theorem 1.2.5$\}$
$= \mathbf{PBMH}(P) \vee \mathbf{RA1} \circ \mathbf{PBMH}(\neg\ ok)$ {Lemma E.4.6}
$= \mathbf{PBMH}(P) \vee \mathbf{RA1}(\neg\ ok)$ {Assumption: P is **PBMH**-healthy}
$= P \vee \mathbf{RA1}(\neg\ ok)$ {Definition of **CSPA1**}
$= \mathbf{CSPA1}(P)$

□

Properties with respect to RA1 and H1

Theorem 1.2.32

$$\mathbf{RA1} \circ \mathbf{CSPA1}(P) = \mathbf{RA1} \circ \mathbf{H1}(P)$$

Proof.

$\mathbf{RA1} \circ \mathbf{H1}(P)$ {Definition of **H1**}
$= \mathbf{RA1}(ok \Rightarrow P)$ {Predicate calculus}
$= \mathbf{RA1}(\neg\ ok \vee P)$ {Theorem 1.2.1}
$= \mathbf{RA1}(\neg\ ok) \vee \mathbf{RA1}(P)$ {**RA1**-idempotent (Theorem 1.2.3)}
$= \mathbf{RA1} \circ \mathbf{RA1}(\neg\ ok) \vee \mathbf{RA1}(P)$ {Theorem 1.2.1}
$= \mathbf{RA1}(\mathbf{RA1}(\neg\ ok) \vee P)$ {Definition of **CSPA1**}
$= \mathbf{RA1} \circ \mathbf{CSPA1}(P)$

□

1.2.7 A2

Predicates that do not exhibit angelic nondeterminism are characterised by the healthiness condition **A2**, whose definition is introduced below.

Definition 9 $\mathbf{A2}(P) \mathrel{\widehat{=}} \mathbf{PBMH}(P\ \ ;_{\mathcal{A}}\ \{s\} = ac')$

This function requires the set of final states in P to be either empty or a singleton, otherwise it becomes *false*. Since this definition purposedly breaks the upward-closure, **PBMH** must be applied as a result. If we consider the definition of **PBMH** and $;_{\mathcal{A}}$, then **A2** can be rewritten as shown by the following Theorem 1.2.33.

Theorem 1.2.33

$$\mathbf{A2}(P) = P[\emptyset/ac'] \vee (\exists\, y \bullet P[\{y\}/ac'] \wedge y \in ac')$$

Proof.

$$\begin{array}{ll}
\mathbf{A2}(P) & \{\text{Predicate calculus}\} \\
= \mathbf{A2}(P \wedge (ac' = \emptyset \vee ac' \neq \emptyset)) & \{\text{Predicate calculus}\} \\
= \mathbf{A2}((P \wedge ac' = \emptyset) \vee (P \wedge ac' \neq \emptyset)) & \{\text{Theorem A.3.2}\} \\
= \mathbf{A2}(P \wedge ac' = \emptyset) \vee \mathbf{A2}(P \wedge ac' \neq \emptyset) & \{\text{Lemmas A.3.8 and A.3.9}\} \\
= P[\emptyset/ac'] \vee (\exists\, z \bullet P[\{z\}/ac'] \wedge z \in ac') &
\end{array}$$

□

This result relies on the distributive properties of **PBMH** and $;_{\mathcal{A}}$ through disjunction. It confirms our intuition, in that **A2** requires the set of final states ac' to be either an empty set or a singleton.

Properties

The following theorems establish that **A2** is monotonic and idempotent.

Theorem 1.2.34 (**A2**-idempotent)

$$\mathbf{A2} \circ \mathbf{A2}(P) = \mathbf{A2}(P)$$

Proof.

$$\begin{array}{ll}
\mathbf{A2} \circ \mathbf{A2}(P) & \{\text{Definition of } \mathbf{A2} \text{ (Theorem 1.2.33)}\} \\
= \mathbf{A2}(P)[\emptyset/ac'] \vee (\exists\, y \bullet \mathbf{A2}(P)[\{y\}/ac'] \wedge y \in ac') & \\
& \{\text{Definition of } \mathbf{A2} \text{ (Theorem 1.2.33)}\} \\
= \left(\begin{array}{l} (P[\emptyset/ac'] \vee (\exists\, y \bullet P[\{y\}/ac'] \wedge y \in ac'))[\emptyset/ac'] \\ \vee \\ (\exists\, y \bullet (P[\emptyset/ac'] \vee (\exists\, y \bullet P[\{y\}/ac'] \wedge y \in ac'))[\{y\}/ac'] \wedge y \in ac') \end{array} \right) & \\
& \{\text{Variable renaming}\} \\
= \left(\begin{array}{l} (P[\emptyset/ac'] \vee (\exists\, y \bullet P[\{y\}/ac'] \wedge y \in ac'))[\emptyset/ac'] \\ \vee \\ (\exists\, y \bullet (P[\emptyset/ac'] \vee (\exists\, z \bullet P[\{z\}/ac'] \wedge z \in ac'))[\{y\}/ac'] \wedge y \in ac') \end{array} \right) & \\
& \{\text{Substitution}\}
\end{array}$$

$$= \left(\begin{array}{l} (P[\emptyset/ac'] \vee (\exists\, y \bullet P[\{y\}/ac'] \wedge y \in \emptyset)) \\ \vee \\ (\exists\, y \bullet (P[\emptyset/ac'] \vee (\exists\, z \bullet P[\{z\}/ac'] \wedge z \in \{y\})) \wedge y \in ac') \end{array} \right)$$

{Property of sets and predicate calculus}

$$= P[\emptyset/ac'] \vee (\exists\, y \bullet (P[\emptyset/ac'] \vee (\exists\, z \bullet P[\{z\}/ac'] \wedge z = y)) \wedge y \in ac')$$

{One-point rule}

$$= P[\emptyset/ac'] \vee (\exists\, y \bullet (P[\emptyset/ac'] \vee P[\{y\}/ac']) \wedge y \in ac')$$

{Predicate calculus}

$$= P[\emptyset/ac'] \vee (\exists\, y \bullet P[\emptyset/ac'] \wedge y \in ac') \vee (\exists\, y \bullet P[\{y\}/ac'] \wedge y \in ac')$$

{Predicate calculus: y not free in P}

$$= P[\emptyset/ac'] \vee (P[\emptyset/ac'] \wedge \exists\, y \bullet y \in ac') \vee (\exists\, y \bullet P[\{y\}/ac'] \wedge y \in ac')$$

{Predicate calculus: absorption law}

$$= P[\emptyset/ac'] \vee (\exists\, y \bullet P[\{y\}/ac'] \wedge y \in ac')$$

{Definition of **A2** (Theorem 1.2.33)}

$$= \mathbf{A2}(P)$$

□

Theorem 1.2.35 (**A2**-monotonic)

$$P \sqsubseteq Q \Rightarrow \mathbf{A2}(P) \sqsubseteq \mathbf{A2}(Q)$$

Proof.

$\mathbf{A2}(Q)$ {Definition of **A2**}

$= \mathbf{PBMH}(Q \ ;_{\mathcal{A}} \{s\} = ac')$ {Assumption: $P \sqsubseteq Q = [Q \Rightarrow P]$}

$= \mathbf{PBMH}((P \wedge Q) \ ;_{\mathcal{A}} \{s\} = ac')$ {Distributivity of $;_{\mathcal{A}}$}

$= \mathbf{PBMH}((P \ ;_{\mathcal{A}} \{s\} = ac') \wedge (Q \ ;_{\mathcal{A}} \{s\} = ac'))$

{Definition of **PBMH** (Lemma E.1.1)}

$= \exists\, ac_0 \bullet ((P \ ;_{\mathcal{A}} \{s\} = ac') \wedge (Q \ ;_{\mathcal{A}} \{s\} = ac'))[ac_0/ac'] \wedge ac_0 \subseteq ac'$

{Substitution}

$= \exists\, ac_0 \bullet ((P \ ;_{\mathcal{A}} \{s\} = ac')[ac_0/ac'] \wedge (Q \ ;_{\mathcal{A}} \{s\} = ac')[ac_0/ac']) \wedge ac_0 \subseteq ac'$

{Predicate calculus}

$\sqsupseteq \exists\, ac_0 \bullet (P \ ;_{\mathcal{A}} \{s\} = ac')[ac_0/ac'] \wedge ac_0 \subseteq ac'$

{Definition of **PBMH** (Lemma E.1.1)}

$= \mathbf{PBMH}(P \ ;_{\mathcal{A}} \{s\} = ac')$ {Definition of **A2**}

$= \mathbf{A2}(P)$

□

1.3 Reactive angelic processes

The healthiness condition **CSPA2** is the same as **H2** but with the alphabet that includes s, ac' and ok and ok'.

Definition 10

$$\mathbf{CSPA2}(P) \mathrel{\widehat{=}} \mathbf{H2}(P)$$

Definition 11 (Reactive angelic process)

$$\mathbf{RAP}(P) \mathrel{\widehat{=}} \mathbf{RA} \circ \mathbf{CSPA1} \circ \mathbf{CSPA2} \circ \mathbf{PBMH}(P)$$

The reactive angelic processes are the fixed points of **RAP**. They are **RA**, **CSPA1**, **CSPA2** and **PBMH**-healthy. Since **PBMH** and **RA1** do not commute, **PBMH** is applied first. Every such process P can be expressed as $\mathbf{RA} \circ \mathbf{A}(\neg\ P_f^f \vdash P_f^t)$ as shown by the following Theorem 1.3.1, where $P_w^o = P[o, s \oplus \{wait \mapsto w\}/s, ok']$. That is, such processes can be specified as the image of an **A**-healthy design through the function **RA**.

Theorem 1.3.1

$$\mathbf{RAP}(P) = \mathbf{RA} \circ \mathbf{A}(\neg\ P_f^f \vdash P_f^t)$$

Proof.

$$\begin{aligned}
&\mathbf{RAP}(P) && \{\text{Definition of } \mathbf{RAP}\}\\
&= \mathbf{RA3} \circ \mathbf{RA2} \circ \mathbf{RA1} \circ \mathbf{CSPA1} \circ \mathbf{CSPA2} \circ \mathbf{PBMH}(P) && \{\text{Theorem 1.2.32}\}\\
&= \mathbf{RA3} \circ \mathbf{RA2} \circ \mathbf{RA1} \circ \mathbf{H1} \circ \mathbf{CSPA2} \circ \mathbf{PBMH}(P) && \{\text{Definition of } \mathbf{CSPA2}\}\\
&= \mathbf{RA3} \circ \mathbf{RA2} \circ \mathbf{RA1} \circ \mathbf{H1} \circ \mathbf{H2} \circ \mathbf{PBMH}(P) && \{\text{Theorem 1.2.6}\}\\
&= \mathbf{RA3} \circ \mathbf{RA2} \circ \mathbf{RA1} \circ \mathbf{A0} \circ \mathbf{H1} \circ \mathbf{H2} \circ \mathbf{PBMH}(P) && \{\text{Theorem E.6.1}\}\\
&= \mathbf{RA3} \circ \mathbf{RA2} \circ \mathbf{RA1} \circ \mathbf{A0} \circ \mathbf{H1} \circ \mathbf{PBMH} \circ \mathbf{H2}(P) && \{\text{Theorem E.6.2}\}\\
&= \mathbf{RA3} \circ \mathbf{RA2} \circ \mathbf{RA1} \circ \mathbf{A0} \circ \mathbf{PBMH} \circ \mathbf{H1} \circ \mathbf{H2}(P) && \{\text{Property of designs}\}
\end{aligned}$$

$= \mathbf{RA3} \circ \mathbf{RA2} \circ \mathbf{RA1} \circ \mathbf{A0} \circ \mathbf{PBMH}(\neg\ P^f \vdash P^t)$ {Definition of **A**}

$= \mathbf{RA3} \circ \mathbf{RA2} \circ \mathbf{RA1} \circ \mathbf{A}(\neg\ P^f \vdash P^t)$ {Lemma 1.2.4}

$= \mathbf{RA1} \circ \mathbf{RA2} \circ \mathbf{RA3} \circ \mathbf{A}(\neg\ P^f \vdash P^t)$ {Lemma B.3.1}

$= \mathbf{RA1} \circ \mathbf{RA2} \circ \mathbf{RA3} \circ \mathbf{A}(\neg\ P^f \vdash P^t)[s \oplus \{wait \mapsto false\}/s]$ {Lemma A.1.1}

$= \mathbf{RA1} \circ \mathbf{RA2} \circ \mathbf{RA3} \circ \mathbf{A}((\neg\ P^f \vdash P^t)[s \oplus \{wait \mapsto false\}/s])$ {Substitution}

$= \mathbf{RA1} \circ \mathbf{RA2} \circ \mathbf{RA3} \circ \mathbf{A}(\neg\ P_f^f \vdash P_f^t)$ {Definition of **RA**}

$= \mathbf{RA} \circ \mathbf{A}(\neg\ P_f^f \vdash P_f^t)$

□

A predicate that is a fixed point of **RAP** can alternatively be expressed as shown in the following lemma.

Lemma 1.3.1

$$\mathbf{RAP}(P) = \mathbf{RA}(\neg\ \mathbf{PBMH}(P)_f^f \vdash \mathbf{PBMH}(P)_f^t)$$

Proof.

$\mathbf{RAP}(P)$ {Theorem 1.3.1}

$= \mathbf{RA} \circ \mathbf{A}(\neg\ P_f^f \vdash P_f^t)$ {Theorem 1.2.27}

$= \mathbf{RA} \circ \mathbf{PBMH}(\neg\ P_f^f \vdash P_f^t)$ {**PBMH** is **A1**}

$= \mathbf{RA}(\neg\ \mathbf{PBMH}(P_f^f) \vdash \mathbf{PBMH}(P_f^t))$ {Lemma E.5.1}

$= \mathbf{RA}(\neg\ \mathbf{PBMH}(P)_f^f \vdash \mathbf{PBMH}(P)_f^t)$

□

It is also possible to infer that if P is a reactive angelic process, then it is also **PBMH**-healthy.

Theorem 1.3.2 *Provided P is* **RAP***-healthy.*

$$\mathbf{PBMH}(P) = P$$

Proof.

$$
\begin{aligned}
&\mathbf{PBMH}(P) && \{\text{Assumption: } P \text{ is } \mathbf{RAP}\text{-healthy}\}\\
&= \mathbf{PBMH} \circ \mathbf{RAP}(P) && \{\text{Definition of } \mathbf{RAP}\}\\
&= \mathbf{PBMH} \circ \mathbf{RA} \circ \mathbf{A}(\neg\ P_f^f \vdash P_f^t) && \{\text{Theorem 1.2.27}\}\\
&= \mathbf{PBMH} \circ \mathbf{RA} \circ \mathbf{PBMH}(\neg\ P_f^f \vdash P_f^t) && \{\text{Theorem 1.2.28}\}\\
&= \mathbf{RA} \circ \mathbf{PBMH}(\neg\ P_f^f \vdash P_f^t) && \{\text{Theorem 1.2.27}\}\\
&= \mathbf{RA} \circ \mathbf{A}(\neg\ P_f^f \vdash P_f^t) && \{\text{Definition of } \mathbf{RAP}\}\\
&= \mathbf{RAP}(P) && \{\text{Assumption: } P \text{ is } \mathbf{RAP}\text{-healthy}\}\\
&= P
\end{aligned}
$$

□

This concludes our discussion regarding the healthiness conditions of the theory of reactive angelic processes.

1.4 Linking

The theories introduced in this report can be related with existing theories, such as the UTP theory for CSP, by introducing suitable linking functions. We introduce two functions that map between predicates with angelic nondeterminism and those without: $ac2p$ that maps from predicates with angelic nondeterminism to those without, and $p2ac$ mapping in the opposite direction.

1.4.1 From angelic predicates to non-angelic ($ac2p$)

The mapping from angelic predicates to non-angelic is defined by $ac2p$, whose goal is to collapse the set of final states ac' into a single state, and, introduce the input and output variables as used in other theories.

Definition 12 ($ac2p$)

$$
\begin{aligned}
&ac2p(P)\\
&\widehat{=}\\
&\mathbf{PBMH}(P)[State_{\mathit{II}}(in\alpha_{-ok})/s]\ \ ;_{\mathcal{A}} \bigwedge x : out\alpha_{-ok'} \bullet dash(s).x = x
\end{aligned}
$$

First, for a predicate P, $acp2$ enforces P to be upward-closed. This is followed by the substitution on s that introduces the corresponding input variables of the set $in\alpha_{-ok}$, which excludes ok. We observe that the variables ok and ok' are not affected by these substitutions as they retain exactly the same meaning in both theories. Finally, the resulting predicate is sequentially composed, using $;_{\mathcal{A}}$, with a predicate that introduces the corresponding output variables of the resulting final state, except for ok'.

This definition can be restated as shown in Lemmas C.1.1 and C.1.2. We considered whether the definition of $ac2p$ could be generalized by avoiding the enforcement of **PBMH**. In this case, it is possible to avoid the provisos for Theorems 1.4.6 and 1.4.7. However, when considering its application to **A**-designs, this makes proofs more complex by still requiring predicates to be upward-closed as a result of **A1**. Therefore, this definition is appropriate in the context of a theory where the set of final states is upward-closed.

Properties

Theorem 1.4.1 ($ac2p$-disjunction-distribute)

$$ac2p(P \vee Q) = ac2p(P) \vee ac2p(Q)$$

Proof.

$$
\begin{array}{ll}
ac2p(P \vee Q) & \{\text{Definition of } ac2p\} \\
= \mathbf{PBMH}(P \vee Q)[State_{\mathit{II}}(in\alpha_{-ok})/s] \;;_{\mathcal{A}} \bigwedge x : out\alpha_{-ok'} \bullet dash(s).x = x & \\
& \{\text{Distributivity of } \mathbf{PBMH} \text{ (Theorem E.2.2)}\} \\
= \left(\begin{array}{l} \mathbf{PBMH}(P) \\ \vee \\ \mathbf{PBMH}(Q) \end{array} \right) [State_{\mathit{II}}(in\alpha_{-ok})/s] \;;_{\mathcal{A}} \bigwedge x : out\alpha_{-ok'} \bullet dash(s).x = x & \\
& \{\text{Property of substitution}\} \\
= \left(\begin{array}{l} (\mathbf{PBMH}(P)[State_{\mathit{II}}(in\alpha_{-ok})/s] \vee \mathbf{PBMH}(Q)[State_{\mathit{II}}(in\alpha_{-ok})/s]) \\ \;;_{\mathcal{A}} \\ \bigwedge x : out\alpha_{-ok'} \bullet dash(s).x = x \end{array} \right) & \\
& \{\text{Distributivity of } ;_{\mathcal{A}} \text{ (Lemma F.1.4)}\} \\
= \left(\begin{array}{l} (\mathbf{PBMH}(P)[State_{\mathit{II}}(in\alpha_{-ok})/s] \;;_{\mathcal{A}} \bigwedge x : out\alpha_{-ok'} \bullet dash(s).x = x) \\ \vee \\ (\mathbf{PBMH}(Q)[State_{\mathit{II}}(in\alpha_{-ok})/s] \;;_{\mathcal{A}} \bigwedge x : out\alpha_{-ok'} \bullet dash(s).x = x) \end{array} \right) & \\
& \{\text{Definition of } ac2p\}
\end{array}
$$

$= ac2p(P) \vee ac2p(Q)$

□

Theorem 1.4.2 ($ac2p$-conjunction-distribute) *Provided P and Q are* **PBMH***-healthy.*

$$ac2p(P \wedge Q) = ac2p(P) \wedge ac2p(Q)$$

Proof.

$ac2p(P \wedge Q)$ {Definition of $ac2p$}

$= \mathbf{PBMH}(P \wedge Q)[State_{\mathtt{II}}(in\alpha_{-ok})/s] \ ;_{\mathcal{A}} \bigwedge x : out\alpha_{-ok'} \bullet dash(s).x = x$

{Assumption: P and Q are **PBMH**-healthy and Lemma E.3.1}

$$= \left(\begin{array}{l} \mathbf{PBMH}(P) \\ \wedge \\ \mathbf{PBMH}(Q) \end{array} \right) [State_{\mathtt{II}}(in\alpha_{-ok})/s] \ ;_{\mathcal{A}} \bigwedge x : out\alpha_{-ok'} \bullet dash(s).x = x$$

{Property of substitution}

$$= \left(\begin{array}{l} \mathbf{PBMH}(P)[State_{\mathtt{II}}(in\alpha_{-ok})/s] \\ \wedge \\ \mathbf{PBMH}(Q)[State_{\mathtt{II}}(in\alpha_{-ok})/s] \end{array} \right) \ ;_{\mathcal{A}} \bigwedge x : out\alpha_{-ok'} \bullet dash(s).x = x$$

{Distributivity of $;_{\mathcal{A}}$ (Lemma F.1.5)}

$$= \left(\begin{array}{l} (\mathbf{PBMH}(P)[State_{\mathtt{II}}(in\alpha_{-ok})/s] \ ;_{\mathcal{A}} \bigwedge x : out\alpha_{-ok'} \bullet dash(s).x = x) \\ \wedge \\ (\mathbf{PBMH}(Q)[State_{\mathtt{II}}(in\alpha_{-ok})/s] \ ;_{\mathcal{A}} \bigwedge x : out\alpha_{-ok'} \bullet dash(s).x = x) \end{array} \right)$$

{Definition of $ac2p$}

$= ac2p(P) \wedge ac2p(Q)$

□

1.4.2 From non-angelic predicates to angelic ones ($p2ac$)

The function mapping in the opposite direction to $ac2p$ is $p2ac$. Its definition is presented below.

Definition 13 ($p2ac$)

$$p2ac(P) \mathrel{\widehat{=}} \exists\, z \bullet P[\mathbf{s}, \mathbf{z}/in\alpha_{-ok}, out\alpha_{-ok'}] \wedge undash(z) \in ac'$$

Properties

Theorem 1.4.3

$$p2ac(P \wedge Q) \Rightarrow p2ac(P) \wedge p2ac(Q)$$

Proof.

$$
\begin{array}{ll}
p2ac(P \wedge Q) & \{\text{Definition of } p2ac\} \\
= \exists\, z \bullet (P \wedge Q)[\mathbf{s}, \mathbf{z}/in\alpha_{-ok}, out\alpha_{-ok'}] \wedge undash(z) \in ac' & \\
& \{\text{Property of substitution}\} \\
= \exists\, z \bullet (P[\mathbf{s}, \mathbf{z}/in\alpha_{-ok}, out\alpha_{-ok'}] \wedge Q[\mathbf{s}, \mathbf{z}/in\alpha_{-ok}, out\alpha_{-ok'}]) \wedge undash(z) \in ac' & \\
& \{\text{Predicate calculus}\} \\
= \exists\, z \bullet \left(\begin{array}{l} (P[\mathbf{s}, \mathbf{z}/in\alpha_{-ok}, out\alpha_{-ok'}] \wedge undash(z) \in ac') \\ \wedge \\ (Q[\mathbf{s}, \mathbf{z}/in\alpha_{-ok}, out\alpha_{-ok'}] \wedge undash(z) \in ac') \end{array} \right) & \\
& \{\text{Predicate calculus}\} \\
\Rightarrow \left(\begin{array}{l} (\exists\, z \bullet P[\mathbf{s}, \mathbf{z}/in\alpha_{-ok}, out\alpha_{-ok'}] \wedge undash(z) \in ac') \\ \wedge \\ (\exists\, z \bullet Q[\mathbf{s}, \mathbf{z}/in\alpha_{-ok}, out\alpha_{-ok'}] \wedge undash(z) \in ac') \end{array} \right) & \\
& \{\text{Definition of } p2ac\} \\
= p2ac(P) \wedge p2ac(Q) &
\end{array}
$$

□

Theorem 1.4.4

$$p2ac(P \vee Q) = p2ac(P) \vee p2ac(Q)$$

Proof.

$$
\begin{array}{ll}
p2ac(P \vee Q) & \{\text{Definition of } p2ac\} \\
= \exists\, z \bullet (P \vee Q)[\mathbf{s}, \mathbf{z}/in\alpha_{-ok}, out\alpha_{-ok'}] \wedge undash(z) \in ac' & \\
& \{\text{Property of substitution}\} \\
= \exists\, z \bullet (P[\mathbf{s}, \mathbf{z}/in\alpha_{-ok}, out\alpha_{-ok'}] \vee Q[\mathbf{s}, \mathbf{z}/in\alpha_{-ok}, out\alpha_{-ok'}]) \wedge undash(z) \in ac' & \\
& \{\text{Predicate calculus}\} \\
= \exists\, z \bullet \left(\begin{array}{l} (P[\mathbf{s}, \mathbf{z}/in\alpha_{-ok}, out\alpha_{-ok'}] \wedge undash(z) \in ac') \\ \vee \\ (Q[\mathbf{s}, \mathbf{z}/in\alpha_{-ok}, out\alpha_{-ok'}] \wedge undash(z) \in ac') \end{array} \right) & \\
& \{\text{Predicate calculus}\}
\end{array}
$$

$$= \left(\begin{array}{l} (\exists\, z \bullet P[\mathbf{s},\mathbf{z}/in\alpha_{-ok}, out\alpha_{-ok'}] \land undash(z) \in ac') \\ \lor \\ (\exists\, z \bullet Q[\mathbf{s},\mathbf{z}/in\alpha_{-ok}, out\alpha_{-ok'}] \land undash(z) \in ac') \end{array} \right)$$

{Definition of $p2ac$}

$$= p2ac(P) \lor p2ac(Q)$$

□

Lemma 1.4.1 *Provided c is a condition.*

$$p2ac(P \lhd c \rhd Q) = p2ac(P) \lhd s.c \rhd p2ac(Q)$$

Proof.

$p2ac(P \lhd c \rhd Q)$ {Definition of $p2ac$}

$= \exists\, z \bullet (P \lhd c \rhd Q)[\mathbf{s},\mathbf{z}/in\alpha_{ok}, out\alpha_{ok'}] \land undash(z) \in ac'$

{Substitution: c is a condition}

$= \exists\, z \bullet (P[\mathbf{s},\mathbf{z}/in\alpha_{ok}, out\alpha_{ok'}] \lhd s.c \rhd Q[\mathbf{s},\mathbf{z}/in\alpha_{ok}, out\alpha_{ok'}]) \land undash(z) \in ac'$

{Predicate calculus}

$$= \left(\begin{array}{l} (\exists\, z \bullet P[\mathbf{s},\mathbf{z}/in\alpha_{ok}, out\alpha_{ok'}] \land undash(z) \in ac') \\ \lhd s.c \rhd \\ (\exists\, z \bullet Q[\mathbf{s},\mathbf{z}/in\alpha_{ok}, out\alpha_{ok'}] \land undash(z) \in ac') \end{array} \right)$$

{Definition of $p2ac$}

$$= p2ac(P) \lhd s.c \rhd p2ac(Q)$$

□

1.4.3 Linking results of $ac2p$

Results with respect to RA

Theorem 1.4.5

$$ac2p \circ \mathbf{RA} \circ \mathbf{A}(\neg\, P_f^f \vdash P_f^t) = \mathbf{R}(\neg\, ac2p(P_f^f) \vdash ac2p(P_f^t))$$

Proof.

$ac2p \circ \mathbf{RA} \circ \mathbf{A}(\neg\, P_f^f \vdash P_f^t)$ {Theorem 1.2.27}

$= ac2p \circ \mathbf{RA} \circ \mathbf{PBMH}(\neg\, P_f^f \vdash P_f^t)$ {Definition of **RA**}

$$
\begin{array}{ll}
= ac2p \circ \mathbf{RA3} \circ \mathbf{RA2} \circ \mathbf{RA1} \circ \mathbf{PBMH}(\neg\ P_f^f \vdash P_f^t) & \\
\qquad \{\text{Theorems 1.2.5, 1.2.11 and 1.4.8}\} & \\
= \mathbf{R3} \circ ac2p \circ \mathbf{RA2} \circ \mathbf{RA1} \circ \mathbf{PBMH}(\neg\ P_f^f \vdash P_f^t) & \{\text{Theorem 1.2.12}\} \\
= \mathbf{R3} \circ ac2p \circ \mathbf{RA1} \circ \mathbf{RA2} \circ \mathbf{PBMH}(\neg\ P_f^f \vdash P_f^t) & \\
\qquad \{\text{Theorems 1.2.5, 1.2.11 and 1.4.7}\} & \\
= \mathbf{R3} \circ \mathbf{R1} \circ \mathbf{R2} \circ ac2p \circ \mathbf{PBMH}(\neg\ P_f^f \vdash P_f^t) & \{\text{Definition of } \mathbf{R}\} \\
= \mathbf{R} \circ ac2p \circ \mathbf{PBMH}(\neg\ P_f^f \vdash P_f^t) & \{\text{Lemma 2.1.2}\} \\
= \mathbf{R} \circ ac2p(\neg\ P_f^f \vdash P_f^t) & \{\text{Lemma C.1.10}\} \\
= \mathbf{R}(\neg\ ac2p(P_f^f) \vdash ac2p(P_f^t)) &
\end{array}
$$

□

Theorem 1.4.6 *Provided P is* **PBMH***-healthy.*

$$ac2p \circ \mathbf{RA1}(P) = \mathbf{R1} \circ ac2p(P)$$

Proof.

$$
\begin{array}{ll}
ac2p \circ \mathbf{RA1}(P) & \{\text{Definition of } ac2p\} \\
= \mathbf{PBMH}(\mathbf{RA1}(P))[State_{\mathtt{II}}(in\alpha_{-ok})/s]\ ;_{\mathcal{A}} \bigwedge x : out\alpha_{-ok'} \bullet dash(s).x = x & \\
\qquad \{\text{Assumption: } P \text{ is } \mathbf{PBMH}\text{-healthy and Theorem 1.2.5}\} & \\
= \mathbf{RA1}(P)[State_{\mathtt{II}}(in\alpha_{-ok})/s]\ ;_{\mathcal{A}} \bigwedge x : out\alpha_{-ok'} \bullet dash(s).x = x & \\
\qquad \{\text{Definition of } \mathbf{RA1} \text{ (Lemma 1.2.1)}\} & \\
= \left(\begin{array}{l} \left(\begin{array}{l} P[\{z \mid z \in ac' \wedge s.tr \leq z.tr\}/ac'] \\ \wedge \\ \exists\, z \bullet s.tr \leq z.tr \wedge z \in ac' \end{array} \right)[State_{\mathtt{II}}(in\alpha_{-ok})/s] \\ ;_{\mathcal{A}} \\ \bigwedge x : out\alpha_{-ok'} \bullet dash(s).x = x \end{array} \right) & \\
\qquad \{\text{Substitution}\} & \\
= \left(\begin{array}{l} \left(\begin{array}{l} P[State_{\mathtt{II}}(in\alpha_{-ok})/s][\{z \mid z \in ac' \wedge tr \leq z.tr\}/ac'] \\ \wedge \\ \exists\, z \bullet tr \leq z.tr \wedge z \in ac' \end{array} \right) \\ ;_{\mathcal{A}} \\ \bigwedge x : out\alpha_{-ok'} \bullet dash(s).x = x \end{array} \right) & \\
\qquad \{\text{Definition of } ;_{\mathcal{A}} \text{ and substitution}\} &
\end{array}
$$

$$
= \left(\begin{array}{l} P[State_{\mathit{II}}(in\alpha_{-ok})/s][\{z \mid z \in \{s \mid \bigwedge x : out\alpha_{-ok'} \bullet dash(s).x = x\} \wedge tr \leq z.tr\}/ac'] \\ \wedge \\ \exists\, z \bullet tr \leq z.tr \wedge z \in \{s \mid \bigwedge x : out\alpha_{-ok'} \bullet dash(s).x = x\} \end{array} \right)
$$

{Property of sets}

$$
= \left(\begin{array}{l} P[State_{\mathit{II}}(in\alpha_{-ok})/s][\{z \mid \bigwedge x : out\alpha_{-ok'} \bullet dash(z).x = x \wedge tr \leq z.tr\}/ac'] \\ \wedge \\ \exists\, z \bullet tr \leq z.tr \wedge (\bigwedge x : out\alpha_{-ok'} \bullet dash(z).x = x) \end{array} \right)
$$

{Property of $dash$}

$$
= \left(\begin{array}{l} P[State_{\mathit{II}}(in\alpha_{-ok})/s][\{z \mid \bigwedge x : out\alpha_{-ok'} \bullet dash(z).x = x \wedge tr \leq dash(z).tr'\}/ac'] \\ \wedge \\ \exists\, z \bullet tr \leq dash(z).tr' \wedge (\bigwedge x : out\alpha_{-ok'} \bullet dash(z).x = x) \end{array} \right)
$$

{Transitivity of equality on $dash(z).tr' = tr'$}

$$
= \left(\begin{array}{l} P[State_{\mathit{II}}(in\alpha_{-ok})/s][\{z \mid \bigwedge x : out\alpha_{-ok'} \bullet dash(z).x = x \wedge tr \leq tr'\}/ac'] \\ \wedge \\ \exists\, z \bullet tr \leq tr' \wedge (\bigwedge x : out\alpha_{-ok'} \bullet dash(z).x = x) \end{array} \right)
$$

{One-point rule}

$$
= \left(\begin{array}{l} P[State_{\mathit{II}}(in\alpha_{-ok})/s][\{z \mid \bigwedge x : out\alpha_{-ok'} \bullet dash(z).x = x \wedge tr \leq tr'\}/ac'] \\ \wedge \\ tr \leq tr' \end{array} \right)
$$

{Definition of $;_{\mathcal{A}}$}

$$
= \left(\begin{array}{l} P[State_{\mathit{II}}(in\alpha_{-ok})/s] \;;_{\mathcal{A}} (\bigwedge x : out\alpha_{-ok'} \bullet dash(s).x = x \wedge tr \leq tr') \\ \wedge \\ tr \leq tr' \end{array} \right)
$$

{Assumption: P is **PBMH**-healthy and Lemma F.2.6}

$$
= \left(\begin{array}{l} (\mathbf{PBMH}(P)[State_{\mathit{II}}(in\alpha_{-ok})/s] \;;_{\mathcal{A}} (\bigwedge x : out\alpha_{-ok'} \bullet dash(s).x = x)) \\ \wedge \\ tr \leq tr' \end{array} \right)
$$

{Definition of $ac2p$}

$$
= ac2p(P) \wedge tr \leq tr'
$$

{Definition of **R1**}

$$
= \mathbf{R1} \circ ac2p(P)
$$

□

Instead of relying on the caveat of $tr \leq tr'$ for **R2**, we can produce a result for $\mathbf{R1} \circ \mathbf{R2}$ directly that poses no such problem.

Theorem 1.4.7 *Provided P is* **PBMH***-healthy.*

$$ac2p \circ \mathbf{RA1} \circ \mathbf{RA2}(P) = \mathbf{R1} \circ \mathbf{R2} \circ ac2p(P)$$

Proof.

$$
\begin{array}{ll}
& ac2p \circ \mathbf{RA1} \circ \mathbf{RA2}(P) \qquad \{\text{Definition of } ac2p\} \\
= & \mathbf{PBMH}(\mathbf{RA1} \circ \mathbf{RA2}(P))[State_{\mathtt{II}}(in\alpha_{-ok})/s] \ ;_{\mathcal{A}} \bigwedge x : out\alpha_{-ok'} \bullet dash(s).x = x \\
& \qquad \{\text{Assumption: } P \text{ is } \mathbf{PBMH}\text{-healthy and Theorems 1.2.5 and 1.2.11}\} \\
= & (\mathbf{RA1} \circ \mathbf{RA2}(P))[State_{\mathtt{II}}(in\alpha_{-ok})/s] \ ;_{\mathcal{A}} \bigwedge x : out\alpha_{-ok'} \bullet dash(s).x = x \\
& \qquad \{\text{Lemma B.1.18 and definition of } \mathbf{RA2}\} \\
= & \left(\begin{array}{l} \left(\begin{array}{l} P[s \oplus \{tr \mapsto \langle\rangle\}/s] \left[\left\{ z \;\middle|\; \begin{array}{l} z \in ac' \wedge s.tr \leq z.tr \\ \bullet\ z \oplus \{tr \mapsto z.tr - s.tr\} \end{array} \right\} / ac' \right] \\ \wedge \\ \exists\, z \bullet z \in ac' \wedge s.tr \leq z.tr \end{array} \right) [State_{\mathtt{II}}(in\alpha_{-ok})/s] \\ ;_{\mathcal{A}} \\ \bigwedge x : out\alpha_{-ok'} \bullet dash(s).x = x \end{array} \right) \\
& \qquad \{\text{Substitution}\} \\
= & \left(\begin{array}{l} \left(\begin{array}{l} P[(State_{\mathtt{II}}(in\alpha)) \oplus \{tr \mapsto \langle\rangle\}/s] \\ \left[\left\{ z \;\middle|\; \begin{array}{l} z \in ac' \wedge (State_{\mathtt{II}}(in\alpha_{-ok})).tr \leq z.tr \\ \bullet\ z \oplus \{tr \mapsto z.tr - (State_{\mathtt{II}}(in\alpha_{-ok})).tr\} \end{array} \right\} / ac' \right] \\ \wedge \\ \exists\, z \bullet z \in ac' \wedge (State_{\mathtt{II}}(in\alpha_{-ok})).tr \leq z.tr \end{array} \right) \\ ;_{\mathcal{A}} \\ \bigwedge x : out\alpha_{-ok'} \bullet dash(s).x = x \end{array} \right) \\
& \qquad \{\text{Property of } State_{\mathtt{II}} \text{ and substitution}\} \\
= & \left(\begin{array}{l} \left(\begin{array}{l} P[(State_{\mathtt{II}}(in\alpha_{-ok})) \oplus \{tr \mapsto \langle\rangle\}/s] \left[\left\{ z \;\middle|\; \begin{array}{l} z \in ac' \wedge tr \leq z.tr \\ \bullet\ z \oplus \{tr \mapsto z.tr - tr\} \end{array} \right\} / ac' \right] \\ \wedge \\ \exists\, z \bullet z \in ac' \wedge tr \leq z.tr \end{array} \right) \\ ;_{\mathcal{A}} \\ \bigwedge x : out\alpha_{-ok'} \bullet dash(s).x = x \end{array} \right) \\
& \qquad \{\text{Property of sets}\}
\end{array}
$$

$$= \left(\begin{array}{l} \left(\begin{array}{l} P[(State_{\mathtt{II}}(in\alpha_{-ok})) \oplus \{tr \mapsto \langle\rangle\}/s] \\ \left[\left\{ y \,\middle|\, y \in \left\{ z \,\middle|\, \begin{array}{l} z \in ac' \wedge tr \leq z.tr \\ \bullet\ z \oplus \{tr \mapsto z.tr - tr\} \end{array} \right\} \right\} /ac' \right] \\ \wedge \\ \exists\, z \bullet z \in ac' \wedge tr \leq z.tr \end{array} \right) \\ ;_{\mathcal{A}} \\ \bigwedge x : out\alpha_{-ok'} \bullet dash(s).x = x \end{array} \right)$$

{Property of sets}

$$= \left(\begin{array}{l} \left(\begin{array}{l} P[(State_{\mathtt{II}}(in\alpha)) \oplus \{tr \mapsto \langle\rangle\}/s] \\ [\{y \mid \exists\, z \bullet z \in ac' \wedge tr \leq z.tr \wedge y = z \oplus \{tr \mapsto z.tr - tr\}\}/ac'] \\ \wedge \\ \exists\, z \bullet z \in ac' \wedge tr \leq z.tr \end{array} \right) \\ ;_{\mathcal{A}} \\ \bigwedge x : out\alpha \bullet dash(s).x = x \end{array} \right)$$

{Lemma B.1.3}

$$= \left(\begin{array}{l} \left(\begin{array}{l} P[(State_{\mathtt{II}}(in\alpha_{-ok})) \oplus \{tr \mapsto \langle\rangle\}/s] \\ [\{y \mid y \oplus \{tr \mapsto tr \frown y.tr\} \in ac'\}/ac'] \\ \wedge \\ \exists\, z \bullet z \in ac' \wedge tr \leq z.tr \end{array} \right) \\ ;_{\mathcal{A}} \\ \bigwedge x : out\alpha_{-ok'} \bullet dash(s).x = x \end{array} \right)$$

{Definition of $;_{\mathcal{A}}$ and substitution}

$$= \left(\begin{array}{l} P[(State_{\mathtt{II}}(in\alpha_{-ok})) \oplus \{tr \mapsto \langle\rangle\}/s] \\ [\{y \mid y \oplus \{tr \mapsto tr \frown y.tr\} \in \{s \mid \bigwedge x : out\alpha_{-ok'} \bullet dash(s).x = x\}\}/ac'] \\ \wedge \\ \exists\, z \bullet z \in \{s \mid \bigwedge x : out\alpha_{-ok'} \bullet dash(s).x = x\} \wedge tr \leq z.tr \end{array} \right)$$

{Property of sets}

$$= \left(\begin{array}{l} P[(State_{\mathtt{II}}(in\alpha_{-ok})) \oplus \{tr \mapsto \langle\rangle\}/s] \\ [\{y \mid \bigwedge x : out\alpha_{-ok'} \bullet dash(y \oplus \{tr \mapsto tr \frown y.tr\}).x = x\}/ac'] \\ \wedge \\ \exists\, z \bullet \bigwedge x : out\alpha_{-ok'} \bullet dash(z).x = x \wedge tr \leq z.tr \end{array} \right)$$

{Property of $\oplus$}

$$= \left(\begin{array}{l} P[(State_{\mathtt{II}}(in\alpha_{-ok})) \oplus \{tr \mapsto \langle\rangle\}/s] \\ [\{y \mid \bigwedge x : out\alpha_{-ok'} \bullet dash(\{tr\} \lhd y).x = x \wedge dash(\{tr \mapsto tr \frown y.tr\}).tr' = tr'\}/ac'] \\ \wedge \\ \exists\, z \bullet \bigwedge x : out\alpha_{-ok'} \bullet dash(z).x = x \wedge tr \leq z.tr \end{array} \right)$$

{Property of $dash$}

$$= \left(\begin{array}{l} P[(State_{\mathtt{II}}(in\alpha_{-ok})) \oplus \{tr \mapsto \langle\rangle\}/s] \\ [\{y \mid \bigwedge x : out\alpha_{-ok'} \bullet dash(\{tr\} \lhd y).x = x \wedge (\{tr' \mapsto tr \frown y.tr\}).tr' = tr'\}/ac'] \\ \wedge \\ \exists\, z \bullet \bigwedge x : out\alpha_{-ok'} \bullet dash(z).x = x \wedge tr \leq dash(z).tr' \end{array} \right)$$

{Value of record component tr'}

$$= \left(\begin{array}{l} P[(State_{\mathtt{II}}(in\alpha_{-ok})) \oplus \{tr \mapsto \langle\rangle\}/s] \\ [\{y \mid \bigwedge x : out\alpha_{-ok'} \bullet dash(\{tr\} \lhd y).x = x \wedge tr \frown y.tr = tr'\}/ac'] \\ \wedge \\ \exists\, z \bullet \bigwedge x : out\alpha_{-ok'} \bullet dash(z).x = x \wedge tr \leq dash(z).tr' \end{array} \right)$$

{Property of sequences}

$$= \left(\begin{array}{l} P[(State_{\mathtt{II}}(in\alpha_{-ok})) \oplus \{tr \mapsto \langle\rangle\}/s] \\ [\{y \mid \bigwedge x : out\alpha_{-ok'} \bullet dash(\{tr\} \lhd y).x = x \wedge tr' - tr = y.tr \wedge tr \leq tr'\}/ac'] \\ \wedge \\ \exists\, z \bullet \bigwedge x : out\alpha_{-ok'} \bullet dash(z).x = x \wedge tr \leq dash(z).tr' \end{array} \right)$$

{Property of $dash$}

$$= \left(\begin{array}{l} P[(State_{\mathtt{II}}(in\alpha_{-ok})) \oplus \{tr \mapsto \langle\rangle\}/s] \\ [\{y \mid \bigwedge x : out\alpha_{-ok'} \bullet dash(\{tr\} \lhd y).x = x \wedge tr' - tr = dash(y).tr' \wedge tr \leq tr'\}/ac'] \\ \wedge \\ \exists\, z \bullet \bigwedge x : out\alpha_{-ok'} \bullet dash(z).x = x \wedge tr \leq dash(z).tr' \end{array} \right)$$

{Transitivity of equality on $tr' \in out\alpha_{-ok'}$}

$$= \left(\begin{array}{l} P[(State_{\mathtt{II}}(in\alpha_{-ok})) \oplus \{tr \mapsto \langle\rangle\}/s] \\ [\{y \mid \bigwedge x : out\alpha_{-ok'} \bullet dash(\{tr\} \lhd y).x = x \wedge tr' - tr = dash(y).tr' \wedge tr \leq tr'\}/ac'] \\ \wedge \\ \exists\, z \bullet \bigwedge x : out\alpha_{-ok'} \bullet dash(z).x = x \wedge tr \leq tr' \end{array} \right)$$

{One-point rule}

$$= \left(\begin{array}{l} P[(State_{\mathtt{II}}(in\alpha_{-ok})) \oplus \{tr \mapsto \langle\rangle\}/s] \\ [\{y \mid \bigwedge x : out\alpha_{-ok'} \bullet dash(\{tr\} \lhd y).x = x \wedge tr' - tr = dash(y).tr' \wedge tr \leq tr'\}/ac'] \\ \wedge \\ tr \leq tr' \end{array} \right)$$

{Assumption: P is **PBMH**-healthy and Lemma F.2.6}

$$= \left(\begin{array}{l} P[(State_{\mathtt{II}}(in\alpha_{-ok})) \oplus \{tr \mapsto \langle\rangle\}/s] \\ [\{y \mid \bigwedge x : out\alpha_{-ok'} \bullet dash(\{tr\} \lhd y).x = x \wedge tr' - tr = dash(y).tr'\}/ac'] \\ \wedge \\ tr \leq tr' \end{array} \right)$$

{Substitution}

$$= \left(\begin{array}{l} P[(State_{\mathtt{II}}(in\alpha_{-ok})) \oplus \{tr \mapsto \langle\rangle\}/s] \\ [\{y \mid \bigwedge x : out\alpha_{-ok'} \bullet dash(\{tr\} \lhd y).x = x \wedge tr' = dash(y).tr'\}/ac'] \, [tr' - tr/tr'] \\ \wedge \\ tr \leq tr' \end{array} \right)$$

{Property of $\lhd$}

$$= \left(\begin{array}{l} P[(State_{\mathtt{II}}(in\alpha_{-ok})) \oplus \{tr \mapsto \langle\rangle\}/s] \\ [\{y \mid \bigwedge x : out\alpha_{-ok'} \bullet dash(y).x = x\}/ac'] \, [tr' - tr/tr'] \\ \wedge \\ tr \leq tr' \end{array} \right)$$

{Property of $State_{\mathtt{II}}$ and substitution}

$$= \left(\begin{array}{l} P[State_{\mathtt{II}}(in\alpha_{-ok})/s][\langle\rangle/tr] \\ [\{y \mid \bigwedge x : out\alpha_{-ok'} \bullet dash(y).x = x\}/ac'] \, [tr' - tr/tr'] \\ \wedge \\ tr \leq tr' \end{array} \right)$$

{Property of substitution: tr not free in set comprehension}

$$= \left(\begin{array}{l} P[State_{\mathtt{II}}(in\alpha_{-ok})/s][\{y \mid \bigwedge x : out\alpha_{-ok'} \bullet dash(y).x = x\}/ac'][\langle\rangle, tr' - tr/tr, tr'] \\ \wedge \\ tr \leq tr' \end{array} \right)$$

{Definition of $;_{\mathcal{A}}$}

$$= \left(\begin{array}{l} (P[State_{\mathtt{II}}(in\alpha_{-ok})/s] \;;_{\mathcal{A}} \bigwedge x : out\alpha_{-ok'} \bullet dash(s).x = x)[\langle\rangle, tr' - tr/tr, tr'] \\ \wedge \\ tr \leq tr' \end{array} \right)$$

{Assumption: P is **PBMH** and definition of $ac2p$}

$= ac2p(P)[\langle\rangle, tr' - tr/tr, tr'] \wedge tr \leq tr'$ {Definition of **R2** and **R1**}

$= \mathbf{R1} \circ \mathbf{R2} \circ ac2p(P)$

□

Theorem 1.4.8

$$ac2p \circ \mathbf{RA3}(P) = \mathbf{R3} \circ ac2p(P)$$

Proof.

$ac2p \circ \mathbf{RA3}(P)$ {Definition of **RA3**}
$= ac2p(\mathit{II}_{\mathcal{R}ac} \lhd s.wait \rhd P)$ {Lemma C.1.14}
$= ac2p(\mathit{II}_{\mathcal{R}ac}) \lhd s.wait[State_{II}(in\alpha_{-ok})/s] \rhd ac2p(P)$
{Definition of $State_{II}$ and substitution}
$= ac2p(\mathit{II}_{\mathcal{R}ac}) \lhd wait \rhd ac2p(P)$ {Theorem 1.4.9}
$= \mathit{II}_{rea} \lhd wait \rhd ac2p(P)$ {Definition of **R3**}
$= \mathbf{R3} \circ ac2p(P)$

□

Theorem 1.4.9 *Provided* $out\alpha = \{tr', ref', wait'\}$

$$ac2p(\mathit{II}_{\mathcal{R}ac}) = \mathit{II}_{rea}$$

Proof.

$ac2p(\mathit{II}_{\mathcal{R}ac})$ {Definition of $\mathit{II}_{\mathcal{R}ac}$}
$= ac2p(\mathbf{RA1}(\neg\ ok) \vee (ok' \wedge s \in ac'))$
{Distributivity of $ac2p$ (Theorem 1.4.1)}
$= ac2p \circ \mathbf{RA1}(\neg\ ok) \vee ac2p(ok' \wedge s \in ac')$
{$\neg\ ok$ is **PBMH**-healthy and Theorem 1.4.6}
$= \mathbf{R1} \circ ac2p(\neg\ ok) \vee ac2p(ok' \wedge s \in ac')$ {Lemma C.1.9}
$= \mathbf{R1}(\neg\ ok) \vee ac2p(ok' \wedge s \in ac')$ {Lemma C.1.8}
$= \mathbf{R1}(\neg\ ok) \vee (ok' \wedge ac2p(s \in ac'))$
{Assumption: $in\alpha_{-ok} = \{tr, ref, wait\}$ and Lemma C.1.16}
$= \mathbf{R1}(\neg\ ok) \vee (ok' \wedge tr' = tr \wedge ref' = ref \wedge wait' = wait)$
{Definition of II_{rea}}
$= \mathit{II}_{rea}$

□

1.4.4 Linking results of $p2ac$

Results with respect to R

Theorem 1.4.10

$$p2ac \circ \mathbf{R}(P) = \mathbf{RA} \circ p2ac(P)$$

Proof.

$$
\begin{aligned}
& p2ac \circ \mathbf{R}(P) && \{\text{Definition of } \mathbf{R}\} \\
&= p2ac \circ \mathbf{R3} \circ \mathbf{R1} \circ \mathbf{R2}(P) && \{\text{Theorem 1.4.17}\} \\
&= \mathbf{RA3} \circ p2ac \circ \mathbf{R1} \circ \mathbf{R2}(P) && \{\mathbf{R1}\text{-idempotent}\} \\
&= \mathbf{RA3} \circ p2ac \circ \mathbf{R1} \circ \mathbf{R1} \circ \mathbf{R2}(P) && \{\text{Theorem 1.4.15}\} \\
&= \mathbf{RA3} \circ \mathbf{RA1} \circ p2ac \circ \mathbf{R1} \circ \mathbf{R2}(P) && \{\text{Theorem 1.4.16}\} \\
&= \mathbf{RA3} \circ \mathbf{RA1} \circ \mathbf{RA2} \circ p2ac(P) && \{\text{Theorem 1.2.12}\} \\
&= \mathbf{RA3} \circ \mathbf{RA2} \circ \mathbf{RA1} \circ p2ac(P) && \{\text{Definition of } \mathbf{RA}\} \\
&= \mathbf{RA} \circ p2ac(P)
\end{aligned}
$$

□

Theorem 1.4.11

$$p2ac \circ \mathbf{R}(\neg\ P^f \vdash P^t) = \mathbf{RA}(\neg\ p2ac(P^f) \vdash p2ac(P^t))$$

Proof.

$$
\begin{aligned}
& p2ac \circ \mathbf{R}(\neg\ P^f \vdash P^t) && \{\text{Theorem 1.4.10}\} \\
&= \mathbf{RA} \circ p2ac(\neg\ P^f \vdash P^t) && \{\text{Definition of } \mathbf{RA}\} \\
&= \mathbf{RA3} \circ \mathbf{RA2} \circ \mathbf{RA1} \circ p2ac(\neg\ P^f \vdash P^t) && \{\text{Definition of } \mathbf{RA1}\} \\
&= \mathbf{RA3} \circ \mathbf{RA2}((p2ac(\neg\ P^f \vdash P^t) \wedge ac' \neq \emptyset)[States_{tr \leq tr'}(s) \cap ac'/ac']) \\
& && \{\text{Theorem 2.1.2}\} \\
&= \mathbf{RA3} \circ \mathbf{RA2}((\neg\ p2ac(P^f) \vdash p2ac(P^t)) \wedge ac' \neq \emptyset)[States_{tr \leq tr'}(s) \cap ac'/ac']) \\
& && \{\text{Definition of } \mathbf{RA1}\} \\
&= \mathbf{RA3} \circ \mathbf{RA2} \circ \mathbf{RA1}(\neg\ p2ac(P^f) \vdash p2ac(P^t)) && \{\text{Definition of } \mathbf{RA}\} \\
&= \mathbf{RA}(\neg\ p2ac(P^f) \vdash p2ac(P^t))
\end{aligned}
$$

□

Theorem 1.4.12

$$p2ac \circ \mathbf{R}(\neg\ P_f^f \vdash P_f^t) = \mathbf{RA} \circ \mathbf{A}(\neg\ p2ac(P_f^f) \vdash p2ac(P_f^t))$$

Proof.

$$
\begin{aligned}
& p2ac \circ \mathbf{R}(\neg\ P_f^f \vdash P_f^t) && \{\text{Theorem 1.4.11}\} \\
&= \mathbf{RA}(\neg\ p2ac(P_f^f) \vdash p2ac(P_f^t)) && \{\text{Lemma C.2.1}\} \\
&= \mathbf{RA}(\neg\ \mathbf{PBMH} \circ p2ac(P_f^f) \vdash \mathbf{PBMH} \circ p2ac(P_f^t)) && \{\text{Lemma E.6.2}\} \\
&= \mathbf{RA} \circ \mathbf{PBMH}(\neg\ p2ac(P_f^f) \vdash p2ac(P_f^t)) && \{\text{Theorem 1.2.27}\} \\
&= \mathbf{RA} \circ \mathbf{A}(\neg\ p2ac(P_f^f) \vdash p2ac(P_f^t))
\end{aligned}
$$

□

Theorem 1.4.13

$$
\begin{aligned}
& p2ac \circ \mathbf{R}(\neg\ P^f \vdash P^t) \\
&= \\
& \mathbf{RA} \circ \mathbf{A}(\neg\ p2ac(P^f) \wedge (\neg\ P^f[\mathbf{s}/in\alpha]\ ;\ true) \vdash p2ac(P^t))
\end{aligned}
$$

Proof.

$$
\begin{aligned}
& p2ac \circ \mathbf{R}(\neg\ P^f \vdash P^t) && \{\text{Theorem 1.4.14}\} \\
&= \mathbf{RA}(\neg\ p2ac(P^f) \wedge (\neg\ P^f[\mathbf{s}/in\alpha]\ ;\ true) \vdash p2ac(P^t)) \\
& && \{\text{Predicate calculus}\} \\
&= \mathbf{RA}(\neg\ (p2ac(P^f) \vee \neg\ (\neg\ P^f[\mathbf{s}/in\alpha]\ ;\ true)) \vdash p2ac(P^t)) \\
& && \{\text{Lemmas C.2.1 and E.4.5}\} \\
&= \mathbf{RA}\left(\begin{array}{l} \neg\ (\mathbf{PBMH} \circ p2ac(P^f) \vee \mathbf{PBMH} \circ (\neg\ (\neg\ P^f[\mathbf{s}/in\alpha]\ ;\ true))) \\ \vdash \\ \mathbf{PBMH} \circ p2ac(P^t) \end{array}\right) \\
& && \{\text{Distributivity of } \mathbf{PBMH} \text{ (Theorem E.2.2)}\} \\
&= \mathbf{RA}\left(\begin{array}{l} \neg\ \mathbf{PBMH}(p2ac(P^f) \vee (\neg\ (\neg\ P^f[\mathbf{s}/in\alpha]\ ;\ true))) \\ \vdash \\ \mathbf{PBMH} \circ p2ac(P^t) \end{array}\right) \\
& && \{\text{Lemma E.6.2}\} \\
&= \mathbf{RA} \circ \mathbf{PBMH}(\neg\ p2ac(P^f) \wedge (\neg\ P^f[\mathbf{s}/in\alpha]\ ;\ true) \vdash p2ac(P^t)) \\
& && \{\text{Theorem 1.2.27}\} \\
&= \mathbf{RA} \circ \mathbf{A}(\neg\ p2ac(P^f) \wedge (\neg\ P^f[\mathbf{s}/in\alpha]\ ;\ true) \vdash p2ac(P^t))
\end{aligned}
$$

□

Theorem 1.4.14

$$p2ac \circ \mathbf{R}(\neg\ P^f \vdash P^t)$$
$$=$$
$$\mathbf{RA}(\neg\ p2ac(P^f) \wedge (\neg\ P^f[\mathbf{s}/in\alpha]\ ;\ true) \vdash p2ac(P^t))$$

Proof.

$$\begin{aligned}
&p2ac \circ \mathbf{R}(\neg\ P^f \vdash P^t) && \{\text{Theorem 1.4.10}\}\\
&= \mathbf{RA} \circ p2ac(\neg\ P^f \vdash P^t) && \{\text{Definition of } \mathbf{RA}\}\\
&= \mathbf{RA3} \circ \mathbf{RA2} \circ \mathbf{RA1} \circ p2ac(\neg\ P^f \vdash P^t) && \{\text{Definition of } \mathbf{RA1}\}\\
&= \mathbf{RA3} \circ \mathbf{RA2}((p2ac(\neg\ P^f \vdash P^t) \wedge ac' \neq \emptyset)[\{z \mid z \in ac' \wedge s.tr \leq z.tr\}/ac']) && \{\text{Theorem 2.1.1}\}\\
&= \mathbf{RA3} \circ \mathbf{RA2}((d2ac(\neg\ P^f \vdash P^t) \wedge ac' \neq \emptyset)[\{z \mid z \in ac' \wedge s.tr \leq z.tr\}/ac']) && \{\text{Definition of } \mathbf{RA1}\}\\
&= \mathbf{RA3} \circ \mathbf{RA2} \circ \mathbf{RA1} \circ d2ac(\neg\ P^f \vdash P^t) && \{\text{Definition of } \mathbf{RA} \text{ and } d2ac\}\\
&= \mathbf{RA}(\neg\ p2ac(P^f) \wedge (\neg\ P^f[\mathbf{s}/in\alpha]\ ;\ true) \vdash p2ac(P^t))
\end{aligned}$$

□

R1

Theorem 1.4.15

$$\mathbf{RA1} \circ p2ac(P) = p2ac \circ \mathbf{R1}(P)$$

Proof.

$$\begin{aligned}
&\mathbf{RA1} \circ p2ac(P) && \{\text{Definition of } p2ac\}\\
&= \mathbf{RA1}(\exists\, z \bullet P[\mathbf{s}, \mathbf{z}/in\alpha_{-ok}, out\alpha_{-ok'}] \wedge undash(z) \in ac') && \{\text{Definition of } \mathbf{RA1} \text{ (Lemma 1.2.1)}\}\\
&= \left(\begin{array}{l} \left(\begin{array}{l} \exists\, z \bullet P[\mathbf{s}, \mathbf{z}/in\alpha_{-ok}, out\alpha_{-ok'}] \\ \wedge \\ undash(z) \in ac' \end{array} \right)[\{z \mid z \in ac' \wedge s.tr \leq z.tr\}/ac'] \\ \wedge \exists\, z \bullet s.tr \leq z.tr \wedge z \in ac' \end{array} \right) && \{\text{Substitution: } ac' \text{ not free in } P\}
\end{aligned}$$

$$= \left(\begin{array}{l} \left(\begin{array}{l} \exists\, z \bullet P[\mathbf{s},\mathbf{z}/in\alpha_{-ok}, out\alpha_{-ok'}] \\ \wedge \\ undash(z) \in \{z \mid z \in ac' \wedge s.tr \leq z.tr\} \end{array} \right) \\ \wedge \exists\, z \bullet s.tr \leq z.tr \wedge z \in ac' \end{array} \right) \quad \{\text{Property of sets}\}$$

$$= \left(\begin{array}{l} \left(\begin{array}{l} \exists\, z \bullet P[\mathbf{s},\mathbf{z}/in\alpha_{-ok}, out\alpha_{-ok'}] \\ \wedge \\ undash(z) \in ac' \wedge s.tr \leq undash(z).tr \end{array} \right) \\ \wedge \exists\, z \bullet s.tr \leq z.tr \wedge z \in ac' \end{array} \right)$$

$\{\text{Predicate calculus: implication}\}$

$$= \left(\begin{array}{l} \exists\, z \bullet P[\mathbf{s},\mathbf{z}/in\alpha_{-ok}, out\alpha_{-ok'}] \\ \wedge \\ undash(z) \in ac' \wedge s.tr \leq undash(z).tr \end{array} \right) \quad \{\text{Property of } undash\}$$

$$= \exists\, z \bullet P[\mathbf{s},\mathbf{z}/in\alpha_{-ok}, out\alpha_{-ok'}] \wedge s.tr \leq z.tr' \wedge undash(z) \in ac'$$

$\{\text{Substitution}\}$

$$= \exists\, z \bullet (P \wedge tr \leq tr')[\mathbf{s},\mathbf{z}/in\alpha_{-ok}, out\alpha_{-ok'}] \wedge undash(z) \in ac'$$

$\{\text{Definition of } p2ac\}$

$$= p2ac(P \wedge tr \leq tr') \quad \{\text{Definition of } \mathbf{R1}\}$$

$$= p2ac \circ \mathbf{R1}(P)$$

□

R2

Theorem 1.4.16

$$p2ac \circ \mathbf{R1} \circ \mathbf{R2}(P) = \mathbf{RA2} \circ p2ac(P)$$

Proof.

$$\mathbf{RA2} \circ p2ac(P) \quad \{\text{Definition of } p2ac\}$$

$$= \mathbf{RA2}(\exists\, z \bullet P[\mathbf{s},\mathbf{z}/in\alpha_{-ok}, out\alpha_{-ok'}] \wedge undash(z) \in ac')$$

$\{\text{Definition of } \mathbf{RA2}\}$

$$= \left(\begin{array}{l} \exists\, z \bullet P[\mathbf{s},\mathbf{z}/in\alpha_{-ok}, out\alpha_{-ok'}] \\ \wedge\ undash(z) \in ac' \end{array} \right) \left[\begin{array}{l} s \oplus \{tr \mapsto \langle\rangle\}/s, \\ \{z \mid z \in ac' \wedge s.tr \leq z.tr \bullet z \oplus \{tr \mapsto z.tr - s.tr\}/ac' \end{array} \right]$$

$\{\text{Substitution: } ac' \text{ not free in } P\}$

$$= \left(\begin{array}{l} \exists\, z \bullet P[\mathbf{s},\mathbf{z}/in\alpha_{-ok}, out\alpha_{-ok'}][s \oplus \{tr \mapsto \langle\rangle\}/s] \\ \wedge\ undash(z) \in \{z \mid z \in ac' \wedge s.tr \leq z.tr \bullet z \oplus \{tr \mapsto z.tr - s.tr\}\} \end{array} \right)$$

$\{\text{Property of sets and variable renaming}\}$

$$= \left(\begin{array}{l} \exists\, z \bullet P[\mathbf{s},\mathbf{z}/in\alpha_{-ok}, out\alpha_{-ok'}][s \oplus \{tr \mapsto \langle\rangle\}/s] \\ \land \exists\, y \bullet y \in ac' \land s.tr \leq y.tr \land undash(z) = y \oplus \{tr \mapsto y.tr - s.tr\} \end{array} \right)$$

{Property of *undash*, *dash*}

$$= \left(\begin{array}{l} \exists\, z \bullet P[\mathbf{s},\mathbf{z}/in\alpha_{-ok}, out\alpha_{-ok'}][s \oplus \{tr \mapsto \langle\rangle\}/s] \\ \land \exists\, y \bullet y \in ac' \land s.tr \leq y.tr \land dash \circ undash(z) = dash(y \oplus \{tr \mapsto y.tr - s.tr\}) \end{array} \right)$$

{$dash \circ undash(z) = z$}

$$= \left(\begin{array}{l} \exists\, z \bullet P[\mathbf{s},\mathbf{z}/in\alpha_{-ok}, out\alpha_{-ok'}][s \oplus \{tr \mapsto \langle\rangle\}/s] \\ \land \exists\, y \bullet y \in ac' \land s.tr \leq y.tr \land z = dash(y \oplus \{tr \mapsto y.tr - s.tr\}) \end{array} \right)$$

{Property of *dash*}

$$= \left(\begin{array}{l} \exists\, z \bullet P[\mathbf{s},\mathbf{z}/in\alpha_{-ok}, out\alpha_{-ok'}][s \oplus \{tr \mapsto \langle\rangle\}/s] \\ \land \exists\, y \bullet y \in ac' \land s.tr \leq y.tr \land z = dash(y) \oplus \{tr' \mapsto y.tr - s.tr\} \end{array} \right)$$

{Introduce fresh variable}

$$= \left(\begin{array}{l} \exists\, z, t \bullet P[\mathbf{s},\mathbf{z}/in\alpha_{-ok}, out\alpha_{-ok'}][s \oplus \{tr \mapsto \langle\rangle\}/s] \\ \land \exists\, y \bullet y \in ac' \land s.tr \leq y.tr \land z = t \oplus \{tr' \mapsto y.tr - s.tr\} \\ \land\ t = dash(y) \end{array} \right)$$

{One-point rule}

$$= \left(\begin{array}{l} \exists\, t, y \bullet P[\mathbf{s},\mathbf{z}/in\alpha_{-ok}, out\alpha_{-ok'}][s \oplus \{tr \mapsto \langle\rangle\}/s][t \oplus \{tr' \mapsto y.tr - s.tr\}/z] \\ \land\ y \in ac' \land s.tr \leq y.tr \\ \land\ t = dash(y) \end{array} \right)$$

{Property of $undash \circ dash$}

$$= \left(\begin{array}{l} \exists\, t, y \bullet P[\mathbf{s},\mathbf{z}/in\alpha_{-ok}, out\alpha_{-ok'}][s \oplus \{tr \mapsto \langle\rangle\}/s][t \oplus \{tr' \mapsto y.tr - s.tr\}/z] \\ \land\ y \in ac' \land s.tr \leq y.tr \\ \land\ undash(t) = y \end{array} \right)$$

{One-point rule}

$$= \left(\begin{array}{l} \exists\, t \bullet P[\mathbf{s},\mathbf{z}/in\alpha_{-ok}, out\alpha_{-ok'}][s \oplus \{tr \mapsto \langle\rangle\}/s][t \oplus \{tr' \mapsto undash(t).tr - s.tr\}/z] \\ \land\ undash(t) \in ac' \land s.tr \leq undash(t).tr \end{array} \right)$$

{Property of *undash*}

$$= \left(\begin{array}{l} \exists\, t \bullet P[\mathbf{s},\mathbf{z}/in\alpha_{-ok}, out\alpha_{-ok'}][s \oplus \{tr \mapsto \langle\rangle\}/s][t \oplus \{tr' \mapsto t.tr' - s.tr\}/z] \\ \land\ undash(t) \in ac' \land s.tr \leq t.tr' \end{array} \right)$$

{Lemma G.1.3}

$$= \left(\begin{array}{l} \exists\, t \bullet P[\mathbf{s},\mathbf{t}/in\alpha_{-ok} \setminus \{tr\}, out\alpha_{-ok'} \setminus \{tr'\}][\langle\rangle/tr][t.tr' - s.tr/tr'] \\ \land\ undash(t) \in ac' \land s.tr \leq t.tr' \end{array} \right)$$

{Substitution}

$$= \left(\begin{array}{l} \exists\, z \bullet P[\mathbf{s}, \mathbf{z}/in\alpha_{-ok} \setminus \{tr\}, out\alpha_{-ok'} \setminus \{tr'\}][\langle\rangle, z.tr' - s.tr/tr, tr'] \\ \land\ s.tr \leq z.tr' \land undash(z) \in ac' \end{array} \right)$$

{Lemma G.1.5 and substitution}

$$= \exists\, z \bullet (P[\langle\rangle, tr' - tr/tr, tr'][\mathbf{s}, \mathbf{z}/in\alpha_{-ok}, out\alpha_{-ok'}] \land s.tr \leq z.tr') \land undash(z) \in ac'$$

{Substitution}

$$= \exists\, z \bullet (P[\langle\rangle, tr' - tr/tr, tr'] \land tr \leq tr')[\mathbf{s}, \mathbf{z}/in\alpha_{-ok}, out\alpha_{-ok'}] \land undash(z) \in ac'$$

{Definition of **R2** and **R1**}

$$= \exists\, z \bullet (\mathbf{R1} \circ \mathbf{R2}(P))[\mathbf{s}, \mathbf{z}/in\alpha_{-ok}, out\alpha_{-ok'}] \land undash(z) \in ac'$$

{Definition of $p2ac$}

$$= p2ac \circ \mathbf{R1} \circ \mathbf{R2}(P)$$

□

R3

Theorem 1.4.17

$$p2ac \circ \mathbf{R3}(P) = \mathbf{RA3} \circ p2ac(P)$$

Proof.

$p2ac \circ \mathbf{R3}(P)$ {Definition of **R3**}

$= p2ac(\mathit{II}_{rea} \lhd wait \rhd P)$ {Lemma 1.4.1}

$= p2ac(\mathit{II}_{rea}) \lhd s.wait \rhd p2ac(P)$ {Lemma 1.4.2}

$= \mathit{II}_{\mathcal{R}ac} \lhd s.wait \rhd p2ac(P)$ {Definition of **RA3**}

$= \mathbf{RA3} \circ p2ac(P)$

□

$\mathit{II}_{\mathcal{R}ac}$

Lemma 1.4.2

$$p2ac(\mathit{II}_{rea}) = \mathit{II}_{\mathcal{R}ac}$$

Proof.

$p2ac(\mathit{II}_{rea})$ {Definition of II_{rea}}

$$= p2ac \left(\begin{array}{l} (\neg\ ok \wedge tr \leq tr') \\ \vee \\ (ok' \wedge tr' = tr \wedge wait' = wait \wedge ref' = ref \wedge v' = v) \end{array} \right)$$

{Definition of $p2ac$}

$$= \exists\, z \bullet \left(\begin{array}{l} \left(\begin{array}{l} (\neg\ ok \wedge tr \leq tr') \\ \vee \\ (ok' \wedge tr' = tr \wedge wait' = wait \wedge ref' = ref \wedge v' = v) \end{array} \right) [\mathbf{s}, \mathbf{z}/in\alpha_{-ok}, out\alpha_{-ok'}] \\ \wedge\ undash(z) \in ac' \end{array} \right)$$

{Substitution}

$$= \exists\, z \bullet \left(\begin{array}{l} \left(\begin{array}{l} (\neg\ ok \wedge s.tr \leq z.tr') \\ \vee \\ (ok' \wedge z.tr' = s.tr \wedge z.wait' = s.wait \wedge z.ref' = s.ref \wedge z.v' = s.v) \end{array} \right) \\ \wedge\ undash(z) \in ac' \end{array} \right)$$

{Lemma G.3.3}

$$= \exists\, y \bullet \left(\begin{array}{l} \left(\begin{array}{l} (\neg\ ok \wedge s.tr \leq z.tr') \\ \vee \\ \left(\begin{array}{l} ok' \wedge z.tr' = s.tr \wedge z.wait' = s.wait \\ \wedge\ z.ref' = s.ref \wedge z.v' = s.v \end{array} \right) \end{array} \right) [dash(y)/z] \\ \wedge\ y \in ac' \end{array} \right)$$

{Substitution}

$$= \exists\, y \bullet \left(\begin{array}{l} \left(\begin{array}{l} (\neg\ ok \wedge s.tr \leq dash(y).tr') \\ \vee \\ \left(\begin{array}{l} ok' \wedge dash(y).tr' = s.tr \wedge dash(y).wait' = s.wait \\ \wedge\ dash(y).ref' = s.ref \wedge dash(y).v' = s.v \end{array} \right) \end{array} \right) \\ \wedge\ y \in ac' \end{array} \right)$$

{Property of $dash$}

$$= \exists\, y \bullet \left(\begin{array}{l} \left(\begin{array}{l} (\neg\ ok \wedge s.tr \leq y.tr) \\ \vee \\ (ok' \wedge y.tr = s.tr \wedge y.wait = s.wait \wedge y.ref = s.ref \wedge y.v = s.v) \end{array} \right) \\ \wedge\ y \in ac' \end{array} \right)$$

{Equality of records}

$$= \exists\, y \bullet ((\neg\ ok \wedge s.tr \leq y.tr) \vee (ok' \wedge y = s)) \wedge y \in ac'$$

{Predicate calculus}

$$= (\neg\ ok \wedge \exists\, y \bullet s.tr \leq y.tr \wedge y \in ac') \vee (\exists\, y \bullet ok' \wedge y = s \wedge y \in ac')$$

{One-point rule}

$= (\neg\ ok \wedge \exists\, y \bullet s.tr \leq y.tr \wedge y \in ac') \vee (ok' \wedge s \in ac')$
{Definition of $\mathbb{I}_{\mathcal{R}ac}$ (Lemma 1.2.3)}
$= \mathbb{I}_{\mathcal{R}ac}$

□

1.4.5 Linking results of $p2ac$ and $ac2p$

Theorem 1.4.18

$$p2ac \circ ac2p(P) \sqsupseteq \mathbf{PBMH}(P)$$

Proof.

