ELSEVIER

Theoretical Computer Science 160 (1996) 1–85

Theoretical Computer Science

Fundamental Study
Relation-algebraic semantics

Roger D. Maddux *

Department of Mathematics, 400 Carver Hall, Iowa State University, Ames, IA 50011-2066, USA

Received February 1993; revised March 1995
Communicated by M. Nivat

Abstract

The first half is a tutorial on orderings, lattices, Boolean algebras, operators on Boolean algebras, Tarski's fixed point theorem, and relation algebras.

In the second half, elements of a complete relation algebra are used as "meanings" for program statements. The use of relation algebras for this purpose was pioneered by de Bakker and de Roever in [10–12]. For a class of programming languages with program schemes, single μ-recursion, `while`-statements, `if-then-else`, sequential composition, and nondeterministic choice, a definition of "correct interpretation" is given which properly reflects the intuitive (or operational) meanings of the program constructs. A correct interpretation includes for each program statement an element serving as "input/output relation" and a domain element specifying that statement's "domain of nontermination". The derivative of Hitchcock and Park [17] is defined and a relation-algebraic version of the extension by de Bakker [8, 9] of the Hitchcock–Park theorem is proved. The predicate transformers $\mathrm{wp}_S(\text{-})$ and $\mathrm{wlp}_S(\text{-})$ are defined and shown to obey all the standard laws in [15]. The "law of the excluded miracle" is shown to hold for an entire language if it holds for that language's basic statements (assignment statements and so on). Determinism is defined and characterized for all the program constructs. A relation-algebraic version of the invariance theorem for `while`-statements is given. An alternative definition of intepretation, called "demonic", is obtained by using "demonic union" in place of ordinary union, and "demonic composition" in place of ordinary relational composition. Such interpretations are shown to arise naturally from a special class of correct interpretations, and to obey the laws of $\mathrm{wp}_S(\text{-})$.

Contents

* E-mail: maddux@vincent.iastate.edu.

0304-3975/96/$15.00 © 1996 — Elsevier Science B.V. All rights reserved
SSDI 0304-3975(95)00082-8

1. Introduction

A basic idea of relational semantics [7] is to let the "meaning" of a program statement S be a binary relation r_S connecting inputs (initial machine states) with outputs (final machine states). An abstract computer has some (finite or infinite) sets of "states" and "computations". Every program statement S has an associated set of terminating computations. Each terminating computation C has an initial state σ_1 and a final state σ_2. Then r_S is the set of those pairs $\langle \sigma_1, \sigma_2 \rangle$ that arise from terminating computations of S. For deterministic program statements the input–output relation r_S is a partial function from states to states. If S is nondeterministic then the input–output relation r_S may not be a function, and may include several pairs that have the same initial state (even infinitely many pairs in the case of unbounded nondeterminism).

Real computer programs get into "infinite loops", so an abstract computer may also have a set of "nonterminating computations". A nonterminating computation has an initial state but no final state. Besides its terminating computations, a program statement S may have an associated set of nonterminating computations. One way to incorporate nontermination into a single relation r_S^+ is to introduce a fictitious state, perhaps called "bottom" or "undefined" or "infinity", denoted by $\perp$, ω, ∞, or some such symbol, and let r_S^+ be the binary relation containing all pairs of states $\langle \sigma_1, \sigma_2 \rangle$ that are connected by a terminating computation of S, together with all pairs of the form $\langle \sigma_3, \perp \rangle$, where σ_3 is the initial state of a nonterminating computation of S. Thus r_S^+ codes up the input–output relation r_S of S and the "domain of nontermination" of S. An alternative is to take the meaning of S to be a pair $\langle \mathrm{r}_S, \mathrm{e}_S \rangle$, where r_S is the input–output relation and e_S is either the domain of nontermination of S (e.g., , [5, 41, p. 511, 3]) or, better yet, a binary relation that codes up this domain, such as the set of pairs $\langle \sigma_3, \sigma_4 \rangle$, where σ_3 is the initial state of a nonterminating computation of S and σ_4 is any state whatsoever. The nontermination relation e_S is completely determined by its domain, so e_S is called a "domain relation". (The domain of a binary relation is the set of elements that appear as the first term of a pair in the relation.) The domain of the nontermination relation e_S is the domain of nontermination of S. (One reason for using a domain relation,

instead of simply a set, is to have only one type of object, namely relations, instead of two, relations and sets.) The "domain of guaranteed termination" is, naturally, the set of states from which no nonterminating computation is possible. It is the domain of the complement of the nontermination relation. By intersecting r_S with the complement of e_S we get an input–output relation with no possibility of nontermination, called the "safe input–output relation".