$p2ac \circ ac2p(P)$ {Lemma C.2.8}
$= \exists\, ac_0, y \bullet P[ac_0/ac'] \wedge ac_0 \subseteq \{y\} \wedge y \in ac'$ {Property of sets}
$= \exists\, ac_0, y \bullet P[ac_0/ac'] \wedge ac_0 \subseteq \{y\} \wedge \{y\} \subseteq ac'$ {Predicate calculus}
$\Rightarrow \exists\, ac_0 \bullet P[ac_0/ac'] \wedge ac_0 \subseteq ac'$ {Definition of **PBMH** (Lemma E.1.1)}
$= \mathbf{PBMH}(P)$

□

Theorem 1.4.19 *Provided P is* **PBMH***-healthy.*

$$p2ac \circ ac2p(P) \sqsupseteq P$$

Proof.

$p2ac \circ ac2p(P)$ {Theorem 1.4.18}
$\Rightarrow \mathbf{PBMH}(P)$ {Assumption: P is **PBMH**-healthy}
$= P$

□

Theorem 1.4.20

$$ac2p \circ p2ac(P) = P$$

Proof.

$$
\begin{aligned}
& ac2p \circ p2ac(P) && \{\text{Definition of } ac2p \text{ (Lemma C.1.1)}\} \\
&= \exists\, ac', s \bullet \left(\begin{array}{l} p2ac(P) \land (\forall\, z \bullet z \in ac' \Rightarrow \bigwedge x : out\alpha_{-ok'} \bullet dash(z).x = x) \\ \land \\ (\bigwedge x : in\alpha_{-ok} \bullet s.x = x) \end{array} \right) \\
& && \{\text{Definition of } p2ac\} \\
&= \exists\, ac', s \bullet \left(\begin{array}{l} (\exists\, z \bullet P[\mathbf{s}, \mathbf{z}/in\alpha_{-ok}, out\alpha_{-ok'}] \land undash(z) \in ac') \\ \land \\ (\forall\, z \bullet z \in ac' \Rightarrow \bigwedge x : out\alpha_{-ok'} \bullet dash(z).x = x) \\ \land \\ (\bigwedge x : in\alpha_{-ok} \bullet s.x = x) \end{array} \right) \\
& && \{\text{Property of sets and predicate calculus}\} \\
&= \exists\, ac', s \bullet \left(\begin{array}{l} (\exists\, z \bullet P[\mathbf{s}, \mathbf{z}/in\alpha_{-ok}, out\alpha_{-ok'}] \land \{undash(z)\} \subseteq ac') \\ \land \\ (ac' \subseteq \{z \mid \bigwedge x : out\alpha_{-ok'} \bullet dash(z).x = x\}) \\ \land \\ (\bigwedge x : in\alpha_{-ok} \bullet s.x = x) \end{array} \right) \\
& && \{\text{Predicate calculus}\} \\
&= \exists\, s, z \bullet \left(\begin{array}{l} P[\mathbf{s}, \mathbf{z}/in\alpha_{-ok}, out\alpha_{-ok'}] \\ \land \\ (\{undash(z)\} \subseteq \{z \mid \bigwedge x : out\alpha_{-ok'} \bullet dash(z).x = x\}) \\ \land \\ (\bigwedge x : in\alpha_{-ok} \bullet s.x = x) \end{array} \right) \\
& && \{\text{Property of sets}\} \\
&= \exists\, s, z \bullet \left(\begin{array}{l} P[\mathbf{s}, \mathbf{z}/in\alpha_{-ok}, out\alpha_{-ok'}] \\ \land \\ (\forall\, y \bullet y = undash(z) \Rightarrow \bigwedge x : out\alpha_{-ok'} \bullet dash(y).x = x) \\ \land \\ (\bigwedge x : in\alpha_{-ok} \bullet s.x = x) \end{array} \right) \\
& && \{\text{Predicate calculus}\} \\
&= \exists\, s, z \bullet \left(\begin{array}{l} P[\mathbf{s}, \mathbf{z}/in\alpha_{-ok}, out\alpha_{-ok'}] \\ \land \\ (\bigwedge x : out\alpha_{-ok'} \bullet dash(undash(z)).x = x) \land (\bigwedge x : in\alpha_{-ok} \bullet s.x = x) \end{array} \right) \\
& && \{\text{Property of } dash \circ undash(z) = z\}
\end{aligned}
$$

$$= \exists\, s, z \bullet \left(\begin{array}{l} P[\mathbf{s}, \mathbf{z}/in\alpha_{-ok}, out\alpha_{-ok'}] \\ \wedge \\ (\bigwedge x : out\alpha_{-ok'} \bullet z.x = x) \wedge (\bigwedge x : in\alpha_{-ok} \bullet s.x = x) \end{array} \right)$$

{Lemma G.2.2}

$$= P[\mathbf{s}, \mathbf{z}/in\alpha_{-ok}, out\alpha_{-ok'}][State_{\mathit{II}}(out\alpha_{-ok'})/z][State_{\mathit{II}}(in\alpha_{-ok})/s]$$

{Lemma G.2.3}

$$= P$$

□

Results with respect to A2

Theorem 1.4.21 *Provided P_f^f and P_f^t are* **A2***-healthy.*

$$p2ac \circ ac2p \circ \mathbf{RA} \circ \mathbf{A}(\neg\, P_f^f \vdash P_f^t) = \mathbf{RA} \circ \mathbf{A}(\neg\, P_f^f \vdash P_f^t)$$

Proof.

$p2ac \circ ac2p \circ \mathbf{RA} \circ \mathbf{A}(\neg\, P_f^f \vdash P_f^t)$ {Theorem 1.4.5}

$= p2ac \circ \mathbf{R}(\neg\, ac2p(P_f^f) \vdash ac2p(P_f^t))$ {Theorem 1.4.11}

$= \mathbf{RA}(\neg\, p2ac \circ ac2p(P_f^f) \vdash p2ac \circ ac2p(P_f^t))$ {Definition of **RA**}

$= \mathbf{RA3} \circ \mathbf{RA2} \circ \mathbf{RA1}(\neg\, p2ac \circ ac2p(P_f^f) \vdash p2ac \circ ac2p(P_f^t))$

{Lemma B.1.13}

$$= \mathbf{RA3} \circ \mathbf{RA2} \circ \mathbf{RA1} \left(\begin{array}{l} \neg\, (p2ac \circ ac2p(P_f^f) \wedge ac' \neq \emptyset) \\ \vdash \\ p2ac \circ ac2p(P_f^t) \wedge ac' \neq \emptyset \end{array} \right)$$

{Assumption: P_f^t and P_f^f are **A2**-healthy}

$$= \mathbf{RA3} \circ \mathbf{RA2} \circ \mathbf{RA1} \left(\begin{array}{l} \neg\, (p2ac \circ ac2p \circ \mathbf{A2}(P_f^f) \wedge ac' \neq \emptyset) \\ \vdash \\ p2ac \circ ac2p \circ \mathbf{A2}(P_f^t) \wedge ac' \neq \emptyset \end{array} \right)$$

{Lemma A.3.13}

$$= \mathbf{RA3} \circ \mathbf{RA2} \circ \mathbf{RA1} \left(\begin{array}{l} \neg\, (\mathbf{A2}(P_f^f) \wedge ac' \neq \emptyset) \\ \vdash \\ \mathbf{A2}(P_f^t) \wedge ac' \neq \emptyset \end{array} \right)$$

{Lemma A.3.12}

$$= \mathbf{RA3} \circ \mathbf{RA2} \circ \mathbf{RA1} \left(\begin{array}{l} \neg\ (\mathbf{PBMH} \circ \mathbf{A2}(P_f^f) \wedge ac' \neq \emptyset) \\ \vdash \\ \mathbf{PBMH} \circ \mathbf{A2}(P_f^t) \wedge ac' \neq \emptyset \end{array} \right)$$

{Assumption: P_f^t and P_f^f are **A2**-healthy}

$$= \mathbf{RA3} \circ \mathbf{RA2} \circ \mathbf{RA1} \left(\begin{array}{l} \neg\ (\mathbf{PBMH}(P_f^f) \wedge ac' \neq \emptyset) \\ \vdash \\ \mathbf{PBMH}(P_f^t) \wedge ac' \neq \emptyset \end{array} \right)$$

{Lemma B.1.13}

$$= \mathbf{RA3} \circ \mathbf{RA2} \circ \mathbf{RA1}(\neg\ \mathbf{PBMH}(P_f^f) \vdash \mathbf{PBMH}(P_f^t))$$

{Definition of **A1**}

$$= \mathbf{RA3} \circ \mathbf{RA2} \circ \mathbf{RA1} \circ \mathbf{A1}(\neg\ P_f^f \vdash P_f^t)$$ {Theorem 1.2.6}

$$= \mathbf{RA3} \circ \mathbf{RA2} \circ \mathbf{RA1} \circ \mathbf{A0} \circ \mathbf{A1}(\neg\ P_f^f \vdash P_f^t)$$ {Definition of **RA**}

$$= \mathbf{RA} \circ \mathbf{A0} \circ \mathbf{A1}(\neg\ P_f^f \vdash P_f^t)$$ {Definition of **A**}

$$= \mathbf{RA} \circ \mathbf{A}(\neg\ P_f^f \vdash P_f^t)$$

□

1.5 Operators

In this section we define the operators of the theory. These include the counterparts to the operators of CSP expressed in the new model, for which we largely re-use the existing definitions by introducing the following predicate.

Definition 14

$$\circledS{\in}^{y}_{ac'}(P) \mathrel{\widehat{=}} \exists\, y \bullet y \in ac' \wedge P$$

For a given predicate P, this states that there is a final state y that is in the set of final states ac'.

1.5.1 Chaos

Divergence is modelled by $Chaos_{\mathbf{RA}}$, whose definition is presented below.

Definition 15

$$Chaos_{\mathbf{RA}} \mathrel{\widehat{=}} \mathbf{RA} \circ \mathbf{A}(false \vdash ac' \neq \emptyset)$$

Theorem 1.5.1

$$p2ac(Chaos_{\mathbf{R}}) = Chaos_{\mathbf{RA}}$$

Proof.

$$
\begin{array}{ll}
p2ac(Chaos_{\mathbf{R}}) & \{\text{Definition of } Chaos_{\mathbf{R}}\} \\
= p2ac \circ \mathbf{R}(false \vdash true) & \{\text{Theorem 1.4.12}\} \\
= \mathbf{RA} \circ \mathbf{A}(\neg\ p2ac(true) \vdash p2ac(true)) & \{\text{Lemma C.2.2}\} \\
= \mathbf{RA} \circ \mathbf{A}(\neg\ ac' \neq \emptyset \vdash ac' \neq \emptyset) & \\
\qquad \{\text{Definition of } \mathbf{A} \text{ and } \mathbf{PBMH}\text{-idempotent (Theorem E.2.1)}\} & \\
= \mathbf{RA} \circ \mathbf{A} \circ \mathbf{PBMH}(\neg\ ac' \neq \emptyset \vdash ac' \neq \emptyset) & \{\text{Lemma E.6.2}\} \\
= \mathbf{RA} \circ \mathbf{A}(\neg\ \mathbf{PBMH}(ac' = \emptyset) \vdash \mathbf{PBMH}(ac' \neq \emptyset)) & \\
\qquad \{\mathbf{PBMH}(ac' = \emptyset) = true\} & \\
= \mathbf{RA} \circ \mathbf{A}(\neg\ true \vdash ac' \neq \emptyset) & \{\text{Predicate calculus}\} \\
= \mathbf{RA} \circ \mathbf{A}(false \vdash ac' \neq \emptyset) & \{\text{Definition of } Chaos_{\mathbf{RA}}\} \\
= Chaos_{\mathbf{RA}} &
\end{array}
$$

□

1.5.2 Choice

The choice operator is originally not a CSP process. This describes a process whose precondition is always *true* and whose precondition establishes any final state.

Definition 16

$$Choice_{\mathbf{RA}} \mathrel{\widehat{=}} \mathbf{RA} \circ \mathbf{A}(true \vdash ac' \neq \emptyset)$$

If we consider the design $Choice = (true \vdash true)$ and the application of $\mathbf{R}$ to it, then it is possible to specify such an operator for the UTP theory of CSP. The application of $p2ac$ to this process yields our $Choice_{\mathbf{RA}}$ process.

Theorem 1.5.2

$$p2ac(Choice_{\mathbf{R}}) = Choice_{\mathbf{RA}}$$

Proof.

$$
\begin{array}{ll}
p2ac(Choice_{\mathbf{R}}) & \{\text{Definition of } Choice_{\mathbf{R}}\} \\
= p2ac \circ \mathbf{R}(true \vdash true) & \{\text{Theorem 1.4.12}\} \\
= \mathbf{RA} \circ \mathbf{A}(\neg\, p2ac(false) \vdash p2ac(true)) & \\
 & \{\text{Lemmas C.2.2 and C.2.3}\} \\
= \mathbf{RA} \circ \mathbf{A}(\neg\, false \vdash ac' \neq \emptyset) & \{\text{Predicate calculus}\} \\
= \mathbf{RA} \circ \mathbf{A}(true \vdash ac' \neq \emptyset) & \{\text{Definition of } Choice_{\mathbf{RA}}\} \\
= Choice_{\mathbf{RA}} &
\end{array}
$$

□

1.5.3 Stop

Deadlock is modelled by $Stop_{\mathbf{RA}}$, whose definition is presented below. This is similar to the definition of $Stop_{\mathbf{R}}$ in CSP.

Definition 17

$$Stop_{\mathbf{RA}} \mathrel{\widehat{=}} \mathbf{RA} \circ \mathbf{A}(true \vdash \circledin{}^{y}_{ac'}(y.tr = s.tr \wedge y.wait))$$

In the following theorem we establish that this definition corresponds exactly to that obtained by applying $p2ac$ to the $Stop_{\mathbf{R}}$ operator of CSP.

Theorem 1.5.3

$$p2ac(Stop_{\mathbf{R}}) = Stop_{\mathbf{RA}}$$

Proof.

$$
\begin{array}{ll}
p2ac(Stop_{\mathbf{R}}) & \{\text{Definition of } Stop_{\mathbf{R}}\} \\
= p2ac \circ \mathbf{R}(true \vdash tr' = tr \wedge wait') & \{\text{Theorem 1.4.12}\} \\
= \mathbf{RA} \circ \mathbf{A}(\neg\, p2ac(false) \vdash p2ac(tr' = tr \wedge wait')) & \{\text{Lemma C.2.3}\} \\
= \mathbf{RA} \circ \mathbf{A}(\neg\, false \vdash p2ac(tr' = tr \wedge wait')) & \{\text{Predicate calculus}\} \\
= \mathbf{RA} \circ \mathbf{A}(true \vdash p2ac(tr' = tr \wedge wait')) & \{\text{Definition of } p2ac\} \\
= \mathbf{RA} \circ \mathbf{A}(true \vdash \exists\, z \bullet z.tr' = s.tr \wedge z.wait' \wedge undash(z) \in ac') & \\
 & \{\text{Introduce fresh variable}\}
\end{array}
$$

$$= \mathbf{RA} \circ \mathbf{A}(true \vdash \exists\, z, y \bullet z.tr' = s.tr \wedge z.wait' \wedge y = undash(z) \wedge y \in ac')$$
$$\{\text{Property of } dash\}$$
$$= \mathbf{RA} \circ \mathbf{A}(true \vdash \exists\, z, y \bullet z.tr' = s.tr \wedge z.wait' \wedge dash(y) = z \wedge y \in ac')$$
$$\{\text{One-point rule}\}$$
$$= \mathbf{RA} \circ \mathbf{A}(true \vdash \exists\, y \bullet dash(y).tr' = s.tr \wedge dash(y).wait' \wedge y \in ac')$$
$$\{\text{Property of } dash\}$$
$$= \mathbf{RA} \circ \mathbf{A}(true \vdash \exists\, y \bullet y.tr = s.tr \wedge y.wait \wedge y \in ac')$$
$$\{\text{Definition of } \circledin^{y}_{ac'}\}$$
$$= \mathbf{RA} \circ \mathbf{A}(true \vdash \circledin^{y}_{ac'}(y.tr = s.tr \wedge y.wait)) \qquad \{\text{Definition of } Stop_{\mathbf{RA}}\}$$
$$= Stop_{\mathbf{RA}}$$

□

1.5.4 Skip

Definition 18

$$Skip_{\mathbf{RA}} \mathrel{\widehat{=}} \mathbf{RA} \circ \mathbf{A}(true \vdash \circledin^{y}_{ac'}(\neg\, y.wait \wedge y.tr = s.tr))$$

1.5.5 External choice

Similarly to the external choice operator of CSP, we define it as follows.

Definition 19

$$P \,\Box_{\mathbf{RA}}\, Q$$
$$\mathrel{\widehat{=}}$$
$$\mathbf{RA} \circ \mathbf{A} \left(\begin{array}{l} (\neg\, P^f_f \wedge \neg\, Q^f_f) \\ \vdash \\ \circledin^{y}_{ac'}((P^t_f \wedge Q^t_f) \lhd y.tr = s.tr \wedge y.wait \rhd (P^t_f \vee Q^t_f)) \end{array} \right)$$

The precondition is the conjunction of the precondition of both P and Q, while the postcondition is split into two cases: when the process is waiting and the trace of events is kept unchanged, then the result is the conjunction of both postconditions, otherwise it is their disjunction.

In the following Theorem 1.5.4 we show the result of applying $p2ac$ to the external choice between the mapping of P and Q into the original theory of CSP. The resulting process is stronger than $P \,\Box_{\mathbf{RA}}\, Q$.

Theorem 1.5.4 *Provided P and Q are reactive angelic processes.*

$$p2ac(ac2p(P)\ \Box_{\mathbf{R}}\ ac2p(Q)) \sqsupseteq P\ \Box_{\mathbf{RA}}\ Q$$

Proof.

$$p2ac(ac2p(P)\ \Box_{\mathbf{R}}\ ac2p(Q)) \qquad \{\text{Definition of } \Box_{\mathbf{R}}\}$$

$$= p2ac \circ \mathbf{R} \left(\begin{array}{l} (\neg\ ac2p(P)^f_f \wedge \neg\ ac2p(P)^f_f) \\ \vdash \\ (ac2p(P)^t_f \wedge ac2p(Q)^t_f) \lhd tr' = tr \wedge wait' \rhd (ac2p(P)^t_f \vee ac2p(Q)^t_f) \end{array} \right)$$

$\{\text{Lemma C.1.13}\}$

$$= p2ac \circ \mathbf{R} \left(\begin{array}{l} (\neg\ ac2p(P^f_f) \wedge \neg\ ac2p(P^f_f)) \\ \vdash \\ (ac2p(P^t_f) \wedge ac2p(Q^t_f)) \lhd tr' = tr \wedge wait' \rhd (ac2p(P^t_f) \vee ac2p(Q^t_f)) \end{array} \right)$$

$\{\text{Theorem 1.4.12}\}$

$$= \mathbf{RA} \circ \mathbf{A} \left(\begin{array}{l} \neg\ p2ac(ac2p(P^f_f) \vee ac2p(Q^f_f)) \\ \vdash \\ p2ac \left(\begin{array}{l} (ac2p(P^t_f) \wedge ac2p(Q^t_f)) \\ \lhd tr' = tr \wedge wait' \rhd \\ (ac2p(P^t_f) \vee ac2p(Q^t_f)) \end{array} \right) \end{array} \right)$$

$\{\text{Definition of conditional and predicate calculus}\}$

$$= \mathbf{RA} \circ \mathbf{A} \left(\begin{array}{l} \neg\ p2ac(ac2p(P^f_f) \vee ac2p(Q^f_f)) \\ \vdash \\ p2ac \left(\begin{array}{l} (tr' = tr \wedge wait' \wedge ac2p(P^t_f) \wedge ac2p(Q^t_f)) \\ \vee \\ (tr' \neq tr \wedge (ac2p(P^t_f) \vee ac2p(Q^t_f))) \\ \vee \\ (\neg\ wait' \wedge (ac2p(P^t_f) \vee ac2p(Q^t_f))) \end{array} \right) \end{array} \right)$$

$\{\text{Distributivity of } ac2p \text{ (Theorem 1.4.1)}\}$

$$= \mathbf{RA} \circ \mathbf{A} \left(\begin{array}{l} \neg\ p2ac \circ ac2p(P^f_f \vee Q^f_f) \\ \vdash \\ p2ac \left(\begin{array}{l} (tr' = tr \wedge wait' \wedge ac2p(P^t_f) \wedge ac2p(Q^t_f)) \\ \vee \\ (tr' \neq tr \wedge ac2p(P^t_f \vee Q^t_f)) \\ \vee \\ (\neg\ wait' \wedge ac2p(P^t_f \vee Q^t_f)) \end{array} \right) \end{array} \right)$$

$\{\text{Theorem 1.4.18}\}$

$$= \mathbf{RA} \circ \mathbf{A} \left(\begin{array}{l} \neg\ (p2ac \circ ac2p(P_f^f \lor Q_f^f) \land \mathbf{PBMH}(P_f^f \lor Q_f^f)) \\ \vdash \\ p2ac \left(\begin{array}{l} (tr' = tr \land wait' \land ac2p(P_f^t) \land ac2p(Q_f^t)) \\ \lor \\ (tr' \neq tr \land ac2p(P_f^t \lor Q_f^t)) \\ \lor \\ (\neg\ wait' \land ac2p(P_f^t \lor Q_f^t)) \end{array} \right) \end{array} \right)$$

{Predicate calculus}

$$= \mathbf{RA} \circ \mathbf{A} \left(\begin{array}{l} (\neg\ p2ac \circ ac2p(P_f^f \lor Q_f^f)) \lor \neg\ \mathbf{PBMH}(P_f^f \lor Q_f^f) \\ \vdash \\ p2ac \left(\begin{array}{l} (tr' = tr \land wait' \land ac2p(P_f^t) \land ac2p(Q_f^t)) \\ \lor \\ (tr' \neq tr \land ac2p(P_f^t \lor Q_f^t)) \\ \lor \\ (\neg\ wait' \land ac2p(P_f^t \lor Q_f^t)) \end{array} \right) \end{array} \right)$$

{Refinement of designs}

$$\sqsupseteq \mathbf{RA} \circ \mathbf{A} \left(\begin{array}{l} \neg\ \mathbf{PBMH}(P_f^f \lor Q_f^f) \\ \vdash \\ p2ac \left(\begin{array}{l} (tr' = tr \land wait' \land ac2p(P_f^t) \land ac2p(Q_f^t)) \\ \lor \\ (tr' \neq tr \land ac2p(P_f^t \lor Q_f^t)) \\ \lor \\ (\neg\ wait' \land ac2p(P_f^t \lor Q_f^t)) \end{array} \right) \end{array} \right)$$

{Distributivity of $p2ac$ (Theorem 1.4.4)}

$$= \mathbf{RA} \circ \mathbf{A} \left(\begin{array}{l} \neg\ \mathbf{PBMH}(P_f^f \lor Q_f^f) \\ \vdash \\ \left(\begin{array}{l} p2ac(tr' = tr \land wait' \land ac2p(P_f^t) \land ac2p(Q_f^t)) \\ \lor \\ p2ac(tr' \neq tr \land ac2p(P_f^t \lor Q_f^t)) \\ \lor \\ p2ac(\neg\ wait' \land ac2p(P_f^t \lor Q_f^t)) \end{array} \right) \end{array} \right)$$

{Theorem 1.4.3 and weaken postcondition}

$$\sqsupseteq \mathbf{RA} \circ \mathbf{A} \left(\begin{array}{l} \neg\, \mathbf{PBMH}(P_f^f \vee Q_f^f) \\ \vdash \\ \left(\begin{array}{l} (p2ac(tr' = tr \wedge wait') \wedge p2ac \circ ac2p(P_f^t) \wedge p2ac \circ ac2p(Q_f^t)) \\ \vee \\ (p2ac(tr' \neq tr) \wedge p2ac \circ ac2p(P_f^t \vee Q_f^t)) \\ \vee \\ (p2ac(\neg\, wait') \wedge p2qc \circ ac2p(P_f^t \vee Q_f^t)) \end{array} \right) \end{array} \right)$$

{Theorem 1.4.18 and weaken postcondition}

$$\sqsupseteq \mathbf{RA} \circ \mathbf{A} \left(\begin{array}{l} \neg\, \mathbf{PBMH}(P_f^f \vee Q_f^f) \\ \vdash \\ \left(\begin{array}{l} (p2ac(tr' = tr \wedge wait') \wedge \mathbf{PBMH}(P_f^t) \wedge \mathbf{PBMH}(Q_f^t)) \\ \vee \\ (p2ac(tr' \neq tr) \wedge \mathbf{PBMH}(P_f^t \vee Q_f^t)) \\ \vee \\ (p2ac(\neg\, wait') \wedge \mathbf{PBMH}(P_f^t \vee Q_f^t)) \end{array} \right) \end{array} \right)$$

{Definition of $p2ac$}

$$= \mathbf{RA} \circ \mathbf{A} \left(\begin{array}{l} \neg\, \mathbf{PBMH}(P_f^f \vee Q_f^f) \\ \vdash \\ \left(\begin{array}{l} \left(\begin{array}{l} (\exists\, z \bullet z'.tr' = s.tr \wedge z'.wait' \wedge z \in ac') \\ \wedge \\ \mathbf{PBMH}(P_f^t) \wedge \mathbf{PBMH}(Q_f^t) \end{array} \right) \\ \vee \\ ((\exists\, z \bullet z'.tr' \neq s.tr \wedge z \in ac') \wedge \mathbf{PBMH}(P_f^t \vee Q_f^t)) \\ \vee \\ ((\exists\, z \bullet \neg\, z'.wait' \wedge z \in ac') \wedge \mathbf{PBMH}(P_f^t \vee Q_f^t)) \end{array} \right) \end{array} \right)$$

{Property of dashed state variable}

$$= \mathbf{RA} \circ \mathbf{A} \left(\begin{array}{l} \neg\, \mathbf{PBMH}(P_f^f \vee Q_f^f) \\ \vdash \\ \left(\begin{array}{l} \left(\begin{array}{l} (\exists\, z \bullet z.tr = s.tr \wedge z.wait \wedge z \in ac') \\ \wedge \\ \mathbf{PBMH}(P_f^t) \wedge \mathbf{PBMH}(Q_f^t) \end{array} \right) \\ \vee \\ ((\exists\, z \bullet z.tr \neq s.tr \wedge z \in ac') \wedge \mathbf{PBMH}(P_f^t \vee Q_f^t)) \\ \vee \\ ((\exists\, z \bullet \neg\, z.wait \wedge z \in ac') \wedge \mathbf{PBMH}(P_f^t \vee Q_f^t)) \end{array} \right) \end{array} \right)$$

{Predicate calculus and distributivity of **PBMH**}

$$= \mathbf{RA} \circ \mathbf{A} \left(\begin{array}{l} \neg\, \mathbf{PBMH}(P_f^f) \wedge \neg\, \mathbf{PBMH}(Q_f^f) \\ \vdash \\ \exists\, z \bullet z \in ac' \\ \wedge \\ \left(\begin{array}{l} ((z.tr = s.tr \wedge z.wait) \wedge \mathbf{PBMH}(P_f^t) \wedge \mathbf{PBMH}(Q_f^t)) \\ \vee \\ ((z.tr \neq s.tr) \wedge \mathbf{PBMH}(P_f^t \vee Q_f^t)) \\ \vee \\ ((\neg\, z.wait) \wedge \mathbf{PBMH}(P_f^t \vee Q_f^t)) \end{array} \right) \end{array} \right)$$

{Predicate calculus}

$$= \mathbf{RA} \circ \mathbf{A} \left(\begin{array}{l} \neg\, \mathbf{PBMH}(P_f^f) \wedge \neg\, \mathbf{PBMH}(Q_f^f) \\ \vdash \\ \exists\, y \bullet y \in ac' \\ \wedge \\ \left(\begin{array}{l} ((y.tr = s.tr \wedge y.wait) \wedge \mathbf{PBMH}(P_f^t) \wedge \mathbf{PBMH}(Q_f^t)) \\ \vee \\ (\neg\, (y.tr = s.tr \wedge y.wait) \wedge \mathbf{PBMH}(P_f^t \vee Q_f^t)) \end{array} \right) \end{array} \right)$$

{Definition of conditional}

$$= \mathbf{RA} \circ \mathbf{A} \left(\begin{array}{l} \neg\, \mathbf{PBMH}(P_f^f) \wedge \neg\, \mathbf{PBMH}(Q_f^f) \\ \vdash \\ \exists\, y \bullet y \in ac' \wedge \left(\begin{array}{l} (\mathbf{PBMH}(P_f^t) \wedge \mathbf{PBMH}(Q_f^t)) \\ \lhd y.tr = s.tr \wedge y.wait \rhd \\ (\mathbf{PBMH}(P_f^t \vee Q_f^t)) \end{array} \right) \end{array} \right)$$

{Distributivity of **PBMH**}

$$= \mathbf{RA} \circ \mathbf{A} \left(\begin{array}{l} \neg\, \mathbf{PBMH}(P_f^f) \wedge \neg\, \mathbf{PBMH}(Q_f^f) \\ \vdash \\ \exists\, y \bullet y \in ac' \wedge \left(\begin{array}{l} (\mathbf{PBMH}(P_f^t) \wedge \mathbf{PBMH}(Q_f^t)) \\ \lhd y.tr = s.tr \wedge y.wait \rhd \\ (\mathbf{PBMH}(P_f^t) \vee \mathbf{PBMH}(Q_f^t)) \end{array} \right) \end{array} \right)$$

{Lemma E.5.1}

$$= \mathbf{RA} \circ \mathbf{A} \left(\begin{array}{l} \neg\, \mathbf{PBMH}(P)_f^f \wedge \neg\, \mathbf{PBMH}(Q)_f^f \\ \vdash \\ \exists\, y \bullet y \in ac' \wedge \left(\begin{array}{l} (\mathbf{PBMH}(P)_f^t \wedge \mathbf{PBMH}(Q)_f^t) \\ \lhd y.tr = s.tr \wedge y.wait \rhd \\ (\mathbf{PBMH}(P)_f^t \vee \mathbf{PBMH}(Q)_f^t) \end{array} \right) \end{array} \right)$$

{Assumption: P and Q are **RAP**-healthy and Theorem 1.3.2}

$$= \mathbf{RA} \circ \mathbf{A} \left(\begin{array}{l} \neg\ P_f^f \wedge \neg\ Q_f^f \\ \vdash \\ \exists\, y \bullet y \in ac' \wedge \left(\begin{array}{l} (P_f^t \wedge Q_f^t) \\ \lhd y.tr = s.tr \wedge y.wait \rhd \\ (P_f^t \vee Q_f^t) \end{array} \right) \end{array} \right)$$

$\{$Definition of $\circledin_{ac'}^{y}\}$

$$= \mathbf{RA} \circ \mathbf{A} \left(\begin{array}{l} \neg\ P_f^f \wedge \neg\ Q_f^f \\ \vdash \\ \circledin_{ac'}^{y} \left((P_f^t \wedge Q_f^t) \lhd y.tr = s.tr \wedge y.wait \rhd (P_f^t \vee Q_f^t) \right) \end{array} \right)$$

$\{$Definition of $\Box_{\mathbf{RA}}\}$

$$= P\ \Box_{\mathbf{RA}}\ Q$$

□

Furthermore, if we consider two CSP processes P and Q, then we can calculate the result of the external choice in the new model by mapping each predicate through $p2ac$. The result of mapping this back into the original model through $ac2p$ yields exactly the same external choice operator of CSP.

Theorem 1.5.5

$$ac2p(p2ac(P)\ \Box_{\mathbf{RA}}\ p2ac(Q)) = P\ \Box_{\mathbf{R}}\ Q$$

Proof.

$ac2p(p2ac(P)\ \Box_{\mathbf{RA}}\ p2ac(Q))$ $\{$Definition of $\Box_{\mathbf{RA}}\}$

$$= ac2p \circ \mathbf{RA} \circ \mathbf{A} \left(\begin{array}{l} \neg\ p2ac(P)_f^f \wedge \neg\ p2ac(P)_f^f \\ \vdash \\ \exists\, y \bullet y \in ac' \wedge \left(\begin{array}{l} (p2ac(P)_f^t \wedge p2ac(Q)_f^t) \\ \lhd y.tr = s.tr \wedge y.wait \rhd \\ (p2ac(P)_f^t \vee p2ac(Q)_f^t) \end{array} \right) \end{array} \right)$$

$\{$Lemma C.2.9$\}$

$$= ac2p \circ \mathbf{RA} \circ \mathbf{A} \left(\begin{array}{l} \neg\ p2ac(P_f^f) \wedge \neg\ p2ac(P_f^f) \\ \vdash \\ \exists\, y \bullet y \in ac' \wedge \left(\begin{array}{l} (p2ac(P_f^t) \wedge p2ac(Q_f^t)) \\ \lhd y.tr = s.tr \wedge y.wait \rhd \\ (p2ac(P_f^t) \vee p2ac(Q_f^t)) \end{array} \right) \end{array} \right)$$

$\{$Theorem 1.4.5$\}$

$$= \mathbf{R}\left(\begin{array}{l} \neg\ ac2p(p2ac(P_f^f) \vee p2ac(P_f^f)) \\ \vdash \\ ac2p\left(\exists\, y \bullet y \in ac' \wedge \left(\begin{array}{l}(p2ac(P_f^t) \wedge p2ac(Q_f^t)) \\ \lhd y.tr = s.tr \wedge y.wait \rhd \\ (p2ac(P_f^t) \vee p2ac(Q_f^t))\end{array}\right)\right)\end{array}\right)$$

{Definition of conditional}

$$= \mathbf{R}\left(\begin{array}{l} \neg\ ac2p(p2ac(P_f^f) \vee p2ac(P_f^f)) \\ \vdash \\ ac2p\left(\exists\, y \bullet y \in ac' \wedge \left(\begin{array}{l}(y.tr = s.tr \wedge y.wait \wedge p2ac(P_f^t) \wedge p2ac(Q_f^t)) \\ \vee \\ (y.tr \neq s.tr \wedge (p2ac(P_f^t) \vee p2ac(Q_f^t))) \\ \vee \\ (\neg\ y.wait \wedge (p2ac(P_f^t) \vee p2ac(Q_f^t)))\end{array}\right)\right)\end{array}\right)$$

{Predicate calculus}

$$= \mathbf{R}\left(\begin{array}{l} \neg\ ac2p(p2ac(P_f^f) \vee p2ac(P_f^f)) \\ \vdash \\ ac2p\left(\begin{array}{l}((\exists\, y \bullet y \in ac' \wedge y.tr = s.tr \wedge y.wait) \wedge p2ac(P_f^t) \wedge p2ac(Q_f^t)) \\ \vee \\ ((\exists\, y \bullet y \in ac' \wedge y.tr \neq s.tr) \wedge (p2ac(P_f^t) \vee p2ac(Q_f^t))) \\ \vee \\ ((\exists\, y \bullet y \in ac' \wedge \neg\ y.wait) \wedge (p2ac(P_f^t) \vee p2ac(Q_f^t)))\end{array}\right)\end{array}\right)$$

{Distributivity of $ac2p$ (Theorem 1.4.1)}

$$= \mathbf{R}\left(\begin{array}{l} \neg\ ac2p(p2ac(P_f^f) \vee p2ac(P_f^f)) \\ \vdash \\ \left(\begin{array}{l}ac2p((\exists\, y \bullet y \in ac' \wedge y.tr = s.tr \wedge y.wait) \wedge p2ac(P_f^t) \wedge p2ac(Q_f^t)) \\ \vee \\ ac2p((\exists\, y \bullet y \in ac' \wedge y.tr \neq s.tr) \wedge (p2ac(P_f^t) \vee p2ac(Q_f^t))) \\ \vee \\ ac2p((\exists\, y \bullet y \in ac' \wedge \neg\ y.wait) \wedge (p2ac(P_f^t) \vee p2ac(Q_f^t)))\end{array}\right)\end{array}\right)$$

{Lemmas C.2.1 and E.4.10 and Theorems 1.4.2 and E.3.2}

$$= \mathbf{R}\left(\begin{array}{l} \neg\ ac2p(p2ac(P_f^f) \vee p2ac(P_f^f)) \\ \vdash \\ \left(\begin{array}{l} (ac2p(\exists\, y \bullet y \in ac' \wedge y.tr = s.tr \wedge y.wait) \wedge ac2p \circ p2ac(P_f^t) \wedge ac2p \circ p2ac(Q_f^t)) \\ \vee \\ (ac2p(\exists\, y \bullet y \in ac' \wedge y.tr \neq s.tr) \wedge ac2p(p2ac(P_f^t) \vee p2ac(Q_f^t))) \\ \vee \\ (ac2p(\exists\, y \bullet y \in ac' \wedge \neg\ y.wait) \wedge ac2p(p2ac(P_f^t) \vee p2ac(Q_f^t))) \end{array}\right) \end{array}\right)$$

{Distributivity of $ac2p$ (Theorem 1.4.1)}

$$= \mathbf{R}\left(\begin{array}{l} \neg\ (ac2p \circ p2ac(P_f^f) \vee ac2p \circ p2ac(P_f^f)) \\ \vdash \\ \left(\begin{array}{l} (ac2p(\exists\, y \bullet y \in ac' \wedge y.tr = s.tr \wedge y.wait) \wedge ac2p \circ p2ac(P_f^t) \wedge ac2p \circ p2ac(Q_f^t)) \\ \vee \\ (ac2p(\exists\, y \bullet y \in ac' \wedge y.tr \neq s.tr) \wedge (ac2p \circ p2ac(P_f^t) \vee ac2p \circ p2ac(Q_f^t))) \\ \vee \\ (ac2p(\exists\, y \bullet y \in ac' \wedge \neg\ y.wait) \wedge (ac2p \circ p2ac(P_f^t) \vee ac2p \circ p2ac(Q_f^t))) \end{array}\right) \end{array}\right)$$

{Theorem 1.4.20}

$$= \mathbf{R}\left(\begin{array}{l} \neg\ (P_f^f \vee P_f^f) \\ \vdash \\ \left(\begin{array}{l} (ac2p(\exists\, y \bullet y \in ac' \wedge y.tr = s.tr \wedge y.wait) \wedge P_f^t \wedge Q_f^t) \\ \vee \\ (ac2p(\exists\, y \bullet y \in ac' \wedge y.tr \neq s.tr) \wedge (P_f^t \vee Q_f^t)) \\ \vee \\ (ac2p(\exists\, y \bullet y \in ac' \wedge \neg\ y.wait) \wedge (P_f^t \vee Q_f^t)) \end{array}\right) \end{array}\right)$$

{Definition of $ac2p$ (Lemma C.1.3)}

$$= \mathbf{R}\left(\begin{array}{l} \neg\ (P_f^f \vee P_f^f) \\ \vdash \\ \left(\begin{array}{l} (tr' = tr \wedge wait' \wedge P_f^t \wedge Q_f^t) \\ \vee \\ (tr' \neq tr \wedge (P_f^t \vee Q_f^t)) \\ \vee \\ (\neg\ wait' \wedge (P_f^t \vee Q_f^t)) \end{array}\right) \end{array}\right)$$

{Predicate calculus and definition of conditional}

$$= \mathbf{R}\left(\begin{array}{l} \neg\ P_f^f \wedge \neg\ P_f^f \\ \vdash \\ (P_f^t \vee Q_f^t) \lhd tr' = tr \wedge wait' \rhd (P_f^t \wedge Q_f^t) \end{array}\right) \qquad \{\text{Definition of } \Box_{\mathbf{R}}\}$$

$= P \ \Box_{\mathbf{R}} \ Q$

□

1.5.6 Event prefixing

Definition 20

$$a \rightarrow_{\mathbf{RA}} \mathit{Skip}_{\mathbf{RA}} \mathrel{\widehat{=}} \mathbf{RA} \circ \mathbf{A} \left(\mathit{true} \vdash \circledin{}^{y}_{ac'} \left(\begin{array}{l} (y.tr = s.tr \wedge a \notin y.ref) \\ \lhd y.wait \rhd \\ (y.tr = s.tr \frown \langle a \rangle) \end{array} \right) \right)$$

Theorem 1.5.6

$$ac2p(a \rightarrow_{\mathbf{RA}} \mathit{Skip}_{\mathbf{RA}}) = a \rightarrow_{\mathbf{R}} \mathit{Skip}_{\mathbf{R}}$$

Proof.

$ac2p(a \rightarrow_{\mathbf{RA}} \mathit{Skip})$ {Definition of $a \rightarrow_{\mathbf{RA}} \mathit{Skip}$}

$= ac2p \circ \mathbf{RA} \circ \mathbf{A} \left(\mathit{true} \vdash \circledin{}^{y}_{ac'} \left(\begin{array}{l} (y.tr = s.tr \wedge a \notin y.ref) \\ \lhd y.wait \rhd \\ (y.tr = s.tr \frown \langle a \rangle) \end{array} \right) \right)$ {Theorem 1.4.5}

$= \mathbf{R} \left(\neg \ ac2p(\mathit{false}) \vdash ac2p \left(\circledin{}^{y}_{ac'} \left(\begin{array}{l} (y.tr = s.tr \wedge a \notin y.ref) \\ \lhd y.wait \rhd \\ (y.tr = s.tr \frown \langle a \rangle) \end{array} \right) \right) \right)$ {Lemma C.1.9 and predicate calculus}

$= \mathbf{R} \left(\mathit{true} \vdash ac2p \left(\circledin{}^{y}_{ac'} \left(\begin{array}{l} (y.tr = s.tr \wedge a \notin y.ref) \\ \lhd y.wait \rhd \\ (y.tr = s.tr \frown \langle a \rangle) \end{array} \right) \right) \right)$ {Definition of $\circledin{}^{y}_{ac'}$ and conditional}

$= \mathbf{R} \left(\mathit{true} \vdash ac2p \left(\begin{array}{l} (\exists\, y \bullet y \in ac' \wedge y.wait \wedge y.tr = s.tr \wedge a \notin y.ref) \\ \vee \\ (\exists\, y \bullet y \in ac' \wedge \neg\ y.wait \wedge y.tr = s.tr \frown \langle a \rangle) \end{array} \right) \right)$ {Theorem 1.4.1}

$= \mathbf{R} \left(\mathit{true} \vdash \left(\begin{array}{l} ac2p(\exists\, y \bullet y \in ac' \wedge y.wait \wedge y.tr = s.tr \wedge a \notin y.ref) \\ \vee \\ ac2p(\exists\, y \bullet y \in ac' \wedge \neg\ y.wait \wedge y.tr = s.tr \frown \langle a \rangle) \end{array} \right) \right)$ {Lemma C.1.3}

$$= \mathbf{R}\left(\begin{array}{l} true \vdash \left(\begin{array}{l} \left(\begin{array}{l} y.wait \\ \wedge \\ y.tr = s.tr \\ \wedge \\ a \notin y.ref \end{array}\right)\left[\begin{array}{cc} State_{\mathtt{II}}(in\alpha_{-ok}) & \Big/ \; s \\ undash(State_{\mathtt{II}}(out\alpha_{-ok'})) & \Big/ \; y \end{array}\right] \\ \vee \\ \left(\begin{array}{l} \neg\, y.wait \\ \wedge \\ y.tr = s.tr \frown \langle a \rangle \end{array}\right)\left[\begin{array}{cc} State_{\mathtt{II}}(in\alpha_{-ok}) & \Big/ \; s \\ undash(State_{\mathtt{II}}(out\alpha_{-ok'})) & \Big/ \; y \end{array}\right] \end{array}\right) \end{array}\right)$$

{Definition of $State_{\mathtt{II}}$, *undash* and substitution}

$$= \mathbf{R}\left(true \vdash \left(\begin{array}{l} (wait' \wedge tr' = tr \wedge a \notin ref') \\ \vee \\ (\neg\, wait' \wedge tr' = tr \frown \langle a \rangle) \end{array}\right)\right)$$

{Definition of conditional}

$$= \mathbf{R}\left(true \vdash \left(\begin{array}{l} (tr' = tr \wedge a \notin ref') \\ \lhd wait' \rhd \\ (tr' = tr \frown \langle a \rangle) \end{array}\right)\right)$$

{Definition of $Skip_{\mathbf{R}}$}

$$= a \rightarrow_{\mathbf{R}} Skip_{\mathbf{R}}$$

□

Theorem 1.5.7

$$p2ac(a \rightarrow_{\mathbf{R}} Skip_{\mathbf{R}}) = a \rightarrow_{\mathbf{RA}} Skip_{\mathbf{RA}}$$

Proof.

$p2ac(a \rightarrow_{\mathbf{R}} Skip_{\mathbf{R}})$ {Definition of $\rightarrow_{\mathbf{R}} Skip_{\mathbf{R}}$}

$$= p2ac \circ \mathbf{R}\left(true \vdash \left(\begin{array}{l} (tr' = tr \wedge a \notin ref') \\ \lhd wait' \rhd \\ (tr' = tr \frown \langle a \rangle) \end{array}\right)\right)$$

{Theorem 1.4.12}

$$= \mathbf{RA} \circ \mathbf{A}\left(\neg\, p2ac(false) \vdash p2ac\left(\begin{array}{l} (tr' = tr \wedge a \notin ref') \\ \lhd wait' \rhd \\ (tr' = tr \frown \langle a \rangle) \end{array}\right)\right)$$

{Lemma C.2.3 and predicate calculus}

$$= \mathbf{RA} \circ \mathbf{A}\left(true \vdash p2ac\left(\begin{array}{l} (tr' = tr \wedge a \notin ref') \\ \lhd wait' \rhd \\ (tr' = tr \frown \langle a \rangle) \end{array}\right)\right)$$

{Definition of conditional}

$$= \mathbf{RA} \circ \mathbf{A} \left(true \vdash p2ac \left(\begin{array}{l} (wait' \wedge tr' = tr \wedge a \notin ref') \\ \vee \\ (\neg\ wait' \wedge tr' = tr \frown \langle a \rangle) \end{array} \right) \right)$$

{Theorem 1.4.4}

$$= \mathbf{RA} \circ \mathbf{A} \left(true \vdash \left(\begin{array}{l} p2ac(wait' \wedge tr' = tr \wedge a \notin ref') \\ \vee \\ p2ac(\neg\ wait' \wedge tr' = tr \frown \langle a \rangle) \end{array} \right) \right)$$

{Definition of $p2ac$ and substitution}

$$= \mathbf{RA} \circ \mathbf{A} \left(true \vdash \left(\begin{array}{l} (\exists\, z \bullet z.wait' \wedge z.tr' = s.tr \wedge a \notin z.ref' \wedge undash(z) \in ac') \\ \vee \\ (\exists\, z \bullet \neg\ z.wait' \wedge z.tr' = s.tr \frown \langle a \rangle \wedge undash(z) \in ac') \end{array} \right) \right)$$

{Introduce auxiliary variable}

$$= \mathbf{RA} \circ \mathbf{A} \left(true \vdash \left(\begin{array}{l} (\exists\, z, y \bullet z.wait' \wedge z.tr' = s.tr \wedge a \notin z.ref' \wedge undash(z) = y \wedge y \in ac') \\ \vee \\ (\exists\, z, y \bullet \neg\ z.wait' \wedge z.tr' = s.tr \frown \langle a \rangle \wedge undash(z) = y \wedge y \in ac') \end{array} \right) \right)$$

{Property of *undash* and *dash*}

$$= \mathbf{RA} \circ \mathbf{A} \left(true \vdash \left(\begin{array}{l} (\exists\, z, y \bullet z.wait' \wedge z.tr' = s.tr \wedge a \notin z.ref' \wedge z = dash(y) \wedge y \in ac') \\ \vee \\ (\exists\, z, y \bullet \neg\ z.wait' \wedge z.tr' = s.tr \frown \langle a \rangle \wedge z = dash(y) \wedge y \in ac') \end{array} \right) \right)$$

{One-point rule}

$$= \mathbf{RA} \circ \mathbf{A} \left(true \vdash \left(\begin{array}{l} (\exists\, y \bullet dash(y).wait' \wedge dash(y).tr' = s.tr \wedge a \notin dash(y).ref' \wedge y \in ac') \\ \vee \\ (\exists\, y \bullet \neg\ dash(y).wait' \wedge dash(y).tr' = s.tr \frown \langle a \rangle \wedge y \in ac') \end{array} \right) \right)$$

{Property of *dash*}

$$= \mathbf{RA} \circ \mathbf{A} \left(true \vdash \left(\begin{array}{l} (\exists\, y \bullet y.wait \wedge y.tr = s.tr \wedge a \notin y.ref \wedge y \in ac') \\ \vee \\ (\exists\, y \bullet \neg\ y.wait \wedge y.tr = s.tr \frown \langle a \rangle \wedge y \in ac') \end{array} \right) \right)$$

{Predicate calculus and definition of $\circledin^{y}_{ac'}$}

$$= \mathbf{RA} \circ \mathbf{A} \left(true \vdash \circledin^{y}_{ac'} \left(\begin{array}{l} (y.wait \wedge y.tr = s.tr \wedge a \notin y.ref') \\ \vee \\ (\neg\ y.wait \wedge y.tr = s.tr \frown \langle a \rangle) \end{array} \right) \right)$$

{Definition of conditional}

$$= \mathbf{RA} \circ \mathbf{A} \left(true \vdash \circledcirc{\in}^{y}_{ac'} \left(\begin{array}{l} (y.tr = s.tr \wedge a \notin y.ref') \\ \lhd y.wait \rhd \\ (y.tr = s.tr \frown \langle a \rangle) \end{array} \right) \right)$$

{Definition of $a \rightarrow_{\mathbf{RA}} Skip_{\mathbf{RA}}$}

$$= a \rightarrow_{\mathbf{RA}} Skip_{\mathbf{RA}}$$

□

1.5.7 Demonic choice

Internal choice, also known as demonic choice, is defined as the greatest lower bound of the lattice, just like in the original theory of CSP.

Definition 21

$$P \sqcap_{\mathbf{RA}} Q \mathrel{\widehat{=}} P \vee Q$$

Theorem 1.5.8

$$\mathbf{RA} \circ \mathbf{A}(P \vdash Q) \sqcap \mathbf{RA} \circ \mathbf{A}(R \vdash S) = \mathbf{RA} \circ \mathbf{A}(P \wedge R \vdash Q \vee S)$$

Proof.

$\mathbf{RA} \circ \mathbf{A}(P \vdash Q) \sqcap \mathbf{RA} \circ \mathbf{A}(R \vdash S)$ {Theorem 1.2.27}

$= \mathbf{RA} \circ \mathbf{PBMH}(P \vdash Q) \sqcap \mathbf{RA} \circ \mathbf{PBMH}(R \vdash S)$ {Definition of $\sqcup$}

$= \mathbf{RA} \circ \mathbf{PBMH}(P \vdash Q) \vee \mathbf{RA} \circ \mathbf{PBMH}(R \vdash S)$ {Theorem 1.2.25}

$= \mathbf{RA}(\mathbf{PBMH}(P \vdash Q) \vee \mathbf{PBMH}(R \vdash S))$ {Theorem E.2.2}

$= \mathbf{RA} \circ \mathbf{PBMH}((P \vdash Q) \vee (R \vdash S))$ {Disjunction of designs}

$= \mathbf{RA} \circ \mathbf{PBMH}(P \wedge R \vdash Q \vee S)$

□

Theorem 1.5.9 *Provided P and Q are reactive angelic processes.*

$$P \sqcap Q = \mathbf{RA} \circ \mathbf{A}(\neg\, P^f_f \wedge \neg\, Q^f_f \vdash P^t_f \vee Q^t_f)$$

Proof.

$P \sqcap Q$ {Assumption: P and Q are **RAP**-healthy}

$= \mathbf{RA} \circ \mathbf{A}(\neg\, P^f_f \vdash P^t_f) \sqcap \mathbf{RA} \circ \mathbf{A}(\neg\, Q^f_f \vdash Q^t_f)$ {Theorem 1.5.8}

$= \mathbf{RA} \circ \mathbf{A}(\neg\, P^f_f \wedge \neg\, Q^f_f \vdash P^t_f \vee Q^t_f)$

□

Properties

Theorem 1.5.10 *Provided P is a reactive angelic process.*

$$Chaos_{\mathbf{RA}} \sqcap P = Chaos_{\mathbf{RA}}$$

Proof.

$$\begin{aligned}
&Chaos_{\mathbf{RA}} \sqcap P && \{\text{Definition of } Chaos_{\mathbf{RA}}\}\\
&= \mathbf{RA} \circ \mathbf{A}(false \vdash ac' \neq \emptyset) \sqcap P && \{\text{Assumption: } P \text{ is } \mathbf{RAP}\text{-healthy}\}\\
&= \mathbf{RA} \circ \mathbf{A}(false \vdash ac' \neq \emptyset) \sqcap \mathbf{RA} \circ \mathbf{A}(\neg\, P_f^f \vdash P_f^t) && \{\text{Theorem 1.5.8}\}\\
&= \mathbf{RA} \circ \mathbf{A}(false \wedge \neg\, P_f^f \vdash ac' \neq \emptyset \vee P_f^t) && \{\text{Predicate calculus}\}\\
&= \mathbf{RA} \circ \mathbf{A}(false \vdash ac' \neq \emptyset \vee P_f^t) && \{\text{Predicate calculus}\}\\
&= \mathbf{RA} \circ \mathbf{A}(false \vdash ac' \neq \emptyset) && \{\text{Definition of } Chaos_{\mathbf{RA}}\}\\
&= Chaos_{\mathbf{RA}}
\end{aligned}$$

□

Theorem 1.5.11

$$p2ac(ac2p(P) \sqcap ac2p(Q)) = p2ac \circ ac2p(P) \sqcap p2ac \circ ac2p(Q)$$

Proof.

$$\begin{aligned}
&p2ac(ac2p(P) \sqcap ac2p(Q)) && \{\text{Definition of } \sqcap\}\\
&= p2ac(ac2p(P) \vee ac2p(Q)) && \{\text{Theorem 1.4.4}\}\\
&= p2ac \circ ac2p(P) \vee p2ac \circ ac2p(Q) && \{\text{Definition of } \sqcap\}\\
&= p2ac \circ ac2p(P) \sqcap p2ac \circ ac2p(Q)
\end{aligned}$$

□

1.5.8 Angelic choice

Angelic choice is defined as the least upper bound of the lattice.

Definition 22

$$P \sqcup Q \mathrel{\widehat{=}} P \wedge Q$$

Theorem 1.5.12

$$\mathbf{RA} \circ \mathbf{A}(P \vdash Q) \sqcup \mathbf{RA} \circ \mathbf{A}(R \vdash S)$$
$$=$$
$$\mathbf{RA} \circ \mathbf{A} \left(\begin{array}{l} (\neg\, \mathbf{PBMH}(\neg\, P) \vee \neg\, \mathbf{PBMH}(\neg\, R)) \\ \vdash \\ \left(\begin{array}{l} (\neg\, \mathbf{PBMH}(\neg\, P) \Rightarrow \mathbf{PBMH}(Q)) \\ \wedge \\ (\neg\, \mathbf{PBMH}(\neg\, R) \Rightarrow \mathbf{PBMH}(S) \end{array} \right) \end{array} \right)$$

Proof.

$$\begin{array}{ll} \mathbf{RA} \circ \mathbf{A}(P \vdash Q) \sqcup \mathbf{RA} \circ \mathbf{A}(R \vdash S) & \{\text{Definition of } \sqcup\} \\ = \mathbf{RA} \circ \mathbf{A}(P \vdash Q) \wedge \mathbf{RA} \circ \mathbf{A}(R \vdash S) & \{\text{Theorem 1.2.27}\} \\ = \mathbf{RA} \circ \mathbf{PBMH}(P \vdash Q) \wedge \mathbf{RA} \circ \mathbf{PBMH}(R \vdash S) & \{\text{Theorem 1.2.24}\} \\ = \mathbf{RA}(\mathbf{PBMH}(P \vdash Q) \wedge \mathbf{PBMH}(R \vdash S)) & \{\text{Theorem E.3.1}\} \\ = \mathbf{RA} \circ \mathbf{PBMH}(\mathbf{PBMH}(P \vdash Q) \wedge \mathbf{PBMH}(R \vdash S)) & \{\text{Lemma E.6.2}\} \\ = \mathbf{RA} \circ \mathbf{PBMH} \left(\begin{array}{l} (\neg\, \mathbf{PBMH}(\neg\, P) \vdash \mathbf{PBMH}(Q)) \\ \wedge \\ (\neg\, \mathbf{PBMH}(\neg\, R) \vdash \mathbf{PBMH}(S)) \end{array} \right) & \{\text{Theorem 1.2.27}\} \\ = \mathbf{RA} \circ \mathbf{A} \left(\begin{array}{l} (\neg\, \mathbf{PBMH}(\neg\, P) \vdash \mathbf{PBMH}(Q)) \\ \wedge \\ (\neg\, \mathbf{PBMH}(\neg\, R) \vdash \mathbf{PBMH}(S)) \end{array} \right) & \{\text{Conjunction of designs}\} \\ = \mathbf{RA} \circ \mathbf{A} \left(\begin{array}{l} (\neg\, \mathbf{PBMH}(\neg\, P) \vee \neg\, \mathbf{PBMH}(R)) \\ \vdash \\ \left(\begin{array}{l} (\neg\, \mathbf{PBMH}(\neg\, P) \Rightarrow \mathbf{PBMH}(Q)) \\ \wedge \\ (\neg\, \mathbf{PBMH}(\neg\, R) \Rightarrow \mathbf{PBMH}(S)) \end{array} \right) \end{array} \right) & \end{array}$$

□

Theorem 1.5.13 *Provided* $\neg\, P$, $\neg\, Q$, R *and* S *are* **PBMH***-healthy.*

$$\mathbf{RA} \circ \mathbf{A}(P \vdash Q) \sqcup \mathbf{RA} \circ \mathbf{A}(R \vdash S)$$
$$=$$
$$\mathbf{RA} \circ \mathbf{A}(P \vee R \vdash (P \Rightarrow Q) \wedge (R \Rightarrow S))$$

Proof.

$$
\begin{array}{ll}
\mathbf{RA} \circ \mathbf{A}(P \vdash Q) \sqcup \mathbf{RA} \circ \mathbf{A}(R \vdash S) & \{\text{Theorem 1.5.12}\} \\
= \mathbf{RA} \circ \mathbf{A} \left(\begin{array}{l} (\neg\, \mathbf{PBMH}(\neg\, P) \vee \neg\, \mathbf{PBMH}(\neg\, R)) \\ \vdash \\ \left(\begin{array}{l} (\neg\, \mathbf{PBMH}(\neg\, P) \Rightarrow \mathbf{PBMH}(Q)) \\ \wedge \\ (\neg\, \mathbf{PBMH}(\neg\, R) \Rightarrow \mathbf{PBMH}(S)) \end{array} \right) \end{array} \right) & \\
\qquad \{\text{Assumption: } \neg\, P, \neg\, R, Q \text{ and } S \text{ are } \mathbf{PBMH}\text{-healthy}\} & \\
= \mathbf{RA} \circ \mathbf{A} \left(\begin{array}{l} (\neg \neg\, P \vee \neg \neg\, R) \\ \vdash \\ (\neg \neg\, P \Rightarrow Q) \wedge (\neg \neg\, R \Rightarrow S) \end{array} \right) & \{\text{Predicate calculus}\} \\
= \mathbf{RA} \circ \mathbf{A}(P \vee R \vdash (P \Rightarrow Q) \wedge (R \Rightarrow S)) &
\end{array}
$$

□

Theorem 1.5.14 *Provided P and Q are reactive angelic processes.*

$$P \sqcup Q = \mathbf{RA} \circ \mathbf{A}(\neg\, P_f^f \vee \neg\, Q_f^f \vdash (\neg\, P_f^f \Rightarrow P_f^t) \wedge (\neg\, Q_f^f \Rightarrow Q_f^t))$$

Proof.

$$
\begin{array}{ll}
P \sqcup Q & \{\text{Assumption: } P \text{ and } Q \text{ are } \mathbf{RAP}\text{-healthy}\} \\
= \mathbf{RA} \circ \mathbf{A}(\neg\, P_f^f \vdash P_f^t) \sqcup \mathbf{RA} \circ \mathbf{A}(\neg\, Q_f^f \vdash Q_f^t) & \{\text{Theorem 1.5.12}\} \\
= \mathbf{RA} \circ \mathbf{A} \left(\begin{array}{l} (\neg\, \mathbf{PBMH}(P_f^f) \vee \neg\, \mathbf{PBMH}(Q_f^f)) \\ \vdash \\ \left(\begin{array}{l} (\neg\, \mathbf{PBMH}(P_f^f) \Rightarrow \mathbf{PBMH}(P_f^t)) \\ \wedge \\ (\neg\, \mathbf{PBMH}(Q_f^f) \Rightarrow \mathbf{PBMH}(Q_f^t)) \end{array} \right) \end{array} \right) & \{\text{Lemma E.5.1}\} \\
= \mathbf{RA} \circ \mathbf{A} \left(\begin{array}{l} (\neg\, \mathbf{PBMH}(P)_f^f \vee \neg\, \mathbf{PBMH}(Q)_f^f) \\ \vdash \\ \left(\begin{array}{l} (\neg\, \mathbf{PBMH}(P)_f^f \Rightarrow \mathbf{PBMH}(P)_f^t) \\ \wedge \\ (\neg\, \mathbf{PBMH}(Q)_f^f \Rightarrow \mathbf{PBMH}(Q)_f^t) \end{array} \right) \end{array} \right) & \\
\qquad \{\text{Assumption: } P \text{ and } Q \text{ are } \mathbf{RAP}\text{-healthy and Theorem 1.3.2}\} & \\
= \mathbf{RA} \circ \mathbf{A}((\neg\, P_f^f \vee \neg\, Q_f^f) \vdash (\neg\, P_f^f \Rightarrow P_f^t) \wedge (\neg\, Q_f^f \Rightarrow Q_f^t)) &
\end{array}
$$

□

1.5.9 Sequential composition

Theorem 1.5.15 *Provided P and Q are reactive angelic processes.*

$$
\begin{array}{l}
P \ ;_{\mathcal{D}\mathbf{ac}} Q \\
= \\
\mathbf{RA} \circ \mathbf{A} \left(\begin{array}{l} \left(\begin{array}{l} \neg \, (\mathbf{RA1}(P_f^f) \ ;_{\mathcal{A}} \mathbf{RA1}(\mathit{true})) \\ \wedge \\ \neg \, (\mathbf{RA1}(P_f^t) \ ;_{\mathcal{A}} (\neg \, s.\mathit{wait} \wedge \mathbf{RA2} \circ \mathbf{RA1}(Q_f^f))) \end{array} \right) \\ \vdash \\ \mathbf{RA1}(P_f^t) \ ;_{\mathcal{A}} (s \in ac' \lhd s.\mathit{wait} \rhd (\mathbf{RA2} \circ \mathbf{RA1}(\neg \, Q_f^f \Rightarrow Q_f^t))) \end{array} \right)
\end{array}
$$

Proof.

$$
\begin{array}{ll}
= P \ ;_{\mathcal{D}\mathbf{ac}} Q & \{\text{Assumption: } P \text{ and } Q \text{ are } \mathbf{RAP}\text{-healthy}\} \\
= \mathbf{RA} \circ \mathbf{A}(\neg \, P_f^f \vdash P_f^t) \ ;_{\mathcal{D}\mathbf{ac}} \mathbf{RA} \circ \mathbf{A}(\neg \, Q_f^f \vdash Q_f^t) & \{\text{Theorem 1.2.27}\} \\
= \mathbf{RA} \circ \mathbf{PBMH}(\neg \, P_f^f \vdash P_f^t) \ ;_{\mathcal{D}\mathbf{ac}} \mathbf{RA} \circ \mathbf{PBMH}(\neg \, Q_f^f \vdash Q_f^t) & \\
& \{\text{Lemma E.6.2}\} \\
= \left(\begin{array}{l} \mathbf{RA}(\neg \, \mathbf{PBMH}(P_f^f) \vdash \mathbf{PBMH}(P_f^t)) \\ \ ;_{\mathcal{D}\mathbf{ac}} \\ \mathbf{RA}(\neg \, \mathbf{PBMH}(Q_f^f) \vdash \mathbf{PBMH}(Q_f^t)) \end{array} \right) & \{\text{Theorem 1.5.16}\} \\
= \mathbf{RA} \left(\begin{array}{l} \left(\begin{array}{l} \neg \, (\mathbf{RA1} \circ \mathbf{PBMH}(P_f^f) \ ;_{\mathcal{A}} \mathbf{RA1}(\mathit{true})) \\ \wedge \\ \neg \left(\begin{array}{l} (\mathbf{RA1} \circ \mathbf{PBMH}(P_f^t)) \\ \ ;_{\mathcal{A}} \\ (\neg \, s.\mathit{wait} \wedge \mathbf{RA2} \circ \mathbf{RA1} \circ \mathbf{PBMH}(Q_f^f)) \end{array} \right) \end{array} \right) \\ \vdash \\ \left(\begin{array}{l} (\mathbf{RA1} \circ \mathbf{PBMH}(P_f^t)) \\ \ ;_{\mathcal{A}} \\ (s \in ac') \lhd s.\mathit{wait} \rhd (\mathbf{RA2} \circ \mathbf{RA1}(\neg \, \mathbf{PBMH}(Q_f^f) \Rightarrow \mathbf{PBMH}(Q_f^t)) \end{array} \right) \end{array} \right) & \\
& \{\text{Predicate calculus and Theorem E.2.2}\}
\end{array}
$$

$$= \mathbf{RA}\left(\begin{array}{l}\left(\begin{array}{l}\neg\,(\mathbf{RA1}\circ\mathbf{PBMH}(P_f^f)\ ;_{\mathcal{A}}\mathbf{RA1}(\mathit{true}))\\ \wedge\\ \neg\left(\begin{array}{l}(\mathbf{RA1}\circ\mathbf{PBMH}(P_f^t))\\ ;_{\mathcal{A}}\\ (\neg\, s.\mathit{wait}\wedge\mathbf{RA2}\circ\mathbf{RA1}\circ\mathbf{PBMH}(Q_f^f))\end{array}\right)\end{array}\right)\\ \vdash\\ \left(\begin{array}{l}(\mathbf{RA1}\circ\mathbf{PBMH}(P_f^t))\\ ;_{\mathcal{A}}\\ (s\in ac')\lhd s.\mathit{wait}\rhd(\mathbf{RA2}\circ\mathbf{RA1}\circ\mathbf{PBMH}(\neg\, Q_f^f\Rightarrow Q_f^t))\end{array}\right)\end{array}\right)$$

{Lemma E.4.1 and Theorems 1.2.5 and F.3.1}

$$= \mathbf{RA}\left(\begin{array}{l}\left(\begin{array}{l}\neg\,\mathbf{PBMH}(\mathbf{RA1}\circ\mathbf{PBMH}(P_f^f)\ ;_{\mathcal{A}}\mathbf{RA1}(\mathit{true}))\\ \wedge\\ \neg\left(\begin{array}{l}(\mathbf{RA1}\circ\mathbf{PBMH}(P_f^t))\\ ;_{\mathcal{A}}\\ (\neg\, s.\mathit{wait}\wedge\mathbf{RA2}\circ\mathbf{RA1}\circ\mathbf{PBMH}(Q_f^f))\end{array}\right)\end{array}\right)\\ \vdash\\ \left(\begin{array}{l}(\mathbf{RA1}\circ\mathbf{PBMH}(P_f^t))\\ ;_{\mathcal{A}}\\ (s\in ac')\lhd s.\mathit{wait}\rhd(\mathbf{RA2}\circ\mathbf{RA1}\circ\mathbf{PBMH}(\neg\, Q_f^f\Rightarrow Q_f^t))\end{array}\right)\end{array}\right)$$

{Theorems 1.2.5, 1.2.11 and F.3.1 and Lemma E.4.8}

$$= \mathbf{RA}\left(\begin{array}{l}\left(\begin{array}{l}\neg\,\mathbf{PBMH}(\mathbf{RA1}\circ\mathbf{PBMH}(P_f^f)\ ;_{\mathcal{A}}\mathbf{RA1}(\mathit{true}))\\ \wedge\\ \neg\,\mathbf{PBMH}\left(\begin{array}{l}(\mathbf{RA1}\circ\mathbf{PBMH}(P_f^t))\\ ;_{\mathcal{A}}\\ (\neg\, s.\mathit{wait}\wedge\mathbf{RA2}\circ\mathbf{RA1}\circ\mathbf{PBMH}(Q_f^f))\end{array}\right)\end{array}\right)\\ \vdash\\ \left(\begin{array}{l}(\mathbf{RA1}\circ\mathbf{PBMH}(P_f^t))\\ ;_{\mathcal{A}}\\ (s\in ac')\lhd s.\mathit{wait}\rhd(\mathbf{RA2}\circ\mathbf{RA1}\circ\mathbf{PBMH}(\neg\, Q_f^f\Rightarrow Q_f^t))\end{array}\right)\end{array}\right)$$

{Theorem 1.2.5}

$$= \mathbf{RA}\left(\begin{array}{l} \left(\begin{array}{l} \neg\ \mathbf{PBMH}(\mathbf{RA1} \circ \mathbf{PBMH}(P_f^f)\ ;_{\mathcal{A}}\ \mathbf{RA1}(true)) \\ \wedge \\ \neg\ \mathbf{PBMH}\left(\begin{array}{l} (\mathbf{RA1} \circ \mathbf{PBMH}(P_f^t)) \\ ;_{\mathcal{A}} \\ (\neg\ s.wait \wedge \mathbf{RA2} \circ \mathbf{RA1} \circ \mathbf{PBMH}(Q_f^f)) \end{array}\right) \end{array}\right) \\ \vdash \\ \left(\begin{array}{l} (\mathbf{PBMH} \circ \mathbf{RA1} \circ \mathbf{PBMH}(P_f^t)) \\ ;_{\mathcal{A}} \\ (s \in ac') \lhd s.wait \rhd (\mathbf{RA2} \circ \mathbf{RA1} \circ \mathbf{PBMH}(\neg\ Q_f^f \Rightarrow Q_f^t)) \end{array}\right) \end{array}\right)$$

{Lemma E.4.3 and Theorems 1.2.5 and 1.2.11}

$$= \mathbf{RA}\left(\begin{array}{l} \left(\begin{array}{l} \neg\ \mathbf{PBMH}(\mathbf{RA1} \circ \mathbf{PBMH}(P_f^f)\ ;_{\mathcal{A}}\ \mathbf{RA1}(true)) \\ \wedge \\ \neg\ \mathbf{PBMH}\left(\begin{array}{l} (\mathbf{RA1} \circ \mathbf{PBMH}(P_f^t)) \\ ;_{\mathcal{A}} \\ (\neg\ s.wait \wedge \mathbf{RA2} \circ \mathbf{RA1} \circ \mathbf{PBMH}(Q_f^f)) \end{array}\right) \end{array}\right) \\ \vdash \\ \left(\begin{array}{l} (\mathbf{PBMH} \circ \mathbf{RA1} \circ \mathbf{PBMH}(P_f^t)) \\ ;_{\mathcal{A}} \\ \mathbf{PBMH}(s \in ac') \lhd s.wait \rhd \mathbf{PBMH}(\mathbf{RA2} \circ \mathbf{RA1} \circ \mathbf{PBMH}(\neg\ Q_f^f \Rightarrow Q_f^t)) \end{array}\right) \end{array}\right)$$

{Lemma E.4.9}

$$= \mathbf{RA}\left(\begin{array}{l} \left(\begin{array}{l} \neg\ \mathbf{PBMH}(\mathbf{RA1} \circ \mathbf{PBMH}(P_f^f)\ ;_{\mathcal{A}}\ \mathbf{RA1}(true)) \\ \wedge \\ \neg\ \mathbf{PBMH}\left(\begin{array}{l} (\mathbf{RA1} \circ \mathbf{PBMH}(P_f^t)) \\ ;_{\mathcal{A}} \\ (\neg\ s.wait \wedge \mathbf{RA2} \circ \mathbf{RA1} \circ \mathbf{PBMH}(Q_f^f)) \end{array}\right) \end{array}\right) \\ \vdash \\ \left(\begin{array}{l} (\mathbf{PBMH} \circ \mathbf{RA1} \circ \mathbf{PBMH}(P_f^t)) \\ ;_{\mathcal{A}} \\ \mathbf{PBMH}(s \in ac' \lhd s.wait \rhd (\mathbf{RA2} \circ \mathbf{RA1} \circ \mathbf{PBMH}(\neg\ Q_f^f \Rightarrow Q_f^t))) \end{array}\right) \end{array}\right)$$

{Theorem F.3.1}

$$
= \mathbf{RA}\left(\begin{array}{l}
\left(\begin{array}{l}
\neg\, \mathbf{PBMH}(\mathbf{RA1} \circ \mathbf{PBMH}(P_f^f)\ ;_{\mathcal{A}} \mathbf{RA1}(true)) \\
\wedge \\
\neg\, \mathbf{PBMH}\left(\begin{array}{l}
(\mathbf{RA1} \circ \mathbf{PBMH}(P_f^t)) \\
;_{\mathcal{A}} \\
(\neg\, s.wait \wedge \mathbf{RA2} \circ \mathbf{RA1} \circ \mathbf{PBMH}(Q_f^f))
\end{array}\right)
\end{array}\right) \\
\vdash \\
\mathbf{PBMH}\left(\begin{array}{l}
(\mathbf{PBMH} \circ \mathbf{RA1} \circ \mathbf{PBMH}(P_f^t)) \\
;_{\mathcal{A}} \\
\mathbf{PBMH}(s \in ac' \lhd s.wait \rhd (\mathbf{RA2} \circ \mathbf{RA1} \circ \mathbf{PBMH}(\neg\, Q_f^f \Rightarrow Q_f^t)))
\end{array}\right)
\end{array}\right)
$$