A natural setting for such algebraic manipulation of relations is the relation algebra of all binary relations on machine states. Let U be the set of states and let $\mathrm{Re}(U)$ be the set of all binary relations on U. Let 1' be the identity relation on U. For any binary relations $x, y \in \mathrm{Re}(U)$, the union of x and y is $x + y$, the complement of x (with respect to $U \times U$) is $\bar{x}$, the relative product of x and y is $x;y$, and the converse of x is $\check{x}$. We thereby obtain the relation algebra

$$\mathfrak{Re}\,(U) = \langle \mathrm{Re}(U), +, {}^{-}, ;, {}^{\check{}}, 1' \rangle$$

of all binary relations on U. The intersection of x and y is defined by $x \cdot y = \overline{\bar{x} + \bar{y}}$, the universal relation 1 is defined by $1 = \overline{1'} + 1'$ (so $1 = U \times U$), and the empty relation 0 is defined by $0 = \overline{1}$. Two of the elements of this algebra are r_S and e_S. A subset $W \subseteq U$ corresponds to the domain relation $W \times U$. The domain relation corresponding to U itself is 1. A relation x is a domain relation iff [1] $x;1 = x$. Thus $e_S;1 = e_S$. The domain relations form a Boolean subalgebra of the Boolean algebra $\langle \mathrm{Re}(U), +, {}^{-} \rangle$, so complements of domain relations are domain relations. For example, the domain relation of guaranteed termination is $\overline{e_S}$. Intersecting this with the input–output relation gives the safe input–output relation $r_S \cdot \overline{e_S}$.

In Dijkstra's predicate transformer semantics [13–15] there are two transformers associated with each statement S, namely $\mathrm{wlp}_S(\text{-})$ and $\mathrm{wp}_S(\text{-})$, called the "weakest liberal precondition" and "weakest precondition", respectively. These transformers map sets of states to sets of states, so they are modeled by functions that map domain relations to domain relations. Let x be a domain relation. According to the intended meaning of $\mathrm{wlp}_S(\text{-})$, a state σ is in the domain of $\mathrm{wlp}_S(x)$ iff every terminating computation of S starting at σ has its final state in the domain of x. This intention is realized by defining

$$\mathrm{wlp}_S(x) = \overline{r_S;\bar{x}}\,. \tag{1}$$

(Note that $\mathrm{wlp}_S(x)$ turns out to be a domain relation because x is a domain relation. For an arbitrary relation x, $\overline{r_S;\bar{x}}$ may not be a domain relation, although $\overline{r_S;\overline{x;1}}$ is always a domain relation.)

The intended meaning of $\mathrm{wp}_S(\text{-})$ is that σ is in the domain of $\mathrm{wp}_S(x)$ iff every computation of S that starts at σ must terminate and must have its final state in the domain of x, that is, σ is in the domain of $\mathrm{wlp}_S(x)$ and σ is in the domain of guaranteed termination. So the proper definition is

$$\mathrm{wp}_S(x) = \overline{r_S;\bar{x}} \cdot \overline{e_S}\,. \tag{2}$$

[1] We use "iff" as an abbreviation for "if and only if".

It is now easy to derive many basic laws governing $\mathrm{wp}_S(\text{-})$ and $\mathrm{wlp}_S(\text{-})$. For example, a state σ is in the domain of $\mathrm{wp}_S(1)$ iff it is in the domain of guaranteed termination of S, i.e.,

$$\mathrm{wp}_S(1) = \overline{\mathrm{e}_S} \tag{3}$$

It follows immediately from (1) and (2) that the connection between the transformers is

$$\mathrm{wp}_S(x) = \mathrm{wlp}_S(x) \cdot \mathrm{wp}_S(1) \ . \tag{4}$$

Definitions (1) and (2) still apply in case $\mathfrak{Re}(U)$ is replaced by an arbitrary relation algebra

$$\mathfrak{A} = \langle A, +, {}^{-}, ;, {}^{\smile}, 1' \rangle \ , \tag{5}$$

with $\mathrm{r}_S, \mathrm{e}_S \in A$. In this case (3) becomes a simple theorem that is easily deduced from the axioms that $\mathfrak{A}$ must satisfy in order to be a relation algebra, namely,

(Ba_1) $(x + y) + z = x + (y + z)$,
(Ba_2) $x + y = y + x$,
(Ba_3) $x = \overline{\overline{x} + \overline{y}} + \overline{\overline{x} + y}$,
(Ra_1) $(x;y);z = x;(y;z)$,
(Ra_2) $(x + y);z = x;z + y;z$,
(Ra_3) $x;1' = x$,
(Ra_4) $\breve{\breve{x}} = x$,
(Ra_5) $(x + y)\breve{} = \breve{x} + \breve{y}$,
(Ra_6) $(x;y)\breve{} = \breve{y};\breve{x}$,
(Ra_7) $\breve{x};\overline{x;y} + \overline{y} = \overline{y}$.

The first three of these axioms insure that $\langle A, +, {}^{-} \rangle$ is a Boolean algebra, and are due to Huntington [21, 22]. The final seven are known from the work of De Morgan [36] and Peirce [43], and were used by Tarski [52] in an axiomatization of a portion of the Peirce–Schröder calculus of binary relations.

The relation algebra $\mathfrak{Re}(U)$ is complete, atomic, simple, and representable, while $\mathfrak{A}$ may have none of these properties. In particular, the elements of $\mathfrak{A}$ may not be actual binary relations, and may also not behave like them, beyond what is guaranteed by the relation-algebraic axioms. In spite of this generality, much can be proved, as is demonstrated by the extent of this and other papers, starting with [10], followed by [11, 12, 47, 48, 3], and others. (See [49] and the references therein.) Some material originally done for $\mathfrak{Re}(U)$ is generalized here to arbitrary complete relation algebras.

Let $\mathscr{S}tat$ be the set of statements of a programming language. In Section 6 we define an $\mathfrak{A}$-interpretation to be a pair $\langle \mathrm{r}, \mathrm{e} \rangle$ of functions that map $\mathscr{S}tat$ to elements of $\mathfrak{A}$ such that $\mathrm{e}_S;1 = \mathrm{e}_S$ for every $S \in \mathscr{S}tat$. Thus, to get an $\mathfrak{A}$-interpretation, we can let r be a completely arbitrary map from statements into the algebra $\mathfrak{A}$, but e must map $\mathscr{S}tat$ into the set of domain elements of $\mathfrak{A}$. Note that absolutely no connection is assumed to hold between the elements of $\mathfrak{A}$ assigned to a compound statement

and the elements assigned to its constituent parts. Nevertheless, many standard laws of predicate transformers are proved in Section 6 on the basis of these very general definitions, such as: (3) and (4) hold, if x is a domain element then so are $\mathrm{wlp}_S(x)$ and $\mathrm{wp}_S(x)$, the function $\mathrm{wlp}_S(\text{-})$ is universally multiplicative, the function $\mathrm{wp}_S(\text{-})$ is completely multiplicative, and S is deterministic iff $\breve{\mathrm{r}}_S;\mathrm{r}_S \leqslant 1'$ and $\mathrm{r}_S \cdot \mathrm{e}_S = 0$.

Of course, to carry out such proofs we need a fair amount of basic material concerning Boolean algebras, operators on Boolean algebras, and relation algebras. Sections 2–5 contain all the background needed for such proofs in the later sections. Except for its organization and presentation in one place, almost none of the material in these sections is new, and much of it is quite elementary. These sections are almost completely self-contained. They start from the axioms (Ba_1)–(Ba_3) and (Ra_1)–(Ra_7) and build up all the results needed for proving the theorems in later sections. Almost all proofs are given in complete detail.

Section 2 ("Orderings, lattices, and Boolean algebras") contains definitions of partial ordering, upper bound, least upper bound, join, lower bound, greatest lower bound, meet, lattice, complete lattice, and Boolean algebra. Theorem **3**[2] gives a list of 21 identities satisfied in every Boolean algebra. The identities are listed in an order that facilitates their proof from Huntington's axioms. (As far as I know, Huntington's proof that his axioms are sufficient for all Boolean identities appears nowhere else in the literature besides his original papers.) Section 2 also contains proofs that the standard ordering $\leqslant$ in a Boolean algebra is a partial ordering that preserves meets and joins and forms a lattice with maximum element 1 and minimum element 0. Some generalized associativity and commutativity theorems for arbitrary meets and joins are stated and proved in **8**–**10**.