{Lemmas E.4.3 and E.4.9 and Theorems 1.2.5 and 1.2.11}

$$
= \mathbf{RA}\left(\begin{array}{l}
\left(\begin{array}{l}
\neg\, \mathbf{PBMH}(\mathbf{RA1} \circ \mathbf{PBMH}(P_f^f)\ ;_{\mathcal{A}} \mathbf{RA1}(true)) \\
\wedge \\
\neg\, \mathbf{PBMH}\left(\begin{array}{l}
(\mathbf{RA1} \circ \mathbf{PBMH}(P_f^t)) \\
;_{\mathcal{A}} \\
(\neg\, s.wait \wedge \mathbf{RA2} \circ \mathbf{RA1} \circ \mathbf{PBMH}(Q_f^f))
\end{array}\right)
\end{array}\right) \\
\vdash \\
\mathbf{PBMH}\left(\begin{array}{l}
(\mathbf{PBMH} \circ \mathbf{RA1} \circ \mathbf{PBMH}(P_f^t)) \\
;_{\mathcal{A}} \\
(s \in ac' \lhd s.wait \rhd (\mathbf{RA2} \circ \mathbf{RA1} \circ \mathbf{PBMH}(\neg\, Q_f^f \Rightarrow Q_f^t)))
\end{array}\right)
\end{array}\right)
$$

{Theorem 1.2.5}

$$
= \mathbf{RA}\left(\begin{array}{l}
\left(\begin{array}{l}
\neg\, \mathbf{PBMH}(\mathbf{RA1} \circ \mathbf{PBMH}(P_f^f)\ ;_{\mathcal{A}} \mathbf{RA1}(true)) \\
\wedge \\
\neg\, \mathbf{PBMH}\left(\begin{array}{l}
(\mathbf{RA1} \circ \mathbf{PBMH}(P_f^t)) \\
;_{\mathcal{A}} \\
(\neg\, s.wait \wedge \mathbf{RA2} \circ \mathbf{RA1} \circ \mathbf{PBMH}(Q_f^f))
\end{array}\right)
\end{array}\right) \\
\vdash \\
\mathbf{PBMH}\left(\begin{array}{l}
(\mathbf{RA1} \circ \mathbf{PBMH}(P_f^t)) \\
;_{\mathcal{A}} \\
(s \in ac' \lhd s.wait \rhd (\mathbf{RA2} \circ \mathbf{RA1} \circ \mathbf{PBMH}(\neg\, Q_f^f \Rightarrow Q_f^t)))
\end{array}\right)
\end{array}\right)
$$

{Predicate calculus}

$$
= \mathbf{RA}\left(\begin{array}{l}
\neg\left(\begin{array}{l}
\mathbf{PBMH}(\mathbf{RA1}\circ\mathbf{PBMH}(P_f^f)\ ;_{\mathcal{A}}\mathbf{RA1}(true)) \\
\vee \\
\mathbf{PBMH}\left(\begin{array}{l}(\mathbf{RA1}\circ\mathbf{PBMH}(P_f^t)) \\ ;_{\mathcal{A}} \\ (\neg\, s.wait \wedge \mathbf{RA2}\circ\mathbf{RA1}\circ\mathbf{PBMH}(Q_f^f))\end{array}\right)
\end{array}\right) \\
\vdash \\
\mathbf{PBMH}\left(\begin{array}{l}(\mathbf{RA1}\circ\mathbf{PBMH}(P_f^t)) \\ ;_{\mathcal{A}} \\ (s\in ac' \lhd s.wait \rhd (\mathbf{RA2}\circ\mathbf{RA1}\circ\mathbf{PBMH}(\neg\, Q_f^f \Rightarrow Q_f^t)))\end{array}\right)
\end{array}\right)
$$

{Distributivity of **PBMH** (Theorem E.2.2)}

$$
= \mathbf{RA}\left(\begin{array}{l}
\neg\,\mathbf{PBMH}\left(\begin{array}{l}
(\mathbf{RA1}\circ\mathbf{PBMH}(P_f^f)\ ;_{\mathcal{A}}\mathbf{RA1}(true)) \\
\vee \\
\left(\begin{array}{l}(\mathbf{RA1}\circ\mathbf{PBMH}(P_f^t)) \\ ;_{\mathcal{A}} \\ (\neg\, s.wait \wedge \mathbf{RA2}\circ\mathbf{RA1}\circ\mathbf{PBMH}(Q_f^f))\end{array}\right)
\end{array}\right) \\
\vdash \\
\mathbf{PBMH}\left(\begin{array}{l}(\mathbf{RA1}\circ\mathbf{PBMH}(P_f^t)) \\ ;_{\mathcal{A}} \\ (s\in ac' \lhd s.wait \rhd (\mathbf{RA2}\circ\mathbf{RA1}\circ\mathbf{PBMH}(\neg\, Q_f^f \Rightarrow Q_f^t)))\end{array}\right)
\end{array}\right)
$$

{Lemma E.6.2 and predicate calculus}

$$
= \mathbf{RA}\circ\mathbf{PBMH}\left(\begin{array}{l}
\left(\begin{array}{l}
\neg\,(\mathbf{RA1}\circ\mathbf{PBMH}(P_f^f)\ ;_{\mathcal{A}}\mathbf{RA1}(true)) \\
\wedge \\
\neg\left(\begin{array}{l}(\mathbf{RA1}\circ\mathbf{PBMH}(P_f^t)) \\ ;_{\mathcal{A}} \\ (\neg\, s.wait \wedge \mathbf{RA2}\circ\mathbf{RA1}\circ\mathbf{PBMH}(Q_f^f))\end{array}\right)
\end{array}\right) \\
\vdash \\
\left(\begin{array}{l}(\mathbf{RA1}\circ\mathbf{PBMH}(P_f^t)) \\ ;_{\mathcal{A}} \\ (s\in ac' \lhd s.wait \rhd (\mathbf{RA2}\circ\mathbf{RA1}\circ\mathbf{PBMH}(\neg\, Q_f^f \Rightarrow Q_f^t)))\end{array}\right)
\end{array}\right)
$$

{Theorem 1.2.27}

$$= \mathbf{RA} \circ \mathbf{A} \left(\begin{array}{l} \left(\begin{array}{l} \neg\ (\mathbf{RA1} \circ \mathbf{PBMH}(P_f^f)\ \ ;_{\mathcal{A}}\ \mathbf{RA1}(\mathit{true})) \\ \wedge \\ \neg \left(\begin{array}{l} (\mathbf{RA1} \circ \mathbf{PBMH}(P_f^t)) \\ ;_{\mathcal{A}} \\ (\neg\ s.\mathit{wait} \wedge \mathbf{RA2} \circ \mathbf{RA1} \circ \mathbf{PBMH}(Q_f^f)) \end{array} \right) \end{array} \right) \\ \vdash \\ \left(\begin{array}{l} (\mathbf{RA1} \circ \mathbf{PBMH}(P_f^t)) \\ ;_{\mathcal{A}} \\ (s \in ac' \lhd s.\mathit{wait} \rhd (\mathbf{RA2} \circ \mathbf{RA1} \circ \mathbf{PBMH}(\neg\ Q_f^f \Rightarrow Q_f^t))) \end{array} \right) \end{array} \right)$$

{Predicate calculus and Theorem E.2.2}

$$= \mathbf{RA} \circ \mathbf{A} \left(\begin{array}{l} \left(\begin{array}{l} \neg\ (\mathbf{RA1} \circ \mathbf{PBMH}(P_f^f)\ \ ;_{\mathcal{A}}\ \mathbf{RA1}(\mathit{true})) \\ \wedge \\ \neg \left(\begin{array}{l} (\mathbf{RA1} \circ \mathbf{PBMH}(P_f^t)) \\ ;_{\mathcal{A}} \\ (\neg\ s.\mathit{wait} \wedge \mathbf{RA2} \circ \mathbf{RA1} \circ \mathbf{PBMH}(Q_f^f)) \end{array} \right) \end{array} \right) \\ \vdash \\ \left(\begin{array}{l} (\mathbf{RA1} \circ \mathbf{PBMH}(P_f^t)) \\ ;_{\mathcal{A}} \\ (s \in ac' \lhd s.\mathit{wait} \rhd (\mathbf{RA2} \circ \mathbf{RA1}(\neg\ \mathbf{PBMH}(Q_f^f) \Rightarrow \mathbf{PBMH}(Q_f^t)))) \end{array} \right) \end{array} \right)$$

{Lemma E.5.1}

$$= \mathbf{RA} \circ \mathbf{A} \left(\begin{array}{l} \left(\begin{array}{l} \neg\ (\mathbf{RA1}(\mathbf{PBMH}(P)_f^f)\ \ ;_{\mathcal{A}}\ \mathbf{RA1}(\mathit{true})) \\ \wedge \\ \neg \left(\begin{array}{l} (\mathbf{RA1}(\mathbf{PBMH}(P)_f^t)) \\ ;_{\mathcal{A}} \\ (\neg\ s.\mathit{wait} \wedge \mathbf{RA2} \circ \mathbf{RA1}(\mathbf{PBMH}(Q)_f^f)) \end{array} \right) \end{array} \right) \\ \vdash \\ \left(\begin{array}{l} (\mathbf{RA1}(\mathbf{PBMH}(P)_f^t)) \\ ;_{\mathcal{A}} \\ (s \in ac' \lhd s.\mathit{wait} \rhd (\mathbf{RA2} \circ \mathbf{RA1}(\neg\ \mathbf{PBMH}(Q)_f^f \Rightarrow \mathbf{PBMH}(Q)_f^t))) \end{array} \right) \end{array} \right)$$

{Assumption: P and Q are **RAP**-healthy and Theorem 1.3.2}

$$= \mathbf{RA} \circ \mathbf{A} \left(\begin{array}{l} \left(\begin{array}{l} \neg\ (\mathbf{RA1}(P_f^f)\ \ ;_{\mathcal{A}}\ \mathbf{RA1}(\mathit{true})) \\ \wedge \\ \neg\ (\mathbf{RA1}(P_f^t)\ \ ;_{\mathcal{A}}\ (\neg\ s.\mathit{wait} \wedge \mathbf{RA2} \circ \mathbf{RA1}(Q_f^f))) \end{array} \right) \\ \vdash \\ \mathbf{RA1}(P_f^t)\ \ ;_{\mathcal{A}}\ (s \in ac' \lhd s.\mathit{wait} \rhd (\mathbf{RA2} \circ \mathbf{RA1}(\neg\ Q_f^f \Rightarrow Q_f^t))) \end{array} \right)$$

□

The following have been revised:

Theorem 1.5.16 *Provided* $\neg\ P$, $\neg\ R$, Q *and* S *are* **PBMH***-healthy and* ok, ok' *are not free in* P, Q, R *and* S.

$$\mathbf{RA}(P \vdash Q)\ ;_{\mathcal{D}_{\mathbf{ac}}} \mathbf{RA}(R \vdash S) = \mathbf{RA}\left(\begin{array}{l}\left(\begin{array}{l}\neg\ (\mathbf{RA1}(\neg\ P)\ ;_{\mathcal{A}} \mathbf{RA1}(true)) \\ \wedge \\ \neg\ (\mathbf{RA1}(Q)\ ;_{\mathcal{A}} (\neg\ s.wait \wedge \mathbf{RA2} \circ \mathbf{RA1}(\neg\ R)))\end{array}\right) \\ \vdash \\ \mathbf{RA1}(Q)\ ;_{\mathcal{A}} (s \in ac' \lhd s.wait \rhd \mathbf{RA2} \circ \mathbf{RA1}(R \Rightarrow S))\end{array}\right)$$

Proof.

$$\begin{array}{ll}
& \mathbf{RA}(P \vdash Q)\ ;_{\mathcal{D}_{\mathbf{ac}}} \mathbf{RA}(R \vdash S) \qquad \{\text{Definition of } \mathbf{RA}\} \\
= & \mathbf{RA3} \circ \mathbf{RA2} \circ \mathbf{RA1}(P \vdash Q)\ ;_{\mathcal{D}_{\mathbf{ac}}} \mathbf{RA3} \circ \mathbf{RA2} \circ \mathbf{RA1}(R \vdash S) \\
& \qquad \{\text{Commutativity of } \mathbf{RA1}\text{-}\mathbf{RA2} \text{ (Theorem 1.2.12)}\} \\
= & \mathbf{RA3} \circ \mathbf{RA1} \circ \mathbf{RA2}(P \vdash Q)\ ;_{\mathcal{D}_{\mathbf{ac}}} \mathbf{RA3} \circ \mathbf{RA1} \circ \mathbf{RA2}(R \vdash S) \\
& \qquad \{\text{Commutativity of } \mathbf{RA1}\text{-}\mathbf{RA3} \text{ (Theorem 1.2.21)}\} \\
= & \mathbf{RA1} \circ \mathbf{RA3} \circ \mathbf{RA2}(P \vdash Q)\ ;_{\mathcal{D}_{\mathbf{ac}}} \mathbf{RA1} \circ \mathbf{RA3} \circ \mathbf{RA2}(R \vdash S) \\
& \qquad \{\text{Lemma B.2.10}\} \\
= & \left(\begin{array}{l}\mathbf{RA1} \circ \mathbf{RA3}(\neg\ \mathbf{RA2}(\neg\ P) \vdash \mathbf{RA2}(Q)) \\ ;_{\mathcal{D}_{\mathbf{ac}}} \\ \mathbf{RA1} \circ \mathbf{RA3}(\neg\ \mathbf{RA2}(\neg\ R) \vdash \mathbf{RA2}(S))\end{array}\right) \qquad \{\text{Lemma B.4.2}\} \\
= & \left(\begin{array}{l}\mathbf{RA1}(true \lhd s.wait \rhd (\neg\ \mathbf{RA2}(\neg\ P)) \vdash s \in ac' \lhd s.wait \rhd \mathbf{RA2}(Q)) \\ ;_{\mathcal{D}_{\mathbf{ac}}} \\ \mathbf{RA1}(true \lhd s.wait \rhd (\neg\ \mathbf{RA2}(\neg\ R)) \vdash s \in ac' \lhd s.wait \rhd \mathbf{RA2}(S))\end{array}\right) \\
& \qquad \{\text{Theorem 1.5.17}\}
\end{array}$$

$$
= \mathbf{RA1}\left(\begin{array}{l}
\left(\begin{array}{l}
\left(\begin{array}{l}
\neg\,(\mathbf{RA1}(\neg\,(\mathit{true} \lhd s.\mathit{wait} \rhd \neg\,\mathbf{RA2}(\neg\,P)))\ ;_{\mathcal{A}}\ \mathbf{RA1}(\mathit{true}))\\
\wedge\\
\neg\left(\begin{array}{l}
\mathbf{RA1}(s \in ac' \lhd s.\mathit{wait} \rhd \mathbf{RA2}(Q))\\
;_{\mathcal{A}}\\
\mathbf{RA1}(\neg\,(\mathit{true} \lhd s.\mathit{wait} \rhd (\neg\,\mathbf{RA2}(\neg\,R))))
\end{array}\right)
\end{array}\right)\\
\vdash\\
\left(\begin{array}{l}
\mathbf{RA1}(s \in ac' \lhd s.\mathit{wait} \rhd \mathbf{RA2}(Q))\\
;_{\mathcal{A}}\\
\mathbf{RA1}\left(\begin{array}{l}
(\mathit{true} \lhd s.\mathit{wait} \rhd (\neg\,\mathbf{RA2}(\neg\,R)))\\
\Rightarrow\\
(s \in ac' \lhd s.\mathit{wait} \rhd \mathbf{RA2}(S))
\end{array}\right)
\end{array}\right)
\end{array}\right)
$$

{Predicate calculus}

$$
= \mathbf{RA1}\left(\begin{array}{l}
\left(\begin{array}{l}
\left(\begin{array}{l}
\neg\,(\mathbf{RA1}(\neg\,(\mathit{true} \lhd s.\mathit{wait} \rhd \neg\,\mathbf{RA2}(\neg\,P)))\ ;_{\mathcal{A}}\ \mathbf{RA1}(\mathit{true}))\\
\wedge\\
\neg\left(\begin{array}{l}
\mathbf{RA1}(s \in ac' \lhd s.\mathit{wait} \rhd \mathbf{RA2}(Q))\\
;_{\mathcal{A}}\\
\mathbf{RA1}(\neg\,(\mathit{true} \lhd s.\mathit{wait} \rhd (\neg\,\mathbf{RA2}(\neg\,R))))
\end{array}\right)
\end{array}\right)\\
\vdash\\
\left(\begin{array}{l}
\mathbf{RA1}(s \in ac' \lhd s.\mathit{wait} \rhd \mathbf{RA2}(Q))\\
;_{\mathcal{A}}\\
\mathbf{RA1}\left(\begin{array}{l}
\neg\,(\mathit{true} \lhd s.\mathit{wait} \rhd (\neg\,\mathbf{RA2}(\neg\,R)))\\
\vee\\
(s \in ac' \lhd s.\mathit{wait} \rhd \mathbf{RA2}(S))
\end{array}\right)
\end{array}\right)
\end{array}\right)
$$

{Lemma B.4.3 and predicate calculus}

$$
= \mathbf{RA1}\left(\begin{array}{l}
\left(\begin{array}{l}
\left(\begin{array}{l}
\neg\,(\mathbf{RA1}(\mathit{false} \lhd s.\mathit{wait} \rhd \mathbf{RA2}(\neg\,P))\ ;_{\mathcal{A}}\ \mathbf{RA1}(\mathit{true}))\\
\wedge\\
\neg\left(\begin{array}{l}
\mathbf{RA1}(s \in ac' \lhd s.\mathit{wait} \rhd \mathbf{RA2}(Q))\\
;_{\mathcal{A}}\\
\mathbf{RA1}(\mathit{false} \lhd s.\mathit{wait} \rhd \mathbf{RA2}(\neg\,R))
\end{array}\right)
\end{array}\right)\\
\vdash\\
\left(\begin{array}{l}
\mathbf{RA1}(s \in ac' \lhd s.\mathit{wait} \rhd \mathbf{RA2}(Q))\\
;_{\mathcal{A}}\\
\mathbf{RA1}\left(\begin{array}{l}
(\mathit{false} \lhd s.\mathit{wait} \rhd \mathbf{RA2}(\neg\,R))\\
\vee\\
(s \in ac' \lhd s.\mathit{wait} \rhd \mathbf{RA2}(S))
\end{array}\right)
\end{array}\right)
\end{array}\right)
$$

{Property of conditional and predicate calculus}

$$= \mathbf{RA1}\left(\begin{array}{l} \left(\begin{array}{l} \neg\ (\mathbf{RA1}(\mathit{false} \lhd s.\mathit{wait} \rhd \mathbf{RA2}(\neg\ P))\ \ ;_{\mathcal{A}}\ \mathbf{RA1}(\mathit{true})) \\ \wedge \\ \neg\ \left(\begin{array}{l} \mathbf{RA1}(s \in ac' \lhd s.\mathit{wait} \rhd \mathbf{RA2}(Q)) \\ ;_{\mathcal{A}} \\ \mathbf{RA1}(\mathit{false} \lhd s.\mathit{wait} \rhd \mathbf{RA2}(\neg\ R)) \end{array}\right) \end{array}\right) \\ \vdash \\ \left(\begin{array}{l} \mathbf{RA1}(s \in ac' \lhd s.\mathit{wait} \rhd \mathbf{RA2}(Q)) \\ ;_{\mathcal{A}} \\ \mathbf{RA1}(s \in ac' \lhd s.\mathit{wait} \rhd (\mathbf{RA2}(S) \vee \mathbf{RA2}(\neg\ R))) \end{array}\right) \end{array}\right)$$

{Theorem 1.2.10 and predicate calculus}

$$= \mathbf{RA1}\left(\begin{array}{l} \left(\begin{array}{l} \neg\ (\mathbf{RA1}(\mathit{false} \lhd s.\mathit{wait} \rhd \mathbf{RA2}(\neg\ P))\ \ ;_{\mathcal{A}}\ \mathbf{RA1}(\mathit{true})) \\ \wedge \\ \neg\ \left(\begin{array}{l} \mathbf{RA1}(s \in ac' \lhd s.\mathit{wait} \rhd \mathbf{RA2}(Q)) \\ ;_{\mathcal{A}} \\ \mathbf{RA1}(\mathit{false} \lhd s.\mathit{wait} \rhd \mathbf{RA2}(\neg\ R)) \end{array}\right) \end{array}\right) \\ \vdash \\ \left(\begin{array}{l} \mathbf{RA1}(s \in ac' \lhd s.\mathit{wait} \rhd \mathbf{RA2}(Q)) \\ ;_{\mathcal{A}} \\ \mathbf{RA1}(s \in ac' \lhd s.\mathit{wait} \rhd (\mathbf{RA2}(R \Rightarrow S))) \end{array}\right) \end{array}\right)$$

{Lemma B.1.10}

$$= \mathbf{RA1}\left(\begin{array}{l} \left(\begin{array}{l} \neg\ ((\mathbf{RA1}(\mathit{false}) \lhd s.\mathit{wait} \rhd \mathbf{RA1} \circ \mathbf{RA2}(\neg\ P))\ \ ;_{\mathcal{A}}\ \mathbf{RA1}(\mathit{true})) \\ \wedge \\ \neg\ \left(\begin{array}{l} (\mathbf{RA1}(s \in ac') \lhd s.\mathit{wait} \rhd \mathbf{RA1} \circ \mathbf{RA2}(Q)) \\ ;_{\mathcal{A}} \\ (\mathbf{RA1}(\mathit{false}) \lhd s.\mathit{wait} \rhd \mathbf{RA1} \circ \mathbf{RA2}(\neg\ R)) \end{array}\right) \end{array}\right) \\ \vdash \\ \left(\begin{array}{l} (\mathbf{RA1}(s \in ac') \lhd s.\mathit{wait} \rhd \mathbf{RA1} \circ \mathbf{RA2}(Q)) \\ ;_{\mathcal{A}} \\ (\mathbf{RA1}(s \in ac') \lhd s.\mathit{wait} \rhd \mathbf{RA1} \circ \mathbf{RA2}(R \Rightarrow S)) \end{array}\right) \end{array}\right)$$

{Lemmas B.1.4 and B.1.9}

$$
\begin{array}{l}
= \mathbf{RA1}\left(\begin{array}{l}
\left(\begin{array}{l}
\neg\ ((\mathit{false} \lhd s.\mathit{wait} \rhd \mathbf{RA1} \circ \mathbf{RA2}(\neg\ P))\ \ ;_{\mathcal{A}}\ \mathbf{RA1}(\mathit{true})) \\
\wedge \\
\neg\ \left(\begin{array}{l}
(s \in ac' \lhd s.\mathit{wait} \rhd \mathbf{RA1} \circ \mathbf{RA2}(Q)) \\
\ ;_{\mathcal{A}} \\
(\mathit{false} \lhd s.\mathit{wait} \rhd \mathbf{RA1} \circ \mathbf{RA2}(\neg\ R))
\end{array}\right)
\end{array}\right) \\
\vdash \\
\left(\begin{array}{l}
(s \in ac' \lhd s.\mathit{wait} \rhd \mathbf{RA1} \circ \mathbf{RA2}(Q)) \\
\ ;_{\mathcal{A}} \\
(s \in ac' \lhd s.\mathit{wait} \rhd \mathbf{RA1} \circ \mathbf{RA2}(R \Rightarrow S))
\end{array}\right)
\end{array}\right) \\
\qquad\qquad \{\text{Property of conditional}\} \\
= \mathbf{RA1}\left(\begin{array}{l}
\left(\begin{array}{l}
\neg\ ((\neg\ s.\mathit{wait} \wedge \mathbf{RA1} \circ \mathbf{RA2}(\neg\ P))\ \ ;_{\mathcal{A}}\ \mathbf{RA1}(\mathit{true})) \\
\wedge \\
\neg\ \left(\begin{array}{l}
(s \in ac' \lhd s.\mathit{wait} \rhd \mathbf{RA1} \circ \mathbf{RA2}(Q)) \\
\ ;_{\mathcal{A}} \\
(\neg\ s.\mathit{wait} \wedge \mathbf{RA1} \circ \mathbf{RA2}(\neg\ R))
\end{array}\right)
\end{array}\right) \\
\vdash \\
\left(\begin{array}{l}
(s \in ac' \lhd s.\mathit{wait} \rhd \mathbf{RA1} \circ \mathbf{RA2}(Q)) \\
\ ;_{\mathcal{A}} \\
(s \in ac' \lhd s.\mathit{wait} \rhd \mathbf{RA1} \circ \mathbf{RA2}(R \Rightarrow S))
\end{array}\right)
\end{array}\right) \\
\qquad\qquad \{\text{Lemma B.4.1}\} \\
= \mathbf{RA1}\left(\begin{array}{l}
\left(\begin{array}{l}
\neg\ ((\neg\ s.\mathit{wait} \wedge \mathbf{RA1} \circ \mathbf{RA2}(\neg\ P))\ \ ;_{\mathcal{A}}\ \mathbf{RA1}(\mathit{true})) \\
\wedge \\
\neg\ \left(\begin{array}{l}
(s \in ac'\ \ ;_{\mathcal{A}}\ (\neg\ s.\mathit{wait} \wedge \mathbf{RA1} \circ \mathbf{RA2}(\neg\ R))) \\
\lhd s.\mathit{wait} \rhd \\
(\mathbf{RA1} \circ \mathbf{RA2}(Q)\ \ ;_{\mathcal{A}}\ (\neg\ s.\mathit{wait} \wedge \mathbf{RA1} \circ \mathbf{RA2}(\neg\ R)))
\end{array}\right)
\end{array}\right) \\
\vdash \\
\left(\begin{array}{l}
(s \in ac'\ \ ;_{\mathcal{A}}\ (s \in ac' \lhd s.\mathit{wait} \rhd \mathbf{RA1} \circ \mathbf{RA2}(R \Rightarrow S))) \\
\lhd s.\mathit{wait} \rhd \\
(\mathbf{RA1} \circ \mathbf{RA2}(Q)\ \ ;_{\mathcal{A}}\ (s \in ac' \lhd s.\mathit{wait} \rhd \mathbf{RA1} \circ \mathbf{RA2}(R \Rightarrow S)))
\end{array}\right)
\end{array}\right) \\
\qquad\qquad \{\text{Lemma F.6.2}\}
\end{array}
$$

$$= \mathbf{RA1}\left(\begin{array}{l} \left(\begin{array}{l} \neg\,((\neg\, s.wait \wedge \mathbf{RA1} \circ \mathbf{RA2}(\neg\, P))\ ;_{\mathcal{A}}\ \mathbf{RA1}(true)) \\ \wedge \\ \neg\ \left(\begin{array}{l} (\neg\, s.wait \wedge \mathbf{RA1} \circ \mathbf{RA2}(\neg\, R)) \\ \lhd s.wait \rhd \\ (\mathbf{RA1} \circ \mathbf{RA2}(Q)\ ;_{\mathcal{A}}\ (\neg\, s.wait \wedge \mathbf{RA1} \circ \mathbf{RA2}(\neg\, R))) \end{array}\right) \end{array}\right) \\ \vdash \\ \left(\begin{array}{l} (s \in ac' \lhd s.wait \rhd \mathbf{RA1} \circ \mathbf{RA2}(R \Rightarrow S)) \\ \lhd s.wait \rhd \\ (\mathbf{RA1} \circ \mathbf{RA2}(Q)\ ;_{\mathcal{A}}\ (s \in ac' \lhd s.wait \rhd \mathbf{RA1} \circ \mathbf{RA2}(R \Rightarrow S))) \end{array}\right) \end{array}\right)$$

{Lemma F.2.7}

$$= \mathbf{RA1}\left(\begin{array}{l} \left(\begin{array}{l} \neg\,(\neg\, s.wait \wedge (\mathbf{RA1} \circ \mathbf{RA2}(\neg\, P)\ ;_{\mathcal{A}}\ \mathbf{RA1}(true))) \\ \wedge \\ \neg\ \left(\begin{array}{l} (\neg\, s.wait \wedge \mathbf{RA1} \circ \mathbf{RA2}(\neg\, R)) \\ \lhd s.wait \rhd \\ (\mathbf{RA1} \circ \mathbf{RA2}(Q)\ ;_{\mathcal{A}}\ (\neg\, s.wait \wedge \mathbf{RA1} \circ \mathbf{RA2}(\neg\, R))) \end{array}\right) \end{array}\right) \\ \vdash \\ \left(\begin{array}{l} (s \in ac' \lhd s.wait \rhd \mathbf{RA1} \circ \mathbf{RA2}(R \Rightarrow S)) \\ \lhd s.wait \rhd \\ (\mathbf{RA1} \circ \mathbf{RA2}(Q)\ ;_{\mathcal{A}}\ (s \in ac' \lhd s.wait \rhd \mathbf{RA1} \circ \mathbf{RA2}(R \Rightarrow S))) \end{array}\right) \end{array}\right)$$

{Property of conditional}

$$= \mathbf{RA1}\left(\begin{array}{l} \left(\begin{array}{l} \neg\,(\neg\, s.wait \wedge (\mathbf{RA1} \circ \mathbf{RA2}(\neg\, P)\ ;_{\mathcal{A}}\ \mathbf{RA1}(true))) \\ \wedge \\ \neg\ \left(\neg\, s.wait \wedge \left(\begin{array}{l} \mathbf{RA1} \circ \mathbf{RA2}(Q) \\ ;_{\mathcal{A}} \\ (\neg\, s.wait \wedge \mathbf{RA1} \circ \mathbf{RA2}(\neg\, R)) \end{array}\right)\right) \end{array}\right) \\ \vdash \\ \left(\begin{array}{l} (s \in ac') \\ \lhd s.wait \rhd \\ (\mathbf{RA1} \circ \mathbf{RA2}(Q)\ ;_{\mathcal{A}}\ (s \in ac' \lhd s.wait \rhd \mathbf{RA1} \circ \mathbf{RA2}(R \Rightarrow S))) \end{array}\right) \end{array}\right)$$

{Predicate calculus}

$$= \mathbf{RA1}\left(\begin{array}{l} \neg\left(\begin{array}{l}(\neg\, s.wait \wedge (\mathbf{RA1} \circ \mathbf{RA2}(\neg\, P)\ ;_{\mathcal{A}} \mathbf{RA1}(true))) \\ \vee \\ \left(\neg\, s.wait \wedge \left(\begin{array}{l}\mathbf{RA1} \circ \mathbf{RA2}(Q) \\ ;_{\mathcal{A}} \\ (\neg\, s.wait \wedge \mathbf{RA1} \circ \mathbf{RA2}(\neg\, R))\end{array}\right)\right)\end{array}\right) \\ \vdash \\ \left(\begin{array}{l}(s \in ac') \\ \lhd s.wait \rhd \\ (\mathbf{RA1} \circ \mathbf{RA2}(Q)\ ;_{\mathcal{A}} (s \in ac' \lhd s.wait \rhd \mathbf{RA1} \circ \mathbf{RA2}(R \Rightarrow S)))\end{array}\right)\end{array}\right)$$

{Predicate calculus and property of conditional}

$$= \mathbf{RA1}\left(\begin{array}{l} \neg\left(\begin{array}{l}false \lhd s.wait \rhd \left(\begin{array}{l}(\mathbf{RA1} \circ \mathbf{RA2}(\neg\, P)\ ;_{\mathcal{A}} \mathbf{RA1}(true)) \\ \vee \\ \left(\begin{array}{l}\mathbf{RA1} \circ \mathbf{RA2}(Q) \\ ;_{\mathcal{A}} \\ (\neg\, s.wait \wedge \mathbf{RA1} \circ \mathbf{RA2}(\neg\, R))\end{array}\right)\end{array}\right)\end{array}\right) \\ \vdash \\ \left(\begin{array}{l}(s \in ac') \\ \lhd s.wait \rhd \\ (\mathbf{RA1} \circ \mathbf{RA2}(Q)\ ;_{\mathcal{A}} (s \in ac' \lhd s.wait \rhd \mathbf{RA1} \circ \mathbf{RA2}(R \Rightarrow S)))\end{array}\right)\end{array}\right)$$

{Lemma B.4.4}

$$= \mathbf{RA1}\left(\begin{array}{l} \left(\begin{array}{l}true \lhd s.wait \rhd \neg \left(\begin{array}{l}(\mathbf{RA1} \circ \mathbf{RA2}(\neg\, P)\ ;_{\mathcal{A}} \mathbf{RA1}(true)) \\ \vee \\ \left(\begin{array}{l}\mathbf{RA1} \circ \mathbf{RA2}(Q) \\ ;_{\mathcal{A}} \\ (\neg\, s.wait \wedge \mathbf{RA1} \circ \mathbf{RA2}(\neg\, R))\end{array}\right)\end{array}\right)\end{array}\right) \\ \vdash \\ \left(\begin{array}{l}(s \in ac') \\ \lhd s.wait \rhd \\ (\mathbf{RA1} \circ \mathbf{RA2}(Q)\ ;_{\mathcal{A}} (s \in ac' \lhd s.wait \rhd \mathbf{RA1} \circ \mathbf{RA2}(R \Rightarrow S)))\end{array}\right)\end{array}\right)$$

{Lemma B.4.2}

$$
\begin{array}{l}
= \mathbf{RA1} \circ \mathbf{RA3} \left(\begin{array}{l} \neg \left(\begin{array}{l} (\mathbf{RA1} \circ \mathbf{RA2}(\neg\, P) \;\; ;_{\mathcal{A}} \mathbf{RA1}(\mathit{true})) \\ \vee \\ \left(\begin{array}{l} \mathbf{RA1} \circ \mathbf{RA2}(Q) \\ \;\; ;_{\mathcal{A}} \\ (\neg\, s.\mathit{wait} \wedge \mathbf{RA1} \circ \mathbf{RA2}(\neg\, R)) \end{array} \right) \end{array} \right) \\ \vdash \\ \left(\begin{array}{l} \mathbf{RA1} \circ \mathbf{RA2}(Q) \\ \;\; ;_{\mathcal{A}} \\ (s \in ac' \lhd s.\mathit{wait} \rhd \mathbf{RA1} \circ \mathbf{RA2}(R \Rightarrow S)) \end{array} \right) \end{array} \right) \\
\qquad\qquad \{\text{Lemmas B.2.2, B.2.3, B.2.7 and B.2.8}\} \\
= \mathbf{RA1} \circ \mathbf{RA3} \left(\begin{array}{l} \neg \left(\begin{array}{l} (\mathbf{RA1} \circ \mathbf{RA2}(\neg\, P) \;\; ;_{\mathcal{A}} \mathbf{RA1} \circ \mathbf{RA2}(\mathit{true})) \\ \vee \\ \left(\begin{array}{l} \mathbf{RA1} \circ \mathbf{RA2}(Q) \\ \;\; ;_{\mathcal{A}} \\ (\mathbf{RA2}(\neg\, s.\mathit{wait}) \wedge \mathbf{RA1} \circ \mathbf{RA2}(\neg\, R)) \end{array} \right) \end{array} \right) \\ \vdash \\ \left(\begin{array}{l} \mathbf{RA1} \circ \mathbf{RA2}(Q) \\ \;\; ;_{\mathcal{A}} \\ (\mathbf{RA2}(s \in ac') \lhd \mathbf{RA2}(s.\mathit{wait}) \rhd \mathbf{RA1} \circ \mathbf{RA2}(R \Rightarrow S)) \end{array} \right) \end{array} \right) \\
\qquad\qquad \{\text{Theorem 1.2.12}\} \\
= \mathbf{RA1} \circ \mathbf{RA3} \left(\begin{array}{l} \neg \left(\begin{array}{l} (\mathbf{RA2} \circ \mathbf{RA1}(\neg\, P) \;\; ;_{\mathcal{A}} \mathbf{RA2} \circ \mathbf{RA1}(\mathit{true})) \\ \vee \\ \left(\begin{array}{l} \mathbf{RA2} \circ \mathbf{RA1}(Q) \\ \;\; ;_{\mathcal{A}} \\ (\mathbf{RA2}(\neg\, s.\mathit{wait}) \wedge \mathbf{RA2} \circ \mathbf{RA1}(\neg\, R)) \end{array} \right) \end{array} \right) \\ \vdash \\ \left(\begin{array}{l} \mathbf{RA2} \circ \mathbf{RA1}(Q) \\ \;\; ;_{\mathcal{A}} \\ (\mathbf{RA2}(s \in ac') \lhd \mathbf{RA2}(s.\mathit{wait}) \rhd \mathbf{RA2} \circ \mathbf{RA1}(R \Rightarrow S)) \end{array} \right) \end{array} \right) \\
\qquad\qquad \{\text{Theorem 1.2.9}\}
\end{array}
$$

$$= \mathbf{RA1} \circ \mathbf{RA3} \left(\begin{array}{l} \neg \left(\begin{array}{l} (\mathbf{RA2} \circ \mathbf{RA1}(\neg\, P) \;\; ;_{\mathcal{A}} \mathbf{RA2} \circ \mathbf{RA1}(\mathit{true})) \\ \vee \\ \left(\begin{array}{l} \mathbf{RA2} \circ \mathbf{RA1}(Q) \\ \;\; ;_{\mathcal{A}} \\ (\mathbf{RA2}(\neg\, s.\mathit{wait} \wedge \mathbf{RA1}(\neg\, R)) \end{array} \right) \end{array} \right) \\ \vdash \\ \left(\begin{array}{l} \mathbf{RA2} \circ \mathbf{RA1}(Q) \\ \;\; ;_{\mathcal{A}} \\ (\mathbf{RA2}(s \in ac') \lhd \mathbf{RA2}(s.\mathit{wait}) \rhd \mathbf{RA2} \circ \mathbf{RA1}(R \Rightarrow S)) \end{array} \right) \end{array} \right)$$

{Lemma B.2.6}

$$= \mathbf{RA1} \circ \mathbf{RA3} \left(\begin{array}{l} \neg \left(\begin{array}{l} (\mathbf{RA2} \circ \mathbf{RA1}(\neg\, P) \;\; ;_{\mathcal{A}} \mathbf{RA2} \circ \mathbf{RA1}(\mathit{true})) \\ \vee \\ \left(\begin{array}{l} \mathbf{RA2} \circ \mathbf{RA1}(Q) \\ \;\; ;_{\mathcal{A}} \\ (\mathbf{RA2}(\neg\, s.\mathit{wait} \wedge \mathbf{RA1}(\neg\, R)) \end{array} \right) \end{array} \right) \\ \vdash \\ \left(\begin{array}{l} \mathbf{RA2} \circ \mathbf{RA1}(Q) \\ \;\; ;_{\mathcal{A}} \\ \mathbf{RA2}(s \in ac' \lhd s.\mathit{wait} \rhd \mathbf{RA1}(R \Rightarrow S)) \end{array} \right) \end{array} \right)$$

{Theorem B.2.1}

$$= \mathbf{RA1} \circ \mathbf{RA3} \left(\begin{array}{l} \neg \left(\begin{array}{l} \mathbf{RA2}(\mathbf{RA1}(\neg\, P) \;\; ;_{\mathcal{A}} \mathbf{RA2} \circ \mathbf{RA1}(\mathit{true})) \\ \vee \\ \mathbf{RA2} \left(\begin{array}{l} \mathbf{RA1}(Q) \\ \;\; ;_{\mathcal{A}} \\ (\mathbf{RA2}(\neg\, s.\mathit{wait} \wedge \mathbf{RA1}(\neg\, R)) \end{array} \right) \end{array} \right) \\ \vdash \\ \mathbf{RA2} \left(\begin{array}{l} \mathbf{RA1}(Q) \\ \;\; ;_{\mathcal{A}} \\ \mathbf{RA2}(s \in ac' \lhd s.\mathit{wait} \rhd \mathbf{RA1}(R \Rightarrow S)) \end{array} \right) \end{array} \right)$$

{Theorem 1.2.10}

$$= \mathbf{RA1} \circ \mathbf{RA3} \left(\begin{array}{l} \neg\, \mathbf{RA2} \left(\begin{array}{l} (\mathbf{RA1}(\neg\, P)\ ;_{\mathcal{A}} \mathbf{RA2} \circ \mathbf{RA1}(\mathit{true})) \\ \vee \\ \left(\begin{array}{l} \mathbf{RA1}(Q) \\ ;_{\mathcal{A}} \\ (\mathbf{RA2}(\neg\, s.\mathit{wait} \wedge \mathbf{RA1}(\neg\, R)) \end{array} \right) \end{array} \right) \\ \vdash \\ \mathbf{RA2} \left(\begin{array}{l} \mathbf{RA1}(Q) \\ ;_{\mathcal{A}} \\ \mathbf{RA2}(s \in ac' \lhd s.\mathit{wait} \rhd \mathbf{RA1}(R \Rightarrow S)) \end{array} \right) \end{array} \right)$$

{Lemma B.2.10}

$$= \mathbf{RA1} \circ \mathbf{RA3} \circ \mathbf{RA2} \left(\begin{array}{l} \neg \left(\begin{array}{l} (\mathbf{RA1}(\neg\, P)\ ;_{\mathcal{A}} \mathbf{RA2} \circ \mathbf{RA1}(\mathit{true})) \\ \vee \\ \left(\begin{array}{l} \mathbf{RA1}(Q) \\ ;_{\mathcal{A}} \\ (\mathbf{RA2}(\neg\, s.\mathit{wait} \wedge \mathbf{RA1}(\neg\, R)) \end{array} \right) \end{array} \right) \\ \vdash \\ \left(\begin{array}{l} \mathbf{RA1}(Q) \\ ;_{\mathcal{A}} \\ \mathbf{RA2}(s \in ac' \lhd s.\mathit{wait} \rhd \mathbf{RA1}(R \Rightarrow S)) \end{array} \right) \end{array} \right)$$

{Commutativity of **RA1**-**RA3** (Theorems 1.2.12 and 1.2.21)}

$$= \mathbf{RA3} \circ \mathbf{RA2} \circ \mathbf{RA1} \left(\begin{array}{l} \neg \left(\begin{array}{l} (\mathbf{RA1}(\neg\, P)\ ;_{\mathcal{A}} \mathbf{RA2} \circ \mathbf{RA1}(\mathit{true})) \\ \vee \\ \left(\begin{array}{l} \mathbf{RA1}(Q) \\ ;_{\mathcal{A}} \\ (\mathbf{RA2}(\neg\, s.\mathit{wait} \wedge \mathbf{RA1}(\neg\, R)) \end{array} \right) \end{array} \right) \\ \vdash \\ \left(\begin{array}{l} \mathbf{RA1}(Q) \\ ;_{\mathcal{A}} \\ \mathbf{RA2}(s \in ac' \lhd s.\mathit{wait} \rhd \mathbf{RA1}(R \Rightarrow S)) \end{array} \right) \end{array} \right)$$

{Definition of **RA**}

$$= \mathbf{RA}\left(\begin{array}{l} \neg\left(\begin{array}{l}(\mathbf{RA1}(\neg\ P)\ ;_{\mathcal{A}}\ \mathbf{RA2}\circ\mathbf{RA1}(\mathit{true}))\\ \vee\\ \left(\begin{array}{l}\mathbf{RA1}(Q)\\ ;_{\mathcal{A}}\\ (\mathbf{RA2}(\neg\ s.\mathit{wait}\wedge\mathbf{RA1}(\neg\ R))\end{array}\right)\end{array}\right)\\ \vdash\\ \left(\begin{array}{l}\mathbf{RA1}(Q)\\ ;_{\mathcal{A}}\\ \mathbf{RA2}(s\in ac'\lhd s.\mathit{wait}\rhd\mathbf{RA1}(R\Rightarrow S))\end{array}\right)\end{array}\right)$$

{Predicate calculus}

$$= \mathbf{RA}\left(\begin{array}{l}\left(\begin{array}{l}\neg\ (\mathbf{RA1}(\neg\ P)\ ;_{\mathcal{A}}\ \mathbf{RA2}\circ\mathbf{RA1}(\mathit{true}))\\ \wedge\\ \neg\ (\mathbf{RA1}(Q)\ ;_{\mathcal{A}}\ (\mathbf{RA2}(\neg\ s.\mathit{wait}\wedge\mathbf{RA1}(\neg\ R))))\end{array}\right)\\ \vdash\\ \mathbf{RA1}(Q)\ ;_{\mathcal{A}}\ \mathbf{RA2}(s\in ac'\lhd s.\mathit{wait}\rhd\mathbf{RA1}(R\Rightarrow S))\end{array}\right)$$

{Theorem 1.2.9 and Lemma B.2.8}

$$= \mathbf{RA}\left(\begin{array}{l}\left(\begin{array}{l}\neg\ (\mathbf{RA1}(\neg\ P)\ ;_{\mathcal{A}}\ \mathbf{RA2}\circ\mathbf{RA1}(\mathit{true}))\\ \wedge\\ \neg\ (\mathbf{RA1}(Q)\ ;_{\mathcal{A}}\ (\neg\ s.\mathit{wait}\wedge\mathbf{RA2}\circ\mathbf{RA1}(\neg\ R)))\end{array}\right)\\ \vdash\\ \mathbf{RA1}(Q)\ ;_{\mathcal{A}}\ \mathbf{RA2}(s\in ac'\lhd s.\mathit{wait}\rhd\mathbf{RA1}(R\Rightarrow S))\end{array}\right)$$

{Lemma B.2.6}

$$= \mathbf{RA}\left(\begin{array}{l}\left(\begin{array}{l}\neg\ (\mathbf{RA1}(\neg\ P)\ ;_{\mathcal{A}}\ \mathbf{RA2}\circ\mathbf{RA1}(\mathit{true}))\\ \wedge\\ \neg\ (\mathbf{RA1}(Q)\ ;_{\mathcal{A}}\ (\neg\ s.\mathit{wait}\wedge\mathbf{RA2}\circ\mathbf{RA1}(\neg\ R)))\end{array}\right)\\ \vdash\\ \mathbf{RA1}(Q)\ ;_{\mathcal{A}}\ (\mathbf{RA2}(s\in ac')\lhd s.\mathit{wait}\rhd\mathbf{RA2}\circ\mathbf{RA1}(R\Rightarrow S))\end{array}\right)$$

{Lemma B.2.3}

$$= \mathbf{RA}\left(\begin{array}{l}\left(\begin{array}{l}\neg\ (\mathbf{RA1}(\neg\ P)\ ;_{\mathcal{A}}\ \mathbf{RA2}\circ\mathbf{RA1}(\mathit{true}))\\ \wedge\\ \neg\ (\mathbf{RA1}(Q)\ ;_{\mathcal{A}}\ (\neg\ s.\mathit{wait}\wedge\mathbf{RA2}\circ\mathbf{RA1}(\neg\ R)))\end{array}\right)\\ \vdash\\ \mathbf{RA1}(Q)\ ;_{\mathcal{A}}\ (s\in ac'\lhd s.\mathit{wait}\rhd\mathbf{RA2}\circ\mathbf{RA1}(R\Rightarrow S))\end{array}\right)$$

{Theorem 1.2.12 and Lemma B.2.2}

$$= \mathbf{RA}\left(\begin{array}{l} \left(\begin{array}{l} \neg\,(\mathbf{RA1}(\neg\ P)\ ;_{\mathcal{A}}\ \mathbf{RA1}(\mathit{true})) \\ \wedge \\ \neg\,(\mathbf{RA1}(Q)\ ;_{\mathcal{A}}\ (\neg\ s.\mathit{wait} \wedge \mathbf{RA2} \circ \mathbf{RA1}(\neg\ R))) \end{array}\right) \\ \vdash \\ \mathbf{RA1}(Q)\ ;_{\mathcal{A}}\ (s \in ac' \lhd s.\mathit{wait} \rhd \mathbf{RA2} \circ \mathbf{RA1}(R \Rightarrow S)) \end{array}\right)$$

□

Theorem 1.5.17 *Provided* $\neg\ P$,Q,$\neg\ R$ *and* S *are* **PBMH***-healthy, and* ok *and* ok' *are not free in* P,Q,R *and* S.

$$\begin{array}{l} \mathbf{RA1}(P \vdash Q)\ \ ;_{\mathcal{D}\mathbf{ac}}\ \mathbf{RA1}(R \vdash S) \\ = \\ \mathbf{RA1}\left(\begin{array}{l} \neg\,(\mathbf{RA1}(\neg\ P)\ \ ;_{\mathcal{A}}\ \mathbf{RA1}(\mathit{true})) \wedge \neg\,(\mathbf{RA1}(Q)\ \ ;_{\mathcal{A}}\ \mathbf{RA1}(\neg\ R)) \\ \vdash \\ \mathbf{RA1}(Q)\ \ ;_{\mathcal{A}}\ \mathbf{RA1}(R \Rightarrow S) \end{array}\right) \end{array}$$

Proof.

$$\begin{array}{ll} \mathbf{RA1}(P \vdash Q)\ ;_{\mathcal{D}\mathbf{ac}}\ \mathbf{RA1}(R \vdash S) & \{\text{Definition of } ;_{\mathcal{D}\mathbf{ac}}\} \\ = \exists\, ok_0 \bullet \mathbf{RA1}(P \vdash Q)[ok_0/ok']\ ;_{\mathcal{A}}\ \mathbf{RA1}(R \vdash S)[ok_0/ok] & \\ & \{\text{Definition of design}\} \\ = \exists\, ok_0 \bullet \left(\begin{array}{l} \mathbf{RA1}((ok \wedge P) \Rightarrow (Q \wedge ok'))[ok_0/ok'] \\ ;_{\mathcal{A}} \\ \mathbf{RA1}((ok \wedge R) \Rightarrow (S \wedge ok'))[ok_0/ok] \end{array}\right) & \\ & \{\text{Substitution } (ok' \notin (fv(Q) \cup fv(P)) \text{ and } ok \notin (fv(R) \cup fv(S)))\} \\ = \exists\, ok_0 \bullet \left(\begin{array}{l} \mathbf{RA1}((ok \wedge P) \Rightarrow (Q \wedge ok_0)) \\ ;_{\mathcal{A}} \\ \mathbf{RA1}((ok_0 \wedge R) \Rightarrow (S \wedge ok')) \end{array}\right) & \{\text{Case-split on } ok_0\} \\ = \left(\begin{array}{l} \left(\begin{array}{l} \mathbf{RA1}((ok \wedge P) \Rightarrow (Q \wedge \mathit{true})) \\ ;_{\mathcal{A}} \\ \mathbf{RA1}((R \wedge \mathit{true}) \Rightarrow (S \wedge ok')) \end{array}\right) \\ \vee \\ \left(\begin{array}{l} \mathbf{RA1}((ok \wedge P) \Rightarrow (Q \wedge \mathit{false})) \\ ;_{\mathcal{A}} \\ \mathbf{RA1}((\mathit{false} \wedge R) \Rightarrow (S \wedge ok')) \end{array}\right) \end{array}\right) & \{\text{Predicate calculus}\} \end{array}$$

$$= \left(\begin{array}{l} \left(\begin{array}{l} \mathbf{RA1}((ok \wedge P) \Rightarrow Q) \\ ;\, _{\mathcal{A}} \\ \mathbf{RA1}(R \Rightarrow (S \wedge ok')) \end{array} \right) \vee (\mathbf{RA1}(\neg\, (ok \wedge P)) \;;\, _{\mathcal{A}}\, \mathbf{RA1}(true)) \end{array} \right)$$

{Predicate calculus}

$$= \left(\begin{array}{l} \left(\begin{array}{l} \mathbf{RA1}(\neg\, ok \vee \neg\, P \vee Q) \\ ;\, _{\mathcal{A}} \\ \mathbf{RA1}(\neg\, R \vee (S \wedge ok')) \end{array} \right) \vee (\mathbf{RA1}(\neg\, ok \vee \neg\, P) \;;\, _{\mathcal{A}}\, \mathbf{RA1}(true)) \end{array} \right)$$

{Distributivity of **RA1** (Theorem 1.2.1)}

$$= \left(\begin{array}{l} \left(\begin{array}{l} (\mathbf{RA1}(\neg\, ok \vee \neg\, P) \vee \mathbf{RA1}(Q)) \\ ;\, _{\mathcal{A}} \\ \mathbf{RA1}(\neg\, R \vee (S \wedge ok')) \end{array} \right) \vee (\mathbf{RA1}(\neg\, ok \vee \neg\, P) \;;\, _{\mathcal{A}}\, \mathbf{RA1}(true)) \end{array} \right)$$

{Distributivity of $;\, _{\mathcal{A}}$ (Lemma F.1.4)}

$$= \left(\begin{array}{l} (\mathbf{RA1}(\neg\, ok \vee \neg\, P) \;;\, _{\mathcal{A}}\, \mathbf{RA1}(\neg\, R \vee (S \wedge ok'))) \\ \vee \\ (\mathbf{RA1}(Q) \;;\, _{\mathcal{A}}\, \mathbf{RA1}(\neg\, R \vee (S \wedge ok'))) \\ \vee \\ (\mathbf{RA1}(\neg\, ok \vee \neg\, P) \;;\, _{\mathcal{A}}\, \mathbf{RA1}(true)) \end{array} \right)$$

{$\neg\, ok$ and $\neg\, P$ are **PBMH**-healthy, Theorems 1.2.5 and B.1.1}

$$= \left(\begin{array}{l} (\mathbf{RA1}(Q) \;;\, _{\mathcal{A}}\, \mathbf{RA1}(\neg\, R \vee (S \wedge ok'))) \\ \vee \\ (\mathbf{RA1}(\neg\, ok \vee \neg\, P) \;;\, _{\mathcal{A}}\, \mathbf{RA1}(true)) \end{array} \right)$$

{Theorem 1.2.1}

$$= \left(\begin{array}{l} (\mathbf{RA1}(Q) \;;\, _{\mathcal{A}}\, (\mathbf{RA1}(\neg\, R) \vee \mathbf{RA1}(S \wedge ok'))) \\ \vee \\ (\mathbf{RA1}(\neg\, ok \vee \neg\, P) \;;\, _{\mathcal{A}}\, \mathbf{RA1}(true)) \end{array} \right)$$

{Lemma B.1.11}

$$= \left(\begin{array}{l} (\mathbf{RA1}(Q) \;;\, _{\mathcal{A}}\, (\mathbf{RA1}(\neg\, R) \vee (\mathbf{RA1}(S) \wedge ok'))) \\ \vee \\ (\mathbf{RA1}(\neg\, ok \vee \neg\, P) \;;\, _{\mathcal{A}}\, \mathbf{RA1}(true)) \end{array} \right)$$

{Predicate calculus}

$$= \left(\begin{array}{l} (\mathbf{RA1}(Q) \;;\, _{\mathcal{A}}\, (\neg\, \mathbf{RA1}(\neg\, R) \Rightarrow (\mathbf{RA1}(S) \wedge ok'))) \\ \vee \\ (\mathbf{RA1}(\neg\, ok \vee \neg\, P) \;;\, _{\mathcal{A}}\, \mathbf{RA1}(true)) \end{array} \right)$$

{Q is **PBMH**-healthy, Theorem 1.2.5 and Lemma F.2.3}

$$
= \left(\begin{array}{l} (\mathbf{RA1}(Q) \ ;_{\mathcal{A}} \mathbf{RA1}(\neg\, R)) \\ \vee \\ ((\mathbf{RA1}(Q) \ ;_{\mathcal{A}} (\neg\, \mathbf{RA1}(\neg\, R) \Rightarrow \mathbf{RA1}(S))) \wedge ok') \\ \vee \\ (\mathbf{RA1}(\neg\, ok \vee \neg\, P) \ ;_{\mathcal{A}} \mathbf{RA1}(true)) \end{array} \right)
$$

{Predicate calculus}

$$
= \left(\begin{array}{l} (\mathbf{RA1}(Q) \ ;_{\mathcal{A}} \mathbf{RA1}(\neg\, R)) \\ \vee \\ ((\mathbf{RA1}(Q) \ ;_{\mathcal{A}} (\mathbf{RA1}(\neg\, R) \vee \mathbf{RA1}(S))) \wedge ok') \\ \vee \\ (\mathbf{RA1}(\neg\, ok \vee \neg\, P) \ ;_{\mathcal{A}} \mathbf{RA1}(true)) \end{array} \right)
$$

{Theorem 1.2.1}

$$
= \left(\begin{array}{l} (\mathbf{RA1}(Q) \ ;_{\mathcal{A}} \mathbf{RA1}(\neg\, R)) \\ \vee \\ ((\mathbf{RA1}(Q) \ ;_{\mathcal{A}} \mathbf{RA1}(\neg\, R \vee S)) \wedge ok') \\ \vee \\ ((\mathbf{RA1}(\neg\, ok) \vee \mathbf{RA1}(\neg\, P)) \ ;_{\mathcal{A}} \mathbf{RA1}(true)) \end{array} \right)
$$

{Predicate calculus}

$$
= \left(\begin{array}{l} (\mathbf{RA1}(Q) \ ;_{\mathcal{A}} \mathbf{RA1}(\neg\, R)) \\ \vee \\ ((\mathbf{RA1}(Q) \ ;_{\mathcal{A}} \mathbf{RA1}(R \Rightarrow S)) \wedge ok') \\ \vee \\ ((\mathbf{RA1}(\neg\, ok) \vee \mathbf{RA1}(\neg\, P)) \ ;_{\mathcal{A}} \mathbf{RA1}(true)) \end{array} \right)
$$

{Right-distributivity of $;_{\mathcal{A}}$ (Lemma F.1.4)}

$$
= \left(\begin{array}{l} (\mathbf{RA1}(Q) \ ;_{\mathcal{A}} \mathbf{RA1}(\neg\, R)) \\ \vee \\ ((\mathbf{RA1}(Q) \ ;_{\mathcal{A}} \mathbf{RA1}(R \Rightarrow S)) \wedge ok') \\ \vee \\ (\mathbf{RA1}(\neg\, ok) \ ;_{\mathcal{A}} \mathbf{RA1}(true)) \\ \vee \\ (\mathbf{RA1}(\neg\, P) \ ;_{\mathcal{A}} \mathbf{RA1}(true)) \end{array} \right)
$$

{Lemma B.1.17}

$$
= \left(\begin{array}{l}
(\mathbf{RA1}(Q) \ ;_{\mathcal{A}} \mathbf{RA1}(\neg\, R)) \\
\vee \\
((\mathbf{RA1}(Q) \ ;_{\mathcal{A}} \mathbf{RA1}(R \Rightarrow S)) \wedge ok') \\
\vee \\
\mathbf{RA1}(\neg\, ok) \\
\vee \\
(\mathbf{RA1}(\neg\, P) \ ;_{\mathcal{A}} \mathbf{RA1}(true))
\end{array}\right)
$$

{Assumption: $\neg\, R$, S are **PBMH**-healthy and Theorems 1.2.5 and B.1.2}

$$
= \left(\begin{array}{l}
\mathbf{RA1}(\mathbf{RA1}(Q) \ ;_{\mathcal{A}} \mathbf{RA1}(\neg\, R)) \\
\vee \\
(\mathbf{RA1}(\mathbf{RA1}(Q) \ ;_{\mathcal{A}} \mathbf{RA1}(R \Rightarrow S)) \wedge ok') \\
\vee \\
\mathbf{RA1}(\neg\, ok) \\
\vee \\
\mathbf{RA1}(\mathbf{RA1}(\neg\, P) \ ;_{\mathcal{A}} \mathbf{RA1}(true))
\end{array}\right)
\qquad \{\text{Lemma B.1.11}\}
$$

$$
= \left(\begin{array}{l}
\mathbf{RA1}(\mathbf{RA1}(Q) \ ;_{\mathcal{A}} \mathbf{RA1}(\neg\, R)) \\
\vee \\
\mathbf{RA1}((\mathbf{RA1}(Q) \ ;_{\mathcal{A}} \mathbf{RA1}(R \Rightarrow S)) \wedge ok') \\
\vee \\
\mathbf{RA1}(\neg\, ok) \\
\vee \\
\mathbf{RA1}(\mathbf{RA1}(\neg\, P) \ ;_{\mathcal{A}} \mathbf{RA1}(true))
\end{array}\right)
\qquad \{\text{Theorem 1.2.1}\}
$$

$$
= \mathbf{RA1} \left(\begin{array}{l}
(\mathbf{RA1}(Q) \ ;_{\mathcal{A}} \mathbf{RA1}(\neg\, R)) \\
\vee \\
((\mathbf{RA1}(Q) \ ;_{\mathcal{A}} \mathbf{RA1}(R \Rightarrow S)) \wedge ok') \\
\vee \\
(\neg\, ok) \\
\vee \\
(\mathbf{RA1}(\neg\, P) \ ;_{\mathcal{A}} \mathbf{RA1}(true))
\end{array}\right)
\qquad \{\text{Predicate calculus}\}
$$

$$
= \mathbf{RA1} \left(\begin{array}{l}
\left(\begin{array}{l}
ok \wedge \neg\, (\mathbf{RA1}(Q) \ ;_{\mathcal{A}} \mathbf{RA1}(\neg\, R)) \\
\wedge \\
\neg\, (\mathbf{RA1}(\neg\, P) \ ;_{\mathcal{A}} \mathbf{RA1}(true))
\end{array}\right) \\
\Rightarrow \\
((\mathbf{RA1}(Q) \ ;_{\mathcal{A}} \mathbf{RA1}(R \Rightarrow S)) \wedge ok')
\end{array}\right)
$$

{Definition of design}

$$= \mathbf{RA1}\left(\begin{array}{l} \neg\,(\mathbf{RA1}(\neg\,P)\ ;_{\mathcal{A}}\ \mathbf{RA1}(\mathit{true})) \wedge \neg\,(\mathbf{RA1}(Q)\ ;_{\mathcal{A}}\ \mathbf{RA1}(\neg\,R)) \\ \vdash \\ \mathbf{RA1}(Q)\ ;_{\mathcal{A}}\ \mathbf{RA1}(R \Rightarrow S) \end{array}\right)$$

□

Chapter 2

Linking relations, designs and angelic nondeterminism

2.1 Relationship with angelic designs

Definition 23

$$d2ac(P) \mathrel{\widehat{=}} (\neg\, p2ac(P^f) \wedge (\neg\, P^f[\mathbf{s}/in\alpha]\ ;\ true) \vdash p2ac(P^t))$$

The function $d2ac$ maps from the theory of designs, characterised by the healthiness conditions **H1-H2**, to the theory of designs with angelic nondeterminism characterised by the healthiness conditions **A0-A1**. The function that maps in the opposite direction is $ac2p$. In what follows we explore the relationship between $p2ac$ and $d2ac$.

Theorem 2.1.1 *Provided P is a design.*

$$ac' \neq \emptyset \wedge p2ac(P) = ac' \neq \emptyset \wedge d2ac(P)$$

Proof.

$$\begin{array}{ll}
ac' \neq \emptyset \wedge p2ac(P) & \{\text{Assumption: } P \text{ is a design}\} \\
= ac' \neq \emptyset \wedge p2ac((ok \wedge \neg\, P^f) \Rightarrow (P^t \wedge ok')) & \{\text{Predicate calculus}\} \\
= ac' \neq \emptyset \wedge p2ac((ok \wedge \neg\, P^f \wedge \exists\, out\alpha \bullet \neg\, P^f) \Rightarrow (P^t \wedge ok')) & \\
& \{\text{Predicate calculus}\} \\
= ac' \neq \emptyset \wedge p2ac(\neg\, ok \vee P^f \vee \neg\, (\exists\, out\alpha \bullet \neg\, P^f) \vee (P^t \wedge ok')) & \\
& \{\text{Distributivity of } p2ac \text{ (Theorem 1.4.4)}\}
\end{array}$$

$$= ac' \neq \emptyset \wedge \left(\begin{array}{l} p2ac(\neg\ ok) \vee p2ac(P^f) \\ \vee \\ p2ac(\neg\ (\exists\, out\alpha \bullet \neg\ P^f)) \vee p2ac(P^t \wedge ok') \end{array} \right)$$

{Lemmas C.2.5 and C.2.6}

$$= ac' \neq \emptyset \wedge \left(\begin{array}{l} (\neg\ ok \wedge ac' \neq \emptyset) \vee p2ac(P^f) \\ \vee \\ \vee\ p2ac(\neg\ (\exists\, out\alpha \bullet \neg\ P^f)) \vee (p2ac(P^t) \wedge ok') \end{array} \right)$$

{Lemma C.2.7}

$$= ac' \neq \emptyset \wedge \left(\begin{array}{l} (\neg\ ok \wedge ac' \neq \emptyset) \vee p2ac(P^f) \\ \vee \\ ((\neg\ (\exists\, out\alpha \bullet \neg\ P^f))[\mathbf{s}/in\alpha] \wedge ac' \neq \emptyset) \vee (p2ac(P^t) \wedge ok') \end{array} \right)$$

{Predicate calculus}

$$= ac' \neq \emptyset \wedge \left(\begin{array}{l} \neg\ ok \vee p2ac(P^f) \\ \vee \\ (\neg\ (\exists\, out\alpha \bullet \neg\ P^f))[\mathbf{s}/in\alpha]) \vee (p2ac(P^t) \wedge ok') \end{array} \right)$$

{Property of substitution}

$$= ac' \neq \emptyset \wedge \left(\begin{array}{l} \neg\ ok \vee p2ac(P^f) \\ \vee \\ \neg\ (\exists\, out\alpha \bullet \neg\ P^f[\mathbf{s}/in\alpha]) \vee (p2ac(P^t) \wedge ok') \end{array} \right)$$

{Predicate calculus}

$$= ac' \neq \emptyset \wedge ((ok \wedge \neg\ p2ac(P^f) \wedge \exists\, out\alpha \bullet \neg\ P^f[\mathbf{s}/in\alpha]) \Rightarrow (p2ac(P^t) \wedge ok'))$$

{Definition of design}

$$= ac' \neq \emptyset \wedge (\neg\ p2ac(P^f) \wedge \exists\, out\alpha \bullet \neg\ P^f[\mathbf{s}/in\alpha] \vdash p2ac(P^t))$$

{Predicate calculus and definition of sequential composition}

$$= ac' \neq \emptyset \wedge (\neg\ p2ac(P^f) \wedge (\neg\ P^f[\mathbf{s}/in\alpha]\ ;\ true) \vdash p2ac(P^t))$$

{Definition of $d2ac$}

$$= ac' \neq \emptyset \wedge d2ac(P)$$

□

Theorem 2.1.2

$$ac' \neq \emptyset \wedge p2ac(\neg\ P^f \vdash P^t) = (\neg\ p2ac(P^f) \vdash p2ac(P^t))$$

Proof.

$ac' \neq \emptyset \wedge p2ac(\neg\ P^f \vdash P^t)$ {Definition of design}

$$
\begin{array}{ll}
= ac' \neq \emptyset \wedge p2ac((ok \wedge \neg\ P^f) \Rightarrow (P^t \wedge ok')) & \{\text{Predicate calculus}\} \\
= ac' \neq \emptyset \wedge p2ac(\neg\ ok \vee P^f \vee (P^t \wedge ok')) & \\
& \{\text{Distributivity of } p2ac \text{ (Theorem 1.4.4)}\} \\
= ac' \neq \emptyset \wedge (p2ac(\neg\ ok) \vee p2ac(P^f) \vee p2ac(P^t \wedge ok')) & \\
& \{\text{Lemmas C.2.5 and C.2.6}\} \\
= ac' \neq \emptyset \wedge ((\neg\ ok \wedge ac' \neq \emptyset) \vee p2ac(P^f) \vee (p2ac(P^t) \wedge ok')) & \\
& \{\text{Predicate calculus}\} \\
= ac' \neq \emptyset \wedge (\neg\ ok \vee p2ac(P^f) \vee (p2ac(P^t) \wedge ok')) & \{\text{Predicate calculus}\} \\
= ac' \neq \emptyset \wedge ((ok \wedge \neg\ p2ac(P^f)) \Rightarrow (p2ac(P^t) \wedge ok')) & \\
& \{\text{Definition of design}\} \\
= ac' \neq \emptyset \wedge (\neg\ p2ac(P^f) \vdash p2ac(P^t)) &
\end{array}
$$

□

Theorem 2.1.3 *Provided that P is a design.*

$$ac2p \circ d2ac(P) = P$$

Proof.

$$
\begin{array}{ll}
ac2p \circ d2ac(P) & \{\text{Assumption: } P \text{ is a design}\} \\
= ac2p \circ d2ac(\neg\ P^f \vdash P^t) & \{\text{Definition of } d2ac\} \\
= ac2p(\neg\ p2ac(P^f) \wedge (\neg\ P^f[\mathbf{s}/in\alpha]\ ;\ true) \vdash p2ac(P^t)) & \\
& \{\text{Definition of design}\} \\
= ac2p((ok \wedge \neg\ p2ac(P^f) \wedge (\neg\ P^f[\mathbf{s}/in\alpha]\ ;\ true)) \Rightarrow (p2ac(P^t) \wedge ok')) & \\
& \{\text{Predicate calculus}\} \\
= ac2p(\neg\ ok \vee p2ac(P^f) \vee \neg\ (\neg\ P^f[\mathbf{s}/in\alpha]\ ;\ true) \vee (p2ac(P^t) \wedge ok')) & \\
& \{\text{Distributivity of } ac2p \text{ (Theorem 1.4.1)}\} \\
= \left(\begin{array}{l} ac2p(\neg\ ok) \vee ac2p \circ p2ac(P^f) \vee ac2p(\neg\ (\neg\ P^f[\mathbf{s}/in\alpha]\ ;\ true)) \\ \vee \\ ac2p(p2ac(P^t) \wedge ok') \end{array} \right) & \\
& \{\text{Lemmas C.1.8 and C.1.9}\} \\
= \left(\begin{array}{l} \neg\ ok \vee ac2p \circ p2ac(P^f) \vee ac2p(\neg\ (\neg\ P^f[\mathbf{s}/in\alpha]\ ;\ true)) \\ \vee \\ (ac2p \circ p2ac(P^t) \wedge ok') \end{array} \right) & \\
& \{\text{Theorem 1.4.20}\}
\end{array}
$$

$$= (\neg\ ok \lor P^f \lor ac2p(\neg\ (\neg\ P^f[\mathbf{s}/in\alpha]\ ;\ true)) \lor (P^t \land ok'))$$
$$\{ac' \text{ not free in } P^f \text{ and Lemma C.1.12}\}$$
$$= (\neg\ ok \lor P^f \lor \neg\ (\neg\ P^f[\mathbf{s}/in\alpha]\ ;\ true))[State_{\mathtt{II}}(in\alpha)/s] \lor (P^t \land ok'))$$
$$\{\text{Property of substitution}\}$$
$$= (\neg\ ok \lor P^f \lor \neg\ (\neg\ P^f[\mathbf{s}/in\alpha][State_{\mathtt{II}}(in\alpha)/s]\ ;\ true)) \lor (P^t \land ok'))$$
$$\{\text{Lemma G.2.3}\}$$
$$= (\neg\ ok \lor P^f \lor \neg\ (\neg\ P^f\ ;\ true)) \lor (P^t \land ok'))$$
$$\{\text{Predicate calculus and definition of design}\}$$
$$= (\neg\ P^f \land (\neg\ P^f\ ;\ true) \vdash P^t) \qquad \{\text{Definition of sequential composition}\}$$
$$= (\neg\ P^f \land (\exists\, out\alpha \bullet \neg\ P^f) \vdash P^t) \qquad \{\text{Predicate calculus}\}$$
$$= (\neg\ P^f \vdash P^t) \qquad \{\text{Assumption: } P \text{ is a design}\}$$
$$= P$$

□

Theorem 2.1.4 *Provided that P is a design.*

$$ac2p \circ \mathbf{A}(P) = (\neg\ ac2p(P^f) \vdash ac2p(P^t))$$

Proof.

$$ac2p \circ \mathbf{A}(P) \qquad \{\text{Assumption: } P \text{ is a design}\}$$
$$= ac2p \circ \mathbf{A}(\neg\ P^f \vdash P^t) \qquad \{\text{Definition of } \mathbf{A}\}$$
$$= ac2p(\neg\ \mathbf{PBMH}(P^f) \vdash \mathbf{PBMH}(P^t) \land ac' \neq \emptyset) \qquad \{\text{Definition of design}\}$$
$$= ac2p((ok \land \neg\ \mathbf{PBMH}(P^f)) \Rightarrow (\mathbf{PBMH}(P^t) \land ac' \neq \emptyset \land ok'))$$
$$\{\text{Predicate calculus}\}$$
$$= ac2p(\neg\ ok \lor \mathbf{PBMH}(P^f) \lor (\mathbf{PBMH}(P^t) \land ac' \neq \emptyset \land ok'))$$
$$\{\text{Distributivity of } ac2p \text{ (Theorem 1.4.1)}\}$$
$$= ac2p(\neg\ ok) \lor ac2p \circ \mathbf{PBMH}(P^f) \lor ac2p(\mathbf{PBMH}(P^t) \land ac' \neq \emptyset \land ok')$$
$$\{\text{Lemma C.1.9}\}$$
$$= \neg\ ok \lor ac2p \circ \mathbf{PBMH}(P^f) \lor ac2p(\mathbf{PBMH}(P^t) \land ac' \neq \emptyset \land ok')$$
$$\{\text{Lemma C.1.8}\}$$
$$= \neg\ ok \lor ac2p \circ \mathbf{PBMH}(P^f) \lor (ac2p(\mathbf{PBMH}(P^t) \land ac' \neq \emptyset) \land ok')$$
$$\{\text{Lemma 2.1.1}\}$$
$$= \neg\ ok \lor ac2p \circ \mathbf{PBMH}(P^f) \lor (ac2p \circ \mathbf{PBMH}(P^t) \land ok')$$
$$\{\text{Lemma 2.1.2}\}$$

$$
\begin{array}{ll}
= \neg\ ok \vee ac2p(P^f) \vee (ac2p(P^t) \wedge ok') & \{\text{Predicate calculus}\} \\
= (ok \wedge \neg\ ac2p(P^f)) \Rightarrow (ac2p(P^t) \wedge ok') & \{\text{Definition of design}\} \\
= (\neg\ ac2p(P^f) \vdash ac2p(P^t)) &
\end{array}
$$

□

Lemma 2.1.1 *Provided P is* **PBMH***-healthy.*

$$ac2p(P \wedge ac' \neq \emptyset) = ac2p(P)$$

Proof.

$$
\begin{array}{ll}
ac2p(P \wedge ac' \neq \emptyset) & \{\text{Definition of } ac2p\} \\
= \mathbf{PBMH}(P \wedge ac' \neq \emptyset)[State_{II}(in\alpha)/s]\ ;_{\mathcal{A}} \bigwedge x' : out\alpha \bullet s.x = x' & \\
& \{\text{Assumption: } P \text{ is } \mathbf{PBMH}\text{-healthy}\} \\
= \mathbf{PBMH}(\mathbf{PBMH}(P) \wedge ac' \neq \emptyset)[State_{II}(in\alpha)/s]\ ;_{\mathcal{A}} \bigwedge x' : out\alpha \bullet s.x = x' & \\
& \{ac' \neq \emptyset \text{ is } \mathbf{PBMH}\text{-healthy}\} \\
= \mathbf{PBMH}\begin{pmatrix} \mathbf{PBMH}(P) \\ \wedge \\ \mathbf{PBMH}(ac' \neq \emptyset) \end{pmatrix}[State_{II}(in\alpha)/s]\ ;_{\mathcal{A}} \bigwedge x' : out\alpha \bullet s.x = x' & \\
& \{\text{Closure of cojunction under } \mathbf{PBMH}\} \\
= \begin{pmatrix} \mathbf{PBMH}(P) \\ \wedge \\ \mathbf{PBMH}(ac' \neq \emptyset) \end{pmatrix}[State_{II}(in\alpha)/s]\ ;_{\mathcal{A}} \bigwedge x' : out\alpha \bullet s.x = x' & \\
& \{ac' \neq \emptyset \text{ is } \mathbf{PBMH}\text{-healthy}\} \\
= (\mathbf{PBMH}(P) \wedge ac' \neq \emptyset)[State_{II}(in\alpha)/s]\ ;_{\mathcal{A}} \bigwedge x' : out\alpha \bullet s.x = x' & \\
& \{\text{Property of substitution}\} \\
= (\mathbf{PBMH}(P)[State_{II}(in\alpha)/s] \wedge ac' \neq \emptyset)\ ;_{\mathcal{A}} \bigwedge x' : out\alpha \bullet s.x = x' & \\
& \{\text{Right-distributivity of } ;_{\mathcal{A}}\} \\
= \begin{pmatrix} (\mathbf{PBMH}(P)[State_{II}(in\alpha)/s]\ ;_{\mathcal{A}} \bigwedge x' : out\alpha \bullet s.x = x') \\ \wedge \\ (ac' \neq \emptyset\ ;_{\mathcal{A}} \bigwedge x' : out\alpha \bullet s.x = x') \end{pmatrix} & \\
& \{\text{Definition of } ac2p\} \\
= ac2p(P) \wedge (ac' \neq \emptyset\ ;_{\mathcal{A}} \bigwedge x' : out\alpha \bullet s.x = x') & \{\text{Property of sets}\}
\end{array}
$$

$= ac2p(P) \wedge ((\exists\, z \bullet z \in ac') \;;_{\mathcal{A}} \bigwedge x' : out\alpha \bullet s.x = x')$

{Definition of $;_{\mathcal{A}}$ and substitution}

$= ac2p(P) \wedge (\exists\, z \bullet z \in \{s \mid \bigwedge x' : out\alpha \bullet s.x = x'\})$ {Property of sets}

$= ac2p(P) \wedge (\exists\, z \bullet \bigwedge x' : out\alpha \bullet z.x = x')$ {One-point rule}

$= ac2p(P)$

□

Lemma 2.1.2

$$ac2p \circ \mathbf{PBMH}(P) = ac2p(P)$$

Proof.