Section 3 is a brief exposition of part of the theory of unary operators on Boolean algebras. Section 3 is based on the work of Jónsson and Tarski [26]. This subject is extensively developed in [26] and is applied to relation algebras and cylindric algebras in [27]. Another account of the theory is given in [16]. We need just a few theorems from [26]. They are used mostly to prove some of the theorems on relation algebras in Section 5, but they are also occasionally used in the later sections, since predicate transformers are unary operators on Boolean algebras. Definitions of normal, monotonic, additive, multiplicative, completely additive, universally additive, completely multiplicative, universally multiplicative, and conjugated functions are given, along with some basic results concerning these concepts, such as: conjugated functions are completely additive and completely additive functions are monotonic. The Jónsson–Tarski characterizations of conjugated functions are also presented.

Section 4 is devoted to a statement and proof of Tarski's fixed point theorem, which asserts that the fixed points of a monotonic function on a complete lattice form a nonempty complete lattice.

[2] References to theorems and definitions are always given in boldface type, usually with no preceding descriptive term such as "Theorem" or "Definition".

Section 5 is a brief introduction to relation algebras. It is confined to the definition of relation algebras, some examples, a list of 35 elementary laws true in all relation algebras, definitions of domain elements and functional elements, a few basic facts about such elements, and some results concerning fixed points of certain monotonic functions on complete relation algebras. Some of these are well-known for $\mathfrak{Re}(U)$, such as: the least fixed point of the function $p+q;(\text{-})$ is $p+q;p+q;q;p+q;q;q;p+\cdots$. Except for the results on fixed points, this material can be found in [6, 27].

After Section 6, in which the internal structure of program statements is irrelevant, we come to Section 7, which introduces "correct interpretations", those which "correctly" connect the elements assigned to the parts of a complex statement with those assigned to the statement itself. After some motivation for these connections, the definition of correct interpretation is given, followed by a few technical results concerning substitutions and free variables. The rest of the section includes the definition of the derivatives, a relation-algebraic version of the Hitchcock–Park–de Bakker theorem, theorems relating the predicate transformers of complex statements to the predicate transformers of their parts, a proof that if the basic statements of the language satisfy the "law of the excluded miracle", then so do all the compound statements, some results concerning determinism, and a generalized invariance theorem for `while`-statements. The final section is devoted to "demonic interpretations". We show that they arise naturally from a special class of correct interpretations and obey all the laws of $\mathrm{wp}_S(\text{-})$.

2. Orderings, lattices, and Boolean algebras

Definition 1. Let B be an arbitrary set and let $\leqslant$ be a binary relation on B.

(i) The relation $\leqslant$ is called a *partial ordering of* B if for all $x, y \in B$ we have

(a) $x \leqslant x$ ($\leqslant$ is reflexive over B),

(b) if $x \leqslant y$ and $y \leqslant z$ then $x \leqslant z$ ($\leqslant$ is transitive),

(c) if $x \leqslant y$ and $y \leqslant x$ then $x = y$ ($\leqslant$ is antisymmetric).

(ii) Let I be an arbitrary set and suppose there is some $x_i \in B$ for every $i \in I$. An element $y \in B$ is an *upper bound of* $\{x_i : i \in I\}$ if $x_i \leqslant y$ for every $i \in I$.

(iii) If y is an upper bound of $\{x_i : i \in I\}$ and $y \leqslant z$ for every upper bound z of $\{x_i : i \in I\}$, then y is called the *least upper bound of* $\{x_i : i \in I\}$ or the *join of* $\{x_i : i \in I\}$ and is denoted by $\sum\{x_i : i \in I\}$ or $\sum_{i \in I} x_i$.

(iv) An element $y \in B$ is a *lower bound of* $\{x_i : i \in I\}$ if $y \leqslant x_i$ for every $i \in I$.

(v) If y is a lower bound of $\{x_i : i \in I\}$ and $z \leqslant y$ for every lower bound z of $\{x_i : i \in I\}$, then y is called the *greatest lower bound of* $\{x_i : i \in I\}$ or the *meet of* $\{x_i : i \in I\}$ and is denoted by $\prod\{x_i : i \in I\}$ or $\prod_{i \in I} x_i$.

(vi) If $\leqslant$ is a partial ordering of B and the join and meet of $\{x_i : i \in I\}$ both exist whenever I is a two-element set, then $\langle B, \leqslant \rangle$ is called a *lattice*.

(vii) A lattice is *complete* if the join and meet of $\{x_i : i \in I\}$ always exist, regardless of the cardinality of I.

We frequently use the notation "$\sum\{f(x):\varphi(x)\}$", where $\varphi(x)$ is some condition on x and f is some function mapping B to B. The meaning of this notation is simply $\sum_{i\in I} y_i$, where $I=\{f(x):\varphi(x)\}$ and $y_i=i$ for every $i\in I$. A similar explanation applies to "$\prod\{f(x):\varphi(x)\}$".

Definition 2. A *Boolean algebra* is an algebraic structure of the form $\mathfrak{B}=\langle B,+,^-\rangle$, where B is a nonempty set, $+$ is a binary operation on B, and $^-$ is a unary operation on B, such that the following axioms are satisfied for all $x,y,z\in B$:

(Ba_1) $x+y+z=x+(y+z)$ ($+$ is associative),

(Ba_2) $x+y=y+x$ ($+$ is commutative),

(Ba_3) $x=\overline{\overline{x}+\overline{y}}+\overline{\overline{x}+y}$.

An additional binary operation $\cdot$ on B is defined by

(Ba_4) $x\cdot y=\overline{\overline{x}+\overline{y}}$.

Parentheses are omitted from Boolean-algebraic terms according to the convention that a repeated binary operation is computed from left to right, e.g., $x+y+z=(x+y)+z$, and $\cdot$ takes precedence over $+$. The scope of joins and meets is always as small as possible.

The axiomatization (Ba_1)–(Ba_3) is due to Huntington [21, 22]. There is a fascinating open problem connected with this axiomatization, due to Herbert Robbins (see Problem 1.1, p. 245, of [16]). The "dual" of (Ba_3) is

(Ba_3') $x=\overline{\overline{x+\overline{y}}+\overline{x+y}}$.

If an algebra $\mathfrak{B}=\langle B,+,^-\rangle$ satisfies (Ba_1), (Ba_2), and (Ba_3'), must it be a Boolean algebra? Probably not. It is interesting to note if $\mathfrak{B}$ is a *finite* algebra satisfying (Ba_1), (Ba_2), and (Ba_3') then $\mathfrak{B}$ is, in fact, a Boolean algebra. The reason for this is that every finite algebra that satisfies (Ba_3') must also satisfy (Ba_3). To see this, suppose $\mathfrak{B}$ is a finite algebra that satisfies (Ba_3'). From the form of (Ba_3') it is clear that the operation $^-$ is onto. Since $\mathfrak{B}$ is finite, the operation $^-$ must also be one-to-one. Substitute $\bar{x}$ for x in (Ba_3') to get $\bar{x}=\overline{\overline{\bar{x}+\overline{y}}+\overline{\bar{x}+y}}$. Since $^-$ is one-to-one, this entails $x=\overline{\overline{x}+\overline{y}}+\overline{\overline{x}+y}$. Thus, ($\mathrm{Ba}_3$) holds in $\mathfrak{B}$.

Theorem 3. *The following identities are satisfied in every Boolean algebra.*

(i) $x+\bar{x}=y+\bar{y}$.

(ii) $\bar{\bar{x}}=x$.

(iii) $\bar{x}=\overline{x+y}+\overline{x+\bar{y}}$.

(iv) $x+(y+\bar{y})=z+\bar{z}$.

(v) $x+x=x+\bar{y}+\bar{y}$.

(vi) $x+x=x$.

(vii) $x\cdot x=x$.

(viii) $x\cdot y=y\cdot x$.

(ix) $x\cdot y\cdot z=x\cdot(y\cdot z)$.

(x) $(x+y)\cdot x=x$.

(xi) $x=x\cdot y+x\cdot\bar{y}$.

(xii) $x = (x + \bar{y}) \cdot (x + y)$.
(xiii) $(x + y) \cdot \bar{x} = y \cdot \bar{x}$.
(xiv) $x + x \cdot y = x$.
(xv) $x \cdot (y + z) = x \cdot y + x \cdot z$.
(xvi) $\overline{x + y} = \bar{x} \cdot \bar{y}$.
(xvii) $\overline{x \cdot y} = \bar{x} + \bar{y}$.
(xviii) $x + y \cdot z = (x + y) \cdot (x + z)$.
(xix) $\bar{x} \cdot y + x \cdot z = (x + y) \cdot (\bar{x} + z)$.
(xx) $(v \cdot w + \bar{v} \cdot x) \cdot \overline{v \cdot y + \bar{v} \cdot z} = v \cdot w \cdot \bar{y} + \bar{v} \cdot x \cdot \bar{z}$.
(xxi) $x + y = x + \bar{x} \cdot y$.