$ac2p \circ \mathbf{PBMH}(P)$ {Definition of $ac2p$}

$= \mathbf{PBMH}(\mathbf{PBMH}(P))[State_{\mathtt{II}}(in\alpha)/s] \;;_{\mathcal{A}} \bigwedge x' : out\alpha \bullet s.x = x'$

{Theorem E.2.1}

$= \mathbf{PBMH}(P)[State_{\mathtt{II}}(in\alpha)/s] \;;_{\mathcal{A}} \bigwedge x' : out\alpha \bullet s.x = x'$

{Definition of $ac2p$}

$= ac2p(P)$

□

Lemma 2.1.3

$$d2ac \circ ac2p(P)$$
$$=$$
$$(\neg\, p2ac(ac2p(P^f)) \wedge (\exists\, out\alpha \bullet \neg\, ac2p(P^f)[\mathbf{s}/in\alpha]) \vdash p2ac(ac2p(P^t)))$$

Proof.

$d2ac \circ ac2p(P)$ {Lemma C.1.10}

$= d2ac(\neg\, ac2p(P^f) \vdash ac2p(P^t))$ {Definition of $d2ac$}

$= (\neg\, p2ac(ac2p(P^f)) \wedge (\neg\, ac2p(P^f)[\mathbf{s}/in\alpha] \;;\; true) \vdash p2ac(ac2p(P^t)))$

{Definition of sequential composition}

$= (\neg\, p2ac(ac2p(P^f)) \wedge (\exists\, out\alpha \bullet \neg\, ac2p(P^f)[\mathbf{s}/in\alpha]) \vdash p2ac(ac2p(P^t)))$

□

Theorem 2.1.5 *Provided P is an* **A***-healthy design.*

$$d2ac \circ ac2p(P) \sqsupseteq P$$

Proof.

$$
\begin{array}{ll}
& d2ac \circ ac2p(P) \qquad \{\text{Lemma 2.1.3}\} \\
= & (\neg\ p2ac(ac2p(P^f)) \wedge (\exists\ out\alpha \bullet \neg\ ac2p(P^f)[\mathbf{s}/in\alpha]) \vdash p2ac(ac2p(P^t))) \\
& \qquad \{\text{Assumption: } P^f \text{ and } P^t \text{ are } \mathbf{PBMH}\text{-healthy and Theorem 1.4.19}\} \\
= & \left(\begin{array}{l} \neg\ (p2ac(ac2p(P^f)) \wedge P^f) \wedge (\exists\ out\alpha \bullet \neg\ ac2p(P^f)[\mathbf{s}/in\alpha]) \\ \vdash \\ p2ac(ac2p(P^t)) \wedge P^t \end{array} \right) \\
& \qquad \{\text{Lemma C.1.11 and predicate calculus}\} \\
= & \left(\begin{array}{l} \left(\begin{array}{l} \neg\ (p2ac(ac2p(P^f)) \wedge P^f) \\ \wedge \\ (\exists\ out\alpha \bullet \neg\ (ac2p(P^f) \wedge (\exists\ ac' \bullet P^f[State_{\mathtt{II}}(in\alpha)/s]))[\mathbf{s}/in\alpha]) \end{array} \right) \\ \vdash \\ p2ac(ac2p(P^t)) \wedge P^t \end{array} \right) \\
& \qquad \{\text{Property of substitution}\} \\
= & \left(\begin{array}{l} \left(\begin{array}{l} \neg\ (p2ac(ac2p(P^f)) \wedge P^f) \\ \wedge \\ (\exists\ out\alpha \bullet \neg\ (ac2p(P^f)[\mathbf{s}/in\alpha] \wedge (\exists\ ac' \bullet P^f[State_{\mathtt{II}}(in\alpha)/s][\mathbf{s}/in\alpha]))) \end{array} \right) \\ \vdash \\ p2ac(ac2p(P^t)) \wedge P^t \end{array} \right) \\
& \qquad \{\text{Lemma G.2.4}\} \\
= & \left(\begin{array}{l} \left(\begin{array}{l} \neg\ (p2ac(ac2p(P^f)) \wedge P^f) \\ \wedge \\ (\exists\ out\alpha \bullet \neg\ (ac2p(P^f)[\mathbf{s}/in\alpha] \wedge (\exists\ ac' \bullet P^f))) \end{array} \right) \\ \vdash \\ p2ac(ac2p(P^t)) \wedge P^t \end{array} \right) \\
& \qquad \{\text{Predicate calculus}\}
\end{array}
$$

$$
= \left(\begin{array}{l}
\left(\begin{array}{l}
(\neg\ p2ac(ac2p(P^f)) \vee \neg\ P^f) \\
\wedge \\
\left(\begin{array}{l}
\exists\, out\alpha \bullet \neg\ (ac2p(P^f)[\mathbf{s}/in\alpha]) \\
\vee \\
(\exists\, out\alpha \bullet \neg\ \exists\, ac' \bullet P^f)
\end{array}\right)
\end{array}\right) \\
\vdash \\
p2ac(ac2p(P^t)) \wedge P^t
\end{array}\right)
$$

{Predicate calculus: $out\alpha$ not free in P}

$$
= \left(\begin{array}{l}
\left(\begin{array}{l}
(\neg\ p2ac(ac2p(P^f)) \vee \neg\ P^f) \\
\wedge \\
\left(\begin{array}{l}
\exists\, out\alpha \bullet \neg\ (ac2p(P^f)[\mathbf{s}/in\alpha]) \\
\vee \\
(\neg\ \exists\, ac' \bullet P^f)
\end{array}\right)
\end{array}\right) \\
\vdash \\
p2ac(ac2p(P^t)) \wedge P^t
\end{array}\right)
$$

{Predicate calculus}

$$
= \left(\begin{array}{l}
\left(\begin{array}{l}
(\neg\ p2ac(ac2p(P^f)) \wedge \exists\, out\alpha \bullet \neg\ (ac2p(P^f)[\mathbf{s}/in\alpha])) \\
\vee \\
(\neg\ p2ac(ac2p(P^f)) \wedge (\neg\ \exists\, ac' \bullet P^f)) \\
\vee \\
(\neg\ P^f \wedge \exists\, out\alpha \bullet \neg\ (ac2p(P^f)[\mathbf{s}/in\alpha])) \\
\vee \\
(\neg\ P^f \wedge (\neg\ \exists\, ac' \bullet P^f))
\end{array}\right) \\
\vdash \\
p2ac(ac2p(P^t)) \wedge P^t
\end{array}\right)
$$

{Refinement of designs}

$$
\sqsupseteq (\neg\ P^f \wedge (\neg\ \exists\, ac' \bullet P^f) \vdash P^t)
$$

{Predicate calculus}

$$
= (\neg\ P^f \vdash P^t)
$$

{Definition of design}

$$
= P
$$

□

Theorem 2.1.6 *Provided P is an* **A0**-**A2**-*healthy design.*

$$d2ac \circ ac2p(P) \sqsubseteq P$$

Proof.

$d2ac \circ ac2p(P)$ {Assumption: P is an **A0**-**A2**-healthy design}

$$= d2ac \circ ac2p(\neg\ \mathbf{A2} \circ \mathbf{PBMH}(P^f) \vdash \mathbf{A2}(\mathbf{PBMH}(P^t) \wedge ac' \neq \emptyset))$$

{Lemma 2.1.3}

$$= \left(\begin{array}{l} \left(\begin{array}{l} \neg\ p2ac \circ ac2p(\mathbf{A2} \circ \mathbf{PBMH}(P^f)) \\ \wedge \\ \exists\, out\alpha \bullet \neg\ ac2p(\mathbf{A2} \circ \mathbf{PBMH}(P^f))[\mathbf{s}/in\alpha] \end{array} \right) \\ \vdash \\ p2ac \circ ac2p(\mathbf{A2}(\mathbf{PBMH}(P^t) \wedge ac' \neq \emptyset)) \end{array} \right)$$

{Lemma C.1.5 and refinement of designs}

$$\sqsubseteq \left(\begin{array}{l} \neg\ p2ac \circ ac2p(\mathbf{A2} \circ \mathbf{PBMH}(P^f)) \wedge \neg\ \mathbf{A2} \circ \mathbf{PBMH}(P^f)[\emptyset/ac'] \\ \vdash \\ p2ac \circ ac2p(\mathbf{A2}(\mathbf{PBMH}(P^t) \wedge ac' \neq \emptyset)) \end{array} \right)$$

{Lemma A.3.10}

$$= \left(\begin{array}{l} \neg\ p2ac \circ ac2p(\mathbf{A2} \circ \mathbf{PBMH}(P^f)) \wedge \neg\ \mathbf{PBMH}(P^f)[\emptyset/ac'] \\ \vdash \\ p2ac \circ ac2p(\mathbf{A2}(\mathbf{PBMH}(P^t) \wedge ac' \neq \emptyset)) \end{array} \right)$$

{Predicate calculus}

$$= \left(\begin{array}{l} \neg\ (p2ac \circ ac2p(\mathbf{A2} \circ \mathbf{PBMH}(P^f)) \vee \mathbf{PBMH}(P^f)[\emptyset/ac']) \\ \vdash \\ p2ac \circ ac2p(\mathbf{A2}(\mathbf{PBMH}(P^t) \wedge ac' \neq \emptyset)) \end{array} \right)$$

{Lemma A.3.16}

$$= \left(\begin{array}{l} \neg\ \left(\begin{array}{l} (\mathbf{PBMH}(P^f)[\emptyset/ac'] \wedge ac' \neq \emptyset) \\ \vee \\ (\exists\, y \bullet \mathbf{PBMH}(P^f)[\{y\}/ac'] \wedge y \in ac') \\ \vee \\ \mathbf{PBMH}(P^f)[\emptyset/ac'] \end{array} \right) \\ \vdash \\ p2ac \circ ac2p(\mathbf{A2}(\mathbf{PBMH}(P^t) \wedge ac' \neq \emptyset)) \end{array} \right)$$

{Predicate calculus: absorption law}

$$= \left(\begin{array}{l} \neg\ \left(\begin{array}{l} (\exists\, y \bullet \mathbf{PBMH}(P^f)[\{y\}/ac'] \wedge y \in ac') \\ \vee \\ \mathbf{PBMH}(P^f)[\emptyset/ac'] \end{array} \right) \\ \vdash \\ p2ac \circ ac2p(\mathbf{A2}(\mathbf{PBMH}(P^t) \wedge ac' \neq \emptyset)) \end{array} \right)$$

{Theorem 1.2.33}

$$
= \left(\begin{array}{l} \neg\ \mathbf{A2} \circ \mathbf{PBMH}(P^f) \\ \vdash \\ p2ac \circ ac2p(\mathbf{A2}(\mathbf{PBMH}(P^t) \wedge ac' \neq \emptyset)) \end{array} \right) \qquad \{\text{Lemma A.3.16}\}
$$

$$
= \left(\begin{array}{l} \neg\ \mathbf{A2} \circ \mathbf{PBMH}(P^f) \\ \vdash \\ \left(\begin{array}{l} ((\mathbf{PBMH}(P^t) \wedge ac' \neq \emptyset)[\emptyset/ac'] \wedge ac' \neq \emptyset) \\ \vee \\ (\exists\, y \bullet (\mathbf{PBMH}(P^t) \wedge ac' \neq \emptyset)[\{y\}/ac'] \wedge y \in ac') \end{array} \right) \end{array} \right)
$$

$$\{\text{Substitution}\}$$

$$
= \left(\begin{array}{l} \neg\ \mathbf{A2} \circ \mathbf{PBMH}(P^f) \\ \vdash \\ \left(\begin{array}{l} (\mathbf{PBMH}(P^t)[\emptyset/ac'] \wedge \emptyset \neq \emptyset \wedge ac' \neq \emptyset) \\ \vee \\ (\exists\, y \bullet \mathbf{PBMH}(P^t)[\{y\}/ac'] \wedge \{y\} \neq \emptyset \wedge y \in ac') \end{array} \right) \end{array} \right)
$$

$$\{\text{Predicate calculus}\}$$

$$
= \left(\begin{array}{l} \neg\ \mathbf{A2} \circ \mathbf{PBMH}(P^f) \\ \vdash \\ (\exists\, y \bullet \mathbf{PBMH}(P^t)[\{y\}/ac'] \wedge \{y\} \neq \emptyset \wedge y \in ac') \end{array} \right)
$$

$$\{\text{Property of sets}\}$$

$$
= \left(\begin{array}{l} \neg\ \mathbf{A2} \circ \mathbf{PBMH}(P^f) \\ \vdash \\ (\exists\, y \bullet \mathbf{PBMH}(P^t)[\{y\}/ac'] \wedge y \in ac') \end{array} \right) \qquad \{\text{Lemma A.3.8}\}
$$

$$
= (\neg\ \mathbf{A2} \circ \mathbf{PBMH}(P^f) \vdash \mathbf{A2}(\mathbf{PBMH}(P^t) \wedge ac' \neq \emptyset))
$$

$$\{\text{Assumption: } P \text{ is an } \mathbf{A0}\text{-}\mathbf{A2}\text{-healthy design}\}$$

$$
= P
$$

□

Theorem 2.1.7 *Provided P is a design that is* **A0**-**A2**-*healthy.*

$$d2ac \circ ac2p(P) = P$$

Proof. Follows from Theorems 2.1.5 and 2.1.6. □

Chapter 3

Examples

3.1 Event prefixing

Lemma 3.1.1

$$a \rightarrow Stop = \mathbf{R}(true \vdash wait' \wedge ((a \notin ref' \wedge tr' = tr) \vee (tr' = tr \frown \langle a \rangle)))$$

Proof.

$$
\begin{array}{ll}
a \rightarrow Stop & \{\text{Definition of event prefixing}\} \\
= a \rightarrow Skip \ ; \ Stop & \{\text{Definition of event prefixing and } Stop\} \\
= \left(\ \mathbf{R}(true \vdash (tr' = tr \wedge a \notin ref') \lhd wait' \rhd (tr' = tr \frown \langle a \rangle)) \ ; \ \mathbf{R}(true \vdash tr' = tr \wedge wait') \ \right) & \\
& \{\text{Definition of sequential composition}\} \\
= \mathbf{R} \left(\begin{array}{l} \left(\begin{array}{l} \neg \ (\mathbf{R1}(\neg \ true) \ ; \ \mathbf{R1}(true)) \\ \wedge \\ \neg \ (\mathbf{R1}((tr' = tr \wedge a \notin ref') \lhd wait' \rhd (tr' = tr \frown \langle a \rangle)) \wedge \neg \ wait' \ ; \ \mathbf{R1}(\neg \ true)) \end{array} \right) \\ \vdash \\ \mathbf{R1}((tr' = tr \wedge a \notin ref') \lhd wait' \rhd (tr' = tr \frown \langle a \rangle)) \ ; \ (\mathit{II} \lhd wait \rhd \mathbf{R1}(tr' = tr \wedge wait')) \end{array} \right) & \\
& \{\text{Predicate calculus and definition of } \mathbf{R1}\} \\
= \mathbf{R} \left(\begin{array}{l} \left(\begin{array}{l} \neg \ (false \ ; \ \mathbf{R1}(true)) \\ \wedge \\ \neg \ (\mathbf{R1}((tr' = tr \wedge a \notin ref') \lhd wait' \rhd (tr' = tr \frown \langle a \rangle)) \wedge \neg \ wait' \ ; \ false) \end{array} \right) \\ \vdash \\ \mathbf{R1}((tr' = tr \wedge a \notin ref') \lhd wait' \rhd (tr' = tr \frown \langle a \rangle)) \ ; \ (\mathit{II} \lhd wait \rhd \mathbf{R1}(tr' = tr \wedge wait')) \end{array} \right) & \\
& \{\text{Definition of sequential composition}\}
\end{array}
$$

$$= \mathbf{R}\left(\begin{array}{l}(\neg\, false \wedge \neg\, false) \\ \vdash \\ \mathbf{R1}((tr' = tr \wedge a \notin ref') \lhd wait' \rhd (tr' = tr \frown \langle a \rangle)) \;;\; (\mathit{II} \lhd wait \rhd \mathbf{R1}(tr' = tr \wedge wait'))\end{array}\right)$$

{Predicate calculus}

$$= \mathbf{R}\left(\begin{array}{l}true \\ \vdash \\ \mathbf{R1}((tr' = tr \wedge a \notin ref') \lhd wait' \rhd (tr' = tr \frown \langle a \rangle)) \;;\; (\mathit{II} \lhd wait \rhd \mathbf{R1}(tr' = tr \wedge wait'))\end{array}\right)$$

{Predicates are **R1**-healthy}

$$= \mathbf{R}\left(\begin{array}{l}true \\ \vdash \\ \left(\begin{array}{l}(tr' = tr \wedge a \notin ref') \\ \lhd wait' \rhd \\ (tr' = tr \frown \langle a \rangle)\end{array}\right) \;;\; (\mathit{II} \lhd wait \rhd tr' = tr \wedge wait')\end{array}\right)$$

{Definition of conditional}

$$= \mathbf{R}\left(\begin{array}{l}true \\ \vdash \\ \left(\begin{array}{l}(wait' \wedge tr' = tr \wedge a \notin ref') \\ \vee \\ (\neg\, wait' \wedge tr' = tr \frown \langle a \rangle)\end{array}\right) \;;\; (wait \wedge \mathit{II}) \vee (\neg\, wait \wedge tr' = tr \wedge wait')\end{array}\right)$$

{Distributivity of sequential composition}

$$= \mathbf{R}\left(\begin{array}{l}true \\ \vdash \\ \left(\begin{array}{l}(wait' \wedge tr' = tr \wedge a \notin ref') \;;\; (wait \wedge \mathit{II}) \\ \vee \\ (\neg\, wait' \wedge tr' = tr \frown \langle a \rangle) \;;\; (wait \wedge \mathit{II}) \\ \vee \\ (wait' \wedge tr' = tr \wedge a \notin ref') \;;\; (\neg\, wait \wedge tr' = tr \wedge wait') \\ \vee \\ (\neg\, wait' \wedge tr' = tr \frown \langle a \rangle) \;;\; (\neg\, wait \wedge tr' = tr \wedge wait')\end{array}\right)\end{array}\right)$$

{Property of sequential composition}

$$= \mathbf{R}\left(\begin{array}{l}true \\ \vdash \\ \left(\begin{array}{l}(wait' \wedge tr' = tr \wedge a \notin ref') \;;\; (wait \wedge \mathit{II}) \\ \vee \\ (\neg\, wait' \wedge tr' = tr \frown \langle a \rangle) \;;\; (\neg\, wait \wedge tr' = tr \wedge wait')\end{array}\right)\end{array}\right)$$

{Definition of sequential composition}

$$= \mathbf{R}\left(\begin{array}{l} true \\ \vdash \\ \left(\begin{array}{l} (\exists\, wait_0, ref_0, tr_0 \bullet wait_0 \wedge tr_0 = tr \wedge a \notin ref_0 \wedge wait_0 \wedge \mathit{II}[wait_0, ref_0, tr_0/wait, ref, tr] \\ \vee \\ (\exists\, wait_0, ref_0, tr_0 \bullet \neg\ wait_0 \wedge tr_0 = tr \frown \langle a \rangle \wedge \neg\ wait_0 \wedge tr' = tr_0 \wedge wait') \end{array}\right) \end{array}\right)$$

{One-point rule}

$$= \mathbf{R}\left(\begin{array}{l} true \\ \vdash \\ \left(\begin{array}{l} (\exists\, ref_0 \bullet a \notin ref_0 \wedge \mathit{II}[true, ref_0, tr/wait, ref, tr] \\ \vee \\ (tr' = tr \frown \langle a \rangle \wedge wait') \end{array}\right) \end{array}\right)$$

{Definition of II}

$$= \mathbf{R}\left(\begin{array}{l} true \\ \vdash \\ \left(\begin{array}{l} (\exists\, ref_0 \bullet a \notin ref_0 \wedge ref' = ref_0 \wedge wait' \wedge tr' = tr \\ \vee \\ (tr' = tr \frown \langle a \rangle \wedge wait') \end{array}\right) \end{array}\right)$$

{One-point rule}

$$= \mathbf{R}\left(\begin{array}{l} true \\ \vdash \\ \left(\begin{array}{l} (a \notin ref' \wedge wait' \wedge tr' = tr) \\ \vee \\ (tr' = tr \frown \langle a \rangle \wedge wait') \end{array}\right) \end{array}\right)$$

{Predicate calculus}

$$= \mathbf{R}(true \vdash wait' \wedge ((a \notin ref' \wedge tr' = tr) \vee (tr' = tr \frown \langle a \rangle)))$$

□

Lemma 3.1.2

$$a \rightarrow Choice = \mathbf{R}\left(\begin{array}{l} true \\ \vdash \\ (tr' = tr \wedge a \notin ref' \wedge wait') \vee (tr \frown \langle a \rangle \leq tr') \end{array}\right)$$

Proof.

$a \rightarrow Choice$ {Definition of prefixing}

$= (a \rightarrow Skip)\ ;\ Choice$ {Definition of prefixing and *Choice*}

$$= \left(\begin{array}{l} \mathbf{R}(\mathit{true} \vdash (tr' = tr \wedge a \notin \mathit{ref}') \lhd \mathit{wait}' \rhd (tr' = tr \frown \langle a \rangle)) \\ ; \\ \mathbf{R}(\mathit{true} \vdash \mathit{true}) \end{array} \right)$$

{Definition of sequential composition}

$$= \mathbf{R} \left(\begin{array}{l} \left(\begin{array}{l} \neg\, (\mathbf{R1}(\neg\, \mathit{true}) \,;\, \mathbf{R1}(\mathit{true})) \\ \wedge \\ \neg\, (\mathbf{R1}((tr' = tr \wedge a \notin \mathit{ref}') \lhd \mathit{wait}' \rhd (tr' = tr \frown \langle a \rangle)) \wedge \neg\, \mathit{wait}' \,;\, \mathbf{R1}(\neg\, \mathit{true})) \end{array} \right) \\ \vdash \\ \mathbf{R1}((tr' = tr \wedge a \notin \mathit{ref}') \lhd \mathit{wait}' \rhd (tr' = tr \frown \langle a \rangle)) \,;\, (\mathit{II} \lhd \mathit{wait} \rhd \mathbf{R1}(\mathit{true})) \end{array} \right)$$

{Predicate calculus}

$$= \mathbf{R} \left(\begin{array}{l} \left(\begin{array}{l} \neg\, (\mathbf{R1}(\mathit{false}) \,;\, \mathbf{R1}(\mathit{true})) \\ \wedge \\ \neg\, (\mathbf{R1}((tr' = tr \wedge a \notin \mathit{ref}') \lhd \mathit{wait}' \rhd (tr' = tr \frown \langle a \rangle)) \wedge \neg\, \mathit{wait}' \,;\, \mathbf{R1}(\mathit{false})) \end{array} \right) \\ \vdash \\ \mathbf{R1}((tr' = tr \wedge a \notin \mathit{ref}') \lhd \mathit{wait}' \rhd (tr' = tr \frown \langle a \rangle)) \,;\, (\mathit{II} \lhd \mathit{wait} \rhd \mathbf{R1}(\mathit{true})) \end{array} \right)$$

{Property of sequential composition}

$$= \mathbf{R} \left(\begin{array}{l} \neg\, \mathit{false} \wedge \neg\, \mathit{false} \\ \vdash \\ \mathbf{R1}((tr' = tr \wedge a \notin \mathit{ref}') \lhd \mathit{wait}' \rhd (tr' = tr \frown \langle a \rangle)) \,;\, (\mathit{II} \lhd \mathit{wait} \rhd \mathbf{R1}(\mathit{true})) \end{array} \right)$$

{Predicate calculus}

$$= \mathbf{R} \left(\begin{array}{l} \mathit{true} \\ \vdash \\ \mathbf{R1}((tr' = tr \wedge a \notin \mathit{ref}') \lhd \mathit{wait}' \rhd (tr' = tr \frown \langle a \rangle)) \,;\, (\mathit{II} \lhd \mathit{wait} \rhd \mathbf{R1}(\mathit{true})) \end{array} \right)$$

{Definition of **R1** and predicate is **R1**-healthy}

$$= \mathbf{R} \left(\begin{array}{l} \mathit{true} \\ \vdash \\ ((tr' = tr \wedge a \notin \mathit{ref}') \lhd \mathit{wait}' \rhd (tr' = tr \frown \langle a \rangle)) \,;\, (\mathit{II} \lhd \mathit{wait} \rhd tr \leq tr') \end{array} \right)$$

{Definition of conditional and predicate calculus}

$$= \mathbf{R} \left(\begin{array}{l} \mathit{true} \\ \vdash \\ \left(\begin{array}{l} (\mathit{wait}' \wedge tr' = tr \wedge a \notin \mathit{ref}') \\ \vee \\ (\neg\, \mathit{wait}' \wedge tr' = tr \frown \langle a \rangle) \end{array} \right) \,;\, \left(\begin{array}{l} (\mathit{wait} \wedge \mathit{II}) \\ \vee \\ (\neg\, \mathit{wait} \wedge tr \leq tr') \end{array} \right) \end{array} \right)$$

{Relational calculus}

$$= \mathbf{R}\left(\begin{array}{l} true \\ \vdash \\ \left(\begin{array}{l} (wait' \wedge tr' = tr \wedge a \notin ref') \ ; \ (wait \wedge \mathit{II}) \\ \vee \\ (wait' \wedge tr' = tr \wedge a \notin ref') \ ; \ (\neg\ wait \wedge tr \leq tr') \\ \vee \\ (\neg\ wait' \wedge tr' = tr \frown \langle a \rangle) \ ; \ (wait \wedge \mathit{II}) \\ \vee \\ (\neg\ wait' \wedge tr' = tr \frown \langle a \rangle) \ ; \ (\neg\ wait \wedge tr \leq tr') \end{array}\right) \end{array}\right)$$

{Property of sequential composition}

$$= \mathbf{R}\left(\begin{array}{l} true \\ \vdash \\ \left(\begin{array}{l} (wait' \wedge tr' = tr \wedge a \notin ref') \ ; \ (wait \wedge \mathit{II}) \\ \vee \\ (\neg\ wait' \wedge tr' = tr \frown \langle a \rangle) \ ; \ (\neg\ wait \wedge tr \leq tr') \end{array}\right) \end{array}\right)$$

{Definition of sequential composition}

$$= \mathbf{R}\left(\begin{array}{l} true \\ \vdash \\ \left(\begin{array}{l} \exists\, wait_0, tr_0, ref_0 \bullet \left(\begin{array}{l} wait_0 \wedge tr_0 = tr \wedge a \notin ref_0 \wedge wait_0 \\ \wedge\ \mathit{II}[wait_0, ref_0, tr_0 / wait, ref, tr] \end{array}\right) \\ \vee \\ (\exists\, wait_0, tr_0, ref_0 \bullet \neg\ wait_0 \wedge tr_0 = tr \frown \langle a \rangle \wedge \neg\ wait_0 \wedge tr_0 \leq tr') \end{array}\right) \end{array}\right)$$

{One-point rule and definition of II}

$$= \mathbf{R}\left(\begin{array}{l} true \\ \vdash \\ (tr' = tr \wedge a \notin ref' \wedge wait') \vee (tr \frown \langle a \rangle \leq tr') \end{array}\right)$$

□

Lemma 3.1.3

$$a \rightarrow Chaos = \mathbf{R}(\neg\ (tr \frown \langle a \rangle \leq tr') \vdash wait' \wedge tr' = tr \wedge a \notin ref')$$

Proof.

$a \rightarrow Chaos$ {Definition of prefixing}

$= a \rightarrow Skip \ ; \ \mathbf{R}(false \vdash true)$ {Definition of prefixing}

$= \mathbf{R}(true \vdash (tr' = tr \wedge a \notin ref') \lhd wait' \rhd (tr' = tr \frown \langle a \rangle)) \ ; \ \mathbf{R}(false \vdash true)$

{Definition of sequence}

$$= \mathbf{R}\left(\begin{array}{l}\left(\begin{array}{l}\neg\,(\mathbf{R1}(\neg\,true)\ ;\ \mathbf{R1}(true))\\ \wedge\\ \neg\,(\mathbf{R1}((tr' = tr \wedge a \notin ref') \lhd wait' \rhd (tr' = tr \frown \langle a\rangle)) \wedge \neg\,wait'\ ;\ \mathbf{R1}(\neg\,false))\end{array}\right)\\ \vdash\\ \mathbf{R1}((tr' = tr \wedge a \notin ref') \lhd wait' \rhd (tr' = tr \frown \langle a\rangle))\ ;\ (\mathtt{II} \lhd wait \rhd \mathbf{R1}(true))\end{array}\right)$$

{Predicate calculus}

$$= \mathbf{R}\left(\begin{array}{l}\left(\begin{array}{l}\neg\,(\mathbf{R1}(false)\ ;\ \mathbf{R1}(true))\\ \wedge\\ \neg\,(\mathbf{R1}((tr' = tr \wedge a \notin ref') \lhd wait' \rhd (tr' = tr \frown \langle a\rangle)) \wedge \neg\,wait'\ ;\ \mathbf{R1}(true))\end{array}\right)\\ \vdash\\ \mathbf{R1}((tr' = tr \wedge a \notin ref') \lhd wait' \rhd (tr' = tr \frown \langle a\rangle))\ ;\ (\mathtt{II} \lhd wait \rhd \mathbf{R1}(true))\end{array}\right)$$

{Property of **R1** and sequential composition}

$$= \mathbf{R}\left(\begin{array}{l}\left(\begin{array}{l}\neg\,false\\ \wedge\\ \neg\,(\mathbf{R1}((tr' = tr \wedge a \notin ref') \lhd wait' \rhd (tr' = tr \frown \langle a\rangle)) \wedge \neg\,wait'\ ;\ \mathbf{R1}(true))\end{array}\right)\\ \vdash\\ \mathbf{R1}((tr' = tr \wedge a \notin ref') \lhd wait' \rhd (tr' = tr \frown \langle a\rangle))\ ;\ (\mathtt{II} \lhd wait \rhd \mathbf{R1}(true))\end{array}\right)$$

{Predicate calculus}

$$= \mathbf{R}\left(\begin{array}{l}\neg\,(\mathbf{R1}((tr' = tr \wedge a \notin ref') \lhd wait' \rhd (tr' = tr \frown \langle a\rangle)) \wedge \neg\,wait'\ ;\ \mathbf{R1}(true))\\ \vdash\\ \mathbf{R1}((tr' = tr \wedge a \notin ref') \lhd wait' \rhd (tr' = tr \frown \langle a\rangle))\ ;\ (\mathtt{II} \lhd wait \rhd \mathbf{R1}(true))\end{array}\right)$$

{Predicates are **R1**-healthy}

$$= \mathbf{R}\left(\begin{array}{l}\neg\,(((tr' = tr \wedge a \notin ref') \lhd wait' \rhd (tr' = tr \frown \langle a\rangle)) \wedge \neg\,wait'\ ;\ \mathbf{R1}(true))\\ \vdash\\ ((tr' = tr \wedge a \notin ref') \lhd wait' \rhd (tr' = tr \frown \langle a\rangle))\ ;\ (\mathtt{II} \lhd wait \rhd \mathbf{R1}(true))\end{array}\right)$$

{Property of conditional}

$$= \mathbf{R}\left(\begin{array}{l}\neg\,((tr' = tr \frown \langle a\rangle \wedge \neg\,wait')\ ;\ \mathbf{R1}(true))\\ \vdash\\ ((tr' = tr \wedge a \notin ref') \lhd wait' \rhd (tr' = tr \frown \langle a\rangle))\ ;\ (\mathtt{II} \lhd wait \rhd \mathbf{R1}(true))\end{array}\right)$$

{Definition of $\mathbf{R1}(true)$}

$$= \mathbf{R}\left(\begin{array}{l}\neg\,((tr' = tr \frown \langle a\rangle \wedge \neg\,wait')\ ;\ tr \leq tr')\\ \vdash\\ ((tr' = tr \wedge a \notin ref') \lhd wait' \rhd (tr' = tr \frown \langle a\rangle))\ ;\ (\mathtt{II} \lhd wait \rhd tr \leq tr')\end{array}\right)$$

{Definition of conditional}

$$= \mathbf{R}\left(\begin{array}{l} \neg\,((tr' = tr \frown \langle a\rangle \wedge \neg\, wait')\ ;\ tr \leq tr') \\ \vdash \\ \left(\begin{array}{l}(wait' \wedge tr' = tr \wedge a \notin ref') \\ \vee \\ (\neg\, wait' \wedge tr' = tr \frown \langle a\rangle)\end{array}\right)\ ;\ \left(\begin{array}{l}(wait \wedge \mathit{II}) \\ \vee \\ (\neg\, wait \wedge tr \leq tr')\end{array}\right)\end{array}\right)$$

{Relational calculus}

$$= \mathbf{R}\left(\begin{array}{l} \neg\,((tr' = tr \frown \langle a\rangle \wedge \neg\, wait')\ ;\ tr \leq tr') \\ \vdash \\ \left(\begin{array}{l}(wait' \wedge tr' = tr \wedge a \notin ref')\ ;\ (wait \wedge \mathit{II}) \\ \vee \\ (wait' \wedge tr' = tr \wedge a \notin ref')\ ;\ (\neg\, wait \wedge tr \leq tr') \\ \vee \\ (\neg\, wait' \wedge tr' = tr \frown \langle a\rangle)\ ;\ (wait \wedge \mathit{II}) \\ \vee \\ (\neg\, wait' \wedge tr' = tr \frown \langle a\rangle)\ ;\ (\neg\, wait \wedge tr \leq tr')\end{array}\right)\end{array}\right)$$

{Property of sequential composition}

$$= \mathbf{R}\left(\begin{array}{l} \neg\,((tr' = tr \frown \langle a\rangle \wedge \neg\, wait')\ ;\ tr \leq tr') \\ \vdash \\ \left(\begin{array}{l}(wait' \wedge tr' = tr \wedge a \notin ref')\ ;\ (wait \wedge \mathit{II}) \\ \vee \\ (\neg\, wait' \wedge tr' = tr \frown \langle a\rangle)\ ;\ (\neg\, wait \wedge tr \leq tr')\end{array}\right)\end{array}\right)$$

{Definition of sequential composition}

$$= \mathbf{R}\left(\begin{array}{l} \neg\,(\exists\, wait_0, tr_0, ref_0 \bullet tr_0 = tr \frown \langle a\rangle \wedge \neg\, wait_0 \wedge tr_0 \leq tr') \\ \vdash \\ \left(\begin{array}{l}\left(\begin{array}{l}\exists\, wait_0, tr_0, ref_0 \bullet wait_0 \wedge tr_0 = tr \wedge a \notin ref_0 \wedge wait_0 \\ \wedge\ \mathit{II}[wait_0, tr_0, ref_0/wait, tr, ref]\end{array}\right) \\ \vee \\ (\exists\, wait_0, tr_0, ref_0 \bullet \neg\, wait_0 \wedge tr_0 = tr \frown \langle a\rangle \wedge \neg\, wait_0 \wedge tr_0 \leq tr')\end{array}\right)\end{array}\right)$$

{Definition of II}

$$= \mathbf{R}\left(\begin{array}{l} \neg\,(\exists\, wait_0, tr_0, ref_0 \bullet tr_0 = tr \frown \langle a\rangle \wedge \neg\, wait_0 \wedge tr_0 \leq tr') \\ \vdash \\ \left(\begin{array}{l}\left(\begin{array}{l}\exists\, wait_0, tr_0, ref_0 \bullet wait_0 \wedge tr_0 = tr \wedge a \notin ref_0 \wedge wait_0 \\ \wedge\ wait_0 = wait' \wedge tr_0 = tr' \wedge ref_0 = ref'\end{array}\right) \\ \vee \\ (\exists\, wait_0, tr_0, ref_0 \bullet \neg\, wait_0 \wedge tr_0 = tr \frown \langle a\rangle \wedge \neg\, wait_0 \wedge tr_0 \leq tr')\end{array}\right)\end{array}\right)$$

{One-point rule}

$$= \mathbf{R}\left(\begin{array}{l} \neg\,(tr \frown \langle a\rangle \leq tr') \\ \vdash \\ (a \notin ref' \wedge wait' \wedge tr = tr') \vee (tr \frown \langle a\rangle \leq tr') \end{array}\right)$$

{Predicate calculus}

$$= \mathbf{R}\left(\begin{array}{l} \neg\,(tr \frown \langle a\rangle \leq tr') \\ \vdash \\ \neg\,(tr \frown \langle a\rangle \leq tr') \wedge ((a \notin ref' \wedge wait' \wedge tr = tr') \vee (tr \frown \langle a\rangle \leq tr')) \end{array}\right)$$

{Predicate calculus}

$$= \mathbf{R}(\neg\,(tr \frown \langle a\rangle \leq tr') \vdash (a \notin ref' \wedge wait' \wedge tr = tr'))$$

□

Lemma 3.1.4

$$p2ac(a \to Stop) \sqcup p2ac(b \to Skip)$$
$$=$$
$$\mathbf{RA} \circ \mathbf{A}\left(\begin{array}{l} true \\ \vdash \\ \left(\begin{array}{l} \left(\begin{array}{l} (\exists\, z \bullet z.wait \wedge a \notin z.ref \wedge z.tr = s.tr \wedge z \in ac') \\ \vee \\ (\exists\, z \bullet z.wait \wedge z.tr = s.tr \frown \langle a\rangle \wedge z \in ac') \end{array}\right) \\ \wedge \\ \left(\begin{array}{l} (\exists\, z \bullet z.wait \wedge b \notin z.ref \wedge z.tr = s.tr \wedge z \in ac') \\ \vee \\ (\exists\, z \bullet \neg\, z.wait \wedge z.tr = s.tr \frown \langle b\rangle \wedge z \in ac') \end{array}\right) \end{array}\right) \end{array}\right)$$

Proof.

$p2ac(a \to Stop) \sqcup p2ac(b \to Skip)$

{Definition of event prefixing and Lemma 3.1.1}

$$= \left(\begin{array}{l} p2ac(\mathbf{R}(true \vdash wait' \wedge ((a \notin ref' \wedge tr' = tr) \vee (tr' = tr \frown \langle a\rangle)))) \\ \sqcup \\ p2ac(\mathbf{R}(true \vdash ((b \notin ref' \wedge tr' = tr) \lhd wait' \rhd (tr' = tr \frown \langle b\rangle)))) \end{array}\right)$$

{??}

$$= \left(\begin{array}{l} \mathbf{RA} \circ \mathbf{A}(\neg\ p2ac(\mathit{false}) \vdash p2ac(\mathit{wait}' \wedge ((a \notin \mathit{ref}' \wedge \mathit{tr}' = \mathit{tr}) \vee (\mathit{tr}' = \mathit{tr} \frown \langle a \rangle)))) \\ \sqcup \\ \mathbf{RA} \circ \mathbf{A}(\neg\ p2ac(\mathit{false}) \vdash p2ac((b \notin \mathit{ref}' \wedge \mathit{tr}' = \mathit{tr}) \lhd \mathit{wait}' \rhd (\mathit{tr}' = \mathit{tr} \frown \langle b \rangle))) \end{array} \right)$$

{Predicate calculus and definition of conditional}

$$= \left(\begin{array}{l} \mathbf{RA} \circ \mathbf{A} \left(\begin{array}{l} \neg\ p2ac(\mathit{false}) \\ \vdash \\ p2ac \left(\begin{array}{l} (\mathit{wait}' \wedge a \notin \mathit{ref}' \wedge \mathit{tr}' = \mathit{tr}) \\ \vee \\ (\mathit{wait}' \wedge \mathit{tr}' = \mathit{tr} \frown \langle a \rangle) \end{array} \right) \end{array} \right) \\ \sqcup \\ \mathbf{RA} \circ \mathbf{A} \left(\begin{array}{l} \neg\ p2ac(\mathit{false}) \\ \vdash \\ p2ac \left(\begin{array}{l} (\mathit{wait}' \wedge b \notin \mathit{ref}' \wedge \mathit{tr}' = \mathit{tr}) \\ \vee \\ (\neg\ \mathit{wait}' \wedge \mathit{tr}' = \mathit{tr} \frown \langle b \rangle) \end{array} \right) \end{array} \right) \end{array} \right)$$

{Theorem 1.4.4}

$$= \left(\begin{array}{l} \mathbf{RA} \circ \mathbf{A} \left(\begin{array}{l} \neg\ p2ac(\mathit{false}) \\ \vdash \\ \left(\begin{array}{l} p2ac(\mathit{wait}' \wedge a \notin \mathit{ref}' \wedge \mathit{tr}' = \mathit{tr}) \\ \vee \\ p2ac(\mathit{wait}' \wedge \mathit{tr}' = \mathit{tr} \frown \langle a \rangle) \end{array} \right) \end{array} \right) \\ \sqcup \\ \mathbf{RA} \circ \mathbf{A} \left(\begin{array}{l} \neg\ p2ac(\mathit{false}) \\ \vdash \\ \left(\begin{array}{l} p2ac(\mathit{wait}' \wedge b \notin \mathit{ref}' \wedge \mathit{tr}' = \mathit{tr}) \\ \vee \\ p2ac(\neg\ \mathit{wait}' \wedge \mathit{tr}' = \mathit{tr} \frown \langle b \rangle) \end{array} \right) \end{array} \right) \end{array} \right)$$

{Definition of $p2ac$ and substitution}

$$
= \left(\begin{array}{l}
\mathbf{RA} \circ \mathbf{A} \left(\begin{array}{l} true \\ \vdash \\ \left(\begin{array}{l} (\exists\, z \bullet z.wait \wedge a \notin z.ref \wedge z.tr = s.tr \wedge z \in ac') \\ \vee \\ (\exists\, z \bullet z.wait \wedge z.tr = s.tr \frown \langle a \rangle \wedge z \in ac') \end{array}\right) \end{array}\right) \\
\sqcup \\
\mathbf{RA} \circ \mathbf{A} \left(\begin{array}{l} true \\ \vdash \\ \left(\begin{array}{l} (\exists\, z \bullet z.wait \wedge b \notin z.ref \wedge z.tr = s.tr \wedge z \in ac') \\ \vee \\ (\exists\, z \bullet \neg\, z.wait \wedge z.tr = s.tr \frown \langle b \rangle \wedge z \in ac') \end{array}\right) \end{array}\right)
\end{array}\right)
$$

{Definition of $\sqcup$ under assumption that postconditions are **PBMH**-healthy}

$$
= \mathbf{RA} \circ \mathbf{A} \left(\begin{array}{l}
true \vee true \\
\vdash \\
\left(\begin{array}{l}
true \Rightarrow \left(\begin{array}{l} (\exists\, z \bullet z.wait \wedge a \notin z.ref \wedge z.tr = s.tr \wedge z \in ac') \\ \vee \\ (\exists\, z \bullet z.wait \wedge z.tr = s.tr \frown \langle a \rangle \wedge z \in ac') \end{array}\right) \\
\wedge \\
true \Rightarrow \left(\begin{array}{l} (\exists\, z \bullet z.wait \wedge b \notin z.ref \wedge z.tr = s.tr \wedge z \in ac') \\ \vee \\ (\exists\, z \bullet \neg\, z.wait \wedge z.tr = s.tr \frown \langle b \rangle \wedge z \in ac') \end{array}\right)
\end{array}\right)
\end{array}\right)
$$

{Predicate calculus}

$$
= \mathbf{RA} \circ \mathbf{A} \left(\begin{array}{l}
true \\
\vdash \\
\left(\begin{array}{l}
\left(\begin{array}{l} (\exists\, z \bullet z.wait \wedge a \notin z.ref \wedge z.tr = s.tr \wedge z \in ac') \\ \vee \\ (\exists\, z \bullet z.wait \wedge z.tr = s.tr \frown \langle a \rangle \wedge z \in ac') \end{array}\right) \\
\wedge \\
\left(\begin{array}{l} (\exists\, z \bullet z.wait \wedge b \notin z.ref \wedge z.tr = s.tr \wedge z \in ac') \\ \vee \\ (\exists\, z \bullet \neg\, z.wait \wedge z.tr = s.tr \frown \langle b \rangle \wedge z \in ac') \end{array}\right)
\end{array}\right)
\end{array}\right)
$$

□

3.1.1 Mapping into RA

Lemma 3.1.5

$$
\begin{array}{l}
p2ac(a \rightarrow Skip) \\
= \\
\mathbf{RA} \circ \mathbf{A} \left(\begin{array}{l} true \\ \vdash \\ \exists\, z \bullet z \in ac' \wedge ((z.tr = s.tr \wedge a \notin z.ref) \lhd z.wait \rhd (z.tr = s.tr \frown \langle a \rangle)) \end{array} \right)
\end{array}
$$

Proof.

$$
\begin{array}{l}
p2ac(a \rightarrow Stop) \qquad \{\text{Definition of event prefixing}\} \\
= p2ac \circ \mathbf{R}(true \vdash (tr' = tr \wedge a \notin ref') \lhd wait' \rhd (tr' = tr \frown \langle a \rangle)) \\
\qquad \{\text{Theorem 1.4.12}\} \\
= \mathbf{RA} \circ \mathbf{A} \left(\begin{array}{l} \neg\, p2ac(false) \\ \vdash \\ p2ac((tr' = tr \wedge a \notin ref') \lhd wait' \rhd (tr' = tr \frown \langle a \rangle)) \end{array} \right) \\
\qquad \{\text{Definition of } p2ac \text{ and substitution}\} \\
= \mathbf{RA} \circ \mathbf{A} \left(\begin{array}{l} \neg\, false \\ \vdash \\ \exists\, z \bullet z \in ac' \wedge ((z.tr = s.tr \wedge a \notin z.ref) \lhd z.wait \rhd (z.tr = s.tr \frown \langle a \rangle)) \end{array} \right) \\
\qquad \{\text{Predicate calculus}\} \\
= \mathbf{RA} \circ \mathbf{A} \left(\begin{array}{l} true \\ \vdash \\ \exists\, z \bullet z \in ac' \wedge ((z.tr = s.tr \wedge a \notin z.ref) \lhd z.wait \rhd (z.tr = s.tr \frown \langle a \rangle)) \end{array} \right)
\end{array}
$$

□

Lemma 3.1.6

$$
\begin{array}{l}
p2ac(a \rightarrow Stop) \\
= \\
\mathbf{RA} \circ \mathbf{A} \left(\begin{array}{l} true \\ \vdash \\ \\ \exists\, z \bullet z \in ac' \wedge z.wait \wedge \left(\begin{array}{l} (a \notin z.ref \wedge z.tr = s.tr) \\ \vee \\ (z.tr = s.tr \frown \langle a \rangle) \end{array} \right) \\ \\ \end{array} \right)
\end{array}
$$

Proof.

$$
\begin{array}{l}
p2ac(a \to Stop) \qquad \{\text{Definition of event prefixing (Lemma 3.1.1)}\} \\
= p2ac \circ \mathbf{R}(true \vdash wait' \wedge ((a \notin ref' \wedge tr' = tr) \vee (tr' = tr \frown \langle a \rangle))) \\
\qquad \{\text{Theorem 1.4.12}\} \\
= \mathbf{RA} \circ \mathbf{A} \left(\begin{array}{l} \neg\ p2ac(false) \\ \vdash \\ p2ac\left(\ wait' \wedge ((a \notin ref' \wedge tr' = tr) \vee (tr' = tr \frown \langle a \rangle))\ \right) \end{array} \right) \\
\qquad \{\text{Definition of } p2ac \text{ and substitution}\} \\
= \mathbf{RA} \circ \mathbf{A} \left(\begin{array}{l} \neg\ false \\ \vdash \\ \exists\, z \bullet z \in ac' \wedge \left(\ z.wait \wedge ((a \notin z.ref \wedge z.tr = s.tr) \vee (z.tr = s.tr \frown \langle a \rangle))\ \right) \end{array} \right) \\
\qquad \{\text{Predicate calculus}\} \\
= \mathbf{RA} \circ \mathbf{A} \left(\begin{array}{l} true \\ \vdash \\ \exists\, z \bullet z \in ac' \wedge z.wait \wedge \left(\begin{array}{l} (a \notin z.ref \wedge z.tr = s.tr) \\ \vee \\ (z.tr = s.tr \frown \langle a \rangle) \end{array} \right) \end{array} \right)
\end{array}
$$

□

Lemma 3.1.7

$$
\begin{array}{l}
p2ac(a \to Chaos) \\
= \\
\mathbf{RA} \circ \mathbf{A} \left(\begin{array}{l} \neg\ (\exists\, z \bullet z \in ac' \wedge s.tr \frown \langle a \rangle \leq z.tr) \\ \vdash \\ \exists\, z \bullet z \in ac' \wedge z.wait \wedge z.tr = s.tr \wedge a \notin z.ref \end{array} \right)
\end{array}
$$

Proof.

$$
\begin{array}{l}
p2ac(a \to Chaos) \qquad \{\text{Definition of event prefixing (Lemma 3.1.3)}\} \\
= p2ac \circ \mathbf{R}(\neg\ (tr \frown \langle a \rangle \leq tr') \vdash wait' \wedge tr' = tr \wedge a \notin ref') \\
\qquad \{\text{Theorem 1.4.12}\} \\
= \mathbf{RA} \circ \mathbf{A}(\neg\ p2ac(tr \frown \langle a \rangle \leq tr') \vdash p2ac(wait' \wedge tr' = tr \wedge a \notin ref')) \\
\qquad \{\text{Definition of } p2ac \text{ and substitution}\} \\
= \mathbf{RA} \circ \mathbf{A} \left(\begin{array}{l} \neg\ (\exists\, z \bullet z \in ac' \wedge s.tr \frown \langle a \rangle \leq z.tr) \\ \vdash \\ \exists\, z \bullet z \in ac' \wedge z.wait \wedge z.tr = s.tr \wedge a \notin z.ref \end{array} \right)
\end{array}
$$

□

Lemma 3.1.8

$$p2ac(a \rightarrow Choice) = \mathbf{RA} \circ \mathbf{A} \left(\begin{array}{l} true \\ \vdash \\ \exists\, z \bullet z \in ac' \wedge (z.tr = s.tr \wedge a \notin z.ref \wedge z.wait) \vee (s.tr \frown \langle a \rangle \leq z.tr)) \end{array} \right)$$

Proof.

$$\begin{array}{ll} & p2ac(a \rightarrow Choice) \qquad \{\text{Lemma 3.1.2}\} \\ = & p2ac \circ \mathbf{R} \left(\begin{array}{l} true \\ \vdash \\ (tr' = tr \wedge a \notin ref' \wedge wait') \vee (tr \frown \langle a \rangle \leq tr') \end{array} \right) \\ & \qquad \{\text{Theorem 1.4.12}\} \\ = & \mathbf{RA} \circ \mathbf{A} \left(\begin{array}{l} \neg\, p2ac(\neg\, true) \\ \vdash \\ p2ac((tr' = tr \wedge a \notin ref' \wedge wait') \vee (tr \frown \langle a \rangle \leq tr')) \end{array} \right) \\ & \qquad \{\text{Definition of } p2ac \text{ and substitution}\} \\ = & \mathbf{RA} \circ \mathbf{A} \left(\begin{array}{l} \neg\, false \\ \vdash \\ \exists\, z \bullet z \in ac' \wedge (z.tr = s.tr \wedge a \notin z.ref \wedge z.wait) \vee (s.tr \frown \langle a \rangle \leq z.tr)) \end{array} \right) \\ & \qquad \{\text{Predicate calculus}\} \\ = & \mathbf{RA} \circ \mathbf{A} \left(\begin{array}{l} true \\ \vdash \\ \exists\, z \bullet z \in ac' \wedge (z.tr = s.tr \wedge a \notin z.ref \wedge z.wait) \vee (s.tr \frown \langle a \rangle \leq z.tr)) \end{array} \right) \end{array}$$

□

3.1.2 Results with operators

Lemma 3.1.9

$$p2ac(a \rightarrow Chaos) \sqcup p2ac(b \rightarrow Skip) = p2ac(a \rightarrow Choice) \sqcup p2ac(b \rightarrow Skip)$$

Proof.

$$
\begin{array}{ll}
p2ac(a \to Chaos) \sqcup p2ac(b \to Skip) & \{\text{Lemmas 3.1.5 and 3.1.7}\} \\
= \left(\begin{array}{l} \mathbf{RA} \circ \mathbf{A} \left(\begin{array}{l} \neg\, (\exists\, z \bullet z \in ac' \wedge s.tr \frown \langle a \rangle \leq z.tr) \\ \vdash \\ \exists\, z \bullet z \in ac' \wedge z.wait \wedge z.tr = s.tr \wedge a \notin z.ref \end{array} \right) \\ \sqcup \\ \mathbf{RA} \circ \mathbf{A} \left(\begin{array}{l} true \\ \vdash \\ \exists\, z \bullet z \in ac' \wedge ((z.tr = s.tr \wedge b \notin z.ref) \lhd z.wait \rhd (z.tr = s.tr \frown \langle b \rangle)) \end{array} \right) \end{array} \right) & \\
& \{\text{Definition of } \sqcup\} \\
= \mathbf{RA} \circ \mathbf{A} \left(\begin{array}{l} \left(\begin{array}{l} \neg\, \mathbf{PBMH}(\exists\, z \bullet z \in ac' \wedge s.tr \frown \langle a \rangle \leq z.tr) \\ \vee \\ \neg\, \mathbf{PBMH}(false) \end{array} \right) \\ \vdash \\ \left(\begin{array}{l} \left(\begin{array}{l} \neg\, \mathbf{PBMH}(\exists\, z \bullet z \in ac' \wedge s.tr \frown \langle a \rangle \leq z.tr) \\ \Rightarrow \\ \mathbf{PBMH}(\exists\, z \bullet z \in ac' \wedge z.wait \wedge z.tr = s.tr \wedge a \notin z.ref) \end{array} \right) \\ \wedge \\ \left(\begin{array}{l} \neg\, \mathbf{PBMH}(false) \\ \Rightarrow \\ \mathbf{PBMH} \left(\exists\, z \bullet z \in ac' \wedge \left(\begin{array}{l} (z.tr = s.tr \wedge b \notin z.ref) \\ \lhd z.wait \rhd \\ (z.tr = s.tr \frown \langle b \rangle) \end{array} \right) \right) \end{array} \right) \end{array} \right) \end{array} \right) & \\
& \{\mathbf{PBMH} \circ p2ac(P) = p2ac(P)\}
\end{array}
$$

$$= \mathbf{RA} \circ \mathbf{A} \left(\begin{array}{l} \left(\begin{array}{l} \neg\ (\exists\, z \bullet z \in ac' \land s.tr \frown \langle a \rangle \leq z.tr) \\ \lor \\ \neg\ (\mathit{false}) \end{array} \right) \\ \vdash \\ \left(\begin{array}{l} \left(\begin{array}{l} \neg\ (\exists\, z \bullet z \in ac' \land s.tr \frown \langle a \rangle \leq z.tr) \\ \Rightarrow \\ (\exists\, z \bullet z \in ac' \land z.wait \land z.tr = s.tr \land a \notin z.ref) \end{array} \right) \\ \land \\ \left(\begin{array}{l} \neg\ (\mathit{false}) \\ \Rightarrow \\ \left(\exists\, z \bullet z \in ac' \land \left(\begin{array}{l} (z.tr = s.tr \land b \notin z.ref) \\ \lhd z.wait \rhd \\ (z.tr = s.tr \frown \langle b \rangle) \end{array} \right) \right) \end{array} \right) \end{array} \right) \end{array} \right)$$

{Predicate calculus}

$$= \mathbf{RA} \circ \mathbf{A} \left(\begin{array}{l} \mathit{true} \\ \vdash \\ \left(\begin{array}{l} \left(\begin{array}{l} (\exists\, z \bullet z \in ac' \land s.tr \frown \langle a \rangle \leq z.tr) \\ \lor \\ (\exists\, z \bullet z \in ac' \land z.wait \land z.tr = s.tr \land a \notin z.ref) \end{array} \right) \\ \land \\ \left(\exists\, z \bullet z \in ac' \land \left(\begin{array}{l} (z.tr = s.tr \land b \notin z.ref) \\ \lhd z.wait \rhd \\ (z.tr = s.tr \frown \langle b \rangle) \end{array} \right) \right) \end{array} \right) \end{array} \right)$$

{Predicate calculus}

$$= \mathbf{RA} \circ \mathbf{A} \left(\begin{array}{l} \mathit{true} \\ \vdash \\ \left(\begin{array}{l} \exists\, z \bullet z \in ac' \land \left(\begin{array}{l} (s.tr \frown \langle a \rangle \leq z.tr) \\ \lor \\ (z.wait \land z.tr = s.tr \land a \notin z.ref) \end{array} \right) \\ \land \\ \left(\exists\, z \bullet z \in ac' \land \left(\begin{array}{l} (z.tr = s.tr \land b \notin z.ref) \\ \lhd z.wait \rhd \\ (z.tr = s.tr \frown \langle b \rangle) \end{array} \right) \right) \end{array} \right) \end{array} \right)$$

{Predicates are **PBMH**-healthy and definition of $\sqcup$}

$$= \left(\begin{array}{l} \left(\begin{array}{l} true \vdash \exists\, z \bullet z \in ac' \wedge \left(\begin{array}{l} (s.tr \frown \langle a \rangle \leq z.tr) \\ \vee \\ (z.wait \wedge z.tr = s.tr \wedge a \notin z.ref) \end{array} \right) \end{array} \right) \\ \sqcup \\ \left(\begin{array}{l} true \vdash \exists\, z \bullet z \in ac' \wedge \left(\begin{array}{l} (z.tr = s.tr \wedge b \notin z.ref) \\ \lhd z.wait \rhd \\ (z.tr = s.tr \frown \langle b \rangle) \end{array} \right) \end{array} \right) \end{array} \right)$$

{Lemmas 3.1.5 and 3.1.8}

$$= p2ac(a \rightarrow Choice) \sqcup p2ac(b \rightarrow Skip)$$

□

Lemma 3.1.10

$$p2ac(a \rightarrow Stop) \sqcup p2ac(a \rightarrow Skip) = ??$$

Proof.

$p2ac(a \rightarrow Stop) \sqcup p2ac(a \rightarrow Skip)$ {Lemma 3.1.4}

$$= \mathbf{RA} \circ \mathbf{A} \left(\begin{array}{l} true \\ \vdash \\ \left(\begin{array}{l} \left(\begin{array}{l} (\exists\, z \bullet z.wait \wedge a \notin z.ref \wedge z.tr = s.tr \wedge z \in ac') \\ \vee \\ (\exists\, z \bullet z.wait \wedge z.tr = s.tr \frown \langle a \rangle \wedge z \in ac') \end{array} \right) \\ \wedge \\ \left(\begin{array}{l} (\exists\, z \bullet z.wait \wedge a \notin z.ref \wedge z.tr = s.tr \wedge z \in ac') \\ \vee \\ (\exists\, z \bullet \neg\, z.wait \wedge z.tr = s.tr \frown \langle a \rangle \wedge z \in ac') \end{array} \right) \end{array} \right) \end{array} \right)$$

{Predicate calculus}

$$= \mathbf{RA} \circ \mathbf{A} \left(\begin{array}{l} true \\ \vdash \\ \left(\begin{array}{l} (\exists\, z \bullet z.wait \wedge a \notin z.ref \wedge z.tr = s.tr \wedge z \in ac') \\ \vee \\ \left(\begin{array}{l} (\exists\, z \bullet z.wait \wedge z.tr = s.tr \frown \langle a \rangle \wedge z \in ac') \\ \wedge \\ (\exists\, z \bullet \neg\, z.wait \wedge z.tr = s.tr \frown \langle a \rangle \wedge z \in ac') \end{array} \right) \end{array} \right) \end{array} \right)$$

□

Lemma 3.1.11

$$p2ac(a \rightarrow Chaos) \sqcup p2ac(a \rightarrow Skip) = p2ac(a \rightarrow Skip)$$

Proof.

$p2ac(a \rightarrow Chaos) \sqcup p2ac(a \rightarrow Skip)$ {Steps from proof of Lemma 3.1.9}

$$= \mathbf{RA} \circ \mathbf{A} \left(\begin{array}{l} true \\ \vdash \\ \left(\begin{array}{l} \exists\, z \bullet z \in ac' \wedge \left(\begin{array}{l} (s.tr \frown \langle a \rangle \leq z.tr) \\ \vee \\ (z.wait \wedge z.tr = s.tr \wedge a \notin z.ref) \end{array} \right) \\ \wedge \\ \left(\exists\, z \bullet z \in ac' \wedge \left(\begin{array}{l} (z.tr = s.tr \wedge a \notin z.ref) \\ \lhd z.wait \rhd \\ (z.tr = s.tr \frown \langle a \rangle) \end{array} \right) \right) \end{array} \right) \end{array} \right)$$

{Definition of conditional and predicate calculus}

$$= \mathbf{RA} \circ \mathbf{A} \left(\begin{array}{l} true \\ \vdash \\ \left(\begin{array}{l} \left(\begin{array}{l} (\exists\, z \bullet z \in ac' \wedge s.tr \frown \langle a \rangle \leq z.tr) \\ \vee \\ (\exists\, z \bullet z \in ac' \wedge z.wait \wedge z.tr = s.tr \wedge a \notin z.ref) \end{array} \right) \\ \wedge \\ \left(\begin{array}{l} (\exists\, z \bullet z \in ac' \wedge z.wait \wedge z.tr = s.tr \wedge a \notin z.ref) \\ \vee \\ (\exists\, z \bullet z \in ac' \wedge \neg\, z.wait \wedge z.tr = s.tr \frown \langle a \rangle) \end{array} \right) \end{array} \right) \end{array} \right)$$

{Predicate calculus}

$$= \mathbf{RA} \circ \mathbf{A} \left(\begin{array}{l} true \\ \vdash \\ \left(\begin{array}{l} (\exists\, z \bullet z \in ac' \wedge z.wait \wedge z.tr = s.tr \wedge a \notin z.ref) \\ \vee \\ \left(\begin{array}{l} (\exists\, z \bullet z \in ac' \wedge s.tr \frown \langle a \rangle \leq z.tr) \\ \wedge \\ (\exists\, z \bullet z \in ac' \wedge \neg\, z.wait \wedge z.tr = s.tr \frown \langle a \rangle) \end{array} \right) \end{array} \right) \end{array} \right)$$

{Predicate calculus}

$$= \mathbf{RA} \circ \mathbf{A} \left(\begin{array}{l} true \\ \vdash \\ \left(\begin{array}{l} (\exists\, z \bullet z \in ac' \wedge z.wait \wedge z.tr = s.tr \wedge a \notin z.ref) \\ \vee \\ (\exists\, z \bullet z \in ac' \wedge \neg\, z.wait \wedge z.tr = s.tr \frown \langle a \rangle) \end{array} \right) \end{array} \right)$$

{Definition of conditional and predicate calculus}

$$= \mathbf{RA} \circ \mathbf{A} \left(\begin{array}{l} true \\ \vdash \\ \exists\, z \bullet z \in ac' \wedge ((z.tr = s.tr \wedge a \notin z.ref) \lhd z.wait \rhd (z.tr = s.tr \frown \langle a \rangle)) \end{array} \right)$$

{Lemma 3.1.5}

$$= p2ac(a \rightarrow Skip)$$

□

Acronyms

CSP Communicating Sequential Processes

ZRC Z Refinement Calculus

VDM Vienna Development Method

ASM Abstract State Machine

FSM Finite State Machines

CCS Calculus of Concurrent Systems

JCSP Java Communicating Sequential Processes

FDR Failures-Divergence Refinement

UTP Unifying Theories of Programming

BNF Backus-Naur Normal Form

Bibliography

[1] J. Woodcock and J. Davies, *Using Z: Specification, Refinement, and Proof*. Prentice Hall, 1996.

[2] A. Cavalcanti, A. Wellings, and J. Woodcock, "The Safety-Critical Java Memory Model: A Formal Account," in *FM 2011: Formal Methods*, ser. Lecture Notes in Computer Science, M. Butler and W. Schulte, Eds. Springer Berlin / Heidelberg, 2011, vol. 6664, pp. 246–261. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-21437-0_20

Appendix A

Lemmas on A

A.1 A

Lemma A.1.1

$$\mathbf{A}(P)[e/s] = \mathbf{A}(P[e/s])$$

Proof.

$$\begin{array}{ll}
\mathbf{A}(P)[e/s] & \{\text{Definition of } \mathbf{A}\} \\
= (\mathbf{A0} \circ \mathbf{PBMH}(P))[e/s] & \{\text{Lemma A.2.1}\} \\
= \mathbf{A0} \circ (\mathbf{PBMH}(P))[e/s] & \{\text{Lemma E.5.2}\} \\
= \mathbf{A0} \circ \mathbf{PBMH}(P[e/s]) & \{\text{Definition of } \mathbf{A}\} \\
= \mathbf{A}(P[e/s]) &
\end{array}$$

□

Lemma A.1.2

$$s.x = v \land P \Leftrightarrow s.x = v \land P[s \oplus \{x \mapsto v\}/s]$$

Proof.

$$\begin{array}{ll}
s.x = v \land P & \{\text{Predicate calculus for fresh variable } z\} \\
\Leftrightarrow \exists\, z \bullet s.x = v \land z = s \land P[z/s] & \{\text{Relational calculus}\} \\
\Leftrightarrow \exists\, z \bullet s.x = v \land z = s \oplus \{x \mapsto v\} \land P[z/s] & \{\text{One-point rule}\} \\
\Leftrightarrow s.x = v \land P[z/s][s \oplus \{x \mapsto v\}/z] & \{\text{Substitution}\} \\
\Leftrightarrow s.x = v \land P[s \oplus \{x \mapsto v\}/s] &
\end{array}$$

□

A.2 A0

Lemma A.2.1 *Provided ok' not free in e.*

$$\mathbf{A0}(P)[e/s] = \mathbf{A0}(P[e/s])$$

Proof.

$\mathbf{A0}(P)[e/s]$ {Definition of **A0**}
$= (P \wedge (ok \wedge \neg\, P^f) \Rightarrow (ok' \Rightarrow ac' \neq \emptyset))[e/s]$ {Property of substitution}
$= (P[z/s] \wedge (ok \wedge \neg\, P^f[e/s]) \Rightarrow (ok' \Rightarrow ac' \neq \emptyset))$
{Property of substitution: ok' not free in e}
$= (P[z/s] \wedge (ok \wedge \neg\, P[e/s]^f) \Rightarrow (ok' \Rightarrow ac' \neq \emptyset))$ {Definition of **A0**}
$= \mathbf{A0}(P[e/s])$

□

A.3 A2

A.3.1 Lemmas

Lemma A.3.1

$$\mathbf{A2}(P) = \exists\, ac_0 \bullet P[\{s \mid \{s\} = ac_0\}/ac'] \wedge ac_0 \subseteq ac'$$

Proof.

$\mathbf{A2}(P)$ {Definition of **A2**}
$= \mathbf{PBMH}(P\ ;_{\mathcal{A}}\ \{s\} = ac')$ {Definition of $;_{\mathcal{A}}$ and substitution}
$= \mathbf{PBMH}(P[\{s \mid \{s\} = ac'\}/ac'])$
{Definition of **PBMH** (Lemma E.1.1)}
$= \exists\, ac_0 \bullet P[\{s \mid \{s\} = ac'\}/ac'][ac_0/ac'] \wedge ac_0 \subseteq ac'$
{Property of substitution}
$= \exists\, ac_0 \bullet P[\{s \mid \{s\} = ac_0\}/ac'] \wedge ac_0 \subseteq ac'$

□

Lemma A.3.2

$$\mathbf{A2} \circ \mathbf{A}(\neg\ P^f \vdash P^t)$$
$$=$$
$$(\neg\ \mathbf{A2} \circ \mathbf{PBMH}(P^f) \vdash \mathbf{A2}(\mathbf{PBMH}(P^t) \wedge ac' \neq \emptyset))$$

Proof.

$\mathbf{A2} \circ \mathbf{A}(\neg\ P^f \vdash P^t)$ {Definition of $\mathbf{A}$}
$= \mathbf{A2}(\neg\ \mathbf{PBMH}(P^f) \vdash \mathbf{PBMH}(P^t) \wedge ac' \neq \emptyset)$ {Definition of design}
$= \mathbf{A2}((ok \wedge \neg\ \mathbf{PBMH}(P^f)) \Rightarrow (\mathbf{PBMH}(P^t) \wedge ac' \neq \emptyset \wedge ok'))$ {Predicate calculus}
$= \mathbf{A2}(\neg\ ok \vee \mathbf{PBMH}(P^f) \vee (\mathbf{PBMH}(P^t) \wedge ac' \neq \emptyset \wedge ok'))$ {Distributivity of **A2** (Theorem A.3.2)}
$= \mathbf{A2}(\neg\ ok) \vee \mathbf{A2} \circ \mathbf{PBMH}(P^f) \vee \mathbf{A2}(\mathbf{PBMH}(P^t) \wedge ac' \neq \emptyset \wedge ok')$ {Lemmas A.3.6 and A.3.7}
$= \neg\ ok \vee \mathbf{A2} \circ \mathbf{PBMH}(P^f) \vee (\mathbf{A2}(\mathbf{PBMH}(P^t) \wedge ac' \neq \emptyset) \wedge ok')$ {Predicate calculus}
$= (ok \wedge \neg\ \mathbf{A2} \circ \mathbf{PBMH}(P^f)) \Rightarrow (\mathbf{A2}(\mathbf{PBMH}(P^t) \wedge ac' \neq \emptyset) \wedge ok')$ {Definition of design}
$= (\neg\ \mathbf{A2} \circ \mathbf{PBMH}(P^f) \vdash \mathbf{A2}(\mathbf{PBMH}(P^t) \wedge ac' \neq \emptyset))$

□

Lemma A.3.3

$$\mathbf{A2}(\mathit{false}) = \mathit{false}$$

Proof.

$\mathbf{A2}(\mathit{false})$ {Definition of $\mathbf{A2}$}
$= \mathbf{PBMH}(\mathit{false}\ ;_{\mathcal{A}}\ \{s\} = ac')$ {Property of $;_{\mathcal{A}}$}
$= \mathbf{PBMH}(\mathit{false})$ {Property of $\mathbf{PBMH}$}
$= \mathit{false}$

□

Lemma A.3.4

$$\mathbf{A2}(\mathit{true}) = \mathit{true}$$

Proof.

$$\begin{array}{ll}
\mathbf{A2}(\mathit{true}) & \{\text{Definition of } \mathbf{A2}\} \\
= \mathbf{PBMH}(\mathit{true} \ ;_{\mathcal{A}} \{s\} = ac') & \{\text{Property of } ;_{\mathcal{A}}\} \\
= \mathbf{PBMH}(\mathit{true}) & \{\text{Property of } \mathbf{PBMH}\} \\
= \mathit{true}
\end{array}$$

□

Lemma A.3.5 *Provided ac' is not free in P.*

$$\mathbf{A2}(\exists\, y \bullet y \in ac' \wedge P) = \exists\, y \bullet y \in ac' \wedge P$$

Proof.

$$\begin{array}{ll}
\mathbf{A2}(\exists\, y \bullet y \in ac' \wedge P) & \{\text{Definition of } \mathbf{A2}\} \\
= \mathbf{PBMH}((\exists\, y \bullet y \in ac' \wedge P) \ ;_{\mathcal{A}} \{s\} = ac') & \\
\qquad \{\text{Definition of } ;_{\mathcal{A}} \text{ and substitution: } ac' \text{ not free in } P\} & \\
= \mathbf{PBMH}(\exists\, y \bullet y \in \{s \mid \{s\} = ac'\} \wedge P) & \{\text{Property of sets}\} \\
= \mathbf{PBMH}(\exists\, y \bullet \{y\} = ac' \wedge P) & \{\text{Definition of } \mathbf{PBMH} \text{ (Lemma E.1.1)}\} \\
= \exists\, ac_0 \bullet (\exists\, y \bullet \{y\} = ac' \wedge P)[ac_0/ac'] \wedge ac_0 \subseteq ac' & \\
\qquad \{\text{Substitution: } ac' \text{ not free in } P\} & \\
= \exists\, ac_0, y \bullet \{y\} = ac_0 \wedge P \wedge ac_0 \subseteq ac' & \{\text{Predicate calculus}\} \\
= \exists\, y \bullet \{y\} \subseteq ac' \wedge P & \{\text{Property of sets}\} \\
= \exists\, y \bullet y \in ac' \wedge P &
\end{array}$$

□

A.3.2 Properties

Theorem A.3.1 (**A2**-idempotent) *Provided P is* **PBMH**-*healthy.*

$$\mathbf{A2} \circ \mathbf{A2}(P) = \mathbf{A2}(P)$$

Proof.

$$
\begin{aligned}
&\mathbf{A2} \circ \mathbf{A2}(P) && \{\text{Definition of } \mathbf{A2} \text{ twice}\} \\
&= \mathbf{PBMH}(\mathbf{PBMH}(P \ ;_{\mathcal{A}} \{s \mid \{s\} = ac'\}) \ ;_{\mathcal{A}} \{s \mid \{s\} = ac'\}) \\
& && \{P \text{ is } \mathbf{PBMH}\text{-healthy and Lemma A.3.11}\} \\
&= \mathbf{PBMH}(P \ ;_{\mathcal{A}} \{s \mid \{s\} = ac'\}) && \{\text{Definition of } \mathbf{A2}\} \\
&= \mathbf{A2}(P)
\end{aligned}
$$

□

Theorem A.3.2

$$\mathbf{A2}(P \vee Q) = \mathbf{A2}(P) \vee \mathbf{A2}(Q)$$

Proof.

$$
\begin{aligned}
&\mathbf{A2}(P \vee Q) && \{\text{Definition of } \mathbf{A2}\} \\
&= \mathbf{PBMH}((P \vee Q) \ ;_{\mathcal{A}} \{s\} = ac') \\
& && \{\text{Distributivity of } ;_{\mathcal{A}} \text{ (Lemma F.1.4)}\} \\
&= \mathbf{PBMH}((P \ ;_{\mathcal{A}} \{s\} = ac') \vee (Q \ ;_{\mathcal{A}} \{s\} = ac')) \\
& && \{\text{Distributivity of } \mathbf{PBMH}\} \\
&= \mathbf{PBMH}(P \ ;_{\mathcal{A}} \{s\} = ac') \vee \mathbf{PBMH}(Q \ ;_{\mathcal{A}} \{s\} = ac') \\
& && \{\text{Definition of } \mathbf{A2}\} \\
&= \mathbf{A2}(P) \vee \mathbf{A2}(Q)
\end{aligned}
$$

□

Lemma A.3.6 *Provided ac' is not free in P.*

$$\mathbf{A2}(P \wedge Q) = P \wedge \mathbf{A2}(Q)$$

Proof.

$$
\begin{aligned}
&\mathbf{A2}(P \wedge Q) && \{\text{Definition of } \mathbf{A2}\} \\
&= \mathbf{PBMH}((P \wedge Q) \ ;_{\mathcal{A}} \{s\} = ac') && \{\text{Distributivity of } ;_{\mathcal{A}}\} \\
&= \mathbf{PBMH}((P \ ;_{\mathcal{A}} \{s\} = ac') \wedge (Q \ ;_{\mathcal{A}} \{s\} = ac')) \\
& && \{\text{Assumption: } ac' \text{ not free in } P\} \\
&= \mathbf{PBMH}(P \wedge (Q \ ;_{\mathcal{A}} \{s\} = ac')) \\
& && \{\text{Assumption: } ac' \text{ not free in } P \text{ and property of } \mathbf{PBMH}\} \\
&= P \wedge \mathbf{PBMH}(Q \ ;_{\mathcal{A}} \{s\} = ac') && \{\text{Definition of } \mathbf{A2}\} \\
&= P \wedge \mathbf{A2}(Q)
\end{aligned}
$$

□

Lemma A.3.7 *Provided ac' not free in P.*

$$\mathbf{A2}(P) = P$$

Proof.

$\mathbf{A2}(P)$ {Definition of **A2**}
$= \mathbf{PBMH}(P \ ;_{\mathcal{A}} \{s\} = ac')$ {Assumption: ac' not free in P}
$= \mathbf{PBMH}(P)$ {Assumption: ac' not free in P and property of **PBMH**}
$= P$

□

Lemma A.3.8

$$\mathbf{A2}(P \wedge ac' \neq \emptyset) = \exists\, z \bullet P[\{z\}/ac'] \wedge z \in ac'$$

Proof.

$\mathbf{A2}(P \wedge ac' \neq \emptyset)$ {Definition of **A2** (Lemma A.3.1)}
$= \exists\, ac_0 \bullet ((P \wedge ac' \neq \emptyset)[\{s \mid \{s\} = ac_0\}/ac'] \wedge ac_0 \subseteq ac')$ {Substitution}
$= \exists\, ac_0 \bullet P[\{s \mid \{s\} = ac_0\}/ac'] \wedge \{s \mid \{s\} = ac_0\} \neq \emptyset \wedge ac_0 \subseteq ac')$
{Property of sets}
$= \exists\, ac_0 \bullet P[\{s \mid \{s\} = ac_0\}/ac'] \wedge \exists\, z \bullet \{z\} = ac_0 \wedge ac_0 \subseteq ac'$
{Predicate calculus}
$= \exists\, ac_0, z \bullet P[\{s \mid \{s\} = ac_0\}/ac'] \wedge \{z\} = ac_0 \wedge ac_0 \subseteq ac'$
{One-point rule}
$= \exists\, z \bullet P[\{s \mid \{s\} = \{z\}\}/ac'] \wedge \{z\} \subseteq ac'$ {Property of sets}
$= \exists\, z \bullet P[\{z\}/ac'] \wedge z \in ac'$

□

Lemma A.3.9

$$\mathbf{A2}(P \wedge ac' = \emptyset) = P[\emptyset/ac']$$

Proof.

$$
\begin{array}{ll}
\mathbf{A2}(P \wedge ac' = \emptyset) & \{\text{Definition of } \mathbf{A2} \text{ (Lemma A.3.1)}\} \\
= \exists\, ac_0 \bullet ((P \wedge ac' = \emptyset)[\{s \mid \{s\} = ac_0\}/ac'] \wedge ac_0 \subseteq ac') & \{\text{Substitution}\} \\
= \exists\, ac_0 \bullet P[\{s \mid \{s\} = ac_0\}/ac'] \wedge \{s \mid \{s\} = ac_0\} = \emptyset \wedge ac_0 \subseteq ac') & \\
& \{\text{Property of sets}\} \\
= \exists\, ac_0 \bullet P[\{s \mid \{s\} = ac_0\}/ac'] \wedge \neg\, (\exists\, z \bullet \{z\} = ac_0) \wedge ac_0 \subseteq ac' & \\
& \{\text{Predicate calculus}\} \\
= \exists\, ac_0 \bullet P[\{s \mid \{s\} = ac_0\}/ac'] \wedge (\forall\, z \bullet \{z\} \neq ac_0) \wedge ac_0 \subseteq ac' & \\
& \{\text{Predicate calculus}\} \\
= \exists\, ac_0 \bullet P[\{s \mid \mathit{false}\}/ac'] \wedge (\forall\, z \bullet \{z\} \neq ac_0) \wedge ac_0 \subseteq ac' & \\
& \{\text{Property of sets}\} \\
= \exists\, ac_0 \bullet P[\emptyset/ac'] \wedge (\forall\, z \bullet \{z\} \neq ac_0) \wedge ac_0 \subseteq ac' & \{\text{Predicate calculus}\} \\
= P[\emptyset/ac'] \wedge \exists\, ac_0 \bullet (\forall\, z \bullet \{z\} \neq ac_0) \wedge ac_0 \subseteq ac' & \{\text{Predicate calculus}\} \\
= P[\emptyset/ac'] &
\end{array}
$$

□

Lemma A.3.10

$$\mathbf{A2}(P)[\emptyset/ac'] = P[\emptyset/ac']$$

Proof.

$$
\begin{array}{ll}
\mathbf{A2}(P)[\emptyset/ac'] & \{\text{Definition of } \mathbf{A2} \text{ (Lemma A.3.1)}\} \\
= (\exists\, ac_0 \bullet P[\{s \mid \{s\} = ac_0\}/ac'] \wedge ac_0 \subseteq ac')[\emptyset/ac'] & \{\text{Substitution}\} \\
= \exists\, ac_0 \bullet P[\{s \mid \{s\} = ac_0\}/ac'] \wedge ac_0 \subseteq \emptyset & \{\text{Property of sets}\} \\
= \exists\, ac_0 \bullet P[\{s \mid \{s\} = ac_0\}/ac'] \wedge ac_0 = \emptyset & \{\text{One-point rule}\} \\
= P[\{s \mid \{s\} = \emptyset\}/ac'] & \{\text{Property of sets}\} \\
= P[\emptyset/ac'] &
\end{array}
$$

□

A.3.3 Properties with respect to PBMH

Lemma A.3.11 *Provided P is* **PBMH***-healthy.*

$$\mathbf{PBMH}(P \;;_{\mathcal{A}} \{s \mid \{s\} = ac'\}) \;;_{\mathcal{A}} \{s \mid \{s\} = ac'\}$$

$$
\begin{array}{l}
= \\
P \ ;_{\mathcal{A}} \{s \mid \{s\} = ac'\}
\end{array}
$$

Proof.

$$
\begin{array}{l}
\mathbf{PBMH}(P \ ;_{\mathcal{A}} \{s \mid \{s\} = ac'\}) \ ;_{\mathcal{A}} \{s \mid \{s\} = ac'\} \\
\qquad \{\text{Assumption: } P \text{ is } \mathbf{PBMH}\text{-healthy and Lemma E.7.1}\} \\
= \left(\begin{array}{l} (\exists\, ac_1, ac_0 \bullet P[ac_0/ac'] \wedge ac_0 \subseteq \{s \mid \{s\} = ac_1\} \wedge ac_1 \subseteq ac') \\ ;_{\mathcal{A}} \\ \{s \mid \{s\} = ac'\} \end{array} \right) \\
\qquad \{\text{Definition of } ;_{\mathcal{A}} \text{ and substitution}\} \\
= \left(\ \exists\, ac_1, ac_0 \bullet P[ac_0/ac'] \wedge ac_0 \subseteq \{s \mid \{s\} = ac_1\} \wedge ac_1 \subseteq \{s \mid \{s\} = ac'\} \ \right) \\
\qquad \{\text{Lemma H.1.5}\} \\
= \left(\begin{array}{l} \exists\, ac_1, ac_0 \bullet P[ac_0/ac'] \\ \wedge\ ac_0 \subseteq ac_1 \wedge ac_0 \subseteq \{s \mid ac_1 \subseteq \{s\}\} \\ \wedge\ ac_1 \subseteq \{s \mid \{s\} = ac'\} \end{array} \right) \qquad \{\text{Lemma H.1.6}\} \\
= \left(\begin{array}{l} \exists\, ac_1, ac_0 \bullet P[ac_0/ac'] \\ \wedge\ ac_0 \subseteq ac_1 \wedge ac_1 \subseteq \{s \mid ac_0 \subseteq \{s\}\} \\ \wedge\ ac_1 \subseteq \{s \mid \{s\} = ac'\} \end{array} \right) \qquad \{\text{Property of sets}\} \\
= \left(\ \exists\, ac_1, ac_0 \bullet P[ac_0/ac'] \wedge ac_0 \subseteq ac_1 \wedge ac_1 \subseteq \{s \mid ac_0 \subseteq \{s\} \wedge \{s\} = ac'\} \ \right) \\
\qquad \{\text{Transitivity of subset inclusion}\} \\
= \left(\ \exists\, ac_0 \bullet P[ac_0/ac'] \wedge ac_0 \subseteq \{s \mid ac_0 \subseteq \{s\} \wedge \{s\} = ac'\} \ \right) \\
\qquad \{\text{Predicate calculus}\} \\
= \left(\ \exists\, ac_0 \bullet P[ac_0/ac'] \wedge ac_0 \subseteq \{s \mid ac_0 \subseteq ac' \wedge \{s\} = ac'\} \ \right) \\
\qquad \{\text{Property of sets}\} \\
= \left(\ \exists\, ac_0 \bullet P[ac_0/ac'] \wedge ac_0 \subseteq \{s \mid ac_0 \subseteq ac'\} \wedge ac_0 \subseteq \{s \mid \{s\} = ac'\} \ \right) \\
\qquad \{\text{Lemma H.1.7}\} \\
= \left(\ \exists\, ac_0 \bullet P[ac_0/ac'] \wedge (ac_0 = \emptyset \vee ac_0 \subseteq ac') \wedge ac_0 \subseteq \{s \mid \{s\} = ac'\} \ \right) \\
\qquad \{\text{Predicate calculus}\} \\
= \left(\begin{array}{l} (\exists\, ac_0 \bullet P[ac_0/ac'] \wedge ac_0 = \emptyset \wedge ac_0 \subseteq \{s \mid \{s\} = ac'\}) \\ \vee \\ (\exists\, ac_0 \bullet P[ac_0/ac'] \wedge ac_0 \subseteq ac' \wedge ac_0 \subseteq \{s \mid \{s\} = ac'\}) \end{array} \right) \\
\qquad \{\text{One-point rule}\}
\end{array}
$$

$$= \left(\begin{array}{l} P[\emptyset/ac'] \\ \vee \\ (\exists\, ac_0 \bullet P[ac_0/ac'] \wedge ac_0 \subseteq ac' \wedge ac_0 \subseteq \{s \mid \{s\} = ac'\}) \end{array} \right)$$

$\{P[\emptyset/ac'] \text{ is an instance of existential quantification}\}$

$= \exists\, ac_0 \bullet P[ac_0/ac'] \wedge ac_0 \subseteq ac' \wedge ac_0 \subseteq \{s \mid \{s\} = ac'\}$

$\{\text{Predicate calculus and Lemma H.1.5}\}$

$= \exists\, ac_0 \bullet P[ac_0/ac'] \wedge ac_0 \subseteq \{s \mid \{s\} = ac'\}$

$\{\text{Definition of } ;_{\mathcal{A}} \text{ and substitution}\}$

$= (\exists\, ac_0 \bullet P[ac_0/ac'] \wedge ac_0 \subseteq ac') \;;_{\mathcal{A}} \{s \mid \{s\} = ac'\}$

$\{\text{Definition of } \mathbf{PBMH} \text{ (Lemma E.1.1)}\}$

$= \mathbf{PBMH}(P) \;;_{\mathcal{A}} \{s \mid \{s\} = ac'\}$ $\{\text{Assumption: } P \text{ is } \mathbf{PBMH}\text{-healthy}\}$

$= P \;;_{\mathcal{A}} \{s \mid \{s\} = ac'\}$

□

Lemma A.3.12

$$\mathbf{PBMH} \circ \mathbf{A2}(P) = \mathbf{A2}(P)$$

Proof.

$\mathbf{PBMH} \circ \mathbf{A2}(P)$ $\{\text{Definition of } \mathbf{A2}\}$

$= \mathbf{PBMH} \circ \mathbf{PBMH}(P \;;_{\mathcal{A}} \{s\} = ac')$

$\{\mathbf{PBMH}\text{-idempotent (Theorem E.2.1)}\}$

$= \mathbf{PBMH}(P \;;_{\mathcal{A}} \{s\} = ac')$ $\{\text{Definition of } \mathbf{A2}\}$

$= \mathbf{A2}(P)$

□

A.3.4 Properties with respect to links

Lemma A.3.13

$$p2ac \circ ac2p \circ \mathbf{A2}(P) = \mathbf{A2}(P) \wedge ac' \neq \emptyset$$

Proof.

$p2ac \circ ac2p \circ \mathbf{A2}(P)$ $\{\text{Lemma A.3.16}\}$

$= (P[\emptyset/ac'] \wedge ac' \neq \emptyset) \vee (\exists\, y \bullet P[\{y\}/ac'] \wedge y \in ac')$
{Predicate calculus}
$= (P[\emptyset/ac'] \wedge ac' \neq \emptyset) \vee (\exists\, y \bullet P[\{y\}/ac'] \wedge y \in ac' \wedge ac' \neq \emptyset)$
{Predicate calculus}
$= (P[\emptyset/ac'] \vee (\exists\, y \bullet P[\{y\}/ac'] \wedge y \in ac')) \wedge ac' \neq \emptyset$ {Theorem 1.2.33}
$= \mathbf{A2}(P) \wedge ac' \neq \emptyset$

□

Lemma A.3.14

$$p2ac \circ ac2p \circ \mathbf{PBMH}(P) = p2ac \circ ac2p(P)$$

Proof.

$p2ac \circ ac2p \circ \mathbf{PBMH}(P)$ {Lemma C.2.8}
$= \exists\, ac_0, y \bullet \mathbf{PBMH}(P)[ac_0/ac'] \wedge ac_0 \subseteq \{y\} \wedge y \in ac'$
{Definition of **PBMH** (Lemma E.1.1)}
$= \exists\, ac_0, y \bullet (\exists\, ac_1 \bullet P[ac_1/ac'] \wedge ac_1 \subseteq ac')[ac_0/ac'] \wedge ac_0 \subseteq \{y\} \wedge y \in ac'$
{Substitution}
$= \exists\, ac_0, y, ac_1 \bullet P[ac_1/ac'] \wedge ac_1 \subseteq ac_0 \wedge ac_0 \subseteq \{y\} \wedge y \in ac'$
{Predicate calculus}
$= \exists\, y, ac_1 \bullet P[ac_1/ac'] \wedge ac_1 \subseteq \{y\} \wedge y \in ac'$ {Lemma C.2.8}
$= p2ac \circ ac2p(P)$

□

Lemma A.3.15

$$p2ac \circ ac2p \circ \mathbf{A2}(P) = p2ac \circ ac2p(P \;;_{\mathcal{A}} \{s\} = ac')$$

Proof.

$p2ac \circ ac2p \circ \mathbf{A2}(P)$ {Definition of **A2**}
$= p2ac \circ ac2p \circ \mathbf{PBMH}(P \;;_{\mathcal{A}} \{s\} = ac')$ {Lemma A.3.14}
$= p2ac \circ ac2p \circ (P \;;_{\mathcal{A}} \{s\} = ac')$

□

Lemma A.3.16

$$p2ac \circ ac2p \circ \mathbf{A2}(P)$$
$$=$$
$$(P[\emptyset/ac'] \wedge ac' \neq \emptyset) \vee (\exists\, y \bullet P[\{y\}/ac'] \wedge y \in ac')$$

Proof.

$$\begin{array}{ll}
p2ac \circ ac2p \circ \mathbf{A2}(P) & \{\text{Lemma A.3.15}\} \\
= p2ac \circ ac2p(P \ ;_{\mathcal{A}} \{s\} = ac') & \{\text{Definition of } ;_{\mathcal{A}} \text{ and substitution}\} \\
= p2ac \circ ac2p(P[\{s \mid \{s\} = ac'\}/ac']) & \{\text{Lemma C.2.8}\} \\
= \exists\, ac_0, y \bullet (P[\{s \mid \{s\} = ac'\}/ac'])[ac_0/ac'] \wedge ac_0 \subseteq \{y\} \wedge y \in ac' & \{\text{Substitution}\} \\
= \exists\, ac_0, y \bullet P[\{s \mid \{s\} = ac_0\}/ac'] \wedge ac_0 \subseteq \{y\} \wedge y \in ac' & \{\text{Property of sets}\} \\
= \exists\, ac_0, y \bullet P[\{s \mid \{s\} = ac_0\}/ac'] \wedge (ac_0 = \emptyset \vee ac_0 = \{y\}) \wedge y \in ac' & \{\text{Predicate calculus}\} \\
= \left(\begin{array}{l} (\exists\, ac_0, y \bullet P[\{s \mid \{s\} = ac_0\}/ac'] \wedge ac_0 = \emptyset \wedge y \in ac') \\ \vee \\ (\exists\, ac_0, y \bullet P[\{s \mid \{s\} = ac_0\}/ac'] \wedge ac_0 = \{y\} \wedge y \in ac') \end{array} \right) & \{\text{One-point rule}\} \\
= \left(\begin{array}{l} (\exists\, y \bullet P[\{s \mid \{s\} = \emptyset\}/ac'] \wedge y \in ac') \\ \vee \\ (\exists\, y \bullet P[\{s \mid \{s\} = \{y\}\}/ac'] \wedge y \in ac') \end{array} \right) & \{\text{Property of sets}\} \\
= (\exists\, y \bullet P[\emptyset/ac'] \wedge y \in ac') \vee (\exists\, y \bullet P[\{y\}/ac'] \wedge y \in ac') & \{\text{Predicate calculus}\} \\
= (P[\emptyset/ac'] \wedge \exists\, y \bullet y \in ac') \vee (\exists\, y \bullet P[\{y\}/ac'] \wedge y \in ac') & \{\text{Property of sets}\} \\
= (P[\emptyset/ac'] \wedge ac' \neq \emptyset) \vee (\exists\, y \bullet P[\{y\}/ac'] \wedge y \in ac') &
\end{array}$$

□

Appendix B

RA

B.1 RA1

B.1.1 Lemmas

Lemma B.1.1

$$\mathbf{RA1}(P) \Rightarrow ac' \neq \emptyset$$

Proof.

$\mathbf{RA1}(P)$ {Definition of **RA1** (Lemma 1.2.1)}
$= P[\{z \mid z \in ac' \wedge s.tr \leq z.tr\}/ac'] \wedge \exists\, z \bullet s.tr \leq z.tr \wedge z \in ac'$
{Predicate calculus}
$\Rightarrow \exists\, z \bullet s.tr \leq z.tr \wedge z \in ac'$ {Predicate calculus}
$\Rightarrow \exists\, z \bullet z \in ac'$ {Property of sets}
$= ac' \neq \emptyset$

□

Lemma B.1.2

$$s \in ac' \Rightarrow \exists\, z \bullet s.tr \leq z.tr \wedge z \in ac'$$

Proof.

$s \in ac'$ {Property of sequences}
$= s.tr \leq s.tr \wedge s \in ac'$ {Predicate calculus}
$\Rightarrow \exists\, z \bullet s.tr \leq z.tr \wedge s \in ac'$

□

Lemma B.1.3

$$\exists\, z \bullet z \in ac' \land tr_0 \leq z.tr \land x = z \oplus \{tr \mapsto z.tr - tr_0\}$$
$$\Leftrightarrow$$
$$x \oplus \{tr \mapsto tr_0 \frown x.tr\} \in ac'$$

Proof.

$$\exists\, z \bullet z \in ac' \land tr_0 \leq z.tr \land x = z \oplus \{tr \mapsto z.tr - tr_0\} \qquad \{\text{Definition of } \oplus\}$$
$$\Leftrightarrow \exists\, z \bullet z \in ac' \land tr_0 \leq z.tr \land x = \{tr\} \lhd z \cup \{tr \mapsto z.tr - tr_0\}$$
$$\{\text{Property of relations}\}$$
$$\Leftrightarrow \left(\begin{array}{l} \exists\, z \bullet z \in ac' \land tr_0 \leq z.tr \land \{tr\} \lhd x = \{tr\} \lhd z \\ \land\ x.tr = z.tr - tr_0 \land \operatorname{dom} x = \operatorname{dom} z \cup \{tr\} \end{array} \right)$$
$$\{\text{Property of sequences}\}$$
$$\Leftrightarrow \left(\begin{array}{l} \exists\, z \bullet z \in ac' \land tr_0 \leq z.tr \land \{tr\} \lhd x = \{tr\} \lhd z \\ \land\ tr_0 \frown x.tr = z.tr \land \operatorname{dom} x = \operatorname{dom} z \cup \{tr\} \end{array} \right)$$
$$\{\text{Property of relations}\}$$
$$\Leftrightarrow \exists\, z \bullet z \in ac' \land tr_0 \leq z.tr \land z = \{tr\} \lhd x \cup \{tr \mapsto tr_0 \frown x.tr\}$$
$$\{\text{Definition of } \oplus\}$$
$$\Leftrightarrow \exists\, z \bullet z \in ac' \land tr_0 \leq z.tr \land z = x \oplus \{tr \mapsto tr_0 \frown x.tr\}$$
$$\{\text{One-point rule}\}$$
$$\Leftrightarrow x \oplus \{tr \mapsto tr_0 \frown x.tr\} \in ac' \land tr_0 \leq (x \oplus \{tr \mapsto tr_0 \frown x.tr\}).tr$$
$$\{\text{Property of } \oplus \text{ and value of } tr\}$$
$$\Leftrightarrow x \oplus \{tr \mapsto tr_0 \frown x.tr\} \in ac' \land tr_0 \leq tr_0 \frown x.tr \qquad \{\text{Property of sequence}\}$$
$$\Leftrightarrow x \oplus \{tr \mapsto tr_0 \frown x.tr\} \in ac'$$

□

Lemma B.1.4

$$\mathbf{RA1}(\mathit{false}) = \mathit{false}$$

Proof.

$$\mathbf{RA1}(\mathit{false}) \qquad \{\text{Definition of } \mathbf{RA1}\}$$

$= (\mathit{false} \wedge ac' \neq \emptyset)[\mathit{States}_{tr \leq tr'}(s) \cap ac'/ac']$ {Predicate calculus}
$= \mathit{false}[\mathit{States}_{tr \leq tr'}(s) \cap ac'/ac']$ {Substitution}
$= \mathit{false}$

□

Lemma B.1.5

$$\mathbf{RA1}(\mathit{true}) = \exists\, z \bullet s.tr \leq z.tr \wedge z \in ac'$$

Proof.

$\mathbf{RA1}(\mathit{true})$ {Definition of **RA1** (Lemma 1.2.1)}
$= \mathit{true}[\{z \mid z \in ac' \wedge s.tr \leq z.tr\}/ac'] \wedge \exists\, z \bullet s.tr \leq z.tr \wedge z \in ac'$ {Property of substitution}
$= \exists\, z \bullet s.tr \leq z.tr \wedge z \in ac'$

□

Lemma B.1.6

$$\mathbf{RA1}(\mathit{true}) = \mathit{States}_{tr \leq tr'}(s) \cap ac' \neq \emptyset$$

Proof.

$\mathbf{RA1}(\mathit{true})$ {Definition of **RA1**}
$= (\mathit{true} \wedge ac' \neq \emptyset)[\mathit{States}_{tr \leq tr'}(s) \cap ac'/ac']$ {Predicate calculus}
$= (ac' \neq \emptyset)[\mathit{States}_{tr \leq tr'}(s) \cap ac'/ac']$ {Substitution}
$= \mathit{States}_{tr \leq tr'}(s) \cap ac' \neq \emptyset$

□

Lemma B.1.7 *Provided x is not in the set $\{s, ac'\}$.*

$$\mathbf{RA1}(\exists\, x \bullet P) = \exists\, x \bullet \mathbf{RA1}(P)$$

Proof.

$\mathbf{RA1}(\exists\, x \bullet P)$ {Definition of **RA1**}

$= ((\exists\, x \bullet P) \wedge ac' \neq \emptyset)[\{z \mid z \in ac' \wedge s.tr \leq z.tr\}/ac']$
{Assumption: x is not ac' and predicate calculus}
$= (\exists\, x \bullet P \wedge ac' \neq \emptyset)[\{z \mid z \in ac' \wedge s.tr \leq z.tr\}/ac']$
{Assumption: x is not s and predicate calculus}
$= \exists\, x \bullet (P \wedge (ac' \neq \emptyset)[\{z \mid z \in ac' \wedge s.tr \leq z.tr\}/ac'])$
{Definition of **RA1**}
$= \exists\, x \bullet \mathbf{RA1}(P)$

□

Lemma B.1.8

$$\mathbf{RA1}(x \in ac') = s.tr \leq x.tr \wedge x \in ac'$$

Proof.

$\mathbf{RA1}(x \in ac')$ {Definition of **RA1** (Lemma 1.2.1)}
$= (x \in ac')[\{z \mid z \in ac' \wedge s.tr \leq z.tr\}/ac'] \wedge \exists\, z \bullet s.tr \leq z.tr \wedge z \in ac'$
{Substitution}
$= x \in \{z \mid z \in ac' \wedge s.tr \leq z.tr\} \wedge \exists\, z \bullet s.tr \leq z.tr \wedge z \in ac$
{Property of sets}
$= x \in ac' \wedge s.tr \leq x.tr \wedge \exists\, z \bullet s.tr \leq z.tr \wedge z \in ac'$ {Predicate calculus}
$= x \in ac' \wedge s.tr \leq x.tr$

□

Lemma B.1.9

$$\mathbf{RA1}(s \in ac') = s \in ac'$$

Proof.

$\mathbf{RA1}(s \in ac')$ {Lemma B.1.8}
$= s.tr \leq s.tr \wedge s \in ac'$ {Property of sequences}
$= s \in ac'$

□

Lemma B.1.10 *Provided c is a condition.*

$$\mathbf{RA1}(P \lhd c \rhd Q) = \mathbf{RA1}(P) \lhd c \rhd \mathbf{RA1}(Q)$$

Proof.

$$\begin{aligned}
&\mathbf{RA1}(P \lhd c \rhd Q) && \{\text{Definition of conditional}\}\\
&= \mathbf{RA1}((c \wedge P) \vee (\neg\, c \wedge Q)) && \{\text{Theorem 1.2.1}\}\\
&= \mathbf{RA1}(c \wedge P) \vee \mathbf{RA1}(\neg\, c \wedge Q)\\
& && \{\text{Assumption: } c \text{ is a condition and Lemma B.1.11}\}\\
&= (c \wedge \mathbf{RA1}(P)) \vee (\neg\, c \wedge \mathbf{RA1}(Q)) && \{\text{Definition of conditional}\}\\
&= \mathbf{RA1}(P) \lhd c \rhd \mathbf{RA1}(Q)
\end{aligned}$$

□

Lemma B.1.11 *Provided ac' is not free in P.*

$$\mathbf{RA1}(P \wedge Q) = P \wedge \mathbf{RA1}(Q)$$

Proof.

$$\begin{aligned}
&\mathbf{RA1}(P \wedge Q) && \{\text{Definition of } \mathbf{RA1} \text{ (Lemma 1.2.1)}\}\\
&= (P \wedge Q)[\{z \mid z \in ac' \wedge s.tr \leq z.tr\}/ac'] \wedge \exists\, z \bullet s.tr \leq z.tr \wedge z \in ac'\\
& && \{\text{Substitution: } ac' \text{ not free in } P\}\\
&= P \wedge Q[\{z \mid z \in ac' \wedge s.tr \leq z.tr\}/ac'] \wedge \exists\, z \bullet s.tr \leq z.tr \wedge z \in ac'\\
& && \{\text{Definition of } \mathbf{RA1} \text{ (Lemma 1.2.1)}\}\\
&= P \wedge \mathbf{RA1}(Q)
\end{aligned}$$

□

Lemma B.1.12

$$\mathbf{RA1}(\neg\, ok) = \neg\, ok \wedge \mathbf{RA1}(true)$$

Proof.

$$\begin{aligned}
&\mathbf{RA1}(\neg\, ok) && \{\text{Definition of } \mathbf{RA1} \text{ (Lemma 1.2.1)}\}\\
&= (\neg\, ok)[\{z \mid z \in ac' \wedge s.tr \leq z.tr\}/ac'] \wedge \exists\, z \bullet s.tr \leq z.tr \wedge z \in ac'\\
& && \{\text{Substitution}\}\\
&= \neg\, ok \wedge \exists\, z \bullet s.tr \leq z.tr \wedge z \in ac' && \{\text{Lemma B.1.5}\}\\
&= \neg\, ok \wedge \mathbf{RA1}(true)
\end{aligned}$$

□

Lemma B.1.13

$$\mathbf{RA1}(\neg\ P_f^f \vdash P_f^t) = \mathbf{RA1}(\neg\ (P_f^f \wedge ac' \neq \emptyset) \vdash P_f^t \wedge ac' \neq \emptyset)$$

Proof.

$$\begin{array}{ll}
& \mathbf{RA1}(\neg\ P_f^f \vdash P_f^t) \qquad \{\text{Definition of } \mathbf{RA1}\} \\
= & ((\neg\ P_f^f \vdash P_f^t) \wedge ac' \neq \emptyset)[States_{tr \leq tr'}(s) \cap ac'/ac'] \qquad \{\text{Definition of design}\} \\
= & (((ok \wedge \neg\ P_f^f) \Rightarrow (P_f^t \wedge ok')) \wedge ac' \neq \emptyset)[States_{tr \leq tr'}(s) \cap ac'/ac'] \\
& \qquad \{\text{Predicate calculus}\} \\
= & ((\neg\ ok \vee P_f^f \vee (P_f^t \wedge ok')) \wedge ac' \neq \emptyset)[States_{tr \leq tr'}(s) \cap ac'/ac'] \\
& \qquad \{\text{Predicate calculus}\} \\
= & \left(\left(\begin{array}{l} \neg\ ok \vee (P_f^f \wedge ac' \neq \emptyset) \\ \vee \\ (P_f^t \wedge ac' \neq \emptyset \wedge ok') \end{array} \right) \wedge ac' \neq \emptyset \right) [States_{tr \leq tr'}(s) \cap ac'/ac'] \\
& \qquad \{\text{Predicate calculus}\} \\
= & \left(\left(\begin{array}{l} (ok \wedge \neg\ (P_f^f \wedge ac' \neq \emptyset)) \\ \Rightarrow \\ (P_f^t \wedge ac' \neq \emptyset \wedge ok') \end{array} \right) \wedge ac' \neq \emptyset \right) [States_{tr \leq tr'}(s) \cap ac'/ac'] \\
& \qquad \{\text{Definition of design}\} \\
= & ((\neg\ (P_f^f \wedge ac' \neq \emptyset) \vdash P_f^t \wedge ac' \neq \emptyset) \wedge ac' \neq \emptyset)[States_{tr \leq tr'}(s) \cap ac'/ac'] \\
& \qquad \{\text{Definition of } \mathbf{RA1}\} \\
= & \mathbf{RA1}(\neg\ (P_f^f \wedge ac' \neq \emptyset) \vdash P_f^t \wedge ac' \neq \emptyset)
\end{array}$$

□

Lemma B.1.14 *Provided ac' is not free in P.*

$$\mathbf{RA1}(P) = P \wedge \mathbf{RA1}(true)$$

Proof.

$$\begin{array}{ll}
& \mathbf{RA1}(P) \qquad \{\text{Predicate calculus}\} \\
= & \mathbf{RA1}(P \wedge true) \qquad \{\text{Assumption: } ac' \text{ not free in } P \text{ and Lemma B.1.11}\} \\
= & P \wedge \mathbf{RA1}(true)
\end{array}$$

□

B.1.2 Substitution properties

Lemma B.1.15

$$\mathbf{RA1}(P)^o_w = \mathbf{RA1}(P^o_w)$$

Proof.

$$\begin{array}{ll}
\mathbf{RA1}(P)^o_w & \{\text{Definition of } \mathbf{RA1}\} \\
= ((P \wedge ac' \neq \emptyset)[\{z \mid z \in ac' \wedge s.tr \leq z.tr\}/ac'])^o_w & \\
& \{\text{Substitution abbreviation}\} \\
= ((P \wedge ac' \neq \emptyset)[\{z \mid z \in ac' \wedge s.tr \leq z.tr\}/ac'])[o, s \oplus \{wait \mapsto w\}/ok', s] & \\
& \{\text{Substitution}\} \\
= (P[o, s \oplus \{wait \mapsto w\}/ok', s] \wedge ac' \neq \emptyset)[\{z \mid z \in ac' \wedge (s \oplus \{wait \mapsto w\}).tr \leq z.tr\}/ac'] & \\
& \{\text{Property of } \oplus\} \\
= (P[o, s \oplus \{wait \mapsto w\}/ok', s] \wedge ac' \neq \emptyset)[\{z \mid z \in ac' \wedge s.tr \leq z.tr\}/ac'] & \\
& \{\text{Substitution abbreviation}\} \\
= (P^o_w \wedge ac' \neq \emptyset)[\{z \mid z \in ac' \wedge s.tr \leq z.tr\}/ac'] & \{\text{Definition of } \mathbf{RA1}\} \\
= \mathbf{RA1}(P^o_w) &
\end{array}$$

□

B.1.3 Properties with respect to $;_{\mathcal{A}}$

Lemma B.1.16

$$\mathbf{RA1}(true) \;;_{\mathcal{A}} \mathbf{RA1}(true) = \mathbf{RA1}(true)$$

Proof.

$$\begin{array}{ll}
\mathbf{RA1}(true) \;;_{\mathcal{A}} \mathbf{RA1}(true) & \{\text{Lemma B.1.5}\} \\
= (\exists\, z \bullet s.tr \leq z.tr \wedge z \in ac') \;;_{\mathcal{A}} (\exists\, z \bullet s.tr \leq z.tr \wedge z \in ac') & \\
& \{\text{Definition of } ;_{\mathcal{A}}\} \\
= (\exists\, z \bullet s.tr \leq z.tr \wedge z \in ac')[\{s \mid \exists\, z \bullet s.tr \leq z.tr \wedge z \in ac'\}/ac'] & \\
& \{\text{Substitution}\} \\
= \exists\, z \bullet s.tr \leq z.tr \wedge z \in \{s \mid \exists\, z \bullet s.tr \leq z.tr \wedge z \in ac'\} & \\
& \{\text{Variable renaming}\}
\end{array}$$

$= \exists\, z \bullet s.tr \leq z.tr \wedge z \in \{s \mid \exists\, y \bullet s.tr \leq y.tr \wedge y \in ac'\}$
{Property of sets}
$= \exists\, z \bullet s.tr \leq z.tr \wedge (\exists\, y \bullet z.tr \leq y.tr \wedge y \in ac')$ {Predicate calculus}
$= \exists\, z, y \bullet s.tr \leq z.tr \wedge z.tr \leq y.tr \wedge y \in ac'$
{Transitivity of sequence prefixing}
$= \exists\, y \bullet s.tr \leq y.tr \wedge y \in ac'$ {Lemma B.1.5}
$= \mathbf{RA1}(true)$

□

Lemma B.1.17 *Provided ac' is not free in P.*

$$\mathbf{RA1}(P) \;;_{\mathcal{A}} \mathbf{RA1}(true) = \mathbf{RA1}(P)$$

Proof.

$\mathbf{RA1}(P) \;;_{\mathcal{A}} \mathbf{RA1}(true)$
{Assumption: ac' not free in P and Lemma B.1.14}
$= (P \wedge \mathbf{RA1}(true)) \;;_{\mathcal{A}} \mathbf{RA1}(true)$ {Distributivity of $;_{\mathcal{A}}$}
$= (P \;;_{\mathcal{A}} \mathbf{RA1}(true)) \wedge (\mathbf{RA1}(true) \;;_{\mathcal{A}} \mathbf{RA1}(true))$
{Property of $;_{\mathcal{A}}$ when ac' not free}
$= P \wedge (\mathbf{RA1}(true) \;;_{\mathcal{A}} \mathbf{RA1}(true))$ {Lemma B.1.16}
$= P \wedge \mathbf{RA1}(true)$ {Lemma B.1.11}
$= \mathbf{RA1}(P \wedge true)$ {Predicate calculus}
$= \mathbf{RA1}(P)$

□

Theorem B.1.1 *Provided P is* **PBMH***-healthy.*

$$(P \;;_{\mathcal{A}} \mathbf{RA1}(true)) \vee (P \;;_{\mathcal{A}} \mathbf{RA1}(Q)) = (P \;;_{\mathcal{A}} \mathbf{RA1}(true))$$

Proof.

$(P \;;_{\mathcal{A}} \mathbf{RA1}(true)) \vee (P \;;_{\mathcal{A}} \mathbf{RA1}(Q))$
{Assumption: P is **PBMH**-healthy and Lemma F.2.1}

$$= ((P \ ;_{\mathcal{A}} \mathbf{RA1}(true)) \vee (P \ ;_{\mathcal{A}} \mathbf{RA1}(Q))) \wedge (P \ ;_{\mathcal{A}} (\mathbf{RA1}(true) \vee \mathbf{RA1}(Q))$$
{Theorem 1.2.1}
$$= ((P \ ;_{\mathcal{A}} \mathbf{RA1}(true)) \vee (P \ ;_{\mathcal{A}} \mathbf{RA1}(Q))) \wedge (P \ ;_{\mathcal{A}} \mathbf{RA1}(true \vee Q))$$
{Predicate calculus}
$$= ((P \ ;_{\mathcal{A}} \mathbf{RA1}(true)) \vee (P \ ;_{\mathcal{A}} \mathbf{RA1}(Q))) \wedge (P \ ;_{\mathcal{A}} \mathbf{RA1}(true))$$
{Predicate calculus: absorption law}
$$= P \ ;_{\mathcal{A}} \mathbf{RA1}(true)$$

□

B.1.4 Properties with respect to RA2

Lemma B.1.18

$$\mathbf{RA1} \circ \mathbf{RA2}(P)$$
$$=$$
$$\mathbf{RA2}(P) \wedge \exists\, z \bullet s.tr \leq z.tr \wedge z \in ac'$$

Proof.

$\mathbf{RA1} \circ \mathbf{RA2}(P)$ {Definition of **RA1** (Lemma 1.2.1)}
$= \mathbf{RA2}(P)[\{z \mid z \in ac' \wedge s.tr \leq z.tr\}/ac'] \wedge \exists\, z \bullet s.tr \leq z.tr \wedge z \in ac'$
{Lemma B.1.19}
$= \mathbf{RA2}(P) \wedge \exists\, z \bullet s.tr \leq z.tr \wedge z \in ac'$

□

Lemma B.1.19

$$\mathbf{RA2}(P)[\{z \mid z \in ac' \wedge s.tr \leq z.tr\}/ac'] = \mathbf{RA2}(P)$$

Proof.

$\mathbf{RA2}(P)[\{z \mid z \in ac' \wedge s.tr \leq z.tr\}/ac']$ {Definition of **RA2**}
$= \left(P\right)[s \oplus \{tr \mapsto \langle\rangle\}, \{z \mid z \in ac' \wedge s.tr \leq z.tr \bullet z \oplus \{tr \mapsto z.tr - s.tr\}\}/s, ac'][\{z \mid z \in ac' \wedge s.tr \leq z.tr\}/ac']$
{Substitution}

$$= \left(P\right)\left[s \oplus \{tr \mapsto \langle\rangle\}, \left\{\ z \;\middle|\; \begin{array}{l} z \in \{z \mid z \in ac' \wedge s.tr \leq z.tr\} \wedge s.tr \leq z.tr \\ \bullet\ z \oplus \{tr \mapsto z.tr - s.tr\} \end{array} \right\} / s, ac'\right]$$

{Property of sets}

$$= \left(P\right)\left[s \oplus \{tr \mapsto \langle\rangle\}, \left\{\ z \;\middle|\; \begin{array}{l} z \in ac' \wedge s.tr \leq z.tr \wedge s.tr \leq z.tr \\ \bullet\ z \oplus \{tr \mapsto z.tr - s.tr\} \end{array} \right\} / s, ac'\right]$$

{Predicate calculus}

$$= P[s \oplus \{tr \mapsto \langle\rangle\}, \{z \mid z \in ac' \wedge s.tr \leq z.tr \bullet z \oplus \{tr \mapsto z.tr - s.tr\}\}/s, ac']$$

{Definition of **RA2**}

$$= \mathbf{RA2}(P)$$

□

B.1.5 Properties with respect to PBMH

Lemma B.1.20 *Provided P is* **PBMH***-healthy.*

$$\mathbf{RA1}(P) = \mathbf{PBMH}(P \wedge ac' \neq \emptyset \wedge ac' \subseteq States_{tr \leq tr'}(s))$$

Proof.

$\mathbf{RA1}(P)$ {Definition of **RA1** (Lemma 1.2.2)}

$= (P \wedge ac' \neq \emptyset)[States_{tr \leq tr'}(s) \cap ac'/ac']$

{Assumption: P is **PBMH**-healthy}

$= (\mathbf{PBMH}(P) \wedge ac' \neq \emptyset)[States_{tr \leq tr'}(s) \cap ac'/ac']$

{$ac' \neq \emptyset$ is **PBMH**-healthy and closure (Theorem E.3.1)}

$= \mathbf{PBMH}(\mathbf{PBMH}(P) \wedge ac' \neq \emptyset)[States_{tr \leq tr'}(s) \cap ac'/ac']$

{Assumption: P is **PBMH**-healthy}

$= \mathbf{PBMH}(P \wedge ac' \neq \emptyset)[States_{tr \leq tr'}(s) \cap ac'/ac']$

{Definition of **PBMH** (Lemma E.1.1)}

$= (\exists\, ac_0 \bullet P[ac_0/ac'] \wedge ac_0 \neq \emptyset \wedge ac_0 \subseteq ac')[States_{tr \leq tr'}(s) \cap ac'/ac']$

{Substitution}

$= \exists\, ac_0 \bullet P[ac_0/ac'] \wedge ac_0 \neq \emptyset \wedge ac_0 \subseteq (States_{tr \leq tr'}(s) \cap ac')$

{Property of sets}

$= \exists\, ac_0 \bullet P[ac_0/ac'] \wedge ac_0 \neq \emptyset \wedge ac_0 \subseteq States_{tr \leq tr'}(s) \wedge ac_0 \subseteq ac'$

{Substitution}

$= \exists\, ac_0 \bullet (P \wedge ac' \neq \emptyset \wedge ac' \subseteq States_{tr \leq tr'}(s))[ac_0/ac'] \wedge ac_0 \subseteq ac'$

{Definition of **PBMH** (Lemma E.1.1)}

$= \mathbf{PBMH}(P \wedge ac' \neq \emptyset \wedge ac' \subseteq States_{tr \leq tr'}(s))$

□

Lemma B.1.21

$$\mathbf{PBMH}(P \wedge ac' \neq \emptyset \wedge ac' \subseteq States_{tr \leq tr'}(s)) \Rightarrow ac' \cap States_{tr \leq tr'}(s) \neq \emptyset$$

Proof.

$\mathbf{PBMH}(P \wedge ac' \neq \emptyset \wedge ac' \subseteq States_{tr \leq tr'}(s))$

{Definition of **PBMH** (Lemma E.1.1)}

$= \exists\, ac_0 \bullet (P \wedge ac' \neq \emptyset \wedge ac' \subseteq States_{tr \leq tr'}(s))[ac_0/ac'] \wedge ac_0 \subseteq ac'$

{Substitution}

$= \exists\, ac_0 \bullet P[ac_0/ac'] \wedge ac_0 \neq \emptyset \wedge ac_0 \subseteq States_{tr \leq tr'}(s) \wedge ac_0 \subseteq ac'$

{Property of sets}

$= \exists\, ac_0 \bullet P[ac_0/ac'] \wedge ac_0 \neq \emptyset \wedge ac_0 \subseteq (States_{tr \leq tr'}(s) \cap ac')$

{Property of sets}

$= \exists\, ac_0 \bullet P[ac_0/ac'] \wedge ac_0 \neq \emptyset \wedge ac_0 \subseteq (States_{tr \leq tr'}(s) \cap ac') \wedge States_{tr \leq tr'}(s) \cap ac' \neq \emptyset$

{Predicate calculus}

$\Rightarrow States_{tr \leq tr'}(s) \cap ac' \neq \emptyset$

□

Lemma B.1.22

$$ac' \cap States_{tr \leq tr'}(s) \neq \emptyset \;\; ;_{\mathcal{A}} \mathbf{PBMH}(P \wedge ac' \neq \emptyset \wedge ac' \subseteq States_{tr \leq tr'}(s))$$
$$\Rightarrow$$
$$ac' \cap States_{tr \leq tr'}(s) \neq \emptyset$$

Proof.

$ac' \cap States_{tr \leq tr'}(s) \neq \emptyset \;\; ;_{\mathcal{A}} \mathbf{PBMH}(P \wedge ac' \neq \emptyset \wedge ac' \subseteq States_{tr \leq tr'}(s))$

{Property of sets}

$= (\exists\, z \bullet z \in States_{tr \leq tr'}(s) \wedge z \in ac') \;\; ;_{\mathcal{A}} \mathbf{PBMH}(P \wedge ac' \neq \emptyset \wedge ac' \subseteq States_{tr \leq tr'}(s))$

{Property of sets and definition of $States_{tr \leq tr'}(s)$}

$$= (\exists\, z \bullet s.tr \leq z.tr \wedge z \in ac') \;;_{\mathcal{A}} \mathbf{PBMH}(P \wedge ac' \neq \emptyset \wedge ac' \subseteq States_{tr \leq tr'}(s))$$
{Definition of $;_{\mathcal{A}}$ and substitution}

$$= (\exists\, z \bullet s.tr \leq z.tr \wedge z \in \{s \mid \mathbf{PBMH}(P \wedge ac' \neq \emptyset \wedge ac' \subseteq States_{tr \leq tr'}(s))\}$$
{Variable renaming and property of sets}

$$= (\exists\, z \bullet s.tr \leq z.tr \wedge \mathbf{PBMH}(P \wedge ac' \neq \emptyset \wedge ac' \subseteq States_{tr \leq tr'}(s))[z/s]$$
{Lemma B.1.21}

$$= \exists\, z \bullet \left(\begin{array}{l} s.tr \leq z.tr \\ \wedge \\ \left(\begin{array}{l} \mathbf{PBMH}(P \wedge ac' \neq \emptyset \wedge ac' \subseteq States_{tr \leq tr'}(s)) \\ \wedge \\ ac' \cap States_{tr \leq tr'}(s) \neq \emptyset \end{array} \right)[z/s] \end{array} \right)$$
{Substitution}

$$= \exists\, z \bullet \left(\begin{array}{l} s.tr \leq z.tr \\ \wedge \\ \left(\begin{array}{l} \mathbf{PBMH}(P \wedge ac' \neq \emptyset \wedge ac' \subseteq States_{tr \leq tr'}(s))[z/s] \\ \wedge \\ ac' \cap States_{tr \leq tr'}(z) \neq \emptyset \end{array} \right) \end{array} \right)$$
{Predicate calculus}

$$\Rightarrow \left(\begin{array}{l} \exists\, z \bullet s.tr \leq z.tr \wedge \mathbf{PBMH}(P \wedge ac' \neq \emptyset \wedge ac' \subseteq States_{tr \leq tr'}(s))[z/s] \\ \wedge \\ \exists\, z \bullet s.tr \leq z.tr \wedge ac' \cap States_{tr \leq tr'}(z) \neq \emptyset \end{array} \right)$$
{Predicate calculus}

$$\Rightarrow \exists\, z \bullet s.tr \leq z.tr \wedge ac' \cap States_{tr \leq tr'}(z) \neq \emptyset$$
{Property of sets and definition of $States_{tr \leq tr'}$}

$$= \exists\, z \bullet s.tr \leq z.tr \wedge (\exists\, y \bullet z.tr \leq y.tr \wedge y \in ac')$$ {Predicate calculus}

$$= \exists\, z, y \bullet s.tr \leq z.tr \wedge z.tr \leq y.tr \wedge y \in ac'$$
{Predicate calculus and transitivity of sequence prefixing}

$$= \exists\, y \bullet s.tr \leq y.tr \wedge y \in ac'$$
{Property of sets and definition of $States_{tr \leq tr'}$}

$$= ac' \cap States_{tr \leq tr'}(s) \neq \emptyset$$

□

Lemma B.1.23

$$\mathbf{RA1}(true) \;;_{\mathcal{A}} \mathbf{RA1}(P) \Rightarrow \mathbf{RA1}(true)$$

Proof.

$$
\begin{array}{ll}
\mathbf{RA1}(\mathit{true}) \ ;_{\mathcal{A}} \mathbf{RA1}(P) & \{\text{Definition of } \mathbf{RA1}\} \\
= \mathbf{RA1}(\mathit{true}) \ ;_{\mathcal{A}} (P[\mathit{States}_{tr \leq tr'}(s) \cap ac'/ac'] \wedge \mathbf{RA1}(\mathit{true})) & \\
& \{\text{Lemma F.1.6}\} \\
\Rightarrow \mathbf{RA1}(\mathit{true}) \ ;_{\mathcal{A}} \mathbf{RA1}(\mathit{true}) & \{\text{Lemma B.1.16}\} \\
= \mathbf{RA1}(\mathit{true}) &
\end{array}
$$

□

B.1.6 Closure properties

Theorem B.1.2 *Provided P and Q are* **RA1***-healthy and Q is* **PBMH***-healthy.*

$$\mathbf{RA1}(P \ ;_{\mathcal{A}} Q) = P \ ;_{\mathcal{A}} Q$$

Proof.

$$
\begin{array}{ll}
P \ ;_{\mathcal{A}} Q & \{\text{Assumption: } P \text{ and } Q \text{ are } \mathbf{RA1}\text{-healthy}\} \\
= \mathbf{RA1}(P) \ ;_{\mathcal{A}} \mathbf{RA1}(Q) & \{\text{Definition of } \mathbf{RA1}\} \\
= (P[\mathit{States}_{tr \leq tr'}(s) \cap ac'/ac'] \wedge \mathbf{RA1}(\mathit{true})) \ ;_{\mathcal{A}} \mathbf{RA1}(Q) & \\
& \{\text{Right-distributivity of } ;_{\mathcal{A}} \text{ (Lemma F.1.5)}\} \\
= \left(\begin{array}{l} (P[\mathit{States}_{tr \leq tr'}(s) \cap ac'/ac'] \ ;_{\mathcal{A}} \mathbf{RA1}(Q)) \\ \wedge \\ (\mathbf{RA1}(\mathit{true}) \ ;_{\mathcal{A}} \mathbf{RA1}(Q)) \end{array} \right) & \{\text{Lemma B.1.23}\} \\
= \left(\begin{array}{l} (P[\mathit{States}_{tr \leq tr'}(s) \cap ac'/ac'] \ ;_{\mathcal{A}} \mathbf{RA1}(Q)) \\ \wedge \\ (\mathbf{RA1}(\mathit{true}) \ ;_{\mathcal{A}} \mathbf{RA1}(Q)) \\ \wedge \\ \mathbf{RA1}(\mathit{true}) \end{array} \right) & \\
& \{\text{Right-distributivity of } ;_{\mathcal{A}} \text{ (Lemma F.1.5)}\} \\
= \left(\begin{array}{l} ((P[\mathit{States}_{tr \leq tr'}(s) \cap ac'/ac'] \wedge \mathbf{RA1}(\mathit{true})) \ ;_{\mathcal{A}} \mathbf{RA1}(Q)) \\ \wedge \\ \mathbf{RA1}(\mathit{true}) \end{array} \right) & \\
& \{\text{Definition of } \mathbf{RA1}\}
\end{array}
$$

$$= \left(\begin{array}{l} ((P \wedge ac' \neq \emptyset)[States_{tr \leq tr'}(s) \cap ac'/ac'] \ ;_{\mathcal{A}} \mathbf{RA1}(Q)) \\ \wedge \\ \mathbf{RA1}(true) \end{array} \right)$$

{Assumption: Q is **PBMH**-healthy and Lemma B.1.20}

$$= \left(\begin{array}{l} \left(\begin{array}{l} (P \wedge ac' \neq \emptyset)[States_{tr \leq tr'}(s) \cap ac'/ac'] \\ ;_{\mathcal{A}} \\ \mathbf{PBMH}(Q \wedge ac' \neq \emptyset \wedge ac' \subseteq States_{tr \leq tr'}(s)) \end{array} \right) \\ \wedge \\ \mathbf{RA1}(true) \end{array} \right)$$

{Definition of $;_{\mathcal{A}}$ and substitution}

$$= \left(\begin{array}{l} \left(\begin{array}{l} (P \wedge ac' \neq \emptyset) \\ \left[\begin{array}{l} States_{tr \leq tr'}(s) \\ \cap \\ \left\{ z \left| \mathbf{PBMH} \left(\begin{array}{l} Q \wedge ac' \neq \emptyset \\ \wedge \\ ac' \subseteq States_{tr \leq tr'}(s) \end{array} \right) [z/s] \right. \right\} \Big/ ac' \end{array} \right] \end{array} \right) \\ \wedge \\ \mathbf{RA1}(true) \end{array} \right)$$

{Definition of **PBMH**}

$$= \left(\begin{array}{l} \left(\begin{array}{l} (P \wedge ac' \neq \emptyset) \\ \left[\begin{array}{l} States_{tr \leq tr'}(s) \\ \cap \\ \left\{ z \left| \left(\begin{array}{l} \exists\, ac_0 \bullet Q[ac_0/ac'] \wedge ac_0 \neq \emptyset \\ \wedge \\ ac_0 \subseteq States_{tr \leq tr'}(s) \\ \wedge \\ ac_0 \subseteq ac' \end{array} \right) [z/s] \right. \right\} \Big/ ac' \end{array} \right] \end{array} \right) \\ \wedge \\ \mathbf{RA1}(true) \end{array} \right)$$

{Substitution}

$$
= \left(\begin{array}{l}
\left(\begin{array}{l}
(P \wedge ac' \neq \emptyset) \\
\left[\begin{array}{l}
States_{tr \leq tr'}(s) \\
\cap \\
\left\{ z \;\middle|\; \left(\begin{array}{l}
\exists\, ac_0 \bullet Q[z/s][ac_0/ac'] \wedge ac_0 \neq \emptyset \\
\wedge \\
ac_0 \subseteq States_{tr \leq tr'}(z) \\
\wedge \\
ac_0 \subseteq ac'
\end{array} \right) \right\} \Big/ ac'
\end{array} \right]
\end{array} \right) \\
\wedge \\
\mathbf{RA1}(true)
\end{array} \right)
$$

{Property of sets}

$$
= \left(\begin{array}{l}
\left(\begin{array}{l}
(P \wedge ac' \neq \emptyset) \\
\left[\left\{ z \;\middle|\; \left(\begin{array}{l}
s.tr \leq z.tr \\
\wedge \\
\exists\, ac_0 \bullet Q[z/s][ac_0/ac'] \wedge ac_0 \neq \emptyset \\
\wedge \\
ac_0 \subseteq States_{tr \leq tr'}(z) \cap ac'
\end{array} \right) \right\} \Big/ ac' \right]
\end{array} \right) \\
\wedge \\
\mathbf{RA1}(true)
\end{array} \right)
$$

{Definition of $States_{tr \leq tr'}$}

$$
= \left(\begin{array}{l}
\left(\begin{array}{l}
(P \wedge ac' \neq \emptyset) \\
\left[\left\{ z \;\middle|\; \left(\begin{array}{l}
s.tr \leq z.tr \\
\wedge \\
\exists\, ac_0 \bullet Q[z/s][ac_0/ac'] \wedge ac_0 \neq \emptyset \\
\wedge \\
ac_0 \subseteq \{x \mid z.tr \leq x.tr \wedge x \in ac'\}
\end{array} \right) \right\} \Big/ ac' \right]
\end{array} \right) \\
\wedge \\
\mathbf{RA1}(true)
\end{array} \right)
$$

{Lemma H.1.9}

$$= \left(\begin{array}{l} \left(\begin{array}{l} (P \wedge ac' \neq \emptyset) \\ \left[\left\{ z \;\middle|\; \left(\begin{array}{l} s.tr \leq z.tr \\ \wedge \\ \exists\, ac_0 \bullet Q[z/s][ac_0/ac'] \wedge ac_0 \neq \emptyset \\ \wedge \\ ac_0 \subseteq \{x \mid z.tr \leq x.tr \wedge s.tr \leq x.tr \wedge x \in ac'\} \end{array} \right) \right\} \Big/ ac' \right] \end{array} \right) \\ \wedge \\ \mathbf{RA1}(true) \end{array} \right)$$

{Property of sets and definition of $States_{tr \leq tr'}$}

$$= \left(\begin{array}{l} \left(\begin{array}{l} (P \wedge ac' \neq \emptyset) \\ \left[\begin{array}{l} States_{tr \leq tr'}(s) \\ \cap \\ \left\{ z \;\middle|\; \left(\begin{array}{l} \exists\, ac_0 \bullet Q[z/s][ac_0/ac'] \wedge ac_0 \neq \emptyset \\ \wedge \\ ac_0 \subseteq States_{tr \leq tr'}(z) \cap States_{tr \leq tr'}(s) \cap ac' \end{array} \right) \right\} \Big/ ac' \end{array} \right] \end{array} \right) \\ \wedge \\ \mathbf{RA1}(true) \end{array} \right)$$

{Property of sets and substitution}

$$= \left(\begin{array}{l} \left(\begin{array}{l} (P \wedge ac' \neq \emptyset) \\ \left[\begin{array}{l} States_{tr \leq tr'}(s) \\ \cap \\ \left\{ z \;\middle|\; \left(\begin{array}{l} \exists\, ac_0 \bullet Q[z/s][ac_0/ac'] \wedge ac_0 \neq \emptyset \\ \wedge \\ ac_0 \subseteq States_{tr \leq tr'}(z) \cap ac' \end{array} \right) \right\} \Big/ ac' \end{array} \right] \\ [States_{tr \leq tr'}(s) \cap ac'/ac'] \end{array} \right) \\ \wedge \\ \mathbf{RA1}(true) \end{array} \right)$$

{Definition of **RA1**}

$$= \mathbf{RA1} \left(\begin{array}{l} (P \wedge ac' \neq \emptyset) \\ \left[\begin{array}{l} States_{tr \leq tr'}(s) \\ \cap \\ \left\{ z \;\middle|\; \left(\begin{array}{l} \exists\, ac_0 \bullet Q[z/s][ac_0/ac'] \wedge ac_0 \neq \emptyset \\ \wedge \\ ac_0 \subseteq States_{tr \leq tr'}(z) \cap ac' \end{array} \right) \right\} \Big/ ac' \end{array} \right] \end{array} \right)$$

{Substitution}

$$= \mathbf{RA1}\left(\begin{array}{l}(P \wedge ac' \neq \emptyset) \\ \left[\begin{array}{l} States_{tr \leq tr'}(s) \\ \cap \\ \left\{ z \;\middle|\; \left(\begin{array}{l} \exists\, ac_0 \bullet Q[ac_0/ac'] \wedge ac_0 \neq \emptyset \\ \wedge \\ ac_0 \subseteq States_{tr \leq tr'}(s) \cap ac' \end{array}\right)[z/s] \right\} \Big/ ac' \end{array}\right] \end{array}\right)$$

{Property of sets and definition of **PBMH**}

$$= \mathbf{RA1}\left(\begin{array}{l}(P \wedge ac' \neq \emptyset) \\ \left[\begin{array}{l} States_{tr \leq tr'}(s) \\ \cap \\ \left\{ z \;\middle|\; \mathbf{PBMH}\left(\begin{array}{l} (Q \wedge ac' \neq \emptyset \\ \wedge \\ ac' \subseteq States_{tr \leq tr'}(s) \end{array}\right)[z/s] \right\} \Big/ ac' \end{array}\right] \end{array}\right)$$

{Assumption: Q is **PBMH**-healthy and Lemma B.1.20}

$$= \mathbf{RA1}((P \wedge ac' \neq \emptyset)[States_{tr \leq tr'}(s) \cap \{z \mid \mathbf{RA1}(Q)[z/s]\}/ac'])$$

{Definition of $;_{\mathcal{A}}$ and substitution}

$$= \mathbf{RA1}((P \wedge ac' \neq \emptyset)[States_{tr \leq tr'}(s) \cap ac'/ac'] \;;_{\mathcal{A}} \mathbf{RA1}(Q))$$

{Definition of **RA1**}

$$= \mathbf{RA1}(\mathbf{RA1}(P) \;;_{\mathcal{A}} \mathbf{RA1}(Q))$$

{Assumption: P and Q are **RA1**-healthy}

$$= \mathbf{RA1}(P \;;_{\mathcal{A}} Q)$$

□

B.2 RA2

B.2.1 Lemmas

Lemma B.2.1

$$\mathbf{RA2}(P) = P[s \oplus \{tr \mapsto \langle\rangle\}, \{y \mid y \oplus \{tr \mapsto s.tr \frown y.tr\} \in ac'\}/s, ac']$$

Proof.

$\mathbf{RA2}(P)$ {Definition of **RA2**}

$$= P[s \oplus \{tr \mapsto \langle\rangle\}, \{z \mid z \in ac' \wedge s.tr \leq z.tr \bullet z \oplus \{tr \mapsto z.tr - s.tr\}\}/s, ac']$$

{Property of sets}

$$= P\left[s \oplus \{tr \mapsto \langle\rangle\}, \left\{ y \,\middle|\, y \in \left\{ z \,\middle|\, \begin{array}{l} z \in ac' \wedge s.tr \leq z.tr \\ \bullet\ z \oplus \{tr \mapsto z.tr - s.tr\} \end{array} \right\} \right\} \middle/ s, ac'\right]$$

{Property of sets}

$$= P\left[s \oplus \{tr \mapsto \langle\rangle\}, \left\{ y \,\middle|\, \begin{array}{l} \exists\, z \bullet z \in ac' \wedge s.tr \leq z.tr \\ \wedge\ y = z \oplus \{tr \mapsto z.tr - s.tr\} \end{array} \right\} \middle/ s, ac'\right]$$

{Lemma B.1.3}

$$= P[s \oplus \{tr \mapsto \langle\rangle\}, \{y \mid y \oplus \{tr \mapsto s.tr \frown y.tr\} \in ac'\}/s, ac']$$

□

Lemma B.2.2

$$\mathbf{RA2}(true) = true$$

Proof.

$\mathbf{RA2}(true)$ {Definition of **RA2**}

$= true[s \oplus \{tr \mapsto \langle\rangle\}, \{z \mid z \in ac' \wedge s.tr \leq z.tr \bullet z \oplus \{tr \mapsto z.tr - s.tr\}\}/s, ac']$

{Substitution}

$= true$

□

Lemma B.2.3

$$\mathbf{RA2}(s \in ac') = s \in ac'$$

Proof.

$\mathbf{RA2}(s \in ac')$ {Definition of **RA2**}

$= (s \in ac')[s \oplus \{tr \mapsto \langle\rangle\}, \{z \mid z \in ac' \wedge s.tr \leq z.tr \bullet z \oplus \{tr \mapsto z.tr - s.tr\}\}/s, ac']$

{Substitution}

$= s \oplus \{tr \mapsto \langle\rangle\} \in \{z \mid z \in ac' \wedge s.tr \leq z.tr \bullet z \oplus \{tr \mapsto z.tr - s.tr\}\}$

{Property of sets}

$= \exists\, z \bullet z \in ac' \wedge s.tr \leq z.tr \wedge s \oplus \{tr \mapsto \langle\rangle\} = z \oplus \{tr \mapsto z.tr - s.tr\}$

{Property of $\oplus$}

$$= \left(\begin{array}{l} \exists\, z \bullet z \in ac' \wedge s.tr \leq z.tr \\ \wedge\ \{tr\} \lhd s \cup \{tr \mapsto \langle\rangle\} = \{tr\} \lhd z \cup \{tr \mapsto z.tr - s.tr\} \end{array} \right)$$

{Property of relations}

$$= \left(\begin{array}{l} \exists\, z \bullet z \in ac' \land s.tr \leq z.tr \\ \land\ \{tr\} \lhd s = \{tr\} \lhd z \land \{tr \mapsto \langle\rangle\} = \{tr \mapsto z.tr - s.tr\} \end{array} \right)$$

{Property of relations}

$$= \left(\begin{array}{l} \exists\, z \bullet z \in ac' \land s.tr \leq z.tr \\ \land\ \{tr\} \lhd s = \{tr\} \lhd z \land \langle\rangle = z.tr - s.tr \end{array} \right)$$

{Property of sequences}

$$= \left(\begin{array}{l} \exists\, z \bullet z \in ac' \land s.tr \leq z.tr \\ \land\ \{tr\} \lhd s = \{tr\} \lhd z \land z.tr = s.tr \end{array} \right)$$

{Property of relations}

$= \exists\, z \bullet z \in ac' \land s.tr \leq z.tr \land s = z$ {One-point rule}

$= s \in ac' \land s.tr \leq s.tr$ {Property of sequences}

$= s \in ac'$

□

Lemma B.2.4 *Provided s and ac' are not free in P.*

$$\mathbf{RA2}(P) = P$$

Proof.

$\mathbf{RA2}(P)$ {Definition of **RA2**}

$= P[s \oplus \{tr \mapsto \langle\rangle\}, \{z \mid z \in ac' \land s.tr \leq z.tr \bullet z \oplus \{tr \mapsto z.tr - s.tr\}\}/s, ac']$

{Assumption and substitution}

$= P$

□

Lemma B.2.5

$$\mathbf{RA2}(P \lhd c \rhd Q)$$

Proof.

$\mathbf{RA2}(P \lhd c \rhd Q)$ {Definition of conditional}

$= \mathbf{RA2}((c \land P) \lor (\neg\, c \land Q))$ {Theorem 1.2.10}

$= \mathbf{RA2}(c \land P) \lor \mathbf{RA2}(\neg\, c \land Q)$ {Theorem 1.2.9}

$= (\mathbf{RA2}(c) \land \mathbf{RA2}(P)) \lor (\mathbf{RA2}(\neg\, c) \land \mathbf{RA2}(Q))$ {Lemma B.2.7}

$= (\mathbf{RA2}(c) \land \mathbf{RA2}(P)) \lor (\neg\, \mathbf{RA2}(c) \land \mathbf{RA2}(Q))$

{Definition of conditional}

$= \mathbf{RA2}(P) \lhd \mathbf{RA2}(c) \rhd \mathbf{RA2}(Q)$

□

Lemma B.2.6 *Provided c is* **RA2***-healthy.*

$$\mathbf{RA2}(P \lhd c \rhd Q) = \mathbf{RA2}(P) \lhd c \rhd \mathbf{RA2}(Q)$$

Proof.

$$\begin{array}{ll}
\mathbf{RA2}(P \lhd c \rhd Q) & \{\text{Lemma B.2.5}\} \\
= \mathbf{RA2}(P) \lhd \mathbf{RA2}(c) \rhd \mathbf{RA2}(Q) & \{\text{Assumption: } c \text{ is } \mathbf{RA2}\text{-healthy}\} \\
= \mathbf{RA2}(P) \lhd c \rhd \mathbf{RA2}(Q) &
\end{array}$$

□

Lemma B.2.7

$$\mathbf{RA2}(\neg\ P) = \neg\ \mathbf{RA2}(P)$$

Proof.

$$\begin{array}{ll}
\mathbf{RA2}(\neg\ P) & \{\text{Definition of } \mathbf{RA2}\} \\
= (\neg\ P)[s \oplus \{tr \mapsto \langle\rangle\}, \{z \mid z \in ac' \wedge s.tr \leq z.tr \bullet z \oplus \{tr \mapsto z.tr - s.tr\}\}/s, ac'] & \\
& \{\text{Property of substitution}\} \\
= \neg\ P[s \oplus \{tr \mapsto \langle\rangle\}, \{z \mid z \in ac' \wedge s.tr \leq z.tr \bullet z \oplus \{tr \mapsto z.tr - s.tr\}\}/s, ac'] & \\
& \{\text{Definition of } \mathbf{RA2}\} \\
= \neg\ \mathbf{RA2}(P) &
\end{array}$$

□

Lemma B.2.8 *Where c is not tr.*

$$\mathbf{RA2}(s.c) = s.c$$

Proof.

$$\begin{array}{ll}
\mathbf{RA2}(s.c) & \{\text{Definition of } \mathbf{RA2}\} \\
= s.c[s \oplus \{tr \mapsto \langle\rangle\}, \{z \mid z \in ac' \wedge s.tr \leq z.tr \bullet z \oplus \{tr \mapsto z.tr - s.tr\}\}/s, ac'] & \\
& \{\text{Substitution}\} \\
= (s \oplus \{tr \mapsto \langle\rangle\}).c & \{\text{Property of } \oplus\} \\
= s.c &
\end{array}$$

□

B.2.2 Substitution properties

Lemma B.2.9

$$\mathbf{RA2}(P)^o_w = \mathbf{RA2}(P^o_w)$$

Proof.

$$
\begin{array}{ll}
& \mathbf{RA2}(P)^o_w \\
& \qquad \{\text{Definition of } \mathbf{RA2}\} \\
= & P[s \oplus \{tr \mapsto \langle\rangle\}, \{z \mid z \in ac' \wedge s.tr \leq z.tr \bullet z \oplus \{tr \mapsto z.tr - s.tr\}\}/s, ac']^o_w \\
& \qquad \{\text{Substitution abbreviation}\} \\
= & \left(P\right) \begin{array}{l} [s \oplus \{tr \mapsto \langle\rangle\}, \{z \mid z \in ac' \wedge s.tr \leq z.tr \bullet z \oplus \{tr \mapsto z.tr - s.tr\}\}/s, ac'] \\ [o, s \oplus \{wait \mapsto w\}/ok', s] \end{array} \\
& \qquad \{\text{Substitution}\} \\
= & \left(P\right) \begin{array}{l} [o/ok'] \\ [s \oplus \{tr \mapsto \langle\rangle\}, \{z \mid z \in ac' \wedge s.tr \leq z.tr \bullet z \oplus \{tr \mapsto z.tr - s.tr\}\}/s, ac'] \\ [s \oplus \{wait \mapsto w\}/s] \end{array} \\
& \qquad \{\text{Substitution}\} \\
= & \left(P\right) \begin{array}{l} [o/ok'] \\ [s \oplus \{wait \mapsto w\} \oplus \{tr \mapsto \langle\rangle\}/s] \\ \left[\left\{ z \;\middle|\; \begin{array}{l} z \in ac' \wedge s \oplus \{wait \mapsto w\}.tr \leq z.tr \\ \bullet\ z \oplus \{tr \mapsto z.tr - s \oplus \{wait \mapsto w\}.tr\} \end{array} \right\}/ac'\right] \end{array} \\
& \qquad \{\text{Property of } \oplus\} \\
= & \left(P\right) \begin{array}{l} [o/ok'] \\ [s \oplus \{wait \mapsto w\} \oplus \{tr \mapsto \langle\rangle\}/s] \\ [\{z \mid z \in ac' \wedge s.tr \leq z.tr \bullet z \oplus \{tr \mapsto z.tr - s.tr\}\}/ac'] \end{array} \\
& \qquad \{\text{Property of } \oplus\text{: distinct record components}\} \\
= & \left(P\right) \begin{array}{l} [o/ok'] \\ [s \oplus \{tr \mapsto \langle\rangle\} \oplus \{wait \mapsto w\}/s] \\ [\{z \mid z \in ac' \wedge s.tr \leq z.tr \bullet z \oplus \{tr \mapsto z.tr - s.tr\}\}/ac'] \end{array} \\
& \qquad \{\text{Substitution}\}
\end{array}
$$

$$= \left(P \right) \begin{array}{l} [o/ok'] \\ [s \oplus \{wait \mapsto w\}/s] \\ [s \oplus \{tr \mapsto \langle\rangle\}/s] \\ [\{z \mid z \in ac' \wedge s.tr \leq z.tr \bullet z \oplus \{tr \mapsto z.tr - s.tr\}\}/ac'] \end{array}$$

{Substitution}

$$= \left(P \right) \begin{array}{l} [o, s \oplus \{wait \mapsto w\}/ok', s] \\ [s \oplus \{tr \mapsto \langle\rangle\}, \{z \mid z \in ac' \wedge s.tr \leq z.tr \bullet z \oplus \{tr \mapsto z.tr - s.tr\}\}/s, ac'] \end{array}$$

{Substitution abbreviation}

$$= \left(P^o_w\right) [s \oplus \{tr \mapsto \langle\rangle\}, \{z \mid z \in ac' \wedge s.tr \leq z.tr \bullet z \oplus \{tr \mapsto z.tr - s.tr\}\}/s, ac']$$

{Definition of **RA2**}

$$= \mathbf{RA2}(P^o_w)$$

□

B.2.3 Properties with respect to designs

Lemma B.2.10

$$\mathbf{RA2}(P \vdash Q) = (\neg\, \mathbf{RA2}(\neg\, P) \vdash \mathbf{RA2}(Q))$$

Proof.

$\mathbf{RA2}(P \vdash Q)$ {Definition of design}
$= \mathbf{RA2}((ok \wedge P) \Rightarrow (Q \wedge ok'))$ {Predicate calculus}
$= \mathbf{RA2}(\neg\, ok \vee \neg\, P \vee (Q \wedge ok'))$ {Theorem 1.2.10}
$= \mathbf{RA2}(\neg\, ok) \vee \mathbf{RA2}(\neg\, P) \vee \mathbf{RA2}(Q \wedge ok')$ {Theorem 1.2.9}
$= \mathbf{RA2}(\neg\, ok) \vee \mathbf{RA2}(\neg\, P) \vee (\mathbf{RA2}(Q) \wedge \mathbf{RA2}(ok'))$ {Lemma B.2.4}
$= \neg\, ok \vee \mathbf{RA2}(\neg\, P) \vee (\mathbf{RA2}(Q) \wedge ok')$ {Predicate calculus}
$= (ok \wedge \neg\, \mathbf{RA2}(\neg\, P)) \Rightarrow (\mathbf{RA2}(Q) \wedge ok')$ {Definition of design}
$= (\neg\, \mathbf{RA2}(\neg\, P) \vdash \mathbf{RA2}(Q))$

□

B.2.4 Properties with respect to $;_{\mathcal{A}}$

Theorem B.2.1

$$\mathbf{RA2}(P \;;_{\mathcal{A}} \mathbf{RA2}(Q)) = \mathbf{RA2}(P) \;;_{\mathcal{A}} \mathbf{RA2}(Q)$$

Proof.

$$
\begin{aligned}
&\mathbf{RA2}(P \ ;_{\mathcal{A}} \mathbf{RA2}(Q)) && \{\text{Definition of } \mathbf{RA2} \text{ (Lemma B.2.1)}\}\\
&= \mathbf{RA2}(P \ ;_{\mathcal{A}} Q[s \oplus \{tr \mapsto \langle\rangle\}, \{y \mid y \oplus \{tr \mapsto s.tr \frown y.tr\} \in ac'\}/s, ac']) \\
& && \{\text{Definition of } ;_{\mathcal{A}} \text{ and substitution}\}\\
&= \mathbf{RA2}\left(P \left[\left\{ s \;\middle|\; \left(Q\right)^{\begin{array}{l}[s \oplus \{tr \mapsto \langle\rangle\}/s] \\ [\{y \mid y \oplus \{tr \mapsto s.tr \frown y.tr\} \in ac'\}/ac']\end{array}} \right\} \Big/ ac' \right]\right) \\
& && \{\text{Variable renaming}\}\\
&= \mathbf{RA2}\left(P \left[\left\{ z \;\middle|\; \left(Q\right)^{\begin{array}{l}[z \oplus \{tr \mapsto \langle\rangle\}/s] \\ [\{y \mid y \oplus \{tr \mapsto z.tr \frown y.tr\} \in ac'\}/ac']\end{array}} \right\} \Big/ ac' \right]\right) \\
& && \{\text{Definition of } \mathbf{RA2} \text{ (Lemma B.2.1)}\}\\
&= \left(P\right)^{[s \oplus \{tr \mapsto \langle\rangle\}, \{y \mid y \oplus \{tr \mapsto s.tr \frown y.tr\} \in ac'\}/s, ac']} \left[\left\{ z \;\middle|\; \left(Q\right)^{\begin{array}{l}[z \oplus \{tr \mapsto \langle\rangle\}/s] \\ [\{y \mid y \oplus \{tr \mapsto z.tr \frown y.tr\} \in ac'\}/ac']\end{array}} \right\} \Big/ ac' \right] \\
& && \{\text{Substitution}\}\\
&= \left(P\right)^{[s \oplus \{tr \mapsto \langle\rangle\}/s]} \left[\left\{ z \;\middle|\; \left(Q\right)^{[z \oplus \{tr \mapsto \langle\rangle\}/s]} \left[\left\{ y \;\middle|\; \begin{array}{l} y \oplus \{tr \mapsto z.tr \frown y.tr\} \\ \in \\ \{y \mid y \oplus \{tr \mapsto s.tr \frown y.tr\} \in ac'\}\end{array} \right\} \Big/ ac' \right] \right\} \Big/ ac' \right] \\
& && \{\text{Property of sets, } \oplus \text{ and value of record component } tr\}\\
&= \left(P\right)^{[s \oplus \{tr \mapsto \langle\rangle\}/s]} \left[\left\{ z \;\middle|\; \left(Q\right)^{\begin{array}{l}[z \oplus \{tr \mapsto \langle\rangle\}/s] \\ \left[\left\{ y \;\middle|\; y \oplus \{tr \mapsto s.tr \frown z.tr \frown y.tr\} \in ac' \right\}/ ac'\right]\end{array}} \right\} \Big/ ac' \right] \\
& && \{\text{Lemma B.2.11}\}\\
&= \mathbf{RA2}(P) \ ;_{\mathcal{A}} \mathbf{RA2}(Q)
\end{aligned}
$$

□

Lemma B.2.11

$$
\begin{aligned}
&\mathbf{RA2}(P) \ ;_{\mathcal{A}} \mathbf{RA2}(Q) \\
&= \\
&\left(P\right)^{[s \oplus \{tr \mapsto \langle\rangle\}/s]} \left[\left\{ t \;\middle|\; \left(Q\right)^{\begin{array}{l}[(t \oplus \{tr \mapsto \langle\rangle\}/s] \\ [\{y \mid y \oplus \{tr \mapsto s.tr \frown t.tr \frown y.tr\} \in ac'\}/ac']\end{array}} \right\} \Big/ ac' \right]
\end{aligned}
$$

Proof.

$$
\begin{array}{ll}
\mathbf{RA2}(P)\ ;_{\mathcal{A}}\ \mathbf{RA2}(Q) & \{\text{Definition of } \mathbf{RA2} \text{ (Lemma B.2.1)}\} \\
= \left(\begin{array}{l} P[s \oplus \{tr \mapsto \langle\rangle\}, \{t \mid t \oplus \{tr \mapsto s.tr \frown t.tr\} \in ac'\}/s, ac'] \\ ;_{\mathcal{A}} \\ Q[s \oplus \{tr \mapsto \langle\rangle\}, \{y \mid y \oplus \{tr \mapsto s.tr \frown y.tr\} \in ac'\}/s, ac'] \end{array}\right) & \{\text{Definition of } ;_{\mathcal{A}}\} \\
= \left(P\right) \begin{array}{l} [s \oplus \{tr \mapsto \langle\rangle\}, \{t \mid t \oplus \{tr \mapsto s.tr \frown t.tr\} \in ac'\}/s, ac'] \\ [\{z \mid Q[s \oplus \{tr \mapsto \langle\rangle\}, \{y \mid y \oplus \{tr \mapsto s.tr \frown y.tr\} \in ac'\}/s, ac'][z/s]\}/ac'] \end{array} & \{\text{Substitution}\} \\
= \left(P\right) \begin{array}{l} [s \oplus \{tr \mapsto \langle\rangle\}, \{t \mid t \oplus \{tr \mapsto s.tr \frown t.tr\} \in ac'\}/s, ac'] \\ [\{z \mid Q[z \oplus \{tr \mapsto \langle\rangle\}, \{y \mid y \oplus \{tr \mapsto z.tr \frown y.tr\} \in ac'\}/s, ac']\}/ac'] \end{array} & \{\text{Substitution}\} \\
= \left(P\right) \begin{array}{l} [s \oplus \{tr \mapsto \langle\rangle\}/s] \\ \left[\left\{ t \;\middle|\; \begin{array}{l} t \oplus \{tr \mapsto s.tr \frown t.tr\} \\ \in \\ \left\{ z \;\middle|\; (Q) \begin{array}{l} [z \oplus \{tr \mapsto \langle\rangle\}/s] \\ [\{y \mid y \oplus \{tr \mapsto z.tr \frown y.tr\} \in ac'\}/ac'] \end{array} \right\} \end{array} \right\} \Big/ ac' \right] \end{array} & \{\text{Property of sets}\} \\
= \left(P\right) \begin{array}{l} [s \oplus \{tr \mapsto \langle\rangle\}/s] \\ \left[\left\{ t \;\middle|\; \left(Q\right) \begin{array}{l} [(t \oplus \{tr \mapsto s.tr \frown t.tr\}) \oplus \{tr \mapsto \langle\rangle\}/s] \\ [\{y \mid y \oplus \{tr \mapsto (t \oplus \{tr \mapsto s.tr \frown t.tr\}).tr \frown y.tr\} \in ac'\}/ac'] \end{array} \right\} \Big/ ac' \right] \end{array} & \{\text{Property of } \oplus \text{ and record component}\} \\
= \left(P\right) \begin{array}{l} [s \oplus \{tr \mapsto \langle\rangle\}/s] \\ \left[\left\{ t \;\middle|\; \left(Q\right) \begin{array}{l} [(t \oplus \{tr \mapsto \langle\rangle\}/s] \\ [\{y \mid y \oplus \{tr \mapsto s.tr \frown t.tr \frown y.tr\} \in ac'\}/ac'] \end{array} \right\} \Big/ ac' \right] \end{array} &
\end{array}
$$

□

B.2.5 Closure properties

Theorem B.2.2 *Provided P and Q are* **RA2***-healthy.*

$$\mathbf{RA2}(P\ ;_{\mathcal{A}}\ Q) = P\ ;_{\mathcal{A}}\ Q$$

Proof.

$\mathbf{RA2}(P\ ;_{\mathcal{A}}\ Q)$ {Assumption: P and Q are **RA2**-healthy}

$$= \mathbf{RA2}(\mathbf{RA2}(P) \ ;_{\mathcal{A}} \mathbf{RA2}(Q)) \qquad \{\text{Lemma B.2.11}\}$$

$$= \mathbf{RA2}\left(\left(P\right)^{[s \oplus \{tr \mapsto \langle\rangle\}/s]}_{\left[\left\{t \,\middle|\, \left(Q\right)^{[(t \oplus \{tr \mapsto \langle\rangle\}/s]}_{[\{y \mid y \oplus \{tr \mapsto s.tr \frown t.tr \frown y.tr\} \in ac'\}/ac']}\right\} \Big/ ac'\right]}\right)$$

$\{\text{Definition of } \mathbf{RA2} \text{ (Lemma B.2.1)}\}$

$$= \left(P\right)^{[s \oplus \{tr \mapsto \langle\rangle\}/s]}_{\left[\left\{t \,\middle|\, \left(Q\right)^{[(t \oplus \{tr \mapsto \langle\rangle\}/s]}_{[\{y \mid y \oplus \{tr \mapsto s.tr \frown t.tr \frown y.tr\} \in ac'\}/ac']}\right\} \Big/ ac'\right]}_{[s \oplus \{tr \mapsto \langle\rangle\}, \{y \mid y \oplus \{tr \mapsto s.tr \frown y.tr\} \in ac'\}/s, ac']}$$

$\{\text{Substitution}\}$

$$= \left(P\right)^{[s \oplus \{tr \mapsto \langle\rangle\} \oplus \{tr \mapsto \langle\rangle\}/s]}_{\left[\left\{t \,\middle|\, \left(Q\right)^{[(t \oplus \{tr \mapsto \langle\rangle\}/s]}_{\left[\left\{y \,\middle|\, \begin{array}{l} y \oplus \{tr \mapsto (s \oplus \{tr \mapsto \langle\rangle\}).tr \frown t.tr \frown y.tr\} \\ \in \\ \{y \mid y \oplus \{tr \mapsto s.tr \frown y.tr\} \in ac'\} \end{array}\right\} \Big/ ac'\right]}\right\} \Big/ ac'\right]}$$

$\{\text{Variable renaming, property of } \oplus \text{ and value of record component } tr\}$

$$= \left(P\right)^{[s \oplus \{tr \mapsto \langle\rangle\}/s]}_{\left[\left\{t \,\middle|\, \left(Q\right)^{[(t \oplus \{tr \mapsto \langle\rangle\}/s]}_{\left[\left\{y \,\middle|\, \begin{array}{l} y \oplus \{tr \mapsto \langle\rangle \frown t.tr \frown y.tr\} \\ \in \\ \{z \mid z \oplus \{tr \mapsto s.tr \frown z.tr\} \in ac'\} \end{array}\right\} \Big/ ac'\right]}\right\} \Big/ ac'\right]}$$

$\{\text{Property of sequences}\}$

$$= \left(P\right)^{[s \oplus \{tr \mapsto \langle\rangle\}/s]}_{\left[\left\{t \,\middle|\, \left(Q\right)^{[(t \oplus \{tr \mapsto \langle\rangle\}/s]}_{\left[\left\{y \,\middle|\, \begin{array}{l} y \oplus \{tr \mapsto t.tr \frown y.tr\} \\ \in \\ \{z \mid z \oplus \{tr \mapsto s.tr \frown z.tr\} \in ac'\} \end{array}\right\} \Big/ ac'\right]}\right\} \Big/ ac'\right]}$$

$\{\text{Property of sets, } \oplus \text{ and value of record component } tr\}$

$$= \left(P\right)^{[s \oplus \{tr \mapsto \langle\rangle\}/s]}_{\left[\left\{t \,\middle|\, \left(Q\right)^{[(t \oplus \{tr \mapsto \langle\rangle\}/s]}_{[\{y \mid y \oplus \{tr \mapsto s.tr \frown t.tr \frown y.tr\} \in ac'\}/ac']}\right\} \Big/ ac'\right]}$$

$\{\text{Lemma B.2.11}\}$

$$= \mathbf{RA2}(P) \ ;_{\mathcal{A}} \mathbf{RA2}(Q) \qquad \{\text{Assumption: } P \text{ and } Q \text{ are } \mathbf{RA2}\text{-healthy}\}$$

$= P \ ;_{\mathcal{A}} Q$

□

B.3 RA3

B.3.1 Substitution lemmas

Lemma B.3.1

$$\mathbf{RA3}(P) = \mathbf{RA3}(P_f)$$

Proof.

$\mathbf{RA3}(P)$ {Definition of **RA3**}
$= (\mathbb{I}_{\mathcal{R}ac} \lhd s.wait \rhd P)$
{Definition of conditional and predicate calculus}
$= (\mathbb{I}_{\mathcal{R}ac} \lhd s.wait \rhd (\neg\, s.wait \wedge P))$ {Predicate calculus}
$= (\mathbb{I}_{\mathcal{R}ac} \lhd s.wait \rhd (s.wait = false \wedge P))$ {Lemma A.1.2}
$= (\mathbb{I}_{\mathcal{R}ac} \lhd s.wait \rhd (s.wait = false \wedge P[s \oplus \{wait \mapsto false\}/s]))$
{Definition of conditional and predicate calculus}
$= (\mathbb{I}_{\mathcal{R}ac} \lhd s.wait \rhd P[s \oplus \{wait \mapsto false\}/s])$ {Definition of **RA3**}
$= \mathbf{RA3}(P[s \oplus \{wait \mapsto false\}/s])$ {Substitution abbreviation}
$= \mathbf{RA3}(P_f)$

□

Lemma B.3.2

$$\mathbf{RA3}(P)^o_f = P^o_f$$

Proof.

$\mathbf{RA3}(P)^o_f$ {Lemma B.3.3}
$= (\mathbb{I}_{\mathcal{R}ac})^o_f \lhd false \rhd P^o_f$ {Property of conditional}
$= P^o_f$

□

Lemma B.3.3

$$\mathbf{RA3}(P)^o_w = (\mathit{II}_{\mathcal{R}ac})^o_w \lhd w \rhd P^o_w$$

Proof.

$\mathbf{RA3}(P)^o_w$ {Definition of **RA3**}
$= (\mathit{II}_{\mathcal{R}ac} \lhd s.wait \rhd P)^o_w$ {Substitution abbreviation}
$= (\mathit{II}_{\mathcal{R}ac} \lhd s.wait \rhd P)[o, s \oplus \{wait \mapsto w\}/ok', s]$ {Substitution}
$= (\mathit{II}_{\mathcal{R}ac}[o, s \oplus \{wait \mapsto w\}/ok', s] \lhd (s \oplus \{wait \mapsto w\}).wait \rhd P[o, s \oplus \{wait \mapsto w\}/ok', s])$
{Value of record component}
$= (\mathit{II}_{\mathcal{R}ac}[o, s \oplus \{wait \mapsto w\}/ok', s] \lhd w \rhd P[o, s \oplus \{wait \mapsto w\}/ok', s])$
{Substitution abbreviation}
$= (\mathit{II}_{\mathcal{R}ac})^o_w \lhd w \rhd P^o_w$

□

B.4 RA

Lemma B.4.1 *Provided ac' is not free in c.*

$$(P \lhd c \rhd Q) \ ;_{\mathcal{A}} R = (P \ ;_{\mathcal{A}} R) \lhd c \rhd (Q \ ;_{\mathcal{A}} R)$$

Proof.

$(P \lhd c \rhd Q) \ ;_{\mathcal{A}} R$ {Definition of conditional}
$= ((c \wedge P) \vee (\neg\, c \wedge Q)) \ ;_{\mathcal{A}} R$ {Distributivity of $;_{\mathcal{A}}$ (Lemma F.1.4)}
$= ((c \wedge P) \ ;_{\mathcal{A}} R) \vee ((\neg\, c \wedge Q) \ ;_{\mathcal{A}} R)$
{Distributivity of $;_{\mathcal{A}}$ (Lemma F.1.5)}
$= ((c \ ;_{\mathcal{A}} R) \wedge (P \ ;_{\mathcal{A}} R)) \vee ((\neg\, c \ ;_{\mathcal{A}} R) \wedge (Q \ ;_{\mathcal{A}} R))$
{ac' not free in c (Lemma F.1.1)}
$= (c \wedge (P \ ;_{\mathcal{A}} R)) \vee (\neg\, c \wedge (Q \ ;_{\mathcal{A}} R))$ {Definition of conditional}
$= (P \ ;_{\mathcal{A}} R) \lhd c \rhd (Q \ ;_{\mathcal{A}} R)$

□

Lemma B.4.2

$$\begin{array}{l}\mathbf{RA1} \circ \mathbf{RA3}(P \vdash Q) \\ = \\ \mathbf{RA1}((\mathit{true} \lhd s.\mathit{wait} \rhd P) \vdash (s \in ac' \lhd s.\mathit{wait} \rhd Q))\end{array}$$

Proof.

$$\begin{array}{ll}
\mathbf{RA1} \circ \mathbf{RA3}(P \vdash Q) & \{\text{Definition of design}\} \\
= \mathbf{RA1} \circ \mathbf{RA3}(((ok \wedge P) \Rightarrow (Q \wedge ok'))) & \{\text{Predicate calculus}\} \\
= \mathbf{RA1} \circ \mathbf{RA3}((\neg\ ok \vee \neg\ P \vee (Q \wedge ok'))) & \{\text{Theorem 1.2.19}\} \\
= \mathbf{RA1}(\mathbf{RA3}(\neg\ ok) \vee \mathbf{RA3}(\neg\ P) \vee \mathbf{RA3}(Q \wedge ok')) & \{\text{Theorem 1.2.1}\} \\
= \mathbf{RA1} \circ \mathbf{RA3}(\neg\ ok) \vee \mathbf{RA1} \circ \mathbf{RA3}(\neg\ P) \vee \mathbf{RA1} \circ \mathbf{RA3}(Q \wedge ok') & \{\text{Lemma B.4.6}\} \\
= \left(\begin{array}{l} \mathbf{RA1}(\neg\ ok) \vee (s.\mathit{wait} \wedge \mathit{II}_{\mathcal{R}ac}) \vee \mathbf{RA1} \circ \mathbf{RA3}(\neg\ P) \\ \vee \\ \mathbf{RA1} \circ \mathbf{RA3}(Q \wedge ok') \end{array}\right) & \{\text{Lemma B.4.9}\} \\
= \left(\begin{array}{l} \mathbf{RA1}(\neg\ ok) \vee (s.\mathit{wait} \wedge \mathit{II}_{\mathcal{R}ac}) \vee (\mathit{II}_{\mathcal{R}ac} \lhd s.\mathit{wait} \rhd \mathbf{RA1}(\neg\ P)) \\ \vee \\ (\mathit{II}_{\mathcal{R}ac} \lhd s.\mathit{wait} \rhd \mathbf{RA1}(Q \wedge ok')) \end{array}\right) & \{\text{Lemma B.1.11}\} \\
= \left(\begin{array}{l} \mathbf{RA1}(\neg\ ok) \vee (s.\mathit{wait} \wedge \mathit{II}_{\mathcal{R}ac}) \vee (\mathit{II}_{\mathcal{R}ac} \lhd s.\mathit{wait} \rhd \mathbf{RA1}(\neg\ P)) \\ \vee \\ (\mathit{II}_{\mathcal{R}ac} \lhd s.\mathit{wait} \rhd \mathbf{RA1}(Q) \wedge ok') \end{array}\right) & \{\text{Definition of conditional and predicate calculus}\} \\
= \left(\begin{array}{l} \mathbf{RA1}(\neg\ ok) \vee (s.\mathit{wait} \wedge \mathit{II}_{\mathcal{R}ac}) \vee (\neg\ s.\mathit{wait} \wedge \mathbf{RA1}(\neg\ P)) \\ \vee \\ (\neg\ s.\mathit{wait} \wedge \mathbf{RA1}(Q) \wedge ok') \end{array}\right) & \{\text{Definition of } \mathit{II}_{\mathcal{R}ac} \text{ and predicate calculus}\} \\
= \left(\begin{array}{l} \mathbf{RA1}(\neg\ ok) \vee (s.\mathit{wait} \wedge \mathbf{RA1}(\neg\ ok)) \vee (s.\mathit{wait} \wedge s \in ac' \wedge ok') \\ \vee \\ (\neg\ s.\mathit{wait} \wedge \mathbf{RA1}(\neg\ P)) \vee (\neg\ s.\mathit{wait} \wedge \mathbf{RA1}(Q) \wedge ok') \end{array}\right) & \{\text{Predicate calculus: absorption law}\}
\end{array}$$

$$= \left(\begin{array}{l} \mathbf{RA1}(\neg\ ok) \vee (s.wait \wedge s \in ac' \wedge ok') \\ \vee \\ (\neg\ s.wait \wedge \mathbf{RA1}(\neg\ P)) \vee (\neg\ s.wait \wedge \mathbf{RA1}(Q) \wedge ok') \end{array} \right)$$

{Predicate calculus}

$$= \left(\begin{array}{l} \mathbf{RA1}(\neg\ ok) \vee (\neg\ s.wait \wedge \mathbf{RA1}(\neg\ P)) \\ \vee \\ ((s.wait \wedge s \in ac') \vee (\neg\ s.wait \wedge \mathbf{RA1}(Q)) \wedge ok') \end{array} \right)$$

{Definition of conditional}

$$= \left(\begin{array}{l} \mathbf{RA1}(\neg\ ok) \vee (false \lhd s.wait \rhd \mathbf{RA1}(\neg\ P)) \\ \vee \\ ((s \in ac' \lhd s.wait \rhd \mathbf{RA1}(Q)) \wedge ok') \end{array} \right)$$

{Lemmas B.1.4 and B.1.9}

$$= \left(\begin{array}{l} \mathbf{RA1}(\neg\ ok) \vee (\mathbf{RA1}(false) \lhd s.wait \rhd \mathbf{RA1}(\neg\ P)) \\ \vee \\ ((\mathbf{RA1}(s \in ac') \lhd s.wait \rhd \mathbf{RA1}(Q)) \wedge ok') \end{array} \right)$$

{Lemma B.1.10}

$$= \left(\begin{array}{l} \mathbf{RA1}(\neg\ ok) \vee \mathbf{RA1}(false \lhd s.wait \rhd \neg\ P) \\ \vee \\ (\mathbf{RA1}(s \in ac' \lhd s.wait \rhd Q) \wedge ok') \end{array} \right)$$

{Lemma B.1.11}

$$= \left(\begin{array}{l} \mathbf{RA1}(\neg\ ok) \vee \mathbf{RA1}(false \lhd s.wait \rhd \neg\ P) \\ \vee \\ \mathbf{RA1}((s \in ac' \lhd s.wait \rhd Q) \wedge ok') \end{array} \right)$$

{Theorem 1.2.1}

$$= \mathbf{RA1}(\neg\ ok \vee (false \lhd s.wait \rhd \neg\ P) \vee ((s \in ac' \lhd s.wait \rhd Q) \wedge ok'))$$

{Predicate calculus}

$$= \mathbf{RA1}((ok \wedge \neg\ (false \lhd s.wait \rhd \neg\ P)) \Rightarrow ((s \in ac' \lhd s.wait \rhd Q) \wedge ok'))$$

{Lemma B.4.4}

$$= \mathbf{RA1}((ok \wedge (true \lhd s.wait \rhd P)) \Rightarrow ((s \in ac' \lhd s.wait \rhd Q) \wedge ok'))$$

{Definition of design}

$$= \mathbf{RA1}((true \lhd s.wait \rhd P) \vdash (s \in ac' \lhd s.wait \rhd Q))$$

□

Lemma B.4.3

$$\neg\ (P \lhd c \rhd Q) = (\neg\ P \lhd c \rhd \neg\ Q)$$

Proof.

$$
\begin{aligned}
&\neg\,(P \lhd c \rhd Q) && \{\text{Definition of conditional}\}\\
&= \neg\,((c \wedge P) \vee (\neg\, c \wedge Q)) && \{\text{Predicate calculus}\}\\
&= (\neg\, c \vee \neg\, P) \wedge (c \vee \neg\, Q) && \{\text{Predicate calculus}\}\\
&= (\neg\, c \wedge c) \vee (\neg\, c \wedge \neg\, Q) \vee (\neg\, P \wedge c) \vee (\neg\, P \wedge \neg\, Q) && \{\text{Predicate calculus}\}\\
&= (\neg\, c \wedge \neg\, Q) \vee (\neg\, P \wedge c) \vee (\neg\, P \wedge \neg\, Q) && \{\text{Predicate calculus}\}\\
&= (\neg\, c \wedge \neg\, Q) \vee (\neg\, P \wedge (c \vee \neg\, Q)) && \{\text{Predicate calculus}\}\\
&= (\neg\, c \vee \neg\, P) \wedge (\neg\, c \vee c \vee \neg\, Q) \wedge (\neg\, Q \vee \neg\, P) \wedge (\neg\, Q \vee c) && \{\text{Predicate calculus}\}\\
&= (\neg\, c \vee \neg\, P) \wedge (\neg\, c \vee c) \wedge (\neg\, Q \vee \neg\, P) \wedge (\neg\, Q \vee c) && \{\text{Predicate calculus}\}\\
&= (c \wedge \neg\, P) \vee (\neg\, c \wedge \neg\, Q) && \{\text{Definition of conditional}\}\\
&= (\neg\, P) \lhd c \rhd (\neg\, Q)
\end{aligned}
$$

□

Lemma B.4.4

$$\neg\,(\mathit{false} \lhd c \rhd Q) = \mathit{true} \lhd c \rhd \neg\, Q$$

Proof.

$$
\begin{aligned}
&\neg\,(\mathit{false} \lhd c \rhd Q) && \{\text{Lemma B.4.3}\}\\
&= (\mathit{true} \lhd c \rhd \neg\, Q)
\end{aligned}
$$

□

Lemma B.4.5

$$\neg\,(\mathit{true} \lhd c \rhd Q) = \mathit{false} \lhd c \rhd \neg\, Q$$

Proof.

$$
\begin{aligned}
&\neg\,(\mathit{true} \lhd c \rhd Q) && \{\text{Lemma B.4.4}\}\\
&= \neg\,\neg\,(\mathit{false} \lhd c \rhd \neg\, Q) && \{\text{Predicate calculus}\}\\
&= \mathit{false} \lhd c \rhd \neg\, Q
\end{aligned}
$$

□

Lemma B.4.6

$$\mathbf{RA1} \circ \mathbf{RA3}(\neg\ ok) = \mathbf{RA1}(\neg\ ok) \vee (s.wait \wedge \mathit{I\!I}_{\mathcal{R}ac})$$

Proof.

$$\begin{array}{ll}
\mathbf{RA1} \circ \mathbf{RA3}(\neg\ ok) & \{\text{Definition of } \mathbf{RA3}\} \\
= \mathbf{RA1}(\mathit{I\!I}_{\mathcal{R}ac} \lhd s.wait \rhd (\neg\ ok)) & \{\text{Lemma B.1.10}\} \\
= \mathbf{RA1}(\mathit{I\!I}_{\mathcal{R}ac}) \lhd s.wait \rhd \mathbf{RA1}(\neg\ ok) & \{\text{Theorem 1.2.13}\} \\
= \mathit{I\!I}_{\mathcal{R}ac} \lhd s.wait \rhd \mathbf{RA1}(\neg\ ok) & \{\text{Lemma B.4.7}\} \\
= (\mathbf{RA1}(\neg\ ok) \vee (ok' \wedge s \in ac')) \lhd s.wait \rhd \mathbf{RA1}(\neg\ ok) & \\
& \{\text{Definition of conditional}\} \\
= (s.wait \wedge \mathbf{RA1}(\neg\ ok)) \vee (s.wait \wedge ok' \wedge s \in ac') \vee (\neg\ s.wait \wedge \mathbf{RA1}(\neg\ ok)) & \\
& \{\text{Predicate calculus}\} \\
= \mathbf{RA1}(\neg\ ok) \vee (s.wait \wedge ok' \wedge s \in ac') & \\
& \{\text{Predicate calculus: absorption law}\} \\
= \mathbf{RA1}(\neg\ ok) \vee (s.wait \wedge \mathbf{RA1}(\neg\ ok)) \vee (s.wait \wedge ok' \wedge s \in ac') & \\
& \{\text{Predicate calculus}\} \\
= \mathbf{RA1}(\neg\ ok) \vee (s.wait \wedge (\mathbf{RA1}(\neg\ ok) \vee (ok' \wedge s \in ac'))) & \\
& \{\text{Lemma B.4.7}\} \\
= \mathbf{RA1}(\neg\ ok) \vee (s.wait \wedge \mathit{I\!I}_{\mathcal{R}ac}) &
\end{array}$$

□

Lemma B.4.7

$$\mathit{I\!I}_{\mathcal{R}ac} = \mathbf{RA1}(\neg\ ok) \vee (ok' \wedge s \in ac')$$

Proof.

$$\begin{array}{ll}
\mathit{I\!I}_{\mathcal{R}ac} & \{\text{Definition of } \mathit{I\!I}_{\mathcal{R}ac}\} \\
= (\neg\ ok \wedge \mathbf{RA1}(\mathit{true})) \vee (ok' \wedge s \in ac') & \{\text{Lemma B.1.12}\} \\
= \mathbf{RA1}(\neg\ ok) \vee (ok' \wedge s \in ac') &
\end{array}$$

□

Lemma B.4.8

$$\mathbf{RA1} \circ \mathbf{RA3}(P) = (s.wait \wedge \mathit{I\!I}_{\mathcal{R}ac}) \vee \mathbf{RA1} \circ \mathbf{RA3}(P)$$

Proof.

$$
\begin{aligned}
&\mathbf{RA1} \circ \mathbf{RA3}(P) && \{\text{Definition of } \mathbf{RA3}\}\\
&= \mathbf{RA1}(\mathbb{I}_{\mathcal{R}ac} \lhd s.wait \rhd P) && \\
& && \{\text{Definition of conditional and predicate calculus}\}\\
&= \mathbf{RA1}((s.wait \wedge \mathbb{I}_{\mathcal{R}ac}) \vee (\mathbb{I}_{\mathcal{R}ac} \lhd s.wait \rhd P)) && \{\text{Theorem 1.2.1}\}\\
&= \mathbf{RA1}(s.wait \wedge \mathbb{I}_{\mathcal{R}ac}) \vee \mathbf{RA1}(\mathbb{I}_{\mathcal{R}ac} \lhd s.wait \rhd P) && \{\text{Lemma B.1.11}\}\\
&= (s.wait \wedge \mathbf{RA1}(\mathbb{I}_{\mathcal{R}ac})) \vee \mathbf{RA1}(\mathbb{I}_{\mathcal{R}ac} \lhd s.wait \rhd P) && \{\text{Theorem 1.2.13}\}\\
&= (s.wait \wedge \mathbb{I}_{\mathcal{R}ac}) \vee \mathbf{RA1}(\mathbb{I}_{\mathcal{R}ac} \lhd s.wait \rhd P) && \{\text{Definition of } \mathbf{RA3}\}\\
&= (s.wait \wedge \mathbb{I}_{\mathcal{R}ac}) \vee \mathbf{RA1} \circ \mathbf{RA3}(P) &&
\end{aligned}
$$

□

Lemma B.4.9

$$\mathbf{RA1} \circ \mathbf{RA3}(P) = \mathbb{I}_{\mathcal{R}ac} \lhd s.wait \rhd \mathbf{RA1}(P)$$

Proof.

$$
\begin{aligned}
&\mathbf{RA1} \circ \mathbf{RA3}(P) && \{\text{Definition of } \mathbf{RA3}\}\\
&= \mathbf{RA1}(\mathbb{I}_{\mathcal{R}ac} \lhd s.wait \rhd P) && \{\text{Lemma B.1.10}\}\\
&= \mathbf{RA1}(\mathbb{I}_{\mathcal{R}ac}) \lhd s.wait \rhd \mathbf{RA1}(P) && \{\text{Theorem 1.2.13}\}\\
&= \mathbb{I}_{\mathcal{R}ac} \lhd s.wait \rhd \mathbf{RA1}(P) &&
\end{aligned}
$$

□

Lemma B.4.10

$$P \lhd c \rhd (Q \vee R) = (P \lhd c \rhd Q) \vee (P \lhd c \rhd R)$$

Proof.

$$
\begin{aligned}
&P \lhd c \rhd (Q \vee R) && \{\text{Definition of conditional}\}\\
&= (c \wedge P) \vee (\neg\, c \wedge (Q \vee R)) && \{\text{Predicate calculus}\}\\
&= (c \wedge P) \vee (\neg\, c \wedge Q) \vee (\neg\, c \wedge R) && \{\text{Predicate calculus}\}\\
&= (c \wedge P) \vee (\neg\, c \wedge Q) \vee (c \wedge P) \vee (\neg\, c \wedge R) && \\
& && \{\text{Definition of conditional}\}\\
&= (P \lhd c \rhd Q) \vee (P \lhd c \rhd R) &&
\end{aligned}
$$

□

Lemma B.4.11

$$\mathbf{RA}(P)^o_f = \mathbf{RA2} \circ \mathbf{RA1}(P^o_f)$$

Proof.

$$\begin{aligned}
&\mathbf{RA}(P)^o_f && \{\text{Definition of } \mathbf{RA}\}\\
&= (\mathbf{RA3} \circ \mathbf{RA2} \circ \mathbf{RA1}(P))^o_f && \{\text{Lemma B.3.1}\}\\
&= (\mathbf{RA2} \circ \mathbf{RA1}(P))^o_f && \{\text{Lemma B.2.9}\}\\
&= \mathbf{RA2} \circ (\mathbf{RA1}(P))^o_f && \{\text{Lemma B.1.15}\}\\
&= \mathbf{RA2} \circ \mathbf{RA1}(P^o_f)
\end{aligned}$$

□

Lemma B.4.12

$$\begin{aligned}
&(\mathbf{RA} \circ \mathbf{A}(\neg\ P^f_f \vdash P^t_f))^o_w\\
&=\\
&\mathbf{RA2} \circ \mathbf{RA1} \circ \mathbf{PBMH}(\neg\ ok \lor P^f_f \lor (P^t_f \land o))
\end{aligned}$$

Proof.

$$\begin{aligned}
&(\mathbf{RA} \circ \mathbf{A}(\neg\ P^f_f \vdash P^t_f))^o_w && \{\text{Theorem 1.2.27}\}\\
&= (\mathbf{RA} \circ \mathbf{PBMH}(\neg\ P^f_f \vdash P^t_f))^o_w && \{\text{Lemma B.4.11}\}\\
&= \mathbf{RA2} \circ \mathbf{RA1} \circ (\mathbf{PBMH}(\neg\ P^f_f \vdash P^t_f))^o_w && \{\text{Lemma E.5.1}\}\\
&= \mathbf{RA2} \circ \mathbf{RA1} \circ \mathbf{PBMH}(\neg\ P^f_f \vdash P^t_f)^o_w && \{\text{Definition of design}\}\\
&= \mathbf{RA2} \circ \mathbf{RA1} \circ \mathbf{PBMH}((ok \land \neg\ P^f_f) \Rightarrow (P^t_f \land ok'))^o_w && \{\text{Substitution}\}\\
&= \mathbf{RA2} \circ \mathbf{RA1} \circ \mathbf{PBMH}((ok \land \neg\ (P^f_f)^o_w) \Rightarrow ((P^t_f)^o_w \land o))\\
&\qquad && \{\text{Substitution: } ok' \text{ not free and property of } \oplus\}\\
&= \mathbf{RA2} \circ \mathbf{RA1} \circ \mathbf{PBMH}((ok \land \neg\ P^f_f) \Rightarrow (P^t_f \land o)) && \{\text{Predicate calculus}\}\\
&= \mathbf{RA2} \circ \mathbf{RA1} \circ \mathbf{PBMH}(\neg\ ok \lor P^f_f \lor (P^t_f \land o))
\end{aligned}$$

□

Lemma B.4.13

$$(\mathbf{RA} \circ \mathbf{A}(\neg\ P_f^f \vdash P_f^t))_f^f$$
$$=$$
$$\mathbf{RA2} \circ \mathbf{RA1} \circ \mathbf{PBMH}(\neg\ ok \vee P_f^f)$$

Proof.

$$\begin{aligned}
&(\mathbf{RA} \circ \mathbf{A}(\neg\ P_f^f \vdash P_f^t))_f^f && \{\text{Lemma B.4.12}\}\\
&= \mathbf{RA2} \circ \mathbf{RA1} \circ \mathbf{PBMH}(\neg\ ok \vee P_f^f \vee (P_f^t \wedge \mathit{false})) \\
& && \{\text{Predicate calculus}\}\\
&= \mathbf{RA2} \circ \mathbf{RA1} \circ \mathbf{PBMH}(\neg\ ok \vee P_f^f)
\end{aligned}$$

□

Lemma B.4.14

$$(\mathbf{RA} \circ \mathbf{A}(\neg\ P_f^f \vdash P_f^t))_f^f$$
$$=$$
$$\mathbf{RA2} \circ \mathbf{RA1} \circ \mathbf{PBMH}(\neg\ ok \vee P_f^f \vee P_f^t)$$

Proof.

$$\begin{aligned}
&(\mathbf{RA} \circ \mathbf{A}(\neg\ P_f^f \vdash P_f^t))_f^f && \{\text{Lemma B.4.12}\}\\
&= \mathbf{RA2} \circ \mathbf{RA1} \circ \mathbf{PBMH}(\neg\ ok \vee P_f^f \vee (P_f^t \wedge \mathit{true})) \\
& && \{\text{Predicate calculus}\}\\
&= \mathbf{RA2} \circ \mathbf{RA1} \circ \mathbf{PBMH}(\neg\ ok \vee P_f^f \vee P_f^t)
\end{aligned}$$

□

Theorem B.4.1

$$\mathbf{RA} \circ \mathbf{A}(\neg\ (\mathbf{RA} \circ \mathbf{A}(\neg\ P_f^f \vdash P_f^t))_f^f \vdash (\mathbf{RA} \circ \mathbf{A}(\neg\ P_f^f \vdash P_f^t))_f^t)$$
$$=$$
$$\mathbf{RA} \circ \mathbf{A}(\neg\ P_f^f \vdash P_f^t)$$

Proof.

$$\mathbf{RA} \circ \mathbf{A}(\neg\, (\mathbf{RA} \circ \mathbf{A}(\neg\, P_f^f \vdash P_f^t))_f^f \vdash (\mathbf{RA} \circ \mathbf{A}(\neg\, P_f^f \vdash P_f^t))_f^t)$$

$$= \mathbf{RA} \circ \mathbf{A} \left(\begin{array}{l} \neg\, \mathbf{RA2} \circ \mathbf{RA1} \circ \mathbf{PBMH}(\neg\, ok \vee P_f^f) \\ \vdash \\ \mathbf{RA2} \circ \mathbf{RA1} \circ \mathbf{PBMH}(\neg\, ok \vee P_f^f \vee P_f^t) \end{array} \right)$$

{Lemmas B.4.13 and B.4.14}

$$= \mathbf{RA} \circ \mathbf{A} \left(\begin{array}{l} (ok \wedge \neg\, \mathbf{RA2} \circ \mathbf{RA1} \circ \mathbf{PBMH}(\neg\, ok \vee P_f^f)) \\ \Rightarrow \\ (\mathbf{RA2} \circ \mathbf{RA1} \circ \mathbf{PBMH}(\neg\, ok \vee P_f^f \vee P_f^t) \wedge ok') \end{array} \right)$$

{Definition of design}

$$= \mathbf{RA} \circ \mathbf{PBMH} \left(\begin{array}{l} (ok \wedge \neg\, \mathbf{RA2} \circ \mathbf{RA1} \circ \mathbf{PBMH}(\neg\, ok \vee P_f^f)) \\ \Rightarrow \\ (\mathbf{RA2} \circ \mathbf{RA1} \circ \mathbf{PBMH}(\neg\, ok \vee P_f^f \vee P_f^t) \wedge ok') \end{array} \right)$$

{Theorem 1.2.27}

$$= \mathbf{RA} \circ \mathbf{PBMH} \left(\begin{array}{l} (\neg\, ok \vee \mathbf{RA2} \circ \mathbf{RA1} \circ \mathbf{PBMH}(\neg\, ok \vee P_f^f)) \\ \vee \\ (\mathbf{RA2} \circ \mathbf{RA1} \circ \mathbf{PBMH}(\neg\, ok \vee P_f^f \vee P_f^t) \wedge ok') \end{array} \right)$$

{Predicate calculus}

$$= \mathbf{RA} \circ \mathbf{PBMH} \left(\begin{array}{l} (\neg\, ok \vee \mathbf{RA2} \circ \mathbf{RA1} \circ \mathbf{PBMH}(\neg\, ok \vee P_f^f)) \\ \vee \\ \mathbf{RA2}(\mathbf{RA1} \circ \mathbf{PBMH}(\neg\, ok \vee P_f^f \vee P_f^t) \wedge ok') \end{array} \right)$$

{Lemma B.4.4 and Theorem 1.2.9}

$$= \mathbf{RA} \circ \mathbf{PBMH} \left(\begin{array}{l} (\neg\, ok \vee \mathbf{RA2} \circ \mathbf{RA1} \circ \mathbf{PBMH}(\neg\, ok \vee P_f^f)) \\ \vee \\ \mathbf{RA2} \circ \mathbf{RA1}(\mathbf{PBMH}(\neg\, ok \vee P_f^f \vee P_f^t) \wedge ok') \end{array} \right)$$

{Lemma B.1.11 and Theorem 1.2.2}

$$= \mathbf{RA} \circ \mathbf{PBMH} \left(\begin{array}{l} (\neg\, ok \vee \mathbf{RA2} \circ \mathbf{RA1} \circ \mathbf{PBMH}(\neg\, ok \vee P_f^f)) \\ \vee \\ \mathbf{RA2} \circ \mathbf{RA1} \circ \mathbf{PBMH}((\neg\, ok \vee P_f^f \vee P_f^t) \wedge ok') \end{array} \right)$$

{Lemma E.4.8}

{Theorems 1.2.25 and E.2.2}

$$
\begin{array}{l}
= \left(\begin{array}{l}
\mathbf{RA} \circ \mathbf{PBMH}(\neg\ ok) \\
\vee \\
\mathbf{RA} \circ \mathbf{PBMH} \circ \mathbf{RA2} \circ \mathbf{RA1} \circ \mathbf{PBMH}(\neg\ ok \vee P_f^f) \\
\vee \\
\mathbf{RA} \circ \mathbf{PBMH} \circ \mathbf{RA2} \circ \mathbf{RA1} \circ \mathbf{PBMH}((\neg\ ok \vee P_f^f \vee P_f^t) \wedge ok')
\end{array} \right) \\
\qquad \{\text{Theorems 1.2.5 and 1.2.11}\} \\
= \left(\begin{array}{l}
\mathbf{RA} \circ \mathbf{PBMH}(\neg\ ok) \\
\vee \\
\mathbf{RA} \circ \mathbf{RA2} \circ \mathbf{RA1} \circ \mathbf{PBMH}(\neg\ ok \vee P_f^f) \\
\vee \\
\mathbf{RA} \circ \mathbf{RA2} \circ \mathbf{RA1} \circ \mathbf{PBMH}((\neg\ ok \vee P_f^f \vee P_f^t) \wedge ok')
\end{array} \right) \\
\qquad \{\text{Definition of } \mathbf{RA}\} \\
= \left(\begin{array}{l}
\mathbf{RA} \circ \mathbf{PBMH}(\neg\ ok) \\
\vee \\
\mathbf{RA3} \circ \mathbf{RA2} \circ \mathbf{RA1} \circ \mathbf{RA2} \circ \mathbf{RA1} \circ \mathbf{PBMH}(\neg\ ok \vee P_f^f) \\
\vee \\
\mathbf{RA3} \circ \mathbf{RA2} \circ \mathbf{RA1} \circ \mathbf{RA2} \circ \mathbf{RA1} \circ \mathbf{PBMH}((\neg\ ok \vee P_f^f \vee P_f^t) \wedge ok')
\end{array} \right) \\
\qquad \{\text{Theorem 1.2.12}\} \\
= \left(\begin{array}{l}
\mathbf{RA} \circ \mathbf{PBMH}(\neg\ ok) \\
\vee \\
\mathbf{RA3} \circ \mathbf{RA2} \circ \mathbf{RA2} \circ \mathbf{RA1} \circ \mathbf{RA1} \circ \mathbf{PBMH}(\neg\ ok \vee P_f^f) \\
\vee \\
\mathbf{RA3} \circ \mathbf{RA2} \circ \mathbf{RA2} \circ \mathbf{RA1} \circ \mathbf{RA1} \circ \mathbf{PBMH}((\neg\ ok \vee P_f^f \vee P_f^t) \wedge ok')
\end{array} \right) \\
\qquad \{\text{Theorems 1.2.3 and 1.2.7}\} \\
= \left(\begin{array}{l}
\mathbf{RA} \circ \mathbf{PBMH}(\neg\ ok) \\
\vee \\
\mathbf{RA3} \circ \mathbf{RA2} \circ \mathbf{RA1} \circ \mathbf{PBMH}(\neg\ ok \vee P_f^f) \\
\vee \\
\mathbf{RA3} \circ \mathbf{RA2} \circ \mathbf{RA1} \circ \mathbf{PBMH}((\neg\ ok \vee P_f^f \vee P_f^t) \wedge ok')
\end{array} \right) \\
\qquad \{\text{Definition of } \mathbf{RA}\}
\end{array}
$$

$$
\begin{array}{ll}
= \left(\begin{array}{l} \mathbf{RA} \circ \mathbf{PBMH}(\neg\ ok) \\ \vee \\ \mathbf{RA} \circ \mathbf{PBMH}(\neg\ ok \vee P_f^f) \\ \vee \\ \mathbf{RA} \circ \mathbf{PBMH}((\neg\ ok \vee P_f^f \vee P_f^t) \wedge ok') \end{array} \right) & \\
& \{\text{Theorems 1.2.25 and E.2.2}\} \\
= \mathbf{RA} \circ \mathbf{PBMH} \left(\begin{array}{l} (\neg\ ok) \\ \vee \\ (\neg\ ok \vee P_f^f) \\ \vee \\ ((\neg\ ok \vee P_f^f \vee P_f^t) \wedge ok') \end{array} \right) & \{\text{Predicate calculus}\} \\
= \mathbf{RA} \circ \mathbf{PBMH} \left(\begin{array}{l} \neg\ ok \vee\vee P_f^f \\ \vee \\ (\neg\ ok \wedge ok') \vee (P_f^f \wedge ok') \vee (P_f^t \wedge ok') \end{array} \right) & \\
& \{\text{Predicate calculus: absorption law}\} \\
= \mathbf{RA} \circ \mathbf{PBMH}(\neg\ ok \vee P_f^f \vee (P_f^t \wedge ok')) & \{\text{Predicate calculus}\} \\
= \mathbf{RA} \circ \mathbf{PBMH}((ok \wedge \neg\ P_f^f) \Rightarrow (P_f^t \wedge ok')) & \{\text{Definition of design}\} \\
= \mathbf{RA} \circ \mathbf{PBMH}(\neg\ P_f^f \vdash P_f^t) & \{\text{Theorem 1.2.27}\} \\
= \mathbf{RA} \circ \mathbf{A}(\neg\ P_f^f \vdash P_f^t) &
\end{array}
$$

□

Appendix C

Links

C.1 $ac2p$

C.1.1 Lemmas

Lemma C.1.1 ($ac2p$-alternative-1)

$$
\begin{array}{l}
ac2p(P) \\
\widehat{=} \\
\left(\begin{array}{l}
\exists\, ac', s \bullet P \wedge (\forall\, z \bullet z \in ac' \Rightarrow \bigwedge x : out\alpha_{-ok'} \bullet dash(z).x = x) \\
\wedge \\
(\bigwedge x : in\alpha_{-ok} \bullet s.x = x)
\end{array} \right)
\end{array}
$$

Proof.

$$
\left(\begin{array}{l}
\exists\, ac', s \bullet P \wedge (\forall\, z \bullet z \in ac' \Rightarrow \bigwedge x : out\alpha \bullet dash(z).x = x) \\
\wedge \\
(\bigwedge x : in\alpha \bullet s.x = x)
\end{array} \right)
$$

{Lemma G.2.2}

$$= \exists\, ac' \bullet P[State_{\mathit{II}}(in\alpha)/s] \wedge (\forall\, z \bullet z \in ac' \Rightarrow \bigwedge x : out\alpha \bullet dash(z).x = x)$$

{Property of sets}

$$= \exists\, ac' \bullet P[State_{\mathit{II}}(in\alpha)/s] \wedge (\forall\, z \bullet z \in ac' \Rightarrow z \in \{s \mid \bigwedge x : out\alpha \bullet dash(s).x = x\})$$

{Property of subset inclusion}

$$= \exists\, ac' \bullet P[State_{\mathit{II}}(in\alpha)/s] \wedge ac' \subseteq \{s \mid \bigwedge x : out\alpha \bullet dash(s).x = x\}$$

{Introduce fresh variable}

$$= \exists\, ac_0 \bullet P[State_{\mathit{II}}(in\alpha)/s][ac_0/ac'] \land ac_0 \subseteq \{s \mid \bigwedge x : out\alpha \bullet dash(s).x = x\}$$
{Substitution}

$$= \exists\, ac_0 \bullet P[ac_0/ac'][State_{\mathit{II}}(in\alpha)/s] \land ac_0 \subseteq \{s \mid \bigwedge x : out\alpha \bullet dash(s).x = x\}$$
{Introduce ac' and definition of $;_{\mathcal{A}}$}

$$= (\exists\, ac_0 \bullet P[ac_0/ac'][State_{\mathit{II}}(in\alpha)/s] \land ac_0 \subseteq ac') \;;_{\mathcal{A}} \bigwedge x : out\alpha \bullet dash(s).x = x$$
{Substitution}

$$= (\exists\, ac_0 \bullet P[ac_0/ac'] \land ac_0 \subseteq ac')[State_{\mathit{II}}(in\alpha)/s] \;;_{\mathcal{A}} \bigwedge x : out\alpha \bullet dash(s).x = x$$
{Definition of **PBMH** (Lemma E.1.1)}

$$= \mathbf{PBMH}(P)[State_{\mathit{II}}(in\alpha)/s] \;;_{\mathcal{A}} \bigwedge x : out\alpha \bullet dash(s).x = x$$

□

Lemma C.1.2 ($ac2p$-alternative-2)

$$ac2p(P)$$
$$=$$
$$\exists\, ac' \bullet P[State_{\mathit{II}}(in\alpha_{-ok})/s] \land ac' \subseteq \{z \mid \bigwedge x : out\alpha_{-ok'} \bullet dash(z).x = x\}$$

Lemma C.1.3 *Provided ac' is not free in e.*

$$ac2p(\exists\, y \bullet y \in ac' \land e) = e[State_{\mathit{II}}(in\alpha_{-ok}), undash(State_{\mathit{II}}(out\alpha_{-ok'}))/s, y]$$

Proof.

$ac2p(\exists\, y \bullet y \in ac' \land e)$ {Definition of $ac2p$}

$$= \mathbf{PBMH}(\exists\, y \bullet y \in ac' \land e)[State_{\mathit{II}}(in\alpha_{-ok})/s] \;;_{\mathcal{A}} \bigwedge x : out\alpha_{-ok'} \bullet dash(s).x = x$$
{Assumption: ac' not free in e and Lemma E.4.10}

$$= (\exists\, y \bullet y \in ac' \land e)[State_{\mathit{II}}(in\alpha_{-ok})/s] \;;_{\mathcal{A}} \bigwedge x : out\alpha_{-ok'} \bullet dash(s).x = x$$
{Substitution}

$$= (\exists\, y \bullet y \in ac' \land e[State_{\mathit{II}}(in\alpha_{-ok})/s]) \;;_{\mathcal{A}} \bigwedge x : out\alpha_{-ok'} \bullet dash(s).x = x$$
{Definition of $;_{\mathcal{A}}$ and substitution, ac' not free in e}

$$= \exists\, y \bullet y \in \left\{s \mid \bigwedge x : out\alpha_{-ok'} \bullet dash(s).x = x\right\} \land e[State_{\mathit{II}}(in\alpha_{-ok})/s]$$
{Property of sets}

$$= \exists\, y \bullet \left(\bigwedge x : out\alpha_{-ok'} \bullet dash(y).x = x\right) \wedge e[State_{\mathtt{II}}(in\alpha_{-ok})/s]$$
{Introduce fresh variable}

$$= \exists\, z, y \bullet \left(\bigwedge x : out\alpha_{-ok'} \bullet z.x = x\right) \wedge z = dash(y) \wedge e[State_{\mathtt{II}}(in\alpha_{-ok})/s]$$
{Property of *dash*}

$$= \exists\, z, y \bullet \left(\bigwedge x : out\alpha_{-ok'} \bullet z.x = x\right) \wedge undash(z) = y \wedge e[State_{\mathtt{II}}(in\alpha_{-ok})/s]$$
{Lemma G.2.2 and substitution}

$$= \exists\, y \bullet undash(State_{\mathtt{II}}(out\alpha_{-ok'})) = y \wedge e[State_{\mathtt{II}}(in\alpha_{-ok})/s]$$
{One-point rule}

$$= e[State_{\mathtt{II}}(in\alpha_{-ok})/s][undash(State_{\mathtt{II}}(out\alpha_{-ok'}))/y]$$ {Substitution}

$$= e[State_{\mathtt{II}}(in\alpha_{-ok}), undash(State_{\mathtt{II}}(out\alpha_{-ok'}))/s, y]$$

□

Lemma C.1.4 *Provided P is* **A2***-healthy.*

$$ac2p(P) = \left(\begin{array}{l} \exists\, ac_0 \bullet P[\{s \mid \{s\} = ac_0\}/ac'][State_{\mathtt{II}}(in\alpha_{-ok})/s] \\ \wedge \\ ac_0 \subseteq \{s \mid \bigwedge x : out\alpha_{-ok'} \bullet dash(s).x = x\} \end{array}\right)$$

Proof.

$ac2p(P)$ {Definition of $ac2p$}

$$= \mathbf{PBMH}(P)[State_{\mathtt{II}}(in\alpha_{-ok})/s] \;;_{\mathcal{A}} \bigwedge x : out\alpha_{-ok'} \bullet dash(s).x = x$$
{Assumption: P is **A2**-healthy}

$$= \left(\begin{array}{l} \mathbf{PBMH}(\mathbf{PBMH}(P \;;_{\mathcal{A}} \{s\} = ac'))[State_{\mathtt{II}}(in\alpha_{-ok})/s] \\ \;;_{\mathcal{A}} \\ \bigwedge x : out\alpha_{-ok'} \bullet dash(s).x = x \end{array}\right)$$
{**PBMH**-idempotent}

$$= \left(\begin{array}{l} \mathbf{PBMH}(P \;;_{\mathcal{A}} \{s\} = ac')[State_{\mathtt{II}}(in\alpha_{-ok})/s] \\ \;;_{\mathcal{A}} \\ \bigwedge x : out\alpha_{-ok'} \bullet dash(s).x = x \end{array}\right)$$
{Definition of $;_{\mathcal{A}}$ and substitution}

$$= \left(\begin{array}{l} \mathbf{PBMH}(P[\{s \mid \{s\} = ac'\}/ac'])[State_{\mathtt{II}}(in\alpha_{-ok})/s] \\ \;;_{\mathcal{A}} \\ \bigwedge x : out\alpha_{-ok'} \bullet dash(s).x = x \end{array}\right)$$
{Definition of **PBMH** (Lemma E.1.1)}

$$= \left(\begin{array}{l} (\exists\, ac_0 \bullet (P[\{s \mid \{s\} = ac'\}/ac'])[ac_0/ac'] \wedge ac_0 \subseteq ac')[State_{\mathit{II}}(in\alpha_{-ok})/s] \\ ;_{\mathcal{A}} \\ \bigwedge x : out\alpha_{-ok'} \bullet dash(s).x = x \end{array} \right)$$

{Substitution}

$$= \left(\begin{array}{l} (\exists\, ac_0 \bullet P[\{s \mid \{s\} = ac_0\}/ac'][State_{\mathit{II}}(in\alpha_{-ok})/s] \wedge ac_0 \subseteq ac') \\ ;_{\mathcal{A}} \\ \bigwedge x : out\alpha_{-ok'} \bullet dash(s).x = x \end{array} \right)$$

{Definition of $;_{\mathcal{A}}$ and substitution}

$$= \left(\begin{array}{l} \exists\, ac_0 \bullet P[\{s \mid \{s\} = ac_0\}/ac'][State_{\mathit{II}}(in\alpha_{-ok})/s] \\ \wedge \\ ac_0 \subseteq \{s \mid \bigwedge x : out\alpha_{-ok'} \bullet dash(s).x = x\} \end{array} \right)$$

□

Lemma C.1.5

$$\exists\, out\alpha \bullet \neg\, ac2p(P)[\mathbf{s}/in\alpha] \Rightarrow \neg\, P[\emptyset/ac']$$

Proof.

$\exists\, out\alpha \bullet \neg\, ac2p(P)[\mathbf{s}/in\alpha]$ {Definition of $ac2p$}

$$= \exists\, out\alpha \bullet \neg \left(\begin{array}{l} \mathbf{PBMH}(P)[State_{\mathit{II}}(in\alpha)/s] \\ ;_{\mathcal{A}} \\ \bigwedge x : out\alpha \bullet dash(s).x = x \end{array} \right)[\mathbf{s}/in\alpha]$$

{Definition of **PBMH** (Lemma E.1.1)}

$$= \exists\, out\alpha \bullet \neg \left(\begin{array}{l} (\exists\, ac_0 \bullet P[ac_0/ac'] \wedge ac_0 \subseteq ac')[State_{\mathit{II}}(in\alpha)/s] \\ ;_{\mathcal{A}} \\ \bigwedge x : out\alpha \bullet dash(s).x = x \end{array} \right)[\mathbf{s}/in\alpha]$$

{Substitution}

$$= \exists\, out\alpha \bullet \neg \left(\begin{array}{l} (\exists\, ac_0 \bullet P[ac_0/ac'][State_{\mathit{II}}(in\alpha)/s] \wedge ac_0 \subseteq ac') \\ ;_{\mathcal{A}} \\ \bigwedge x : out\alpha \bullet dash(s).x = x \end{array} \right)[\mathbf{s}/in\alpha]$$

{Definition of $;_{\mathcal{A}}$ and substitution}

$$= \exists\, out\alpha \bullet \neg \left(\begin{array}{l} \exists\, ac_0 \bullet P[ac_0/ac'][State_{\mathit{II}}(in\alpha)/s] \\ \wedge \\ ac_0 \subseteq \{s \mid \bigwedge x : out\alpha \bullet dash(s).x = x\} \end{array} \right)[\mathbf{s}/in\alpha]$$

{Substitution}

$$= \exists\, out\alpha \bullet \neg \left(\begin{array}{l} \exists\, ac_0 \bullet P[ac_0/ac'][State_{\mathit{II}}(in\alpha)/s][\mathbf{s}/in\alpha] \\ \wedge \\ ac_0 \subseteq \{s \mid \bigwedge x : out\alpha \bullet dash(s).x = x\} \end{array} \right)$$

{Lemma G.2.4}

$$= \exists\, out\alpha \bullet \neg\, (\exists\, ac_0 \bullet P[ac_0/ac'] \wedge ac_0 \subseteq \{s \mid \bigwedge x : out\alpha \bullet dash(s).x = x\})$$

{Predicate calculus}

$$= \exists\, out\alpha \bullet (\forall\, ac_0 \bullet \neg\, P[ac_0/ac'] \vee \neg\, (ac_0 \subseteq \{s \mid \bigwedge x : out\alpha \bullet dash(s).x = x\}))$$

{Predicate calculus}

$$\Rightarrow \forall\, ac_0 \bullet (\exists\, out\alpha \bullet \neg\, P[ac_0/ac'] \vee \neg\, (ac_0 \subseteq \{s \mid \bigwedge x : out\alpha \bullet dash(s).x = x\}))$$

{Predicate calculus: $out\alpha$ not free in P}

$$= \forall\, ac_0 \bullet (\neg\, P[ac_0/ac'] \vee \exists\, out\alpha \bullet \neg\, (ac_0 \subseteq \{s \mid \bigwedge x : out\alpha \bullet dash(s).x = x\}))$$

{Definition of subset inclusion}

$$= \forall\, ac_0 \bullet \left(\begin{array}{l} \neg\, P[ac_0/ac'] \\ \vee \\ \exists\, out\alpha \bullet \neg\, (\forall\, y \bullet y \in ac_0 \Rightarrow (\bigwedge x : out\alpha \bullet dash(y).x = x)) \end{array} \right)$$

{Predicate calculus}

$$= \forall\, ac_0 \bullet \left(\begin{array}{l} \neg\, P[ac_0/ac'] \\ \vee \\ \exists\, out\alpha \bullet (\exists\, y \bullet y \in ac_0 \wedge \neg\, (\bigwedge x : out\alpha \bullet dash(y).x = x)) \end{array} \right)$$

{Predicate calculus}

$$\Rightarrow \forall\, ac_0 \bullet (\neg\, P[ac_0/ac'] \vee (\exists\, out\alpha \bullet \exists\, y \bullet y \in ac_0))$$ {Predicate calculus}

$$= \neg\ \exists\, ac_0 \bullet P[ac_0/ac'] \wedge ac_0 = \emptyset$$ {One-point rule}

$$= \neg\, P[\emptyset/ac']$$

□

The following lemma can be restated in a few different ways. Namely it can also imply:

$$\exists\, out\alpha \bullet (\neg\, P[State_{\mathit{II}}(in\alpha)/s]\ ;_{\mathcal{A}} \bigwedge x : out\alpha \bullet dash(s).x = x)$$

Lemma C.1.6 *Provided P is* **PBMH***-healthy*

$$\exists\, out\alpha \bullet \neg\, ac2p(P) \Rightarrow \exists\, out\alpha \bullet ac2p(\neg\, P)$$

Proof.

$$
\begin{array}{ll}
\exists\, out\alpha \bullet \neg\, ac2p(P) & \{\text{Definition of } ac2p\} \\
= \exists\, out\alpha \bullet \neg\, (\mathbf{PBMH}(P)[State_{\mathit{II}}(in\alpha)/s] \ ;_{\mathcal{A}} \bigwedge x : out\alpha \bullet dash(s).x = x) & \\
& \{\text{Assumption: } P \text{ is } \mathbf{PBMH}\text{-healthy}\} \\
= \exists\, out\alpha \bullet \neg\, (P[State_{\mathit{II}}(in\alpha)/s] \ ;_{\mathcal{A}} \bigwedge x : out\alpha \bullet dash(s).x = x) & \\
& \{\text{Property of } ;_{\mathcal{A}}\} \\
= \exists\, out\alpha \bullet ((\neg\, P[State_{\mathit{II}}(in\alpha)/s]) \ ;_{\mathcal{A}} \bigwedge x : out\alpha \bullet dash(s).x = x) & \\
& \{\text{Predicate calculus (Lemma E.2.1)}\} \\
= \exists\, out\alpha \bullet \left(\begin{array}{l} (\neg\, P \wedge \mathbf{PBMH}(\neg\, P))[State_{\mathit{II}}(in\alpha)/s] \\ ;_{\mathcal{A}} \\ \bigwedge x : out\alpha \bullet dash(s).x = x \end{array} \right) & \\
& \{\text{Property of substitution}\} \\
= \exists\, out\alpha \bullet \left(\begin{array}{l} (\neg\, P[State_{\mathit{II}}(in\alpha)/s] \wedge \mathbf{PBMH}(\neg\, P)[State_{\mathit{II}}(in\alpha)/s]) \\ ;_{\mathcal{A}} \\ \bigwedge x : out\alpha \bullet dash(s).x = x \end{array} \right) & \\
& \{\text{Distributivity of } ;_{\mathcal{A}} \text{ (Lemma F.1.5) and substitution}\} \\
= \exists\, out\alpha \bullet \left(\begin{array}{l} (\neg\, P[State_{\mathit{II}}(in\alpha)/s] \ ;_{\mathcal{A}} \bigwedge x : out\alpha \bullet dash(s).x = x) \\ \wedge \\ (\mathbf{PBMH}(\neg\, P)[State_{\mathit{II}}(in\alpha)/s] \ ;_{\mathcal{A}} \bigwedge x : out\alpha \bullet dash(s).x = x) \end{array} \right) & \\
& \{\text{Predicate calculus}\} \\
\Rightarrow \exists\, out\alpha \bullet \mathbf{PBMH}(\neg\, P)[State_{\mathit{II}}(in\alpha)/s] \ ;_{\mathcal{A}} \bigwedge x : out\alpha \bullet dash(s).x = x & \\
& \{\text{Definition of } ac2p\} \\
= \exists\, out\alpha \bullet ac2p(\neg\, P) &
\end{array}
$$

□

Lemma C.1.7 *Provided none of the variables in $out\alpha$ are free in P*

$$\exists\, out\alpha \bullet ac2p(P) \Rightarrow \exists\, ac' \bullet P[State_{\mathit{II}}(in\alpha)/s]$$

Proof.

$$
\begin{array}{ll}
\exists\, out\alpha \bullet ac2p(P) & \{\text{Definition of } ac2p\}
\end{array}
$$

$$= \exists\, out\alpha \bullet \left(\begin{array}{l} \mathbf{PBMH}(P)[State_{\mathit{II}}(in\alpha)/s] \\ ;_{\mathcal{A}} \\ \bigwedge x : out\alpha \bullet dash(s).x = x \end{array} \right)$$

{Definition of **PBMH** (Lemma E.1.1)}

$$= \exists\, out\alpha \bullet \left(\begin{array}{l} (\exists\, ac_0 \bullet P[ac_0/ac'] \wedge ac_0 \subseteq ac')[State_{\mathit{II}}(in\alpha)/s] \\ ;_{\mathcal{A}} \\ \bigwedge x : out\alpha \bullet dash(s).x = x \end{array} \right)$$

{Substitution}

$$= \exists\, out\alpha \bullet \left(\begin{array}{l} (\exists\, ac_0 \bullet P[ac_0/ac'][State_{\mathit{II}}(in\alpha)/s] \wedge ac_0 \subseteq ac') \\ ;_{\mathcal{A}} \\ \bigwedge x : out\alpha \bullet dash(s).x = x \end{array} \right)$$

{Definition of $;_{\mathcal{A}}$ and substitution}

$$= \exists\, out\alpha \bullet \left(\begin{array}{l} \exists\, ac_0 \bullet P[ac_0/ac'][State_{\mathit{II}}(in\alpha)/s] \wedge \\ ac_0 \subseteq \{s \mid \bigwedge x : out\alpha \bullet dash(s).x = x\} \end{array} \right)$$

{Property of sets}

$$= \exists\, out\alpha \bullet \left(\begin{array}{l} \exists\, ac_0 \bullet P[ac_0/ac'][State_{\mathit{II}}(in\alpha)/s] \wedge \\ \forall\, z \bullet z \in ac_0 \Rightarrow (\bigwedge x : out\alpha \bullet dash(z).x = x) \end{array} \right)$$

{Predicate calculus: $out\alpha$ not free in P}

$$= \left(\begin{array}{l} \exists\, ac_0 \bullet P[ac_0/ac'][State_{\mathit{II}}(in\alpha)/s] \\ \wedge \\ \exists\, out\alpha \bullet \forall\, z \bullet z \in ac_0 \Rightarrow (\bigwedge x : out\alpha \bullet dash(z).x = x) \end{array} \right)$$

{Predicate calculus}

$$\Rightarrow \left(\begin{array}{l} \exists\, ac_0 \bullet P[ac_0/ac'][State_{\mathit{II}}(in\alpha)/s] \\ \wedge \\ \forall\, z \bullet \exists\, out\alpha \bullet (z \in ac_0 \Rightarrow (\bigwedge x : out\alpha \bullet dash(z).x = x)) \end{array} \right)$$

{Predicate calculus}

$$= \left(\begin{array}{l} \exists\, ac_0 \bullet P[ac_0/ac'][State_{\mathit{II}}(in\alpha)/s] \\ \wedge \\ \forall\, z \bullet z \in ac_0 \Rightarrow (\exists\, out\alpha \bullet (\bigwedge x : out\alpha \bullet dash(z).x = x)) \end{array} \right)$$

{One-point rule}

$$= \left(\begin{array}{l} \exists\, ac_0 \bullet P[ac_0/ac'][State_{\mathit{II}}(in\alpha)/s] \\ \wedge \\ \forall\, z \bullet z \in ac_0 \Rightarrow true \end{array} \right)$$

{Predicate calculus}

$$= \exists\, ac_0 \bullet P[ac_0/ac'][State_{\mathit{II}}(in\alpha)/s]$$

{Predicate calculus}

$= \exists\, ac' \bullet P[State_{\mathtt{II}}(in\alpha)/s]$

□

Lemma C.1.8 *Provided that s and ac' are not free in P*

$$ac2p(P \wedge Q) = P \wedge ac2p(Q)$$

Proof.

$ac2p(P \wedge Q)$ {Definition of $ac2p$}

$= \exists\, ac' \bullet (P \wedge Q)[State_{\mathtt{II}}(in\alpha)/s] \wedge ac' \subseteq \{z \mid \bigwedge x : out\alpha \bullet dash(z).x = x\}$ {Subtitution: s not free in P}

$= \exists\, ac' \bullet P \wedge Q[State_{\mathtt{II}}(in\alpha)/s] \wedge ac' \subseteq \{z \mid \bigwedge x : out\alpha \bullet dash(z).x = x\}$ {Predicate calculus: ac' not free in P}

$= P \wedge \exists\, ac' \bullet Q[State_{\mathtt{II}}(in\alpha)/s] \wedge ac' \subseteq \{z \mid \bigwedge x : out\alpha \bullet dash(z).x = x\}$ {Definition of $ac2p$}

$= P \wedge ac2p(Q)$

□

Lemma C.1.9 *Provided that s and ac' are not free in P*

$$ac2p(P) = P$$

Proof.

$ac2p(P)$ {Definition of $ac2p$}

$= \exists\, ac' \bullet P[State_{\mathtt{II}}(in\alpha)/s] \wedge ac' \subseteq \{z \mid \bigwedge x : out\alpha \bullet dash(z).x = x\}$ {Subtitution: s not free in P}

$= \exists\, ac' \bullet P \wedge ac' \subseteq \{z \mid \bigwedge x : out\alpha \bullet dash(z).x = x\}$ {Predicate calculus: ac' not free in P}

$= P \wedge \exists\, ac' \bullet ac' \subseteq \{z \mid \bigwedge x : out\alpha \bullet dash(z).x = x\}$ {Property of subset inclusion}

$= P$

□

Lemma C.1.10 *Provided P is a design.*

$$ac2p(P) = (\neg\ ac2p(P^f) \vdash ac2p(P^t))$$

Proof.

$$\begin{array}{ll}
ac2p(P) & \{\text{Assumption: } P \text{ is a design}\} \\
= ac2p(\neg\ P^f \vdash P^t) & \{\text{Definition of design}\} \\
= ac2p((ok \wedge \neg\ P^f) \Rightarrow (P^t \wedge ok')) & \\
\multicolumn{2}{r}{\{\text{Predicate calculus and distributivity of } ac2p \text{ (Theorem 1.4.1)}\}} \\
= ac2p(\neg\ ok) \vee ac2p(P^f) \vee ac2p(P^t \wedge ok') & \{\text{Lemmas C.1.8 and C.1.9}\} \\
= \neg\ ok \vee ac2p(P^f) \vee (ac2p(P^t) \wedge ok') & \{\text{Predicate calculus}\} \\
= (ok \wedge \neg\ ac2p(P^f)) \Rightarrow (ac2p(P^t) \wedge ok') & \{\text{Definition of design}\} \\
= (\neg\ ac2p(P^f) \vdash ac2p(P^t)) &
\end{array}$$

□

Lemma C.1.11

$$ac2p(P) \Rightarrow \exists\, ac' \bullet P[State_{\mathtt{II}}(in\alpha)/s]$$

Proof.

$$\begin{array}{ll}
ac2p(P) & \{\text{Definition of } ac2p\} \\
= \exists\, ac' \bullet P[State_{\mathtt{II}}(in\alpha)/s] \wedge ac' \subseteq \{z \mid \bigwedge x : out\alpha \bullet dash(z).x = x\} & \\
\multicolumn{2}{r}{\{\text{Predicate calculus}\}} \\
\Rightarrow (\exists\, ac' \bullet P[State_{\mathtt{II}}(in\alpha)/s]) \wedge (\exists\, ac' \bullet ac' \subseteq \{z \mid \bigwedge x : out\alpha \bullet dash(z).x = x\}) & \\
\multicolumn{2}{r}{\{\text{Property of sets}\}} \\
= \exists\, ac' \bullet P[State_{\mathtt{II}}(in\alpha)/s] &
\end{array}$$

□

Lemma C.1.12 *Provided ac' is not free in P*

$$ac2p(P) = P[State_{II}(in\alpha)/s]$$

Proof.

$$
\begin{aligned}
& ac2p(P) && \{\text{Definition of } ac2p\} \\
&= \mathbf{PBMH}(P)[State_{II}(in\alpha)/s] \ ;_{\mathcal{A}} \bigwedge x : out\alpha \bullet dash(s).x = x \\
& && \{\text{Assumption: } ac' \text{ not free in } P \text{ and property of } \mathbf{PBMH}\} \\
&= P[State_{II}(in\alpha)/s] \ ;_{\mathcal{A}} \bigwedge x : out\alpha \bullet dash(s).x = x \\
& && \{\text{Definition of } ;_{\mathcal{A}} \text{ and substitution}\} \\
&= P[State_{II}(in\alpha)/s][\{s \mid \bigwedge x : out\alpha \bullet dash(s).x = x\}/ac'] \\
& && \{\text{Assumption: } ac' \text{ not free in } P\} \\
&= P[State_{II}(in\alpha)/s]
\end{aligned}
$$

□

Lemma C.1.13

$$ac2p(P)^o_w = ac2p(P^o_w)$$

Proof.

$$
\begin{aligned}
& ac2p(P)^o_w && \{\text{Substitution abbreviation}\} \\
&= ac2p(P)[o, w/ok', wait] && \{\text{Definition of } ac2p \text{ (Lemma C.1.2)}\} \\
&= (\exists\, ac' \bullet P[State_{\mathtt{II}}(in\alpha)/s] \wedge ac' \subseteq \{s \mid \bigwedge x' : out\alpha \bullet s.x = x'\})[o, w/ok', wait] \\
& && \{\text{Substitution: } ok' \text{ and } wait \text{ not in } out\alpha\} \\
&= \exists\, ac' \bullet P[State_{\mathtt{II}}(in\alpha)/s][o, w/ok', wait] \wedge ac' \subseteq \{s \mid \bigwedge x' : out\alpha \bullet s.x = x'\} \\
& && \{\text{Substitution: } ok' \text{ not in } in\alpha\} \\
&= \exists\, ac' \bullet P[o/ok'][State_{\mathtt{II}}(in\alpha)/s][w/wait] \wedge ac' \subseteq \{s \mid \bigwedge x' : out\alpha \bullet s.x = x'\} \\
& && \{\text{Lemma G.2.5}\} \\
&= \exists\, ac' \bullet P[o/ok'][s \oplus \{wait \mapsto w\}/s][State_{\mathtt{II}}(in\alpha)/s] \wedge ac' \subseteq \{s \mid \bigwedge x' : out\alpha \bullet s.x = x'\} \\
& && \{\text{Substitution abbreviation}\} \\
&= \exists\, ac' \bullet P^o_w[State_{\mathtt{II}}(in\alpha)/s] \wedge ac' \subseteq \{s \mid \bigwedge x' : out\alpha \bullet s.x = x'\} \\
& && \{\text{Definition of } ac2p \text{ (Lemma C.1.2)}\} \\
&= ac2p(P^o_w)
\end{aligned}
$$

□

Lemma C.1.14 *Provided ac' is not free in c.*

$$ac2p(P \lhd c \rhd Q) = ac2p(P) \lhd c[State_{\mathit{II}}(in\alpha_{-ok})/s] \rhd ac2p(Q)$$

Proof.

$$\begin{array}{ll}
ac2p(P \lhd c \rhd Q) & \{\text{Definition of conditional}\} \\
= ac2p((c \wedge P) \vee (\neg\ c \wedge Q)) & \{\text{Distributivity of } ac2p \text{ (Theorem 1.4.2)}\} \\
= ac2p(c \wedge P) \vee ac2p(\neg\ c \wedge Q) & \\
& \{\text{Assumption: } ac' \text{ not free in } c \text{ and Lemma C.1.15}\} \\
= (c[State_{\mathit{II}}(in\alpha_{-ok})/s] \wedge ac2p(P)) \vee (\neg\ c[State_{\mathit{II}}(in\alpha_{-ok})/s] \wedge ac2p(Q)) & \\
& \{\text{Property of substitution}\} \\
= (c[State_{\mathit{II}}(in\alpha_{-ok})/s] \wedge ac2p(P)) \vee (\neg\ (c[State_{\mathit{II}}(in\alpha_{-ok})/s]) \wedge ac2p(Q)) & \\
& \{\text{Definition of conditional}\} \\
= ac2p(P) \lhd c[State_{\mathit{II}}(in\alpha_{-ok})/s] \rhd ac2p(Q) &
\end{array}$$

□

Lemma C.1.15 *Provided ac' is not free in P.*

$$ac2p(P \wedge Q) = P[State_{\mathit{II}}(in\alpha_{-ok})/s] \wedge ac2p(Q)$$

Proof.

$$\begin{array}{ll}
ac2p(P \wedge Q) & \{\text{Definition of } ac2p\} \\
= \mathbf{PBMH}(P \wedge Q)[State_{\mathit{II}}(in\alpha_{-ok})/s]\ ;_{\mathcal{A}} \bigwedge x : out\alpha_{-ok'} \bullet dash(s).x = x & \\
& \{\text{Assumption: } ac' \text{ not free in } P \text{ and Lemma E.4.8}\} \\
= (P \wedge \mathbf{PBMH}(Q))[State_{\mathit{II}}(in\alpha_{-ok})/s]\ ;_{\mathcal{A}} \bigwedge x : out\alpha_{-ok'} \bullet dash(s).x = x & \\
& \{\text{Property of substitution}\} \\
= \left(\begin{array}{l} (P[State_{\mathit{II}}(in\alpha_{-ok})/s] \wedge \mathbf{PBMH}(Q)[State_{\mathit{II}}(in\alpha_{-ok})/s]) \\ ;_{\mathcal{A}} \\ \bigwedge x : out\alpha_{-ok'} \bullet dash(s).x = x \end{array} \right) & \\
& \{\text{Distributivity of } ;_{\mathcal{A}} \text{ (Lemma F.1.5)}\} \\
= \left(\begin{array}{l} (P[State_{\mathit{II}}(in\alpha_{-ok})/s]\ ;_{\mathcal{A}} \bigwedge x : out\alpha_{-ok'} \bullet dash(s).x = x) \\ \wedge \\ (\mathbf{PBMH}(Q)[State_{\mathit{II}}(in\alpha_{-ok})/s]\ ;_{\mathcal{A}} \bigwedge x : out\alpha_{-ok'} \bullet dash(s).x = x) \end{array} \right) & \\
& \{\text{Assumption: } ac' \text{ not free in } P \text{ and Lemma F.1.1}\}
\end{array}$$

$$= \left(\begin{array}{l} P[State_{\mathtt{II}}(in\alpha_{-ok})/s] \\ \wedge \\ (\mathbf{PBMH}(Q)[State_{\mathtt{II}}(in\alpha_{-ok})/s] \ ;_{\mathcal{A}} \bigwedge x : out\alpha_{-ok'} \bullet dash(s).x = x) \end{array} \right)$$

{Definition of $ac2p$}

$$= P[State_{\mathtt{II}}(in\alpha_{-ok})/s] \wedge ac2p(Q)$$

□

Lemma C.1.16 *Provided* $in\alpha_{-ok} = \{x_0, \ldots, x_i\}$ *and* $in\alpha'_{-ok} = out\alpha_{-ok'}$.

$$ac2p(s \in ac') = x_0 = x'_0 \wedge \ldots \wedge x_i = x'_i$$

Proof.

$ac2p(s \in ac')$ {Definition of $ac2p$}

$= \mathbf{PBMH}(s \in ac')[State_{\mathtt{II}}(in\alpha_{-ok})/s] \ ;_{\mathcal{A}} \bigwedge x : out\alpha_{-ok'} \bullet dash(s).x = x$

{Lemma E.4.3}

$= (s \in ac')[State_{\mathtt{II}}(in\alpha_{-ok})/s] \ ;_{\mathcal{A}} \bigwedge x : out\alpha_{-ok'} \bullet dash(s).x = x$

{Substitution}

$= State_{\mathtt{II}}(in\alpha_{-ok}) \in ac' \ ;_{\mathcal{A}} \bigwedge x : out\alpha_{-ok'} \bullet dash(s).x = x$

{Definition of $;_{\mathcal{A}}$ and sustitution}

$= State_{\mathtt{II}}(in\alpha_{-ok}) \in \{s \mid \bigwedge x : out\alpha_{-ok'} \bullet dash(s).x = x\}$

{Property of sets}

$= \bigwedge x : out\alpha_{-ok'} \bullet dash(State_{\mathtt{II}}(in\alpha_{-ok})).x = x$ {Definition of $State_{\mathtt{II}}$}

$= \bigwedge x : out\alpha_{-ok'} \bullet dash(\{x_0 \mapsto x_0, \ldots, x_i \mapsto x_i\}).x = x$

{Application of $dash$}

$= \bigwedge x : out\alpha_{-ok'} \bullet \{x'_0 \mapsto x_0, \ldots, x'_i \mapsto x_i\}.x = x$

{Expansion of conjunction}

$= \{x'_0 \mapsto x_0, \ldots, x'_i \mapsto x_i\}.x'_0 = x'_0 \wedge \ldots \wedge \{x'_0 \mapsto x_0, \ldots, x'_i \mapsto x_i\}.x'_i = x'_i$

{Value of record component}

$= x_0 = x'_0 \wedge \ldots \wedge x_i = x'_i$

□

C.2 $p2ac$

C.2.1 Lemmas

Lemma C.2.1

$$\mathbf{PBMH} \circ p2ac(P) = p2ac(P)$$

Proof.

$$\begin{array}{ll}
\mathbf{PBMH} \circ p2ac(P) & \{\text{Definition of } \mathbf{PBMH} \text{ (Lemma E.1.1)}\} \\
= \exists\, ac_0 \bullet p2ac(P)[ac_0/ac'] \wedge ac_0 \subseteq ac' & \{\text{Definition of } p2ac\} \\
= \exists\, ac_0 \bullet (\exists\, z \bullet P[\mathbf{s}, \mathbf{z}'/in\alpha_{-ok}, out\alpha_{-ok'}] \wedge z \in ac')[ac_0/ac'] \wedge ac_0 \subseteq ac' & \{\text{Substitution}\} \\
= \exists\, ac_0 \bullet (\exists\, z \bullet P[\mathbf{s}, \mathbf{z}'/in\alpha_{-ok}, out\alpha_{-ok'}] \wedge z \in ac_0) \wedge ac_0 \subseteq ac' & \{\text{Property of sets}\} \\
= \exists\, z \bullet P[\mathbf{s}, \mathbf{z}'/in\alpha_{-ok}, out\alpha_{-ok'}] \wedge z \in ac' & \{\text{Definition of } p2ac\} \\
= p2ac(P) &
\end{array}$$

□

Lemma C.2.2

$$p2ac(true) = ac' \neq \emptyset$$

Proof.

$$\begin{array}{ll}
p2ac(true) & \{\text{Definition of } p2ac\} \\
= \exists\, z \bullet true[\mathbf{s}, \mathbf{z}/in\alpha_{-ok}, out\alpha_{-ok'}] \wedge undash(z) \in ac' & \{\text{Substitution}\} \\
= \exists\, z \bullet true \wedge undash(z) \in ac' & \{\text{Predicate calculus}\} \\
= \exists\, z \bullet undash(z) \in ac' & \{\text{Property of sets}\} \\
= ac' \neq \emptyset &
\end{array}$$

□

Lemma C.2.3

$$p2ac(false) = false$$

Proof.

$$
\begin{aligned}
& p2ac(false) && \{\text{Definition of } p2ac\} \\
& = \exists\, z \bullet false[\mathbf{s}, \mathbf{z}/in\alpha_{-ok}, out\alpha_{-ok'}] \wedge undash(z) \in ac' \\
& && \{\text{Predicate calculus}\} \\
& = false
\end{aligned}
$$

□

Lemma C.2.4

$$\exists\, out\alpha_{-ok'} \bullet P = \exists\, z \bullet P[\mathbf{z}/out\alpha_{-ok'}]$$

Proof.

$$
\begin{aligned}
& \exists\, out\alpha_{-ok'} \bullet P && \{\text{Introduce fresh state variable } z\} \\
& = \exists\, z, out\alpha \bullet P \wedge z.x_0 = x_0 \wedge \ldots \wedge z.x_n = x.n \\
& && \{\text{One-point rule for each } x_i \text{ in } out\alpha_{-ok'}\} \\
& = \exists\, z \bullet P[z.x_0, \ldots, z.x_n/x_0, \ldots, x_n] && \{\text{Definition of state substitution}\} \\
& = \exists\, z \bullet P[\mathbf{z}/out\alpha_{-ok'}]
\end{aligned}
$$

□

Lemma C.2.5 *Provided that no variable in* $in\alpha_{-ok} \cup out\alpha_{-ok'}$ *is free in* P

$$p2ac(P \wedge Q) = P \wedge p2ac(Q)$$

Proof.

$$
\begin{aligned}
& p2ac(P \wedge Q) && \{\text{Definition of } ac2p\} \\
& = \exists\, z \bullet (P \wedge Q)[\mathbf{s}, \mathbf{z}/in\alpha_{-ok}, out\alpha_{-ok'}] \wedge undash(z) \in ac' \\
& && \{\text{Substitution: assumption}\} \\
& = \exists\, z \bullet (P \wedge Q[\mathbf{s}, \mathbf{z}/in\alpha_{-ok}, out\alpha_{-ok'}]) \wedge undash(z) \in ac' \\
& && \{\text{Predicate calculus}\} \\
& = P \wedge (\exists\, z \bullet Q[\mathbf{s}, \mathbf{z}/in\alpha_{-ok}, out\alpha_{-ok'}] \wedge undash(z) \in ac') \\
& && \{\text{Definition of } ac2p\} \\
& = P \wedge ac2p(Q)
\end{aligned}
$$

□

Lemma C.2.6 *Provided that no variable in $in\alpha_{-ok} \cup out\alpha_{-ok'}$ is free in P*

$$p2ac(P) = P \wedge ac' \neq \emptyset$$

Proof.

$$\begin{array}{ll}
p2ac(P) & \{\text{Definition of } ac2p\} \\
= \exists\, z \bullet P[\mathbf{s}, \mathbf{z}/in\alpha_{-ok}, out\alpha_{-ok'}] \wedge undash(z) \in ac' & \\
& \{\text{Substitution: variables of } out\alpha_{-ok'} \cup in\alpha_{-ok} \text{ not free in } P\} \\
= \exists\, z \bullet P \wedge undash(z) \in ac' & \{\text{Predicate calculus: } z \text{ not free in } P\} \\
= P \wedge \exists\, z \bullet undash(z) \in ac' & \{\text{Property of sets}\} \\
= P \wedge ac' \neq \emptyset &
\end{array}$$

□

Lemma C.2.7 *Provided that no dashed variable in $out\alpha_{-ok}$ is free in P.*

$$p2ac(P) = P[\mathbf{s}/in\alpha] \wedge ac' \neq \emptyset$$

Proof.

$$\begin{array}{ll}
p2ac(P) & \{\text{Definition of } p2ac\} \\
= \exists\, z \bullet P[\mathbf{s}, \mathbf{z}/in\alpha_{-ok}, out\alpha_{-ok'}] \wedge undash(z) \in ac' & \\
& \{\text{Substitution: variables of } out\alpha \text{ not free in } P\} \\
= \exists\, z \bullet P[\mathbf{s}/in\alpha_{-ok}] \wedge undash(z) \in ac' & \\
& \{\text{Predicate calculus: } z \text{ not free in } P\} \\
= P[\mathbf{s}/in\alpha_{-ok}] \wedge \exists\, z \bullet undash(z) \in ac' & \{\text{Property of sets}\} \\
= P[\mathbf{s}/in\alpha_{-ok}] \wedge ac' \neq \emptyset &
\end{array}$$

□

Lemma C.2.8

$$p2ac \circ ac2p(P) = \exists\, ac_0, y \bullet P[ac_0/ac'] \wedge ac_0 \subseteq \{y\} \wedge y \in ac'$$

Proof.

$$\begin{array}{ll}
p2ac \circ ac2p(P) & \{\text{Definition of } p2ac\}
\end{array}$$

$$= \exists\, z \bullet ac2p(P)[\mathbf{s}, \mathbf{z}/in\alpha_{-ok}, out\alpha_{-ok'}] \land undash(z) \in ac'$$
{Definition of $ac2p$ (Lemma C.1.2)}

$$= \left(\begin{array}{l} \exists\, z \bullet \left(\begin{array}{l} \exists\, ac' \bullet P[State_{\mathtt{II}}(in\alpha_{-ok})/s] \\ \land \\ ac' \subseteq \{z \mid \bigwedge x : out\alpha_{-ok'} \bullet dash(z).x = x\} \end{array} \right) [\mathbf{s}, \mathbf{z}/in\alpha_{-ok}, out\alpha_{-ok'}] \\ \land\ undash(z) \in ac' \end{array} \right)$$
{Variable renaming}

$$= \left(\begin{array}{l} \exists\, z \bullet \left(\begin{array}{l} \exists\, ac' \bullet P[State_{\mathtt{II}}(in\alpha)/s] \\ \land \\ ac' \subseteq \{y \mid \bigwedge x : out\alpha_{-ok'} \bullet dash(y).x = x\} \end{array} \right) [\mathbf{s}, \mathbf{z}/in\alpha_{-ok}, out\alpha_{-ok'}] \\ \land\ undash(z) \in ac' \end{array} \right)$$
{Substitution}

$$= \exists\, z \bullet \left(\begin{array}{l} \exists\, ac' \bullet P[State_{\mathtt{II}}(in\alpha_{-ok})/s][\mathbf{s}/in\alpha_{-ok}] \\ \land \\ ac' \subseteq \{y \mid \bigwedge x : out\alpha_{-ok'} \bullet dash(y).x = z.x\} \end{array} \right) \land undash(z) \in ac'$$
{Lemma G.2.4}

$$= \exists\, z \bullet \left(\begin{array}{l} \exists\, ac' \bullet P \\ \land \\ ac' \subseteq \{y \mid \bigwedge x : out\alpha_{-ok'} \bullet dash(y).x = z.x\} \end{array} \right) \land undash(z) \in ac'$$
{Equality of records}

$$= \exists\, z \bullet (\exists\, ac' \bullet P \land ac' \subseteq \{y \mid dash(y) = z\}) \land undash(z) \in ac'$$
{Property of $dash$ and $undash$}

$$= \exists\, z \bullet (\exists\, ac' \bullet P \land ac' \subseteq \{y \mid y = undash(z)\}) \land undash(z) \in ac'$$
{Property of sets}

$$= \exists\, z \bullet (\exists\, ac' \bullet P \land ac' \subseteq \{undash(z)\}) \land undash(z) \in ac'$$
{Introduce fresh variable y}

$$= \exists\, y, z \bullet (\exists\, ac' \bullet P \land ac' \subseteq \{undash(z)\}) \land undash(z) \in ac' \land undash(z) = y$$
{One-point rule: z not free in P}

$$= \exists\, y \bullet (\exists\, ac' \bullet P \land ac' \subseteq \{y\}) \land y \in ac'$$ {Variable renaming}

$$= \exists\, y \bullet (\exists\, ac_0 \bullet P[ac_0/ac'] \land ac_0 \subseteq \{y\}) \land y \in ac'$$ {Predicate calculus}

$$= \exists\, ac_0, y \bullet P[ac_0/ac'] \land ac_0 \subseteq \{y\} \land y \in ac'$$

□

Lemma C.2.9

$$p2ac(P)^o_w = p2ac(P^o_w)$$

Proof.

$$
\begin{array}{ll}
p2ac(P)^o_w & \{\text{Substitution abbreviation}\} \\
= p2ac(P)[o, s \oplus \{wait \mapsto w\}/ok', s] & \{\text{Definition of } p2ac\} \\
= (\exists\, z \bullet P[\mathbf{s}, \mathbf{z}'/in\alpha, out\alpha] \land z \in ac')[o, s \oplus \{wait \mapsto w\}/ok', s] & \\
& \{\text{Substitution: } ok' \text{ not in } out\alpha\} \\
= (\exists\, z \bullet P[o/ok'][\mathbf{s}, \mathbf{z}'/in\alpha, out\alpha] \land z \in ac')[s \oplus \{wait \mapsto w\}/s] & \\
& \{wait \text{ is not } w \text{ and Lemma G.1.4}\} \\
= \exists\, z \bullet P[o, w/ok', wait][\mathbf{s}, \mathbf{z}'/in\alpha, out\alpha] \land z \in ac' & \\
& \{\text{Substitution abbreviation}\} \\
= \exists\, z \bullet P^o_w[\mathbf{s}, \mathbf{z}'/in\alpha, out\alpha] \land z \in ac' & \{\text{Definition of } p2ac\} \\
= p2ac(P^o_w) &
\end{array}
$$

□

Appendix D

Theory of designs

D.1 Healthiness conditions

H2A

Definition 24

$$\mathbf{H2A}(P) \mathrel{\widehat{=}} \neg\, P^f \Rightarrow (P^t \wedge ok')$$

Law D.1.1 (**H2A** $\Leftrightarrow$ **H2**) *The definition of* **H2A** *implies that the fixpoints are the same as those of* **H2**.

Proof for implication. The following proof is based on [1].

$$\begin{aligned}
& P && \{\text{Introduce fresh variable and substitution}\} \\
&= \exists\, ok_0 \bullet P \wedge ok' = ok_0 && \{\text{Case-split on } ok_0\} \\
&= (\neg\, ok' \wedge P^f) \vee (ok' \wedge P^t) && \{\text{Assumption: P is } \mathbf{H2}\text{-healthy}\} \\
&= (\neg\, ok' \wedge P^f \wedge P^t) \vee (ok' \wedge P^t) && \{\text{Propositional calculus}\} \\
&= (((\neg\, ok' \wedge P^f) \vee ok') \wedge P^t) && \{\text{Propositional calculus}\} \\
&= ((P^f \vee ok') \wedge P^t) && \{\text{Propositional calculus}\} \\
&= (P^f \wedge P^t) \vee (ok' \wedge P^t) && \{\text{Assumption: P is } \mathbf{H2}\text{-healthy}\} \\
&= P^f \vee (ok' \wedge P^t) && \{\text{Propositional calculus}\} \\
&= \neg\, P^f \Rightarrow (P^t \wedge ok')
\end{aligned}$$

□

Proof for reverse implication.

$$
\begin{aligned}
&[(\mathbf{H2A}(P))^f \Rightarrow (\mathbf{H2A}(P))^t] && \{\text{Definition of } \mathbf{H2A}\}\\
&= [(\neg\ P^f \Rightarrow (P^t \wedge ok'))^f \Rightarrow (\neg\ P^f \Rightarrow (P^t \wedge ok'))^t] && \{\text{Substitution}\}\\
&= [(P^f \Rightarrow (\neg\ P^f \Rightarrow P^t)] && \{\text{Propositional calculus}\}\\
&= [\neg\ P^f \vee P^f \vee P^t] && \{\text{Propositional calculus}\}\\
&= \mathit{true}
\end{aligned}
$$

□

D.2 Lemmas

Law D.2.1 (design-true-ok') *Provided $ok \wedge P$ and ok' is not free in P.*

$$(P \vdash Q)^t = Q$$

Proof. As stated and proved in [2] (Lemma 4.2). □

Law D.2.2 (design-false-ok') *Provided ok' is not free in P.*

$$ok \wedge \neg\ (P \vdash Q)^f = ok \wedge P$$

Proof. As stated and proved in [2] (Lemma 4.3). □

Law D.2.3 (design-exists-ok')

$$\exists\, ok' \bullet (P \vdash Q) = (ok \wedge P) \Rightarrow Q$$

Proof.

$$
\begin{aligned}
&\exists\, ok' \bullet (P \vdash Q) && \{\text{Definition of design}\}\\
&= \exists\, ok' \bullet (ok \wedge P) \Rightarrow (Q \wedge ok') && \{\text{Case-split on } ok'\}\\
&= ((ok \wedge P) \Rightarrow Q) \vee \neg\ (ok \wedge P) && \{\text{Propositional calculus}\}\\
&= (ok \wedge P) \Rightarrow Q
\end{aligned}
$$

□

Law D.2.4 (design-⊔)

$$(\neg\ P^f \vdash P^t) \sqcup (\neg\ Q^f \vdash Q^t)$$
$$=$$
$$(\neg\ P^f \vee \neg\ Q^f \vdash (\neg\ P^f \Rightarrow P^t) \wedge (\neg\ Q^f \Rightarrow Q^t))$$

Proof.

$$\begin{aligned}
&(\neg\ P^f \vdash P^t) \sqcup (\neg\ Q^f \vdash Q^t) && \{\text{Definition of design}\}\\
&= ((ok \wedge \neg\ P^f) \Rightarrow (P^t \wedge ok')) \sqcup ((ok \wedge \neg\ Q^f) \Rightarrow (Q^t \wedge ok')) \\
& && \{\text{Definition of } \sqcup\}\\
&= ((ok \wedge \neg\ P^f) \Rightarrow (P^t \wedge ok')) \wedge ((ok \wedge \neg\ Q^f) \Rightarrow (Q^t \wedge ok')) \\
& && \{\text{Propositional calculus}\}\\
&= ok \Rightarrow ((P^t \wedge ok') \vee P^f) \wedge ((Q^t \wedge ok') \vee Q^f) && \{\text{Propositional calculus}\}\\
&= ok \Rightarrow (P^t \vee P^f) \wedge (ok' \vee P^f) \wedge (Q^t \vee Q^f) \wedge (ok' \vee Q^f) \\
& && \{\text{Propositional calculus}\}\\
&= ok \Rightarrow (P^t \vee P^f) \wedge (Q^t \vee Q^f) \wedge (ok' \vee (P^f \wedge Q^f)) \\
& && \{\text{Propositional calculus: absorption law}\}\\
&= ok \Rightarrow ((P^f \wedge Q^f) \vee P^t \vee P^f) \wedge ((P^f \wedge Q^f) \vee Q^t \vee Q^f) \wedge (ok' \vee (P^f \wedge Q^f)) \\
& && \{\text{Propositional calculus}\}\\
&= ok \Rightarrow (P^f \wedge Q^f) \vee ((P^t \vee P^f) \wedge (Q^t \vee Q^f) \wedge ok') \\
& && \{\text{Propositional calculus}\}\\
&= (ok \wedge \neg\ (P^f \wedge Q^f)) \Rightarrow ((\neg\ P^f \Rightarrow P^t) \wedge (\neg\ Q^f \Rightarrow Q^t) \wedge ok') \\
& && \{\text{Definition of design}\}\\
&= (\neg\ P^f \vee \neg\ Q^f \vdash (\neg\ P^f \Rightarrow P^t) \wedge (\neg\ Q^f \Rightarrow Q^t))
\end{aligned}$$

□

Law D.2.5 (design-exists-ok'-⊔) *Provided P and Q are designs.*

$$\exists\, ok' \bullet (P \wedge Q) = (\exists\, ok' \bullet P) \wedge (\exists\, ok' \bullet Q)$$

Proof.

$$\begin{aligned}
&(\exists\, ok' \bullet P) \wedge (\exists\, ok' \bullet Q) && \{\text{Assumption: } P \text{ and } Q \text{ are designs}\}\\
&= (\exists\, ok' \bullet (\neg\ P^f \vdash P^t)) \wedge (\exists\, ok' \bullet (\neg\ Q^f \vdash Q^t)) && \{\text{Law D.2.3}\}
\end{aligned}$$

$$
\begin{array}{ll}
= ((ok \wedge \neg\, P^f) \Rightarrow P^t) \wedge ((ok \wedge \neg\, Q^f) \Rightarrow Q^t) & \{\text{Propositional calculus}\} \\
= (ok \Rightarrow (P^t \vee P^f)) \wedge (ok \Rightarrow (Q^t \vee Q^f)) & \{\text{Propositional calculus}\} \\
= ok \Rightarrow ((P^t \vee P^f) \wedge (Q^t \vee Q^f)) & \\
\qquad \{\text{Propositional calculus: absorption law}\} & \\
= ok \Rightarrow (((P^f \wedge Q^f) \vee P^t \vee P^f) \wedge ((P^f \wedge Q^f) \vee Q^t \vee Q^f)) & \\
\qquad \{\text{Propositional calculus}\} & \\
= ok \Rightarrow ((P^f \wedge Q^f) \vee ((P^t \vee P^f) \wedge (Q^t \vee Q^f))) & \{\text{Propositional calculus}\} \\
= (ok \wedge \neg\, (P^f \wedge Q^f)) \Rightarrow ((\neg\, P^f \Rightarrow P^t) \wedge (\neg\, Q^f \Rightarrow Q^t)) & \{\text{Law D.2.3}\} \\
= \exists\, ok' \bullet (\neg\, (P^f \wedge Q^f) \vdash (\neg\, P^f \Rightarrow P^t) \wedge (\neg\, Q^f \Rightarrow Q^t)) & \\
\qquad \{\text{Conjunction of designs}\} & \\
= \exists\, ok' \bullet (\neg\, P^f \vdash P^t) \wedge (\neg\, Q^f \vdash Q^t) & \\
\qquad \{\text{Assumption: } P \text{ and } Q \text{ are designs}\} & \\
= \exists\, ok' \bullet (P \wedge Q) &
\end{array}
$$

□

Law D.2.6

$$
\begin{array}{l}
(\neg\, P^f \vdash P^t) \sqcup (\neg\, Q^f \vdash Q^t) \\
= \\
(\neg\, P^f \vee \neg\, Q^f \vdash (P^f \wedge Q^t) \vee (P^t \wedge Q^f) \vee (P^t \wedge Q^t))
\end{array}
$$

Proof.

$$
\begin{array}{ll}
(\neg\, P^f \vdash P^t) \sqcup (\neg\, Q^f \vdash Q^t) & \{\text{Conjunction of designs}\} \\
= (\neg\, P^f \vee \neg\, Q^f \vdash (\neg\, P^f \Rightarrow P^t) \wedge (\neg\, Q^f \Rightarrow Q^t)) & \\
\qquad \{\text{Propositional calculus}\} & \\
= (\neg\, P^f \vee \neg\, Q^f \vdash (P^f \vee P^t) \wedge (Q^f \vee Q^t)) & \{\text{Predicate calculus}\} \\
= (\neg\, (P^f \wedge Q^f) \vdash (P^f \wedge Q^f) \vee (P^f \wedge Q^t) \vee (P^t \wedge Q^f) \vee (P^t \wedge Q^t)) & \\
\qquad \{\text{Definition of design}\} & \\
= \left(\begin{array}{l} (ok \wedge \neg\, (P^f \wedge Q^f)) \\ \Rightarrow \\ (((P^f \wedge Q^f) \vee (P^f \wedge Q^t) \vee (P^t \wedge Q^f) \vee (P^t \wedge Q^t)) \wedge ok') \end{array} \right) & \\
\qquad \{\text{Predicate calculus}\} &
\end{array}
$$

$$= \left(\begin{array}{l} (ok \wedge \neg\, (P^f \wedge Q^f) \wedge (\neg\, (P^f \wedge Q^f) \vee \neg\, ok')) \\ \Rightarrow \\ (((P^f \wedge Q^t) \vee (P^t \wedge Q^f) \vee (P^t \wedge Q^t)) \wedge ok') \end{array} \right)$$

{Predicate calculus: absorption law}

$$= (ok \wedge \neg\, (P^f \wedge Q^f)) \Rightarrow (((P^f \wedge Q^t) \vee (P^t \wedge Q^f) \vee (P^t \wedge Q^t)) \wedge ok')$$

{Definition of design}

$$= (\neg\, (P^f \wedge Q^f) \vdash (P^f \wedge Q^t) \vee (P^t \wedge Q^f) \vee (P^t \wedge Q^t))$$

{Predicate calculus}

$$= (\neg\, P^f \vee \neg\, Q^f \vdash (P^f \wedge Q^t) \vee (P^t \wedge Q^f) \vee (P^t \wedge Q^t))$$

□

Appendix E

PBMH

E.1 Definition

Definition 25

$$\mathbf{PBMH}(P) \mathrel{\widehat{=}} P \ ; \ ac \subseteq ac' \land v' = v$$

Lemma E.1.1 (**PBMH**-alternative-1)

$$\mathbf{PBMH}(P) = \exists\, ac_0 \bullet P[ac_0/ac'] \land ac_0 \subseteq ac'$$

Proof.

$$\begin{array}{ll}
\mathbf{PBMH}(P) & \{\text{Definition of } \mathbf{PBMH}\} \\
= P \ ; \ ac \subseteq ac' \land v' = v & \{\text{Definition of sequential composition}\} \\
= \exists\, ac_0, v_0 \bullet P[ac_0, v_0/ac', v'] \land ac_0 \subseteq ac' \land v' = v_0 & \{\text{One-point rule}\} \\
= \exists\, ac_0 \bullet P[ac_0/ac'] \land ac_0 \subseteq ac' &
\end{array}$$

□

E.2 Properties

Theorem E.2.1 (**PBMH**-idempotent)

$$\mathbf{PBMH} \circ \mathbf{PBMH}(P) = \mathbf{PBMH}(P)$$

Proof.

$$
\begin{array}{ll}
& \mathbf{PBMH} \circ \mathbf{PBMH}(P) \qquad \{\text{Definition of } \mathbf{PBMH}\} \\
= & \mathbf{PBMH}(P \ ; \ ac \subseteq ac' \wedge v' = v) \qquad \{\text{Definition of } \mathbf{PBMH}\} \\
= & ((P \ ; \ ac \subseteq ac' \wedge v' = v) \ ; \ ac \subseteq ac' \wedge v' = v) \\
& \qquad \{\text{Associativity of sequential composition}\} \\
= & (P \ ; \ (ac \subseteq ac' \wedge v' = v \ ; \ ac \subseteq ac' \wedge v' = v)) \\
& \qquad \{\text{Definition of sequential composition}\} \\
= & (P \ ; \ (\exists \, ac_0 \bullet ac \subseteq ac_0 \wedge ac_0 \subseteq ac')) \qquad \{\text{Transitivity of subset inclusion}\} \\
= & (P \ ; \ ac \subseteq ac') \qquad \{\text{Definition of sequential composition}\} \\
= & (P \ ; \ ac \subseteq ac' \wedge v' = v) \qquad \{\text{Definition of } \mathbf{PBMH}\} \\
= & \mathbf{PBMH}(P)
\end{array}
$$

□

Theorem E.2.2

$$\mathbf{PBMH}(P \vee Q) = \mathbf{PBMH}(P) \vee \mathbf{PBMH}(Q)$$

Proof.

$$
\begin{array}{ll}
& \mathbf{PBMH}(P \vee Q) \qquad \{\text{Definition of } \mathbf{PBMH} \text{ (Lemma E.1.1)}\} \\
= & \exists \, ac_0 \bullet (P \vee Q)[ac_0/ac'] \wedge ac_0 \subseteq ac' \qquad \{\text{Property of substition}\} \\
= & \exists \, ac_0 \bullet (P[ac_0/ac'] \vee Q[ac_0/ac']) \wedge ac_0 \subseteq ac' \qquad \{\text{Predicate calculus}\} \\
= & \exists \, ac_0 \bullet (P[ac_0/ac'] \wedge ac_0 \subseteq ac') \vee (Q[ac_0/ac'] \wedge ac_0 \subseteq ac') \\
& \qquad \{\text{Predicate calculus}\} \\
= & \left(\begin{array}{l} (\exists \, ac_0 \bullet P[ac_0/ac'] \wedge ac_0 \subseteq ac') \\ \vee \\ (\exists \, ac_0 \bullet Q[ac_0/ac'] \wedge ac_0 \subseteq ac') \end{array} \right) \\
& \qquad \{\text{Definition of } \mathbf{PBMH} \text{ (Lemma E.1.1)}\} \\
= & \mathbf{PBMH}(P) \vee \mathbf{PBMH}(Q)
\end{array}
$$

□

Lemma E.2.1

$$P \Rightarrow \mathbf{PBMH}(P)$$

Proof.

$$
\begin{array}{ll}
P & \{\text{Predicate calculus}\} \\
= \exists\, ac_0 \bullet P[ac_0/ac'] \wedge ac_0 = ac' & \{\text{Property of sets}\} \\
\Rightarrow \exists\, ac_0 \bullet P[ac_0/ac'] \wedge ac_0 \subseteq ac' & \{\text{Definition of } \mathbf{PBMH} \text{ (Lemma E.1.1)}\} \\
= \mathbf{PBMH}(P) &
\end{array}
$$

□

E.3 Closure properties

Theorem E.3.1 *Provided P and Q are* **PBMH***-healthy.*

$$\mathbf{PBMH}(P \wedge Q) = P \wedge Q$$

Proof.

$$
\begin{array}{ll}
\mathbf{PBMH}(P \wedge Q) & \{\text{Assumption: } P \text{ and } Q \text{ are } \mathbf{PBMH}\text{-healthy}\} \\
= \mathbf{PBMH}(\mathbf{PBMH}(P) \wedge \mathbf{PBMH}(Q)) & \\
& \{\text{Definition of } \mathbf{PBMH} \text{ (Lemma E.1.1)}\} \\
= \exists\, ac_0 \bullet (\mathbf{PBMH}(P) \wedge \mathbf{PBMH}(Q))[ac_0/ac'] \wedge ac_0 \subseteq ac' & \\
& \{\text{Definition of } \mathbf{PBMH} \text{ (Lemma E.1.1)}\} \\
= \exists\, ac_0 \bullet \left(\begin{array}{l} (\exists\, ac_0 \bullet P[ac_0/ac'] \wedge ac_0 \subseteq ac') \\ \wedge \\ (\exists\, ac_0 \bullet Q[ac_0/ac'] \wedge ac_0 \subseteq ac') \end{array} \right) [ac_0/ac'] \wedge ac_0 \subseteq ac' & \\
& \{\text{Variable renaming}\} \\
= \exists\, ac_0 \bullet \left(\begin{array}{l} (\exists\, ac_1 \bullet P[ac_1/ac'] \wedge ac_1 \subseteq ac') \\ \wedge \\ (\exists\, ac_2 \bullet Q[ac_1/ac'] \wedge ac_2 \subseteq ac') \end{array} \right) [ac_0/ac'] \wedge ac_0 \subseteq ac' & \\
& \{\text{Substitution}\} \\
= \exists\, ac_0 \bullet \left(\begin{array}{l} (\exists\, ac_1 \bullet P[ac_1/ac'] \wedge ac_1 \subseteq ac_0) \\ \wedge \\ (\exists\, ac_2 \bullet Q[ac_2/ac'] \wedge ac_2 \subseteq ac_0) \end{array} \right) \wedge ac_0 \subseteq ac' & \\
& \{\text{Predicate calculus}\} \\
= \left(\begin{array}{l} (\exists\, ac_1 \bullet P[ac_1/ac'] \wedge ac_1 \subseteq ac') \\ \wedge \\ (\exists\, ac_2 \bullet Q[ac_2/ac'] \wedge ac_2 \subseteq ac') \end{array} \right) & \\
& \{\text{Definition of } \mathbf{PBMH} \text{ (Lemma E.1.1)}\}
\end{array}
$$

$$= \mathbf{PBMH}(P) \wedge \mathbf{PBMH}(Q)$$
$$\{\text{Assumption: } P \text{ and } Q \text{ are } \mathbf{PBMH}\text{-healthy}\}$$
$$= P \wedge Q$$

□

Lemma E.3.1 (**PBMH**-distribute-conjunction) *Provided P and Q satisfy* **PBMH**.

$$\mathbf{PBMH}(P \wedge Q) = \mathbf{PBMH}(P) \wedge \mathbf{PBMH}(Q)$$

Proof.

$$\mathbf{PBMH}(P \wedge Q)$$
$$\{\text{Assumption: } P \text{ and } Q \text{ are } \mathbf{PBMH}\text{-healthy and Theorem E.3.1}\}$$
$$= \mathbf{PBMH}(P) \wedge \mathbf{PBMH}(Q)$$

□

Lemma E.3.2

$$\mathbf{PBMH}(P \wedge Q) \Rightarrow \mathbf{PBMH}(P) \wedge \mathbf{PBMH}(Q)$$

Proof.

$$\mathbf{PBMH}(P \wedge Q) \qquad \{\text{Definition of } \mathbf{PBMH} \text{ (Lemma E.1.1)}\}$$
$$= \exists\, ac_0 \bullet (P \wedge Q)[ac_0/ac'] \wedge ac_0 \subseteq ac' \qquad \{\text{Substitution}\}$$
$$= \exists\, ac_0 \bullet P[ac_0/ac'] \wedge Q[ac_0/ac'] \wedge ac_0 \subseteq ac' \qquad \{\text{Predicate calculus}\}$$
$$\Rightarrow \left(\begin{array}{l} (\exists\, ac_0 \bullet P[ac_0/ac'] \wedge ac_0 \subseteq ac') \\ \wedge \\ (\exists\, ac_0 \bullet Q[ac_0/ac'] \wedge ac_0 \subseteq ac') \end{array} \right)$$
$$\{\text{Definition of } \mathbf{PBMH} \text{ (Lemma E.1.1)}\}$$
$$= \mathbf{PBMH}(P) \wedge \mathbf{PBMH}(Q)$$

□

Theorem E.3.2 (**PBMH**-disjunction-closure) *Provided P and Q satisfy* **PBMH**.

$$\mathbf{PBMH}(P \vee Q) = P \vee Q$$

Proof.

$$\begin{aligned}
&\mathbf{PBMH}(P \vee Q) && \{\text{Theorem E.2.2}\}\\
&= \mathbf{PBMH}(P) \vee \mathbf{PBMH}(Q) && \{\text{Assumption: } P \text{ and } Q \text{ satisfy } \mathbf{PBMH}\}\\
&= P \vee Q
\end{aligned}$$

□

E.4 Lemmas

Lemma E.4.1

$$\mathbf{PBMH}(\mathit{true}) = \mathit{true}$$

Proof.

$$\begin{aligned}
&\mathbf{PBMH}(\mathit{true}) && \{\text{Definition of } \mathbf{PBMH} \text{ (Lemma E.1.1)}\}\\
&= \exists\, ac_0 \bullet \mathit{true}[ac_0/ac'] \wedge ac_0 \subseteq ac' \\
& && \{\text{Property of substitution and predicate calculus}\}\\
&= \mathit{true}
\end{aligned}$$

□

Lemma E.4.2

$$\mathbf{PBMH}(\mathit{false}) = \mathit{false}$$

Proof.

$$\begin{aligned}
&\mathbf{PBMH}(\mathit{false}) && \{\text{Definition of } \mathbf{PBMH} \text{ (Lemma E.1.1)}\}\\
&= \exists\, ac_0 \bullet \mathit{false}[ac_0/ac'] \wedge ac_0 \subseteq ac' \\
& && \{\text{Substitution and predicate calculus}\}\\
&= \mathit{false}
\end{aligned}$$

□

Lemma E.4.3

$$\mathbf{PBMH}(s \in ac') = s \in ac'$$

Proof.

$$
\begin{aligned}
&\mathbf{PBMH}(s \in ac') && \{\text{Definition of } \mathbf{PBMH} \text{ (Lemma E.1.1)}\} \\
&= \exists\, ac_0 \bullet (s \in ac')[ac_0/ac'] \land ac_0 \subseteq ac' && \{\text{Substitution}\} \\
&= \exists\, ac_0 \bullet s \in ac_0 \land ac_0 \subseteq ac' && \{\text{Property of sets}\} \\
&= s \in ac'
\end{aligned}
$$

□

Lemma E.4.4

$$\mathbf{PBMH}(ac' \neq \emptyset) = ac' \neq \emptyset$$

Proof.

$$
\begin{aligned}
&\mathbf{PBMH}(ac' \neq \emptyset) && \{\text{Definition of } \mathbf{PBMH} \text{ (Lemma E.1.1)}\} \\
&= \exists\, ac_0 \bullet ac_0 \neq \emptyset \land ac_0 \subseteq ac' && \{\text{Property of sets (Lemma H.1.12)}\} \\
&= ac' \neq \emptyset
\end{aligned}
$$

□

Lemma E.4.5 *Provided ac' is not free in P.*

$$\mathbf{PBMH}(P) = P$$

Proof.

$$
\begin{aligned}
&\mathbf{PBMH}(P) && \{\text{Definition of } \mathbf{PBMH} \text{ (Lemma E.1.1)}\} \\
&= \exists\, ac_0 \bullet P[ac_0/ac'] \land ac_0 \subseteq ac' \\
& && \{\text{Assumption: } ac' \text{ not free in } P \text{ and predicate calculus}\} \\
&= P \land \exists\, ac_0 \bullet ac_0 \subseteq ac' && \{\text{Case-analysis on } ac_0\} \\
&= P
\end{aligned}
$$

□

Lemma E.4.6 *Provided c is a condition.*

$$\mathbf{PBMH}(c) = c$$

Proof.

$$
\begin{aligned}
&\mathbf{PBMH}(c) && \{\text{Definition of } \mathbf{PBMH} \text{ (Lemma E.1.1)}\} \\
&= \exists\, ac_0 \bullet c[ac_0/ac'] \land ac_0 \subseteq ac' \\
& && \{\text{Assumption: } c \text{ is a condition, hence } ac' \text{ is not free}\} \\
&= \exists\, ac_0 \bullet c \land ac_0 \subseteq ac' && \{\text{Predicate calculus}\} \\
&= c
\end{aligned}
$$

□

Lemma E.4.7

$$\mathbf{PBMH}(x \in ac') = x \in ac'$$

Proof.

$$
\begin{aligned}
&\mathbf{PBMH}(x \in ac') && \{\text{Lemma E.1.1}\} \\
&= \exists\, ac_0 \bullet x \in ac_0 \land ac_0 \subseteq ac' && \{\text{Predicate calculus}\} \\
&= x \in ac'
\end{aligned}
$$

□

Lemma E.4.8 *Provided ac' is not free in c.*

$$\mathbf{PBMH}(c \land P) = \mathbf{PBMH}(P)$$

Proof.

$$
\begin{aligned}
&\mathbf{PBMH}(c \land P) && \{\text{Lemma E.1.1}\} \\
&= \exists\, ac_0 \bullet (c \land P)[ac_0/ac'] \land ac_0 \subseteq ac' \\
& && \{\text{Assumption: } c \text{ is a condition, hence } ac' \text{ is not free}\} \\
&= \exists\, ac_0 \bullet c \land P[ac_0/ac'] \land ac_0 \subseteq ac' && \{\text{Predicate calculus}\} \\
&= c \land \exists\, ac_0 \bullet P[ac_0/ac'] \land ac_0 \subseteq ac' && \{\text{Lemma E.1.1}\} \\
&= c \land \mathbf{PBMH}(P)
\end{aligned}
$$

□

Lemma E.4.9 *Provided ac' is not free in c*

$$\mathbf{PBMH}(P \lhd c \rhd Q) = \mathbf{PBMH}(P) \lhd c \rhd \mathbf{PBMH}(Q)$$

Proof.

$$
\begin{array}{ll}
\mathbf{PBMH}(P \lhd c \rhd Q) & \{\text{Definition of conditional}\} \\
= \mathbf{PBMH}((c \wedge P) \vee (\neg\, c \wedge Q)) & \{\text{Distributivity of } \mathbf{PBMH}\} \\
= \mathbf{PBMH}(c \wedge P) \vee \mathbf{PBMH}(\neg\, c \wedge Q) & \{\text{Lemma E.4.8}\} \\
= (c \wedge \mathbf{PBMH}(P)) \vee (\neg\, c \wedge \mathbf{PBMH}(Q)) & \{\text{Definition of conditional}\} \\
= \mathbf{PBMH}(P) \lhd c \rhd \mathbf{PBMH}(Q) &
\end{array}
$$

□

Lemma E.4.10 *Provided ac' is not free in e.*

$$\mathbf{PBMH}(\exists\, y \bullet y \in ac' \wedge e) = \exists\, y \bullet y \in ac' \wedge e$$

Proof.

$$
\begin{array}{ll}
\mathbf{PBMH}(\exists\, y \bullet y \in ac' \wedge e) & \{\text{Definition of } \mathbf{PBMH} \text{ (Lemma E.1.1)}\} \\
= \exists\, ac_0 \bullet (\exists\, y \bullet y \in ac' \wedge e)[ac_0/ac'] \wedge ac_0 \subseteq ac' & \\
& \{\text{Substitution: } ac' \text{ not free in } e\} \\
= \exists\, ac_0 \bullet (\exists\, y \bullet y \in ac_0 \wedge e) \wedge ac_0 \subseteq ac' & \{\text{Property of sets}\} \\
= \exists\, y \bullet y \in ac' \wedge e &
\end{array}
$$

□

Lemma E.4.11

$$
\begin{array}{l}
(P \wedge ac' \neq \emptyset)\ ;_{\mathcal{A}}\ (Q \wedge ac' \neq \emptyset) \\
= \\
(P \wedge ac' \neq \emptyset)\ ;_{\mathcal{A}}\ (Q \wedge ac' \neq \emptyset)) \wedge ac' \neq \emptyset
\end{array}
$$

Proof.

$$
\begin{array}{ll}
(P \wedge ac' \neq \emptyset)\ ;_{\mathcal{A}}\ (Q \wedge ac' \neq \emptyset) & \\
& \{\text{Definition of } ;_{\mathcal{A}}\} \\
= (P \wedge ac' \neq \emptyset)[\{z \mid Q \wedge ac' \neq \emptyset)[z/s]\}/ac'] & \{\text{Substitution}\} \\
= (P \wedge ac' \neq \emptyset)[\{z \mid Q[z/s] \wedge ac' \neq \emptyset\}/ac'] & \{\text{Substitution}\} \\
= \left(\begin{array}{l} P[\{z \mid Q[z/s] \wedge ac' \neq \emptyset\}/ac'] \\ \wedge \\ \{z \mid Q[z/s] \wedge ac' \neq \emptyset\} \neq \emptyset \end{array} \right) & \{\text{Propositional calculus}\}
\end{array}
$$

$$= \left(\begin{array}{l} P[\{z \mid Q[z/s] \land ac' \neq \emptyset\}/ac'] \\ \land \\ \exists\, z \bullet z \in \{z \mid Q[z/s] \land ac' \neq \emptyset\} \end{array} \right) \qquad \{\text{Property of sets}\}$$

$$= \left(\begin{array}{l} P[\{z \mid Q[z/s] \land ac' \neq \emptyset\}/ac'] \\ \land \\ \exists\, z \bullet Q[z/s] \land ac' \neq \emptyset \end{array} \right)$$

$$\{\text{Predicate calculus: quantifier scope and duplicate term}\}$$

$$= \left(\begin{array}{l} P[\{z \mid Q[z/s] \land ac' \neq \emptyset\}/ac'] \\ \land \\ (\exists\, z \bullet Q[z/s] \land ac' \neq \emptyset) \end{array} \right) \land ac' \neq \emptyset \qquad \{\text{Property of sets}\}$$

$$= \left(\begin{array}{l} P[\{z \mid Q[z/s] \land ac' \neq \emptyset\}/ac'] \\ \land \\ \{z \mid Q[z/s] \land ac' \neq \emptyset\} \neq \emptyset \end{array} \right) \land ac' \neq \emptyset$$

$$\{\text{Re-introduce } ac' \text{ and substitution}\}$$

$$= ((P \land ac' \neq \emptyset)[\{z \mid Q[z/s] \land ac' \neq \emptyset\}/ac']) \land ac' \neq \emptyset \qquad \{\text{Substitution}\}$$

$$= ((P \land ac' \neq \emptyset)[\{z \mid (Q \land ac' \neq \emptyset)[z/s]\}/ac']) \land ac' \neq \emptyset$$

$$\{\text{Definition of } ;_{\mathcal{A}}\}$$

$$= ((P \land ac' \neq \emptyset) \;;_{\mathcal{A}} (Q \land ac' \neq \emptyset)) \land ac' \neq \emptyset$$

□

Lemma E.4.12

$$\mathbf{PBMH}(P \;;\; ac = \emptyset) = P \;;\; ac = \emptyset$$

Proof.

$$\mathbf{PBMH}(P \;;\; ac = \emptyset) \qquad \{\text{Definition of } \mathbf{PBMH}\}$$

$$= (P \;;\; ac = \emptyset) \;;\; ac \subseteq ac' \land v' = v$$

$$\{\text{Associativity of sequential composition}\}$$

$$= P \;;\; (ac = \emptyset \;;\; ac \subseteq ac' \land v' = v)$$

$$\{\text{Definition of sequential composition}\}$$

$$= P \;;\; (\exists\, ac_0, v_0 \bullet ac = \emptyset \land ac_0 \subseteq ac' \land v' = v_0) \qquad \{\text{One-point rule}\}$$

$$= P \;;\; (\exists\, ac_0 \bullet ac = \emptyset \land ac_0 \subseteq ac') \qquad \{\text{Propositional calculus}\}$$

$$= P \;;\; (ac = \emptyset \land \exists\, ac_0 \bullet ac_0 \subseteq ac') \qquad \{\text{Choose } ac_0 = \emptyset\}$$

$$= P \;;\; (ac = \emptyset \land \mathit{true}) \qquad \{\text{Propositional calculus}\}$$

$$= P \;;\; ac = \emptyset$$

□

Lemma E.4.13 *Provided ac_1 is not free in $F(x)$.*

$$\exists\, ac_1 \bullet (\forall\, x \bullet x \in ac_0 \Rightarrow F(x) \in ac_1) \land ac_1 \subseteq ac'$$
$$\Leftrightarrow$$
$$\forall\, x \bullet x \in ac_0 \Rightarrow F(x) \in ac'$$

Proof. (Implication)

$\exists\, ac_1 \bullet (\forall\, x \bullet x \in ac_0 \Rightarrow F(x) \in ac_1) \land ac_1 \subseteq ac'$ {Predicate calculus}
$\Rightarrow \forall\, x \bullet \exists\, ac_1 \bullet (x \in ac_0 \Rightarrow F(x) \in ac_1) \land ac_1 \subseteq ac'$ {Predicate calculus}
$= \forall\, x \bullet \exists\, ac_1 \bullet (x \notin ac_0 \land ac_1 \subseteq ac') \lor (F(x) \in ac_1 \land ac_1 \subseteq ac')$ {Predicate calculus}
$= \forall\, x \bullet (\exists\, ac_1 \bullet x \notin ac_0 \land ac_1 \subseteq ac') \lor (\exists\, ac_1 \bullet F(x) \in ac_1 \land ac_1 \subseteq ac')$ {Predicate calculus}
$= \forall\, x \bullet (x \notin ac_0) \lor (\exists\, ac_1 \bullet F(x) \in ac_1 \land ac_1 \subseteq ac')$ {Assumption: ac_1 not free in $F(x)$ and predicate calculus}
$= \forall\, x \bullet x \notin ac_0 \lor F(x) \in ac'$ {Predicate calculus}
$= \forall\, x \bullet x \in ac_0 \Rightarrow F(x) \in ac'$

□

Proof. (Reverse implication)

$\forall\, x \bullet x \in ac_0 \Rightarrow f(x) \in ac'$ {Introduce fresh variable}
$= \exists\, ac_1 \bullet (\forall\, x \bullet x \in ac_0 \Rightarrow f(x) \in ac_1) \land ac_1 = ac'$ {Predicate calculus}
$\Rightarrow \exists\, ac_1 \bullet (\forall\, x \bullet x \in ac_0 \Rightarrow f(x) \in ac_1) \land ac_1 \subseteq ac'$

□

Lemma E.4.14

$$P \sqsubseteq Q \Leftrightarrow [\{ac' \mid Q\} \subseteq \{ac' \mid P\}]$$

Proof.

$P \sqsubseteq Q$ {Definition of $\sqsubseteq$}

$\Leftrightarrow [Q \Rightarrow P]$ {Universal quantification}
$\Leftrightarrow \forall\, ac', ok', ok, s \bullet Q \Rightarrow P$ {Property of sets}
$\Leftrightarrow \forall\, ac', ok', ok, s \bullet ac' \in \{ac' \mid Q\} \Rightarrow ac' \in \{ac' \mid P\}$ {Property of sets}
$\Leftrightarrow \forall\, ac', ok', ok, s \bullet \{ac' \mid Q\} \subseteq \{ac' \mid P\}$ {Universal quantification}
$\Leftrightarrow [\{ac' \mid Q\} \subseteq \{ac' \mid P\}]$

□

E.5 Substitution lemmas

Lemma E.5.1

$$\mathbf{PBMH}(P)^o_w = \mathbf{PBMH}(P^o_w)$$

Proof.

$\mathbf{PBMH}(P)^o_w$ {Definition of **PBMH** (Lemma E.1.1)}
$= (\exists\, ac_0 \bullet P[ac_0/ac'] \land ac_0 \subseteq ac')^o_w$ {Substitution abbreviation}
$= (\exists\, ac_0 \bullet P[ac_0/ac'] \land ac_0 \subseteq ac')[o, s \oplus \{wait \mapsto w\}/ok', s]$ {Substitution}
$= \exists\, ac_0 \bullet P[ac_0/ac'][o, s \oplus \{wait \mapsto w\}/ok', s] \land ac_0 \subseteq ac'$ {Substitution}
$= \exists\, ac_0 \bullet P[o, s \oplus \{wait \mapsto w\}/ok', s][ac_0/ac'] \land ac_0 \subseteq ac'$ {Substitution abbreviation}
$= \exists\, ac_0 \bullet P^o_w[ac_0/ac'] \land ac_0 \subseteq ac'$ {Definition of **PBMH** (Lemma E.1.1)}
$= \mathbf{PBMH}(P^o_w)$

□

Lemma E.5.2 *Provided ac' is not free in e.*

$$\mathbf{PBMH}(P)[e/s] = \mathbf{PBMH}(P[e/s])$$

Proof.

$\mathbf{PBMH}(P)[e/s]$ {Definition of **PBMH** (Lemma E.1.1)}
$= (\exists\, ac_0 \bullet P[ac_0/ac'] \land ac_0 \subseteq ac')[e/s]$ {Property of substitution}

$= (\exists\, ac_0 \bullet P[ac_0/ac'][e/s] \land ac_0 \subseteq ac')$
{Property of substitution: ac' not free in e and ac_0 is fresh}
$= (\exists\, ac_0 \bullet P[e/s][ac_0/ac'] \land ac_0 \subseteq ac')$
{Definition of **PBMH** (Lemma E.1.1)}
$= \mathbf{PBMH}(P[e/s])$

□

E.6 Properties with respect to designs

Theorem E.6.1

$$\mathbf{H2} \circ \mathbf{PBMH}(P) = \mathbf{PBMH} \circ \mathbf{H2}(P)$$

Proof.

$\mathbf{H2} \circ \mathbf{PBMH}(P)$ {Definition of **H2** (J-split)}
$= \mathbf{PBMH}(P)\ ;\ J$ {Definition of **PBMH**}
$= (P\ ;\ ac \subseteq ac' \land ok' = ok)\ ;\ J$
{Associativity of sequential composition}
$= P\ ;\ ((ac \subseteq ac' \land ok' = ok)\ ;\ J)$ {Lemma E.6.1}
$= P\ ;\ (J\ ;\ (ac \subseteq ac' \land ok' = ok))$
{Associativity of sequential composition}
$= (P\ ;\ J)\ ;\ (ac \subseteq ac' \land ok' = ok)$ {Definition of **PBMH**}
$= \mathbf{PBMH}(P\ ;\ J)$ {Definition of **H2** (J-split)}
$= \mathbf{PBMH} \circ \mathbf{H2}(P)$

□

Theorem E.6.2

$$\mathbf{H1} \circ \mathbf{PBMH}(P) = \mathbf{PBMH} \circ \mathbf{H1}(P)$$

Proof.

$\mathbf{PBMH} \circ \mathbf{H1}(P)$ {Definition of **H1**}
$= \mathbf{PBMH}(ok \Rightarrow P)$ {Predicate calculus}

$= \mathbf{PBMH}(\neg\ ok \vee P)$ {Distributivity of **PBMH**}
$= \mathbf{PBMH}(\neg\ ok) \vee \mathbf{PBMH}(P)$ {Lemma E.4.6}
$= \neg\ ok \vee \mathbf{PBMH}(P)$ {Predicate calculus}
$= ok \Rightarrow \mathbf{PBMH}(P)$ {Definition of **H1**}
$= \mathbf{H1} \circ \mathbf{PBMH}(P)$

□

Lemma E.6.1

$$J\ ;\ (ac \subseteq ac' \wedge ok' = ok) = (ac \subseteq ac' \wedge ok' = ok)\ ;\ J$$

Proof.

$J\ ;\ (ac \subseteq ac' \wedge ok' = ok)$ {Definition of J}
$= (ac' = ac \wedge ok \Rightarrow ok')\ ;\ (ac \subseteq ac' \wedge ok' = ok)$
{Definition of sequential composition}
$= \exists\, ac_0, ok_0 \bullet ac_0 = ac \wedge (ok \Rightarrow ok_0) \wedge ac_0 \subseteq ac' \wedge ok' = ok_0$
{One-point rule}
$= (ok \Rightarrow ok') \wedge ac \subseteq ac'$ {One-point rule}
$= \exists\, ac_0, ok_0 \bullet ac \subseteq ac_0 \wedge ok_0 = ok \wedge ac' = ac_0 \wedge ok_0 \Rightarrow ok'$
{Definition of sequential composition}
$= (ac \subseteq ac' \wedge ok' = ok)\ ;\ (ac' = ac \wedge ok \Rightarrow ok')$ {Definition of J}
$= (ac \subseteq ac' \wedge ok' = ok)\ ;\ J$

□

Lemma E.6.2

$$\mathbf{PBMH}(P \vdash Q) = (\neg\ \mathbf{PBMH}(\neg\ P) \vdash \mathbf{PBMH}(Q))$$

Proof.

PBMH$(P \vdash Q)$ {Definition of design}
$= \mathbf{PBMH}((ok \wedge P) \Rightarrow (Q \wedge ok'))$ {Predicate calculus}
$= \mathbf{PBMH}(\neg\ ok \vee \neg\ P \vee (Q \wedge ok'))$ {Theorem E.2.2}
$= \mathbf{PBMH}(\neg\ ok) \vee \mathbf{PBMH}(\neg\ P) \vee \mathbf{PBMH}(Q \wedge ok')$ {Lemma E.4.6}

$$
\begin{array}{ll}
= \neg\ ok \vee \mathbf{PBMH}(\neg\ P) \vee \mathbf{PBMH}(Q \wedge ok') & \{\text{Lemma E.4.8}\} \\
= \neg\ ok \vee \mathbf{PBMH}(\neg\ P) \vee (\mathbf{PBMH}(Q) \wedge ok') & \{\text{Predicate calculus}\} \\
= (ok \wedge \neg\ \mathbf{PBMH}(\neg\ P)) \Rightarrow (\mathbf{PBMH}(Q) \wedge ok') & \{\text{Definition of design}\} \\
= (\neg\ \mathbf{PBMH}(\neg\ P) \vdash \mathbf{PBMH}(Q)) &
\end{array}
$$

□

E.7 Properties with respect to A2

Lemma E.7.1 *Provided P is* **PBMH***-healthy.*

$$
\begin{array}{l}
\mathbf{PBMH}(P\ ;_{\mathcal{A}}\ \{s \mid \{s\} = ac'\}) \\
= \\
\exists\, ac_1, ac_0 \bullet P[ac_0/ac'] \wedge ac_0 \subseteq \{s \mid \{s\} = ac_1\} \wedge ac_1 \subseteq ac'
\end{array}
$$

Proof.

$$
\begin{array}{ll}
\mathbf{PBMH}(P\ ;_{\mathcal{A}}\ \{s \mid \{s\} = ac'\}) & \{\text{Assumption: } P \text{ is } \mathbf{PBMH}\text{-healthy}\} \\
= \mathbf{PBMH}(\mathbf{PBMH}(P)\ ;_{\mathcal{A}}\ \{s \mid \{s\} = ac'\}) & \\
& \{\text{Definition of } \mathbf{PBMH} \text{ (Lemma E.1.1)}\} \\
= \mathbf{PBMH}((\exists\, ac_0 \bullet P[ac_0/ac'] \wedge ac_0 \subseteq ac')\ ;_{\mathcal{A}}\ \{s \mid \{s\} = ac'\}) & \\
& \{\text{Definition of } ;_{\mathcal{A}} \text{ and substitution}\} \\
= \mathbf{PBMH}(\exists\, ac_0 \bullet P[ac_0/ac'] \wedge ac_0 \subseteq \{s \mid \{s\} = ac'\}) & \\
& \{\text{Definition of } \mathbf{PBMH} \text{ (Lemma E.1.1)}\} \\
= (\exists\, ac_1 \bullet (\exists\, ac_0 \bullet P[ac_0/ac'] \wedge ac_0 \subseteq \{s \mid \{s\} = ac'\})[ac_1/ac'] \wedge ac_1 \subseteq ac') & \\
& \{\text{Substitution and predicate calculus}\} \\
= \exists\, ac_1, ac_0 \bullet P[ac_0/ac'] \wedge ac_0 \subseteq \{s \mid \{s\} = ac_1\} \wedge ac_1 \subseteq ac' &
\end{array}
$$

□

Theorem E.7.1 *Provided P is* **PBMH***-healthy and v is not free in P*

$$\exists\, v \bullet (P\ ;_{\mathcal{A}}\ Q) \Rightarrow P\ ;_{\mathcal{A}}\ (\exists\, v \bullet Q)$$

Proof.

$$
\begin{array}{ll}
\exists\, v \bullet (P\ ;_{\mathcal{A}}\ Q) & \{\text{Assumption: } P \text{ is } \mathbf{PBMH}\text{-healthy}\}
\end{array}
$$

$$
\begin{aligned}
&= \exists\, v \bullet (\mathbf{PBMH}(P) \ ;_{\mathcal{A}}\ Q) && \{\text{Definition of } \mathbf{PBMH} \text{ (Lemma E.1.1)}\}\\
&= \exists\, v \bullet ((\exists\, ac_0 \bullet P[ac_0/ac'] \wedge ac_0 \subseteq ac') \ ;_{\mathcal{A}}\ Q) \\
&\qquad\qquad \{\text{Definition of } ;_{\mathcal{A}} \text{ and substitution}\}\\
&= \exists\, v \bullet (\exists\, ac_0 \bullet P[ac_0/ac'] \wedge ac_0 \subseteq \{s \mid Q\}) \\
&\qquad\qquad \{\text{Predicate calculus: } v \text{ is not free in } P\}\\
&= \exists\, ac_0 \bullet P[ac_0/ac'] \wedge (\exists\, v \bullet ac_0 \subseteq \{s \mid Q\}) && \{\text{Lemma H.1.8}\}\\
&\Rightarrow \exists\, ac_0 \bullet P[ac_0/ac'] \wedge ac_0 \subseteq \{s \mid \exists\, v \bullet Q\} \\
&\qquad\qquad \{\text{Definition of } ;_{\mathcal{A}} \text{ and substitution}\}\\
&= (\exists\, ac_0 \bullet P[ac_0/ac'] \wedge ac_0 \subseteq ac') \ ;_{\mathcal{A}}\ (\exists\, v \bullet Q) \\
&\qquad\qquad \{\text{Definition of } \mathbf{PBMH} \text{ (Lemma E.1.1)}\}\\
&= \mathbf{PBMH}(P) \ ;_{\mathcal{A}}\ (\exists\, v \bullet Q) && \{\text{Assumption: } P \text{ is } \mathbf{PBMH}\text{-healthy}\}\\
&= P \ ;_{\mathcal{A}}\ (\exists\, v \bullet Q)
\end{aligned}
$$

□

Appendix F

Sequential composition ($\mathcal{A}$)

F.1 Properties

Lemma F.1.1 (; $_{\mathcal{A}}$-ac'-not-free) *Provided ac' is not free in P.*

$$P \ ; _{\mathcal{A}} \ Q = P$$

Proof.

$P \ ; _{\mathcal{A}} \ Q$ {Definition of $; _{\mathcal{A}}$}
$= P[\{z : State \mid Q[z/s]\}/ac']$ {Assumption: ac' not free in P}
$= P$

□

Lemma F.1.2 (; $_{\mathcal{A}}$-negation)

$$\neg \ (P \ ; _{\mathcal{A}} \ Q) = (\neg \ P \ ; _{\mathcal{A}} \ Q)$$

Proof.

$\neg \ (P \ ; _{\mathcal{A}} \ Q)$ {Definition of sequential composition}
$= \neg \ (P[\{z \mid Q[z/s]\}/ac'])$ {Propositional calculus}
$= (\neg \ P[\{z \mid Q[z/s]\}/ac'])$ {Definition of sequential composition}
$= (\neg \ P \ ; _{\mathcal{A}} \ Q)$

□

Lemma F.1.3 (; $_{\mathcal{A}}$-associativity) *Provided P and Q satisfy* **PBMH**.

$$P \ ;_{\mathcal{A}} (Q \ ;_{\mathcal{A}} R) = (P \ ;_{\mathcal{A}} Q) \ ;_{\mathcal{A}} R$$

Proof.

$$\begin{array}{ll}
P \ ;_{\mathcal{A}} (Q \ ;_{\mathcal{A}} R) & \{\text{Definition of } ;_{\mathcal{A}}\} \\
= P[\{s \mid Q \ ;_{\mathcal{A}} R\}/ac'] & \{\text{Definition of } ;_{\mathcal{A}}\} \\
= P[\{s \mid Q[\{s \mid R\}/ac']\}/ac'] & \{\text{Property of substitution}\} \\
= P[\{s \mid Q\}/ac'][\{s \mid R\}/ac'] & \{\text{Definition of } ;_{\mathcal{A}}\} \\
= P[\{s \mid Q\}/ac'] \ ;_{\mathcal{A}} R & \{\text{Definition of } ;_{\mathcal{A}}\} \\
= (P \ ;_{\mathcal{A}} Q) \ ;_{\mathcal{A}} R &
\end{array}$$

□

Lemma F.1.4 (; $_{\mathcal{A}}$-right-distributivity-disjunction)

$$(P \vee Q) \ ;_{\mathcal{A}} R = (P \ ;_{\mathcal{A}} R) \vee (Q \ ;_{\mathcal{A}} R)$$

Proof.

$$\begin{array}{ll}
(P \vee Q) \ ;_{\mathcal{A}} R & \{\text{Definition of } ;_{\mathcal{A}}\} \\
= (P \vee Q)[\{z \mid R[z/s]\}/ac'] & \{\text{Substitution}\} \\
= (P[\{z \mid R[z/s]\}/ac'] \vee Q[\{z \mid R[z/s]\}/ac']) & \{\text{Definition of } ;_{\mathcal{A}}\} \\
= (P \ ;_{\mathcal{A}} R) \vee (Q \ ;_{\mathcal{A}} R) &
\end{array}$$

□

Lemma F.1.5 (; $_{\mathcal{A}}$-right-distributivity-conjunction)

$$(P \wedge Q) \ ;_{\mathcal{A}} R = (P \ ;_{\mathcal{A}} R) \wedge (Q \ ;_{\mathcal{A}} R)$$

Proof.

$$\begin{array}{ll}
(P \wedge Q) \ ;_{\mathcal{A}} R & \{\text{Definition of } ;_{\mathcal{A}}\} \\
= (P \wedge Q)[\{z \mid R[z/s]\}/ac'] & \{\text{Property of substitution}\} \\
= (P[\{z \mid R[z/s]\}/ac'] \wedge Q[\{z \mid R[z/s]\}/ac']) & \{\text{Definition of } ;_{\mathcal{A}}\} \\
= (P \ ;_{\mathcal{A}} R) \wedge (Q \ ;_{\mathcal{A}} R) &
\end{array}$$

□

Lemma F.1.6 *Provided P is* **PBMH***-healthy.*

$$P \ ;_{\mathcal{A}} (Q \wedge R) \Rightarrow (P \ ;_{\mathcal{A}} Q) \wedge (P \ ;_{\mathcal{A}} R)$$

Proof.

$$
\begin{array}{ll}
P \ ;_{\mathcal{A}} (Q \wedge R) & \{\text{Assumption: } P \text{ is } \mathbf{PBMH}\text{-healthy}\} \\
= \mathbf{PBMH}(P) \ ;_{\mathcal{A}} (Q \wedge R) & \{\text{Definition of } \mathbf{PBMH} \text{ (Lemma E.1.1)}\} \\
= (\exists\, ac_0 \bullet P[ac_0/ac'] \wedge ac_0 \subseteq ac') \ ;_{\mathcal{A}} (Q \wedge R) & \\
& \{\text{Definition of } ;_{\mathcal{A}} \text{ and substitution}\} \\
= \exists\, ac_0 \bullet P[ac_0/ac'] \wedge ac_0 \subseteq \{s \mid Q \wedge R\} & \{\text{Property of sets}\} \\
= \exists\, ac_0 \bullet P[ac_0/ac'] \wedge ac_0 \subseteq \{s \mid Q\} \wedge ac_0 \subseteq \{s \mid R\} & \\
& \{\text{Predicate calculus}\} \\
\Rightarrow \left(\begin{array}{l} (\exists\, ac_0 \bullet P[ac_0/ac'] \wedge ac_0 \subseteq \{s \mid Q\}) \\ \wedge \\ (\exists\, ac_0 \bullet P[ac_0/ac'] \wedge ac_0 \subseteq \{s \mid R\}) \end{array} \right) & \\
& \{\text{Definition of } ;_{\mathcal{A}} \text{ and substitution}\} \\
= \left(\begin{array}{l} ((\exists\, ac_0 \bullet P[ac_0/ac'] \wedge ac_0 \subseteq ac') \ ;_{\mathcal{A}} Q) \\ \wedge \\ ((\exists\, ac_0 \bullet P[ac_0/ac'] \wedge ac_0 \subseteq ac') \ ;_{\mathcal{A}} R) \end{array} \right) & \\
& \{\text{Definition of } \mathbf{PBMH} \text{ (Lemma E.1.1)}\} \\
= (\mathbf{PBMH}(P) \ ;_{\mathcal{A}} Q) \wedge (\mathbf{PBMH}(P) \ ;_{\mathcal{A}} R) & \\
& \{\text{Assumption: } P \text{ is } \mathbf{PBMH}\text{-healthy}\} \\
= (P \ ;_{\mathcal{A}} Q) \wedge (P \ ;_{\mathcal{A}} R) &
\end{array}
$$

□

F.2 Lemmas

Lemma F.2.1 *Provided P is* **PBMH***-healthy.*

$$(P \ ;_{\mathcal{A}} Q) \vee (P \ ;_{\mathcal{A}} R) \Rightarrow (P \ ;_{\mathcal{A}} (Q \vee R))$$

Proof.

$$
\begin{array}{ll}
(P \ ;_{\mathcal{A}} Q) \vee (P \ ;_{\mathcal{A}} R) & \\
& \{\text{Assumption: } P \text{ is } \mathbf{PBMH}\text{-healthy (Lemma E.1.1)}\}
\end{array}
$$

$$= \left(\begin{array}{l} ((\exists\, ac_0 \bullet P[ac_0/ac'] \wedge ac_0 \subseteq ac') \;;_{\mathcal{A}}\; Q) \\ \vee \\ ((\exists\, ac_0 \bullet P[ac_0/ac'] \wedge ac_0 \subseteq ac') \;;_{\mathcal{A}}\; R) \end{array} \right)$$

{Definition of $;_{\mathcal{A}}$ and substitution}

$$= \left(\begin{array}{l} (\exists\, ac_0 \bullet P[ac_0/ac'] \wedge ac_0 \subseteq \{s \mid Q\}) \\ \vee \\ (\exists\, ac_0 \bullet P[ac_0/ac'] \wedge ac_0 \subseteq \{s \mid R\}) \end{array} \right)$$

{Predicate calculus}

$$= \exists\, ac_0 \bullet P[ac_0/ac'] \wedge (ac_0 \subseteq \{s \mid Q\} \vee ac_0 \subseteq \{s \mid R\})$$

{Property of sets and predicate calculus}

$$\Rightarrow \exists\, ac_0 \bullet P[ac_0/ac'] \wedge ac_0 \subseteq \{s \mid Q\} \cup \{s \mid R\}$$

{Property of sets}

$$= \exists\, ac_0 \bullet P[ac_0/ac'] \wedge ac_0 \subseteq \{s \mid Q \vee R\}$$

{Definition of $;_{\mathcal{A}}$ and substitution}

$$= (\exists\, ac_0 \bullet P[ac_0/ac'] \wedge ac_0 \subseteq ac') \;;_{\mathcal{A}}\; (Q \vee R)$$

{Assumption: P is **PBMH**-healthy (Lemma E.1.1)}

$$= P \;;_{\mathcal{A}}\; (Q \vee R)$$

□

Lemma F.2.2 *Provided P is* **PBMH***-healthy.*

$$(P \;;_{\mathcal{A}}\; Q) \vee (P \;;_{\mathcal{A}}\; true) = P \;;_{\mathcal{A}}\; true$$

Proof.

$$(P \;;_{\mathcal{A}}\; Q) \vee (P \;;_{\mathcal{A}}\; true)$$

{Lemma F.2.1}

$$= ((P \;;_{\mathcal{A}}\; Q) \vee (P \;;_{\mathcal{A}}\; true)) \wedge (P \;;_{\mathcal{A}}\; (Q \vee true))$$

{Predicate calculus}

$$= ((P \;;_{\mathcal{A}}\; Q) \vee (P \;;_{\mathcal{A}}\; true)) \wedge (P \;;_{\mathcal{A}}\; true)$$

{Predicate calculus: absorption law}

$$= (P \;;_{\mathcal{A}}\; true)$$

□

Theorem F.2.1 *Provided P is* **PBMH***-healthy.*

$$(P \;;_{\mathcal{A}}\; Q) \vee (P \;;_{\mathcal{A}}\; false) = P \;;_{\mathcal{A}}\; Q$$

Proof.

$$
\begin{array}{ll}
(P \ ;_{\mathcal{A}} Q) \vee (P \ ;_{\mathcal{A}} \mathit{false}) & \{\text{Lemma F.2.1}\} \\
= ((P \ ;_{\mathcal{A}} Q) \vee (P \ ;_{\mathcal{A}} \mathit{false})) \wedge (P \ ;_{\mathcal{A}} (Q \vee \mathit{false})) & \\
& \{\text{Predicate calculus}\} \\
= ((P \ ;_{\mathcal{A}} Q) \vee (P \ ;_{\mathcal{A}} \mathit{false})) \wedge (P \ ;_{\mathcal{A}} Q) & \\
& \{\text{Predicate calculus: absorption law}\} \\
= P \ ;_{\mathcal{A}} Q &
\end{array}
$$

□

Lemma F.2.3 *Provided P is* **PBMH***-healthy.*

$$P \ ;_{\mathcal{A}} (Q \Rightarrow (R \wedge ok')) = (P \ ;_{\mathcal{A}} \neg Q) \vee ((P \ ;_{\mathcal{A}} (Q \Rightarrow R)) \wedge ok')$$

Proof.

$$
\begin{array}{ll}
P \ ;_{\mathcal{A}} (Q \Rightarrow (R \wedge ok')) & \\
& \{\text{Assumption: } P \text{ is } \mathbf{PBMH}\text{-healthy (Lemma E.1.1)}\} \\
= (\exists\, ac_0 \bullet P[ac_0/ac'] \wedge ac_0 \subseteq ac') \ ;_{\mathcal{A}} (Q \Rightarrow (R \wedge ok')) & \\
& \{\text{Definition of } ;_{\mathcal{A}} \text{ and substitution}\} \\
= \exists\, ac_0 \bullet P[ac_0/ac'] \wedge ac_0 \subseteq \{s \mid Q \Rightarrow (R \wedge ok')\} & \{\text{Property of sets}\} \\
= \exists\, ac_0 \bullet P[ac_0/ac'] \wedge \forall\, z \bullet z \in ac_0 \Rightarrow (Q[z/s] \Rightarrow (R[z/s] \wedge ok')) & \\
& \{\text{Lemma F.2.4}\} \\
= \exists\, ac_0 \bullet P[ac_0/ac'] \wedge \left(\begin{array}{l} (\forall\, z \bullet z \in ac_0 \Rightarrow \neg\, Q[z/s]) \\ \vee \\ ((\forall\, z \bullet z \in ac_0 \Rightarrow (Q[z/s] \Rightarrow R[z/s])) \wedge ok') \end{array} \right) & \\
& \{\text{Predicate calculus}\} \\
= \left(\begin{array}{l} (\exists\, ac_0 \bullet P[ac_0/ac'] \wedge (\forall\, z \bullet z \in ac_0 \Rightarrow \neg\, Q[z/s])) \\ \vee \\ (\exists\, ac_0 \bullet P[ac_0/ac'] \wedge ((\forall\, z \bullet z \in ac_0 \Rightarrow (Q[z/s] \Rightarrow R[z/s])) \wedge ok')) \end{array} \right) & \\
& \{\text{Property of sets}\} \\
= \left(\begin{array}{l} (\exists\, ac_0 \bullet P[ac_0/ac'] \wedge (\forall\, z \bullet z \in ac_0 \Rightarrow z \in \{s \mid \neg\, Q\})) \\ \vee \\ (\exists\, ac_0 \bullet P[ac_0/ac'] \wedge ((\forall\, z \bullet z \in ac_0 \Rightarrow z \in \{s \mid Q \Rightarrow R\}) \wedge ok')) \end{array} \right) & \\
& \{\text{Property of sets}\}
\end{array}
$$

$$= \left(\begin{array}{l} (\exists\, ac_0 \bullet P[ac_0/ac'] \land ac_0 \subseteq \{s \mid \neg\, Q\}) \\ \lor \\ (\exists\, ac_0 \bullet P[ac_0/ac'] \land ac_0 \subseteq \{s \mid Q \Rightarrow R\} \land ok') \end{array} \right)$$

$$\{\text{Predicate calculus}\}$$

$$= \left(\begin{array}{l} (\exists\, ac_0 \bullet P[ac_0/ac'] \land ac_0 \subseteq \{s \mid \neg\, Q\}) \\ \lor \\ ((\exists\, ac_0 \bullet P[ac_0/ac'] \land ac_0 \subseteq \{s \mid Q \Rightarrow R\}) \land ok') \end{array} \right)$$

$$\{\text{Definition of } ;_{\mathcal{A}} \text{ and substitution}\}$$

$$= \left(\begin{array}{l} ((\exists\, ac_0 \bullet P[ac_0/ac'] \land ac_0 \subseteq ac') \;;_{\mathcal{A}} \neg\, Q) \\ \lor \\ (((\exists\, ac_0 \bullet P[ac_0/ac'] \land ac_0 \subseteq ac') \;;_{\mathcal{A}} (Q \Rightarrow R)) \land ok') \end{array} \right)$$

$$\{\text{Assumption: } P \text{ is } \mathbf{PBMH}\text{-healthy (Lemma E.1.1)}\}$$

$$= (P \;;_{\mathcal{A}} \neg\, Q) \lor ((P \;;_{\mathcal{A}} (Q \Rightarrow R)) \land ok')$$

□

Lemma F.2.4 *Provided x is not free in e*

$$\begin{array}{l} \forall\, x \bullet P \Rightarrow (Q \Rightarrow (R \land e)) \\ = \\ (\forall\, x \bullet P \Rightarrow \neg\, Q) \lor ((\forall\, x \bullet P \Rightarrow (Q \Rightarrow R)) \land e) \end{array}$$

Proof.

$$\begin{array}{ll} \forall\, x \bullet P \Rightarrow (Q \Rightarrow (R \land e)) & \{\text{Predicate calculus}\} \\ = \forall\, x \bullet (P \land Q) \Rightarrow (R \land e) & \{\text{Predicate calculus}\} \\ = \forall\, x \bullet ((P \land Q) \Rightarrow R) \land ((P \land Q) \Rightarrow e) & \{\text{Predicate calculus}\} \\ = \forall\, x \bullet ((P \land Q) \Rightarrow R) \land (\neg\, (P \land Q) \lor e) & \{\text{Predicate calculus}\} \\ = (\forall\, x \bullet (P \land Q) \Rightarrow R) \land (\forall\, x \bullet \neg\, (P \land Q) \lor e) & \\ \qquad \{\text{Predicate calculus: } x \text{ is not free in } e\} & \\ = (\forall\, x \bullet (P \land Q) \Rightarrow R) \land ((\forall\, x \bullet \neg\, (P \land Q)) \lor e) & \{\text{Predicate calculus}\} \\ = \left(\begin{array}{l} ((\forall\, x \bullet (P \land Q) \Rightarrow R) \land (\forall\, x \bullet \neg\, (P \land Q))) \\ \lor \\ ((\forall\, x \bullet (P \land Q) \Rightarrow R) \land e) \end{array} \right) & \{\text{Predicate calculus}\} \\ = \left(\begin{array}{l} (\forall\, x \bullet ((P \land Q) \Rightarrow R) \land \neg\, (P \land Q)) \\ \lor \\ ((\forall\, x \bullet ((P \land Q) \Rightarrow R)) \land e) \end{array} \right) & \{\text{Predicate calculus}\} \end{array}$$

$$= \left(\begin{array}{l} (\forall\, x \bullet \neg\, (P \wedge Q)) \\ \vee \\ ((\forall\, x \bullet ((P \wedge Q) \Rightarrow R)) \wedge e) \end{array} \right) \qquad \{\text{Predicate calculus}\}$$

$$= (\forall\, x \bullet P \Rightarrow \neg\, Q) \vee ((\forall\, x \bullet P \Rightarrow (Q \Rightarrow R)) \wedge e)$$

□

Lemma F.2.5 *Provided P is* **PBMH***-healthy.*

$$P \;;_{\mathcal{A}}\, (Q \wedge ok') = (P \;;_{\mathcal{A}}\, \mathit{false}) \vee ((P \;;_{\mathcal{A}}\, Q) \wedge ok')$$

Proof.

$$P \;;_{\mathcal{A}}\, (Q \wedge ok') \qquad \{\text{Assumption: } P \text{ is } \mathbf{PBMH}\text{-healthy}\}$$

$$= \mathbf{PBMH}(P) \;;_{\mathcal{A}}\, (Q \wedge ok') \qquad \{\text{Definition of } \mathbf{PBMH} \text{ (Lemma E.1.1)}\}$$

$$= (\exists\, ac_0 \bullet P[ac_0/ac'] \wedge ac_0 \subseteq ac') \;;_{\mathcal{A}}\, (Q \wedge ok') \qquad \{\text{Definition of } ;_{\mathcal{A}} \text{ and substitution}\}$$

$$= \exists\, ac_0 \bullet P[ac_0/ac'] \wedge ac_0 \subseteq \{z \mid (Q \wedge ok')[z/s]\} \qquad \{\text{Property of substitution}\}$$

$$= \exists\, ac_0 \bullet P[ac_0/ac'] \wedge ac_0 \subseteq \{z \mid Q[z/s] \wedge ok'\} \qquad \{\text{Property of sets}\}$$

$$= \exists\, ac_0 \bullet P[ac_0/ac'] \wedge (\forall\, z \bullet z \in ac_0 \Rightarrow (Q[z/s] \wedge ok')) \qquad \{\text{Propositional calculus}\}$$

$$= \exists\, ac_0 \bullet P[ac_0/ac'] \wedge (\forall\, z \bullet z \in ac_0 \Rightarrow Q[z/s]) \wedge (\forall\, z \bullet z \in ac_0 \Rightarrow ok') \qquad \{\text{Propositional calculus}\}$$

$$= \exists\, ac_0 \bullet P[ac_0/ac'] \wedge (\forall\, z \bullet z \in ac_0 \Rightarrow Q[z/s]) \wedge (\forall\, z \bullet z \notin ac_0 \vee ok') \qquad \{\text{Predicate calculus: } ok' \neq z, \text{ move quantifier}\}$$

$$= \exists\, ac_0 \bullet P[ac_0/ac'] \wedge (\forall\, z \bullet z \in ac_0 \Rightarrow Q[z/s]) \wedge ((\forall\, z \bullet z \notin ac_0) \vee ok') \qquad \{\text{Predicate calculus: distribution}\}$$

$$= \exists\, ac_0 \bullet P[ac_0/ac'] \wedge \left(\begin{array}{l} ((\forall\, z \bullet z \in ac_0 \Rightarrow Q[z/s]) \wedge (\forall\, z \bullet z \notin ac_0)) \\ \vee \\ ((\forall\, z \bullet z \in ac_0 \Rightarrow Q[z/s]) \wedge ok') \end{array} \right) \qquad \{\text{Predicate calculus}\}$$

$$= \exists\, ac_0 \bullet P[ac_0/ac'] \wedge \left(\begin{array}{l} (\forall\, z \bullet (z \in ac_0 \Rightarrow Q[z/s]) \wedge z \notin ac_0) \\ \vee \\ ((\forall\, z \bullet z \in ac_0 \Rightarrow Q[z/s]) \wedge ok') \end{array} \right) \qquad \{\text{Propositional calculus}\}$$

$$= \exists\, ac_0 \bullet P[ac_0/ac'] \wedge ((\forall\, z \bullet z \notin ac_0) \vee ((\forall\, z \bullet z \in ac_0 \Rightarrow Q[z/s]) \wedge ok'))$$

{Propositional calculus}

$$= \left(\begin{array}{l} (\exists\, ac_0 \bullet P[ac_0/ac'] \wedge \forall\, z \bullet z \notin ac_0) \\ \vee \\ (\exists\, ac_0 \bullet P[ac_0/ac'] \wedge (\forall\, z \bullet z \in ac_0 \Rightarrow Q[z/s]) \wedge ok') \end{array} \right)$$

{Property of sets and introduce set comprehension}

$$= \left(\begin{array}{l} (\exists\, ac_0 \bullet P[ac_0/ac'] \wedge ac_0 = \emptyset) \\ \vee \\ ((\exists\, ac_0 \bullet P[ac_0/ac'] \wedge ac_0 \subseteq \{z \mid Q[z/s]\}) \wedge ok') \end{array} \right)$$

{One-point rule and substitution}

$$= \left(\begin{array}{l} P[\emptyset/ac'] \\ \vee \\ ((\exists\, ac_0 \bullet P[ac_0/ac'] \wedge ac_0 \subseteq \{z \mid Q[z/s]\}) \wedge ok') \end{array} \right)$$

{Re-introduce ac'}

$$= \left(\begin{array}{l} P[\emptyset/ac'] \\ \vee \\ ((\exists\, ac_0 \bullet P[ac_0/ac'] \wedge ac_0 \subseteq ac')[\{z \mid Q[z/s]\}/ac'] \wedge ok') \end{array} \right)$$

{Definition of $;_{\mathcal{A}}$}

$$= \left(\begin{array}{l} P[\emptyset/ac'] \\ \vee \\ (((\exists\, ac_0 \bullet P[ac_0/ac'] \wedge ac_0 \subseteq ac') \;;_{\mathcal{A}}\; Q) \wedge ok') \end{array} \right)$$

{Definition of **PBMH** (Lemma E.1.1)}

$$= P[\emptyset/ac'] \vee ((\mathbf{PBMH}(P) \;;_{\mathcal{A}}\; Q) \wedge ok')$$

{Assumption: P is **PBMH**-healthy}

$$= P[\emptyset/ac'] \vee ((P \;;_{\mathcal{A}}\; Q) \wedge ok')$$

{Lemma F.4.1}

$$= (P \;;_{\mathcal{A}}\; \mathit{false}) \vee ((P \;;_{\mathcal{A}}\; Q) \wedge ok')$$

□

Lemma F.2.6 *Provided s is not free in R and P is* **PBMH***-healthy.*

$$(P \;;_{\mathcal{A}}\; (Q \wedge R)) \wedge R = (P \;;_{\mathcal{A}}\; Q) \wedge R$$

Proof.

$$(P \;;_{\mathcal{A}}\; (Q \wedge R)) \wedge R$$

{Assumption: P is **PBMH**-healthy (Lemma E.1.1)}

$= ((\exists\, ac_0 \bullet P[ac_0/ac'] \land ac_0 \subseteq ac')\ ;_{\mathcal{A}}\ (Q \land R)) \land R$
{Definition of $;_{\mathcal{A}}$ and substitution}

$= (\exists\, ac_0 \bullet P[ac_0/ac'] \land ac_0 \subseteq \{s \mid Q \land R\}) \land R$ {Property of sets}

$= \exists\, ac_0 \bullet P[ac_0/ac'] \land ac_0 \subseteq \{s \mid Q\} \land ac_0 \subseteq \{s \mid R\} \land R$
{Property of sets}

$= \exists\, ac_0 \bullet P[ac_0/ac'] \land ac_0 \subseteq \{s \mid Q\} \land (\forall\, s \bullet s \in ac_0 \Rightarrow R) \land R$
{Assumption: s is not free in R and predicate calculus}

$= \exists\, ac_0 \bullet P[ac_0/ac'] \land ac_0 \subseteq \{s \mid Q\} \land ((\forall\, s \bullet s \notin ac_0) \lor R) \land R$
{Predicate calculus: absorption law}

$= \exists\, ac_0 \bullet P[ac_0/ac'] \land ac_0 \subseteq \{s \mid Q\} \land R$ {Predicate calculus}

$= (\exists\, ac_0 \bullet P[ac_0/ac'] \land ac_0 \subseteq \{s \mid Q\}) \land R$
{Definition of $;_{\mathcal{A}}$ and substitution}

$= ((\exists\, ac_0 \bullet P[ac_0/ac'] \land ac_0 \subseteq ac')\ ;_{\mathcal{A}}\ Q) \land R$
{Assumption: P is **PBMH**-healthy (Lemma E.1.1)}

$= (P\ ;_{\mathcal{A}}\ Q) \land R$

□

Lemma F.2.7 *Provided ac' is not free in P.*

$$(P \land Q)\ ;_{\mathcal{A}}\ R = P \land (Q\ ;_{\mathcal{A}}\ R)$$

Proof.

$(P \land Q)\ ;_{\mathcal{A}}\ R$ {Lemma F.1.5}

$= (P\ ;_{\mathcal{A}}\ R) \land (Q\ ;_{\mathcal{A}}\ R)$
{Assumption: ac' not free in P and Lemma F.1.1}

$= P \land (Q\ ;_{\mathcal{A}}\ R)$

□

F.3 Closure properties

Theorem F.3.1 *Provided P and Q are* **PBMH***-healthy.*

$$\mathbf{PBMH}(P\ ;_{\mathcal{A}}\ Q) = P\ ;_{\mathcal{A}}\ Q$$

Proof. (Implication)

$$
\begin{array}{ll}
& \mathbf{PBMH}(P \ ;_{\mathcal{A}} Q) \qquad \{\text{Assumption: } P \text{ is } \mathbf{PBMH}\text{-healthy (Lemma E.1.1)}\} \\
= & \mathbf{PBMH}((\exists\, ac_1 \bullet P[ac_1/ac'] \wedge ac_1 \subseteq ac') \ ;_{\mathcal{A}} Q) \\
& \qquad \{\text{Definition of } ;_{\mathcal{A}} \text{ and substitution}\} \\
= & \mathbf{PBMH}(\exists\, ac_1 \bullet P[ac_1/ac'] \wedge ac_1 \subseteq \{s \mid Q\}) \qquad \{\text{Property of sets}\} \\
= & \mathbf{PBMH}(\exists\, ac_1 \bullet P[ac_1/ac'] \wedge (\forall\, z \bullet z \in ac_1 \Rightarrow Q[z/s])) \\
& \qquad \{\text{Definition of } \mathbf{PBMH} \text{ (Lemma E.1.1)}\} \\
= & \exists\, ac_0 \bullet (\exists\, ac_1 \bullet P[ac_1/ac'] \wedge (\forall\, z \bullet z \in ac_1 \Rightarrow Q[z/s]))[ac_0/ac'] \wedge ac_0 \subseteq ac' \\
& \qquad \{\text{Predicate calculus and substitution}\} \\
= & \exists\, ac_0, ac_1 \bullet P[ac_1/ac'] \wedge (\forall\, z \bullet z \in ac_1 \Rightarrow Q[z/s][ac_0/ac']) \wedge ac_0 \subseteq ac' \\
& \qquad \{\text{Predicate calculus: quantifier scope}\} \\
= & \exists\, ac_1 \bullet P[ac_1/ac'] \wedge (\exists\, ac_0 \bullet (\forall\, z \bullet z \in ac_1 \Rightarrow Q[z/s][ac_0/ac']) \wedge ac_0 \subseteq ac') \\
& \qquad \{\text{Predicate calculus: quantifier scope}\} \\
= & \exists\, ac_1 \bullet P[ac_1/ac'] \wedge (\exists\, ac_0 \bullet (\forall\, z \bullet (z \in ac_1 \Rightarrow Q[z/s][ac_0/ac']) \wedge ac_0 \subseteq ac')) \\
& \qquad \{\text{Predicate calculus}\} \\
= & \exists\, ac_1 \bullet \left(\begin{array}{l} P[ac_1/ac'] \\ \wedge \\ \exists\, ac_0 \bullet \left(\forall\, z \bullet \left(\begin{array}{l} (z \notin ac_1 \wedge ac_0 \subseteq ac') \\ \vee \\ (Q[z/s][ac_0/ac'] \wedge ac_0 \subseteq ac') \end{array} \right) \right) \end{array} \right) \\
& \qquad \{\text{Predicate calculus}\} \\
\Rightarrow & \exists\, ac_1 \bullet \left(\begin{array}{l} P[ac_1/ac'] \\ \wedge \\ \left(\forall\, z \bullet \exists\, ac_0 \bullet \left(\begin{array}{l} (z \notin ac_1 \wedge ac_0 \subseteq ac') \\ \vee \\ (Q[z/s][ac_0/ac'] \wedge ac_0 \subseteq ac') \end{array} \right) \right) \end{array} \right) \\
& \qquad \{\text{Predicate calculus}\} \\
= & \exists\, ac_1 \bullet \left(\begin{array}{l} P[ac_1/ac'] \\ \wedge \\ \left(\forall\, z \bullet \left(\begin{array}{l} (z \notin ac_1 \wedge \exists\, ac_0 \bullet ac_0 \subseteq ac') \\ \vee \\ (\exists\, ac_0 \bullet Q[z/s][ac_0/ac'] \wedge ac_0 \subseteq ac') \end{array} \right) \right) \end{array} \right) \\
& \qquad \{\text{Property of sets and predicate calculus}\}
\end{array}
$$

$$= \exists\, ac_1 \bullet \left(\begin{array}{l} P[ac_1/ac'] \\ \wedge \\ \left(\forall\, z \bullet \left(\begin{array}{l} (z \in ac_1) \\ \Rightarrow \\ (\exists\, ac_0 \bullet Q[z/s][ac_0/ac'] \wedge ac_0 \subseteq ac') \end{array} \right) \right) \end{array} \right)$$

{Substitution}

$$= \exists\, ac_1 \bullet \left(\begin{array}{l} P[ac_1/ac'] \\ \wedge \\ \left(\forall\, z \bullet \left(\begin{array}{l} (z \in ac_1) \\ \Rightarrow \\ (\exists\, ac_0 \bullet Q[ac_0/ac'] \wedge ac_0 \subseteq ac')[z/s] \end{array} \right) \right) \end{array} \right)$$

{Definition of **PBMH** (Lemma E.1.1)}

$$= \exists\, ac_1 \bullet P[ac_1/ac'] \wedge (\forall\, z \bullet z \in ac_1 \Rightarrow \mathbf{PBMH}(Q)[z/s])$$

{Property of sets}

$$= \exists\, ac_1 \bullet P[ac_1/ac'] \wedge ac_1 \subseteq \{s \mid \mathbf{PBMH}(Q)\}$$

{Definition of $;_{\mathcal{A}}$ and substitution}

$$= (\exists\, ac_1 \bullet P[ac_1/ac'] \wedge ac_1 \subseteq ac') \;;_{\mathcal{A}} \mathbf{PBMH}(Q)$$

{Definition of **PBMH** (Lemma E.1.1)}

$$= \mathbf{PBMH}(P) \;;_{\mathcal{A}} \mathbf{PBMH}(Q)$$

{Assumption: P and Q are **PBMH**-healthy (Lemma E.1.1)}

$$= P \;;_{\mathcal{A}} Q$$

□

Proof. (Reverse implication)

$$P \;;_{\mathcal{A}} Q \qquad \{\text{Lemma E.2.1}\}$$
$$\Rightarrow \mathbf{PBMH}(P \;;_{\mathcal{A}} Q)$$

□

F.4 Extreme points

Lemma F.4.1 ($;_{\mathcal{A}}$-P-sequence-*false*:1) *Provided P is* **PBMH**-*healthy.*

$$P \;;_{\mathcal{A}} \mathbf{false} = P[\emptyset/ac']$$

Proof.

$$
\begin{array}{lr}
P \ ;_{\mathcal{A}} \mathbf{false} & \{\text{Assumption: } P \text{ is } \mathbf{PBMH}\text{-healthy}\} \\
= \mathbf{PBMH}(P) \ ;_{\mathcal{A}} \mathit{false} & \{\text{Definition of } \mathbf{PBMH} \text{ (Lemma E.1.1)}\} \\
= (\exists\, ac_0 \bullet P[ac_0/ac'] \wedge ac_0 \subseteq ac') \ ;_{\mathcal{A}} \mathit{false} & \{\text{Definition of } ;_{\mathcal{A}}\} \\
= \exists\, ac_0 \bullet P[ac_0/ac'] \wedge ac_0 \subseteq \emptyset & \{\text{Property of sets and one-point rule}\} \\
= P[\emptyset/ac']
\end{array}
$$

□

Lemma F.4.2 ($;_{\mathcal{A}}$-P-sequence-*true*) *Provided P is* **PBMH***-healthy.*

$$P \ ;_{\mathcal{A}} \mathbf{true} = \exists\, ac' \bullet P$$

Proof.

$$
\begin{array}{lr}
P \ ;_{\mathcal{A}} \mathbf{true} & \{\text{Assumption: } P \text{ is } \mathbf{PBMH}\text{-healthy}\} \\
= \mathbf{PBMH}(P) \ ;_{\mathcal{A}} \mathit{true} & \{\text{Lemma E.1.1}\} \\
= (\exists\, ac_0 \bullet P[ac_0/ac'] \wedge ac_0 \subseteq ac') \ ;_{\mathcal{A}} \mathit{true} & \{\text{Definition of } ;_{\mathcal{A}}\} \\
= \exists\, ac_0 \bullet P[ac_0/ac'] \wedge ac_0 \subseteq \{z \mid \mathit{true}\} & \{\text{Property of sets}\} \\
= \exists\, ac_0 \bullet P[ac_0/ac'] \wedge (\forall\, z \bullet z \in ac_0 \Rightarrow \mathit{true}) & \{\text{Propositional calculus}\} \\
= \exists\, ac_0 \bullet P[ac_0/ac'] & \{\text{One-point rule}\} \\
= \exists\, ac_0 \bullet (\exists\, ac' \bullet P \wedge ac' = ac_0) & \{\text{One-point rule: } ac_0 \text{ not free in } P\} \\
= \exists\, ac' \bullet P
\end{array}
$$

□

F.5 Algebraic properties and sequential composition

Law F.5.1 ($;_{\mathcal{A}}$-sequence-left-associativity) *Provided ok and ac are not free in R.*

$$(P \ ; \ Q) \ ;_{\mathcal{A}} R = P \ ; (Q \ ;_{\mathcal{A}} R)$$

Proof.

$$
\begin{array}{ll}
(P \;;\; Q) \;;_{\mathcal{A}} R & \{\text{Definition of sequential composition}\} \\
= (\exists\, ok_0, ac_0 \bullet P[ok_0, ac_0/ok, ac'] \wedge Q[ok_0, ac_0/ok, ac]) \;;_{\mathcal{A}} R & \\
& \{\text{Definition of } ;_{\mathcal{A}}\} \\
= (\exists\, ok_0, ac_0 \bullet P[ok_0, ac_0/ok, ac'] \wedge Q[ok_0, ac_0/ok, ac])[\{z \mid R[z/s]\}/ac'] & \\
& \{\text{Substitution: } ac' \text{ not free in } ac_0\} \\
= (\exists\, ok_0, ac_0 \bullet P[ok_0, ac_0/ok, ac'] \wedge Q[ok_0, ac_0/ok, ac][\{z \mid R[z/s]\}/ac']) & \\
& \{\text{Assumption: } \{ok, ac\} \text{ not free in } R\} \\
= (\exists\, ok_0, ac_0 \bullet P[ok_0, ac_0/ok, ac'] \wedge Q[\{z \mid R[z/s]\}/ac'][ok_0, ac_0/ok, ac]) & \\
& \{\text{Definition of sequential composition}\} \\
= P \;;\; Q[\{z \mid R[z/s]\}/ac'] & \{\text{Definition of } ;_{\mathcal{A}}\} \\
= P \;;\; (Q \;;_{\mathcal{A}} R) &
\end{array}
$$

□

F.6 Skip

Definition 26

$$\mathbb{I}_{\mathcal{A}} \mathrel{\widehat{=}} s \in ac'$$

Lemma F.6.1 *$\mathbb{I}_{\mathcal{A}}$ is a fixed point of* **PBMH**.

$$\mathbf{PBMH}(\mathbb{I}_{\mathcal{A}}) = \mathbb{I}_{\mathcal{A}}$$

Proof.

$$
\begin{array}{ll}
\mathbf{PBMH}(\mathbb{I}_{\mathcal{A}}) & \{\text{Definition of } \mathbb{I}_{\mathcal{A}} \text{ and } \mathbf{PBMH} \text{ (Lemma E.1.1)}\} \\
= \exists\, ac_0 \bullet s \in ac_0 \wedge ac_0 \subseteq ac' & \{\text{Law H.1.13}\} \\
= s \in ac' &
\end{array}
$$

□

Lemma F.6.2 ($;_{\mathcal{A}}$-$\mathbb{I}_{\mathcal{A}}$-left-unit)

$$\mathbb{I}_{\mathcal{A}} \;;_{\mathcal{A}} P = P$$

Proof.

$$
\begin{array}{ll}
\Pi_{\mathcal{A}} \ ;_{\mathcal{A}} P & \{\text{Definition of } \Pi_{\mathcal{A}}\} \\
= s \in ac' \ ;_{\mathcal{A}} P & \{\text{Definition of } ;_{\mathcal{A}} \text{ and substitution}\} \\
= s \in \{z \mid P[z/s]\} & \{\text{Property of sets}\} \\
= P[z/s][s/z] & \{\text{Substitution}\} \\
= P &
\end{array}
$$

□

Law F.6.1 ($;_{\mathcal{A}}$-$\Pi_{\mathcal{A}}$-right-unit) *Provided P is* **PBMH***-healthy.*

$$P \ ;_{\mathcal{A}} \Pi_{\mathcal{A}}$$

Proof.

$$
\begin{array}{ll}
P \ ;_{\mathcal{A}} \Pi_{\mathcal{A}} & \{\text{Definition of } \Pi_{\mathcal{A}}\} \\
= P \ ;_{\mathcal{A}} (s \in ac') & \{\text{Assumption: } P \text{ is } \mathbf{PBMH}\text{-healthy}\} \\
= \mathbf{PBMH}(P) \ ;_{\mathcal{A}} (s \in ac') & \{\text{Lemma E.1.1}\} \\
= (\exists\, ac_0 \bullet P[ac_0/ac'] \land ac_0 \subseteq ac') \ ;_{\mathcal{A}} (s \in ac') & \{\text{Definition of } ;_{\mathcal{A}}\} \\
= \exists\, ac_0 \bullet P[ac_0/ac'] \land ac_0 \subseteq \{z \mid z \in ac'\} & \{\text{Property of sets}\} \\
= \exists\, ac_0 \bullet P[ac_0/ac'] \land ac_0 \subseteq ac' & \{\text{Lemma E.1.1}\} \\
= \mathbf{PBMH}(P) & \{\text{Assumption: } P \text{ satisfies } \mathbf{PBMH}\} \\
= P &
\end{array}
$$

□

Appendix G

State substitution rules

G.1 State substitution

Definition 27 *The substitution of the variables in the set $S\alpha$ for state components of $\mathbf{z}$ ranges over the variables in $S\alpha$. It is important to note that if z is defined as $z : State(T\alpha)$, then it must be the case that $S\alpha \subseteq T\alpha$.*

$$P[\mathbf{z}/S\alpha] \mathrel{\widehat{=}} P[z.s_0, \ldots, x.s_n/s_0, \ldots, s_n]$$

Provided $S\alpha = \{s_0, \ldots, s_n\}$.

Lemma G.1.1 *Provided that $A\alpha \cap B\alpha = \emptyset$, $A\alpha \subseteq S\alpha$ and $B\alpha \subseteq S\alpha$.*

$$P[\mathbf{z}/S\alpha] = P[\mathbf{z}/A\alpha][\mathbf{z}/B\alpha]$$

Proof. Suppose:

- $S\alpha = \{s_0, \ldots, s_n, \ldots, s_m\}$, $A\alpha = \{s_0, \ldots, s_n\}$, $B\alpha = \{s_{n+1}, \ldots, s_m\}$

Then:

$$\begin{aligned}
&P[\mathbf{z}/S\alpha] && \{\text{Definition 27}\}\\
&= P[z.s_0, \ldots, z.s_n, z.s_{n+1}, \ldots, s_m/s_0, \ldots, s_n, s_{n+1}, \ldots, s_m] \\
& && \{\text{Property of substitution}\}\\
&= P[z.s_0, \ldots, z.s_n/s_0, \ldots, s_n][z.s_{n+1}, \ldots, s_m/s_{n+1}, \ldots, s_m] && \{\text{Definition 27}\}\\
&= P[\mathbf{z}/A\alpha][\mathbf{z}/B\alpha]
\end{aligned}$$

□

Lemma G.1.2 *Provided that* $A\alpha \cap B\alpha = \emptyset$, $A\alpha \subseteq S\alpha$ *and* $B\alpha \subseteq S\alpha$.

$$P[\mathbf{z}/S\alpha] = \left(\begin{array}{l} \exists\, z_A, z_B \bullet P[\mathbf{z}_A/A\alpha][\mathbf{z}_B/B\alpha] \\ \land \\ (\bigwedge x : A\alpha \bullet z_A.x = z.x) \land (\bigwedge x : B\alpha \bullet z_B.x = z.x) \end{array} \right)$$

Proof. Suppose:

- $S\alpha = \{s_0, \ldots, s_n, \ldots, s_m\}$, $A\alpha = \{s_0, \ldots, s_n\}$, $B\alpha = \{s_{n+1}, \ldots, s_m\}$

Then:

$$\left(\begin{array}{l} \exists\, z_A : \mathit{State}(A\alpha), z_B : \mathit{State}(B\alpha) \bullet P[\mathbf{z}_A/A\alpha][\mathbf{z}_B/B\alpha] \\ \land \\ (\bigwedge x : A\alpha \bullet z_A.x = z.x) \land (\bigwedge x : B\alpha \bullet z_B.x = z.x) \end{array} \right)$$

{Predicate calculus}

$$= \left(\begin{array}{l} \exists\, z_A : \mathit{State}(A\alpha), z_B : \mathit{State}(B\alpha) \bullet P[\mathbf{z}_A/A\alpha][\mathbf{z}_B/B\alpha] \\ \land \\ (z_A.s_0 = z.s_0 \land \ldots \land z_A.s_n = z.s_n) \\ \land \\ (z_B.s_{n+1} = z.s_{n+1} \land \ldots \land z_B.s_m = z.s_m) \end{array} \right)$$

{Definition 27}

$$= \left(\begin{array}{l} \exists\, z_A : \mathit{State}(A\alpha), z_B : \mathit{State}(B\alpha) \bullet \\ P[z_A.s_0, \ldots, z_A.s_n/s_0, \ldots, s_n][z_B.s_{n+1}, \ldots, z_B.s_m/s_{n+1}, \ldots, s_m] \\ \land \\ (z_A.s_0 = z.s_0 \land \ldots \land z_A.s_n = z.s_n) \\ \land \\ (z_B.s_{n+1} = z.s_{n+1} \land \ldots \land z_B.s_m = z.s_m) \end{array} \right)$$

{Equality of records}

$$= \left(\begin{array}{l} \exists\, z_A : \mathit{State}(A\alpha), z_B : \mathit{State}(B\alpha) \bullet \\ P[z_A.s_0, \ldots, z_A.s_n/s_0, \ldots, s_n][z_B.s_{n+1}, \ldots, z_B.s_m/s_{n+1}, \ldots, s_m] \\ \land \\ z_A = \{s_0 \mapsto z.s_0, \ldots, s_n \mapsto z.s_n\} \\ \land \\ z_B = \{s_{n+1} \mapsto z.s_{n+1}, \ldots, s_m \mapsto z.s_m\} \end{array} \right)$$

{One-point rule and substitution}

$$= P\left[\begin{array}{l} \left\{\begin{array}{l} s_0 \mapsto z.s_0, \\ \ldots, \\ s_n \mapsto z.s_n \end{array}\right\}.s_0, \ldots, \left\{\begin{array}{l} s_0 \mapsto z.s_0, \\ \ldots, \\ s_n \mapsto z.s_n \end{array}\right\}.s_n \Big/ s_0, \ldots, s_n \\ \left\{\begin{array}{l} s_{n+1} \mapsto z.s_{n+1}, \\ \ldots, \\ s_m \mapsto z.s_m \end{array}\right\}.s_{n+1}, \ldots, \left\{\begin{array}{l} s_{n+1} \mapsto z.s_{n+1}, \\ \ldots, \\ s_m \mapsto z.s_m \end{array}\right\}.s_m \Big/ s_{n+1}, \ldots, s_m \end{array}\right]$$

{Record component}

$= P[z.s_0, \ldots, z.s_n/s_0, \ldots, s_n][z.s_{n+1}, \ldots, z.s_m/s_{n+1}, \ldots, s_m]$

{Definition 27}

$= P[\mathbf{z}/A\alpha][\mathbf{z}/B\alpha]$ {Lemma G.1.1}

$= P[\mathbf{z}/S\alpha]$

□

Lemma G.1.3 *Provided $z, y : State(S\alpha)$.*

$$P[\mathbf{z}/S\alpha][y \oplus \{s_i \mapsto e\}/z] = P[\mathbf{y}/(S\alpha \setminus \{s_i\})][e/s_i]$$

Proof.

$P[\mathbf{z}/S\alpha][y \oplus \{s_i \mapsto e\}/z]$ {Definition 27}

$= P[z.s_0, \ldots, z.s_i, \ldots, z.s_n/s_0, \ldots, s_i, \ldots, s_n][y \oplus \{s_i \mapsto e\}/z]$

{Substitution}

$= P[(y \oplus \{s_i \mapsto e\}).s_0, \ldots, (y \oplus \{s_i \mapsto e\}).s_i, \ldots, (y \oplus \{s_i \mapsto e\}).s_n/s_0, \ldots, s_i, \ldots, s_n]$

{Property of record components}

$= P[y.s_0, \ldots, e, \ldots, y.s_n/s_0, \ldots, s_i, \ldots, s_n]$ {Property of substitution}

$= P[y.s_0, \ldots, y.s_n/s_0, \ldots, s_n][e/s_i]$ {Definition 27}

$= P[\mathbf{y}/(S\alpha \setminus \{s_i\})][e/s_i]$

□

Lemma G.1.4 *Provided $z, y : State(S\alpha)$ and s_i not free in e.*

$$P[\mathbf{z}/S\alpha][y \oplus \{s_i \mapsto e\}/z] = P[e/s_i][\mathbf{y}/(S\alpha)]$$

Proof.

$P[\mathbf{z}/S\alpha][y \oplus \{s_i \mapsto e\}/z]$ {Definition 27}

$$
\begin{aligned}
&= P[z.s_0, \ldots, z.s_i, \ldots, z.s_n / s_0, \ldots, s_i, \ldots, s_n][y \oplus \{s_i \mapsto e\}/z] \\
&\qquad \{\text{Substitution}\} \\
&= P[(y \oplus \{s_i \mapsto e\}).s_0, \ldots, (y \oplus \{s_i \mapsto e\}).s_i, \ldots, (y \oplus \{s_i \mapsto e\}).s_n / s_0, \ldots, s_i, \ldots, s_n] \\
&\qquad \{\text{Property of record components}\} \\
&= P[y.s_0, \ldots, e, \ldots, y.s_n / s_0, \ldots, s_i, \ldots, s_n] \qquad \{\text{Property of substitution}\} \\
&= P[e/s_i][y.s_0, \ldots, y.s_n / s_0, \ldots, s_n] \qquad \{\text{Substitution: } s_i \text{ not free in } e\} \\
&= P[e/s_i][z.s_0, \ldots, z.s_i, \ldots, z.s_n / s_0, \ldots, s_i, \ldots, s_n] \qquad \{\text{Definition 27}\} \\
&= P[e/s_i][\mathbf{y}/S\alpha]
\end{aligned}
$$

□

Lemma G.1.5 *Provided* $s_i \in S\alpha$

$$P[e/s_i][\mathbf{z}/S\alpha] = P[\mathbf{z}/S\alpha \setminus \{s_i\}][e[\mathbf{z}/S\alpha]/s_i]$$

Proof.

$$
\begin{aligned}
&P[e/s_i][\mathbf{z}/S\alpha] \qquad \{\text{Definition 27}\} \\
&= P[e/s_i][z.s_0, \ldots, z.s_i, \ldots, z.s_n / s_0, \ldots, s_i, \ldots, s_n] \\
&\qquad \{\text{Substitution: } s_i \text{ not free in } P\} \\
&= P[z.s_0, \ldots, z.s_n / s_0, \ldots, s_n][e[z.s_0, \ldots, z.s_i, \ldots, z.s_n / s_0, \ldots, s_i, \ldots, s_n]/s_i] \\
&\qquad \{\text{Definition 27}\} \\
&= P[\mathbf{z}/S\alpha \setminus \{s_i\}][e[\mathbf{z}/S\alpha]/s_i]
\end{aligned}
$$

□

Lemma G.1.6

$$P[z/(S\alpha \cup T\alpha)] = P[z/S\alpha][z/T\alpha]$$

Proof.

$$
\begin{aligned}
&P[z/(S\alpha \cup T\alpha)] \qquad \{\text{Definition 27}\} \\
&= P[z.s_0, z.t_0, \ldots, z.s_n, z.t_n / s'_0, t'_0, \ldots, s'_n, t'_n] \qquad \{\text{Substitution}\} \\
&= P[z.s_0, \ldots, z.s_n / s'_0, \ldots, s'_n][z.t_0, \ldots, z.t_n / t'_0, \ldots, t'_n] \qquad \{\text{Definition 27}\} \\
&= P[z/S\alpha][z/T\alpha]
\end{aligned}
$$

□

Lemma G.1.7

$$P[e_0, \ldots, e_n/x_0, \ldots, x_n][z/S\alpha]$$
$$=$$
$$P[z/(S\alpha \setminus T\alpha)][e_0[z/T\alpha], \ldots, e_n[z/T\alpha]/x_0, \ldots, x_n]$$

Provided that:

1. $T\alpha \subseteq S\alpha$
2. $T\alpha = \{x_0, \ldots, x_n\}$
3. $\forall\, y \bullet y \in (S\alpha \setminus T\alpha) \Rightarrow y \notin fv(e_0, \ldots, e_n)$

Proof.

$$\begin{aligned}
&P[e_0, \ldots, e_n/x_0, \ldots, x_n][z/S\alpha] && \{\text{Property of sets}\}\\
&= P[e_0, \ldots, e_n/x_0, \ldots, x_n][z/(S\alpha \setminus T\alpha) \cup T\alpha] && \{\text{Lemma G.1.6}\}\\
&= P[e_0, \ldots, e_n/x_0, \ldots, x_n][z/(S\alpha \setminus T\alpha)][z/T\alpha] \\
& && \{\text{Substitution: Assumption 1}\}\\
&= P[z/(S\alpha \setminus T\alpha)][e_0, \ldots, e_n/x_0, \ldots, x_n][z/T\alpha] && \{\text{Substitution}\}\\
&= P[z/(S\alpha \setminus T\alpha)][e_0[z/T\alpha], \ldots, e_n[z/T\alpha]/x_0, \ldots, x_n] \\
& && \{\text{Property of substitution}\}\\
&= P[z/(S\alpha \setminus T\alpha)][z/T\alpha][T\alpha/z][e_0[z/T\alpha], \ldots, e_n[z/T\alpha]/x_0, \ldots, x_n] \\
& && \{\text{Lemma G.1.6}\}\\
&= P[z/(S\alpha \setminus T\alpha) \cup T\alpha][T\alpha/z][e_0[z/T\alpha], \ldots, e_n[z/T\alpha]/x_0, \ldots, x_n] \\
& && \{\text{Property of sets}\}\\
&= P[z/S\alpha][T\alpha/z][e_0[z/T\alpha], \ldots, e_n[z/T\alpha]/x_0, \ldots, x_n] && \{\text{Definition}\}\\
&= P[z/S\alpha][x_0, \ldots, x_n/z.x, \ldots, z.n][e_0[z/T\alpha], \ldots, e_n[z/T\alpha]/x_0, \ldots, x_n] \\
& && \{\text{Property of substitution}\}\\
&= P[z/S\alpha][e_0[z/T\alpha], \ldots, e_n[z/T\alpha]/z.x, \ldots, z.n] && \{\text{Definition}\}\\
&= P[z/S\alpha][e_0[z/T\alpha], \ldots, e_n[z/T\alpha]/z.x, \ldots, z.n]
\end{aligned}$$

□

G.2 Substitution additions

Definition 28 *For* $S\alpha = \{x_0, \ldots, x_n\}$

$$State_{\mathtt{II}}(S\alpha) \mathrel{\widehat{=}} \{x_0 \mapsto x_0, \ldots, x_n \mapsto x_n\}$$

Lemma G.2.1

$$State_{\mathtt{II}}(S\alpha)' = \{x_0' \mapsto x_0, \ldots, x_n' \mapsto x_n\}$$

Proof.

$$\begin{array}{ll} State_{\mathtt{II}}(S\alpha)' & \{\text{Definition of } State_{\mathtt{II}}(S\alpha)\} \\ = (\{x_0' \mapsto x_0, \ldots, x_n' \mapsto x_n\})' & \{\text{Definition of } ' \text{ on } State\} \\ = \{x_0' \mapsto x_0, \ldots, x_n' \mapsto x_n\} & \end{array}$$

□

Lemma G.2.2

$$\exists\, z : State(S\alpha) \bullet P \wedge (\bigwedge x : S\alpha \bullet z.x = x) = P[State_{\mathtt{II}}(S\alpha)/z]$$

Proof.

$$\begin{array}{ll} \exists\, z : State(S\alpha) \bullet P \wedge (\bigwedge x : S\alpha \bullet z.x = x) & \{\text{Equality of records}\} \\ = \exists\, z : State(S\alpha) \bullet P \wedge z = \{x_0 \mapsto x_0, \ldots, x_n \mapsto x_n\} & \\ & \{\text{Definition of } State_{\mathtt{II}}\} \\ = \exists\, z : State(S\alpha) \bullet P \wedge State_{\mathtt{II}}(S\alpha) = z & \{\text{One-point rule}\} \\ = P[State_{\mathtt{II}}(S\alpha)/z] & \end{array}$$

□

Lemma G.2.3 *Provided* z *is not free in* P

$$P[\mathbf{z}/S\alpha][State_{\mathtt{II}}(S\alpha)/z] = P$$

Proof.

$$
\begin{aligned}
& P[\mathbf{z}/S\alpha][\mathit{State}_{\mathit{II}}(S\alpha)/z] && \{\text{Definition of state substitution}\}\\
&= P[z.x_0, \ldots, z.x_n/x_0, \ldots, x_n][\mathit{State}_{\mathit{II}}(S\alpha)/z] \\
& && \{\text{Definition of } \mathit{State}_{\mathit{II}}(S\alpha)\}\\
&= P[z.x_0, \ldots, z.x_n/x_0, \ldots, x_n][\{x_0 \mapsto x_0, \ldots, x_n \mapsto x_n\}/z] \\
& && \{\text{Substitution: } z \text{ is not free in } P\}\\
&= P[\{x_0 \mapsto x_0, \ldots, x_n \mapsto x_n\}.x_0, \ldots, \{x_0 \mapsto x_0, \ldots, x_n \mapsto x_n\}.x_n/x_0, \ldots, x_n] \\
& && \{\text{Value of state component}\}\\
&= P[x_0, \ldots, x_n/x_0, \ldots, x_n] && \{\text{Property of substitution}\}\\
&= P
\end{aligned}
$$

□

Lemma G.2.4 *Provided none of the varibles in $S\alpha$ are free in P*

$$P[\mathit{State}_{\mathit{II}}(S\alpha)/z][\mathbf{z}/S\alpha] = P$$

Proof.

$$
\begin{aligned}
& P[\mathit{State}_{\mathit{II}}(S\alpha)/z][\mathbf{z}/S\alpha] \\
& && \{\text{Definition of } \mathit{State}_{\mathit{II}}(S\alpha) \text{ and state substitution}\}\\
&= P[\{x_0 \mapsto x_0, \ldots, x_n \mapsto x_n\}/z][z.x_0, \ldots, z.x_n/x_0, \ldots, x_n] \\
& && \{\text{Substitution: } x_i \notin fv(P)\}\\
&= P[\{x_0 \mapsto z.x_0, \ldots, x_n \mapsto z.x_n\}/z] && \{\text{Equality of records}\}\\
&= P[z/z] && \{\text{Property of substitution}\}\\
&= P
\end{aligned}
$$

□

Lemma G.2.5 *Provided $x_i \in S\alpha$ and x_i is not free in P nor in e.*

$$P[\mathit{State}_{\mathit{II}}(S\alpha)/z][e/x_i] = P[z \oplus x_i \mapsto e\}/z][\mathit{State}_{\mathit{II}}(S\alpha)/z]$$

Proof.

$$
\begin{aligned}
& P[\mathit{State}_{\mathit{II}}(S\alpha)/z][e/x_i] && \{\text{Definition of } \mathit{State}_{\mathit{II}}(S\alpha)\}\\
&= P[\{x_0 \mapsto x_0, \ldots, x_i \mapsto x_i, \ldots, x_n \mapsto x_n\}/z][e/x_i] \\
& && \{\text{Substitution: } x_i \text{ not free in } P\}
\end{aligned}
$$

$= P[\{x_0 \mapsto x_0, \ldots, x_i \mapsto e, \ldots, x_n \mapsto x_n\}/z]$ {Property of sets}

$= P[\{x_0 \mapsto x_0, \ldots, x_i \mapsto x_i, \ldots, x_n \mapsto x_n\} \oplus \{x_i \mapsto e\}/z]$ {Definition of $State_{II}(S\alpha)$}

$= P[State_{II}(S\alpha) \oplus \{x_i \mapsto e\}/z]$ {Substitution}

$= P[z \oplus \{x_i \mapsto e\}/z][State_{II}(S\alpha)/z]$

□

G.3 Dash and undash

Definition 29 (*dash*)

$$dash(z) \mathrel{\widehat{=}} \{x, e \mid (x \mapsto e) \in z \bullet x' \mapsto e\}$$

Definition 30 (*undash*)

$$undash(z) \mathrel{\widehat{=}} \{x, e \mid (x' \mapsto e) \in z \bullet x \mapsto e\}$$

Lemma G.3.1

$$undash(z).x = z.x'$$

Proof.

□

Lemma G.3.2

$$dash(z).x' = z.x$$

Proof.

□

Lemma G.3.3 *Provided y is fresh.*

$$\exists\, z \bullet P \wedge undash(z) \in ac' = \exists\, y \bullet P[dash(y)/z] \wedge y \in ac'$$

Proof.

$$
\begin{aligned}
&\exists\, z \bullet P \wedge undash(z) \in ac' && \{\text{Introduce fresh variable}\}\\
&= \exists\, z, y \bullet P \wedge y \in ac' \wedge y = undash(z) && \{\text{Property of } dash\}\\
&= \exists\, z, y \bullet P \wedge y \in ac' \wedge dash(y) = dash \circ undash(z) && \{dash \circ undash(z) = z\}\\
&= \exists\, z, y \bullet P \wedge y \in ac' \wedge dash(y) = z && \{\text{One-point rule}\}\\
&= \exists\, y \bullet P[dash(y)/z] \wedge y \in ac'
\end{aligned}
$$

□

Appendix H

Set theory

H.1 Lemmas

Auxiliary properties related to sets and generalized set intersection.

Lemma H.1.1 *Provided A is of type $\mathbb{P}\ T$ and x not free in p.*

$$\bigcap(A \cap \{x : \mathbb{P}\ T \mid p\}) = B \Leftrightarrow (\bigcap A = B \land p) \lor (\emptyset = B \land \neg\ p)$$

Proof.

$$\begin{array}{ll}
\bigcap(A \cap \{x : \mathbb{P}\ T \mid p\}) = B & \{\text{Introduce fresh variables}\} \\
\Leftrightarrow \exists\ Y : \mathbb{P}\ T \bullet \bigcap Y = B \land\ Y = (A \cap \{x : T \mid p\}) & \{\text{Lemma H.1.3}\} \\
\Leftrightarrow \exists\ Y : \mathbb{P}\ T \bullet \bigcap Y = B \land ((p \land\ Y = A) \lor (\neg\ p \land\ Y = \emptyset)) & \\
& \{\text{Predicate calculus}\} \\
\Leftrightarrow \left(\begin{array}{l} (\exists\ Y : \mathbb{P}\ T \bullet \bigcap Y = B \land p \land\ Y = A) \\ \lor \\ (\exists\ Y : \mathbb{P}\ T \bullet \bigcap Y = B \land \neg\ p \land\ Y = \emptyset) \end{array} \right) & \{\text{One-point rule}\} \\
\Leftrightarrow (\bigcap A = B \land p) \lor (\emptyset = B \land \neg\ p) &
\end{array}$$

□

Lemma H.1.2 *Provided x is not free in P.*

$$A = \{x : T \mid p\} \Leftrightarrow (p \land A = T) \lor (\neg\ p \land A = \emptyset)$$

Proof.

$$
\begin{array}{ll}
A = \{x : T \mid p\} & \{\text{Equivalence of sets}\} \\
\Leftrightarrow (\forall\, x : T \bullet x \in A \Leftrightarrow x \in \{x : T \mid p\}) & \{\text{Property of sets}\} \\
\Leftrightarrow (\forall\, x : T \bullet x \in A \Leftrightarrow p) & \{\text{Predicate calculus}\} \\
\Leftrightarrow (\forall\, x : T \bullet x \in A \Rightarrow p) \land (\forall\, x : T \bullet p \Rightarrow x \in A) & \{\text{Predicate calculus}\} \\
\Leftrightarrow (\forall\, x : T \bullet \neg\, p \Rightarrow x \notin A) \land (\forall\, x : T \bullet p \Rightarrow x \in A) & \{\text{Predicate calculus}\} \\
\Leftrightarrow (p \lor \forall\, x : T \bullet x \notin A) \land (\neg\, p \lor \forall\, x : T \bullet x \in A) & \{\text{Property of sets}\} \\
\Leftrightarrow (p \lor A = \emptyset) \land (\neg\, p \lor A = T) & \{\text{Predicate calculus}\} \\
\Leftrightarrow (p \land A = T) \lor (\neg\, p \land A = \emptyset) &
\end{array}
$$

□

Lemma H.1.3 *Provided A is of type T and x not free in p.*

$$A \cap \{x : T \mid p\} = B \Leftrightarrow (p \land B = A) \lor (\neg\, p \land B = \emptyset)$$

Proof.

$$
\begin{array}{ll}
A \cap \{x : T \mid p\} = B & \{\text{Predicate calculus: introduce fresh variable}\} \\
\Leftrightarrow \exists\, C : T \bullet (A \cap C) = B \land C = \{x : T \mid p\} & \{\text{Lemma H.1.2}\} \\
\Leftrightarrow \exists\, C : T \bullet (A \cap C) = B \land ((p \land C = T) \lor (\neg\, p \land C = \emptyset)) & \\
 & \{\text{Predicate calculus}\} \\
\Leftrightarrow \left(\begin{array}{l} (\exists\, C : T \bullet (A \cap C) = B \land p \land C = T) \\ \lor \\ (\exists\, C : T \bullet (A \cap C) = B \land \neg\, p \land C = \emptyset) \end{array} \right) & \{\text{One-point rule}\} \\
\Leftrightarrow ((A \cap T) = B \land p) \lor ((A \cap \emptyset) = B \land \neg\, p) & \{\text{Property of sets}\} \\
\Leftrightarrow (p \land B = A) \lor (\neg\, p \land B = \emptyset) &
\end{array}
$$

□

Lemma H.1.4 *Provided A is of type $\mathbb{P}\, T$.*

$$A \cup \{x : T \mid p\} = B \Leftrightarrow (p \land B = T) \lor (\neg\, p \land B = A)$$

Proof.

$$A \cup \{x : T \mid p\} = B \qquad \{\text{Predicate calculus: introduce fresh variable}\}$$

$\Leftrightarrow \exists\, C : T \bullet (A \cup C) = B \wedge C = \{x : T \mid p\}$ {Lemma H.1.2}

$\Leftrightarrow \exists\, C : T \bullet (A \cup C) = B \wedge ((p \wedge C = T) \vee (\neg\, p \wedge C = \emptyset))$
{Predicate calculus}

$$\Leftrightarrow \left(\begin{array}{l} (\exists\, C : T \bullet (A \cup C) = B \wedge p \wedge C = T) \\ \vee \\ (\exists\, C : T \bullet (A \cup C) = B \wedge \neg\, p \wedge C = \emptyset) \end{array} \right)$$ {One-point rule}

$\Leftrightarrow ((A \cup T) = B \wedge p) \vee ((A \cup \emptyset) = B \wedge \neg\, p)$ {Property of sets}

$\Leftrightarrow (p \wedge B = T) \vee (\neg\, p \wedge B = A)$

□

Lemma H.1.5

$$ac_0 \subseteq \{s \mid \{s\} = ac_1\} = ac_0 \subseteq ac_1 \wedge ac_0 \subseteq \{s \mid ac_1 \subseteq \{s\}\}$$

Proof.

$ac_0 \subseteq \{s \mid \{s\} = ac_1\}$ {Definition of subset inclusion}

$= \forall\, x \bullet x \in ac_0 \Rightarrow x \in \{s \mid \{s\} = ac_1\}$ {Property of sets}

$= \forall\, x \bullet x \in ac_0 \Rightarrow \{x\} = ac_1$ {Property of sets}

$= \forall\, x \bullet x \in ac_0 \Rightarrow (\{x\} \subseteq ac_1 \wedge ac_1 \subseteq \{x\})$ {Property of sets}

$= \forall\, x \bullet x \in ac_0 \Rightarrow (x \in ac_1 \wedge ac_1 \subseteq \{x\})$ {Predicate calculus}

$= (\forall\, x \bullet x \in ac_0 \Rightarrow x \in ac_1) \wedge (\forall\, x \bullet x \in ac_0 \Rightarrow ac_1 \subseteq \{x\})$
{Property of sets}

$= (\forall\, x \bullet x \in ac_0 \Rightarrow x \in ac_1) \wedge (\forall\, x \bullet x \in ac_0 \Rightarrow x \in \{s \mid ac_1 \subseteq \{s\}\}$
{Definition of subset inclusion}

$= ac_0 \subseteq ac_1 \wedge ac_0 \subseteq \{s \mid ac_1 \subseteq \{s\}\}$

□

Lemma H.1.6

$$ac_0 \subseteq \{s \mid ac_1 \subseteq \{s\}\} = ac_1 \subseteq \{s \mid ac_0 \subseteq \{s\}\}$$

Proof.

$ac_0 \subseteq \{s \mid ac_1 \subseteq \{s\}\}$ {Definition of subset inclusion}

$= \forall\, x \bullet x \in ac_0 \Rightarrow x \in \{s \mid ac_1 \subseteq \{s\}\}$ {Property of sets}
$= \forall\, x \bullet x \in ac_0 \Rightarrow ac_1 \subseteq \{x\}$ {Definition of subset inclusion}
$= \forall\, x \bullet x \in ac_0 \Rightarrow (\forall\, y \bullet y \in ac_1 \Rightarrow y \in \{x\})$ {Property of sets}
$= \forall\, x \bullet x \in ac_0 \Rightarrow (\forall\, y \bullet y \in ac_1 \Rightarrow y = x)$ {Predicate calculus}
$= \forall\, x, y \bullet x \in ac_0 \Rightarrow (y \in ac_1 \Rightarrow y \in y = x)$ {Predicate calculus}
$= \forall\, x, y \bullet x \in ac_0 \wedge y \in ac_1 \Rightarrow y = x$ {Predicate calculus}
$= \forall\, x, y \bullet y \in ac_1 \Rightarrow (x \in ac_0 \Rightarrow y = x)$ {Predicate calculus}
$= \forall\, y \bullet y \in ac_1 \Rightarrow (\forall\, x \bullet x \in ac_0 \Rightarrow y = x)$ {Property of sets}
$= \forall\, y \bullet y \in ac_1 \Rightarrow (\forall\, x \bullet x \in ac_0 \Rightarrow x \in \{y\})$ {Definition of subset inclusion}
$= \forall\, y \bullet y \in ac_1 \Rightarrow ac_0 \subseteq \{y\}$ {Property of sets}
$= \forall\, y \bullet y \in ac_1 \Rightarrow y \in \{s \mid ac_0 \subseteq \{s\}\}$ {Definition of subset inclusion}
$= ac_1 \subseteq \{s \mid ac_0 \subseteq \{s\}\}$

□

Lemma H.1.7

$$ac_0 \subseteq \{s \mid ac_0 \subseteq ac'\} = ac_0 = \emptyset \vee ac_0 \subseteq ac'$$

Proof.

$ac_0 \subseteq \{s \mid ac_0 \subseteq ac'\}$ {Definition of subset inclusion}
$= \forall\, x \bullet x \in ac_0 \Rightarrow x \in \{s \mid ac_0 \subseteq ac'\}$ {Property of sets}
$= \forall\, x \bullet x \in ac_0 \Rightarrow ac_0 \subseteq ac'$ {Predicate calculus}
$= \forall\, x \bullet (x \notin ac_0 \vee ac_0 \subseteq ac')$ {Predicate calculus}
$= (\forall\, x \bullet x \notin ac_0) \vee ac_0 \subseteq ac'$ {Property of sets}
$= ac_0 = \emptyset \vee ac_0 \subseteq ac'$

□

Lemma H.1.8 *Provided v is not s.*

$$\exists\, v \bullet t \subseteq \{s \mid Q\} \Rightarrow t \subseteq \{s \mid \exists\, v \bullet Q\}$$

Proof.

$\exists\, v \bullet t \subseteq \{s \mid Q\}$ {Property of sets, x is fresh}

$= \exists\, v \bullet (\forall\, x \bullet x \in t \Rightarrow (\exists\, s \bullet Q \wedge x = s))$ {Predicate calculus}
$\Rightarrow \forall\, x \bullet (\exists\, v \bullet x \in t \Rightarrow (\exists\, s \bullet Q \wedge x = s))$ {Predicate calculus}
$= \forall\, x \bullet x \in t \Rightarrow (\exists\, v \bullet (\exists\, s \bullet Q \wedge x = s))$ {Predicate calculus: v is not s}
$= \forall\, x \bullet x \in t \Rightarrow (\exists\, s \bullet (\exists\, v \bullet Q) \wedge x = s))$ {Property of sets}
$= \forall\, x \bullet x \in t \Rightarrow x \in \{s \mid \exists\, v \bullet Q\}$ {Property of sets}
$= t \subseteq \{s \mid \exists\, v \bullet Q\}$

□

Lemma H.1.9 *Provided $\preceq$ is transitive.*

$$x \preceq y \wedge A \subseteq \{z \mid y \preceq z \wedge x \preceq z \wedge e\} = x \preceq y \wedge A \subseteq \{z \mid y \preceq z \wedge e\}$$

Proof.

$x \preceq y \wedge A \subseteq \{z \mid x \preceq z \wedge e\}$ {Property of sets}
$= x \preceq y \wedge \forall\, z \bullet z \in A \Rightarrow (y \preceq z \wedge x \preceq z \wedge e)$ {Predicate calculus}
$= \forall\, z \bullet x \preceq y \wedge (z \in A \Rightarrow (y \preceq z \wedge x \preceq z \wedge e))$
{Predicate calculus: $\preceq$ is transitivite}
$= \forall\, z \bullet x \preceq y \wedge (z \in A \Rightarrow (y \preceq z \wedge e))$ {Predicate calculus}
$= x \preceq y \wedge \forall\, z \bullet z \in A \Rightarrow (y \preceq z \wedge e)$ {Property of sets}
$= x \preceq y \wedge A \subseteq \{z \mid y \preceq z \wedge e\}$

□

Lemma H.1.10 ($\subseteq$-transitivity-multiple)

$\exists\, D \bullet (\exists\, A \bullet P(A) \wedge A \subseteq D) \wedge (\exists\, B \bullet P(B) \wedge B \subseteq D) \wedge D \subseteq E$
$= (\exists\, A \bullet P(A) \wedge A \subseteq E) \wedge (\exists\, B \bullet P(B) \wedge B \subseteq E)$

Proof. (Implication)

$\exists\, D \bullet (\exists\, A \bullet P(A) \wedge A \subseteq D) \wedge (\exists\, B \bullet P(B) \wedge B \subseteq D) \wedge D \subseteq E$
{Propositional calculus}
$\Rightarrow (\exists\, D, A \bullet P(A) \wedge A \subseteq D \wedge D \subseteq E) \wedge (\exists\, D, B \bullet P(B) \wedge B \subseteq D \wedge D \subseteq E)$
{Propositional calculus and transitivity of subset inclusion}
$= (\exists\, A \bullet P(A) \wedge A \subseteq E) \wedge (\exists\, B \bullet P(B) \wedge B \subseteq E)$

□

Proof. (Reverse implication)

$$\left(\begin{array}{l} (\exists\, A \bullet P(A) \wedge A \subseteq E) \wedge (\exists\, B \bullet P(B) \wedge B \subseteq E) \\ \Rightarrow \exists\, D \bullet (\exists\, A \bullet P(A) \wedge A \subseteq D) \wedge (\exists\, B \bullet P(B) \wedge B \subseteq D) \wedge D \subseteq E \end{array} \right)$$

$$\{\text{Set } D = E\}$$

$$= \left(\begin{array}{l} (\exists\, A \bullet P(A) \wedge A \subseteq E) \wedge (\exists\, B \bullet P(B) \wedge B \subseteq E) \\ \Rightarrow (\exists\, A \bullet P(A) \wedge A \subseteq E) \wedge (\exists\, B \bullet P(B) \wedge B \subseteq E) \wedge E \subseteq E \end{array} \right)$$

$$\{\text{Reflexivity of subset inclusion and propositional calculus}\}$$

$$= \mathit{true}$$

□

Lemma H.1.11

$s \in A \Rightarrow A \neq \emptyset$

Proof.

$s \in A \Rightarrow A \neq \emptyset$ $\{\text{Property of sets}\}$

$= s \in A \Rightarrow \exists\, z \bullet z \in A$ $\{\text{Choose } z = s\}$

$= s \in A \Rightarrow s \in A$ $\{\text{Propositional calculus}\}$

$= \mathit{true}$

□

Lemma H.1.12

$\exists\, B \bullet B \neq \emptyset \wedge B \subseteq C \Leftrightarrow C \neq \emptyset$

Proof. (Implication) By contradiction: Suppose the consequent is false yet the antecedent is true. Then $C = \emptyset$.

$\exists\, B \bullet B \neq \emptyset \wedge B \subseteq C$ $\{\text{Assumption: } C = \emptyset\}$

$= \exists\, B \bullet B \neq \emptyset \wedge B \subseteq \emptyset$ $\{\text{Property of subset inclusion}\}$

$= \exists\, B \bullet B \neq \emptyset \wedge B = \emptyset$ $\{\text{Propositional calculus}\}$

$= \mathit{false}$

□

Proof. (Reverse implication)

$$
\begin{aligned}
& C \neq \emptyset \Rightarrow \exists\, B \bullet B \neq \emptyset \wedge B \subseteq C && \{\text{Choose } B = C\} \\
& = C \neq \emptyset \Rightarrow C \neq \emptyset \wedge C \subset C && \{\text{Reflexivity of subset inclusion}\} \\
& = C \neq \emptyset \Rightarrow C \neq \emptyset && \{\text{Propositional calculus}\} \\
& = \mathit{true}
\end{aligned}
$$

□

Lemma H.1.13

$\exists\, ac_0 \bullet s \in ac_0 \wedge ac_0 \subseteq ac' \Leftrightarrow s \in ac'$

Proof. (Implication)

$$
\begin{aligned}
& \exists\, ac_0 \bullet s \in ac_0 \wedge ac_0 \subseteq ac' && \{\text{Definition of subset inclusion}\} \\
& = \exists\, ac_0 \bullet s \in ac_0 \wedge (\forall\, z \bullet z \in ac_0 \Rightarrow z \in ac') \\
& && \{\text{Assume } s \in ac_0 \text{ then there is a case when } z = s\} \\
& = \exists\, ac_0 \bullet s \in ac_0 \wedge (\forall\, z \bullet z \in ac_0 \Rightarrow z \in ac') \wedge (s \in ac_0 \Rightarrow s \in ac') \\
& && \{\text{Assume } s \in ac_0 \text{ and propositional calculus}\} \\
& \Rightarrow s \in ac'
\end{aligned}
$$

□

Proof. (Reverse implication)

$$
\begin{aligned}
& s \in ac' \Rightarrow (\exists\, ac_0 \bullet s \in ac_0 \wedge ac_0 \subseteq ac') && \{\text{Choose } ac_0 = ac'\} \\
& = (s \in ac') \Rightarrow (s \in ac' \wedge ac' \subseteq ac') \\
& && \{\text{Reflexivity of subset inclusion and propositional calculus}\} \\
& = \mathit{true}
\end{aligned}
$$

□