Proof.

3(i):
$$\begin{aligned} x + \bar{x} &= \left(\overline{\bar{x} + \bar{\bar{y}}} + \overline{\bar{x} + \bar{y}}\right) + \left(\overline{\bar{\bar{x}} + \bar{\bar{y}}} + \overline{\bar{\bar{x}} + \bar{y}}\right) && (\mathrm{Ba}_3) \\ &= \left(\overline{\bar{\bar{y}} + \bar{x}} + \overline{\bar{y} + \bar{x}}\right) + \left(\overline{\bar{\bar{y}} + \bar{\bar{x}}} + \overline{\bar{y} + \bar{\bar{x}}}\right) && (\mathrm{Ba}_2) \\ &= \left(\overline{\bar{y} + \bar{\bar{x}}} + \overline{\bar{y} + \bar{x}}\right) + \left(\overline{\bar{\bar{y}} + \bar{\bar{x}}} + \overline{\bar{\bar{y}} + \bar{x}}\right) && (\mathrm{Ba}_1), (\mathrm{Ba}_2) \\ &= y + \bar{y} && (\mathrm{Ba}_3). \end{aligned}$$

3(ii):
$$\begin{aligned} \bar{\bar{x}} &= \overline{\bar{\bar{x}} + \bar{\bar{x}}} + \overline{\bar{\bar{x}} + \bar{x}} && (\mathrm{Ba}_3) \\ &= \overline{\bar{x} + \bar{\bar{x}}} + \overline{\bar{\bar{x}} + \bar{\bar{x}}} && (\mathrm{Ba}_2) \\ &= \overline{\bar{x} + \bar{\bar{x}}} + \overline{\bar{x} + \bar{x}} && \mathbf{3}(\mathrm{i}) \\ &= x && (\mathrm{Ba}_3). \end{aligned}$$

3(iii):
$$\begin{aligned} \bar{x} &= \overline{\bar{\bar{x}} + \bar{y}} + \overline{\bar{\bar{x}} + y} && (\mathrm{Ba}_3) \\ &= \overline{x + \bar{y}} + \overline{x + y} && \mathbf{3}(\mathrm{ii}) \\ &= \overline{x + y} + \overline{x + \bar{y}} && (\mathrm{Ba}_2). \end{aligned}$$

3(iv):
$$\begin{aligned} x + (y + \bar{y}) &= x + (x + \bar{x}) && \mathbf{3}(\mathrm{i}) \\ &= x + x + \bar{x} && (\mathrm{Ba}_1) \\ &= x + x + \left(\overline{x + x} + \overline{x + \bar{x}}\right) && \mathbf{3}(\mathrm{iii}) \\ &= x + x + \overline{x + x} + \overline{x + \bar{x}} && (\mathrm{Ba}_1) \\ &= x + \bar{x} + \overline{x + \bar{x}} && \mathbf{3}(\mathrm{i}) \\ &= z + \bar{z} && \mathbf{3}(\mathrm{i}). \end{aligned}$$

3(v):
$$\begin{aligned} x + x &= \overline{\overline{x + x} + \overline{x + \bar{x}}} + \overline{\overline{x + x} + (x + \bar{x})} && (\mathrm{Ba}_3) \\ &= \overline{\overline{x + x} + \overline{x + \bar{x}}} + \overline{y + \bar{y}} && \mathbf{3}(\mathrm{iv}) \\ &= \bar{\bar{x}} + \overline{y + \bar{y}} && \mathbf{3}(\mathrm{iii}) \\ &= x + \overline{y + \bar{y}} && \mathbf{3}(\mathrm{ii}). \end{aligned}$$

3(vi):
$$\begin{aligned} x + x &= \overline{\overline{x + x} + \overline{\overline{x + \bar{x}} + \bar{x}}} + \overline{\overline{x + x} + \left(\overline{x + \bar{x}} + \bar{x}\right)} && (\mathrm{Ba}_3) \\ &= \overline{\overline{x + x} + \overline{\overline{x + \bar{x}} + \bar{x}}} + \overline{\overline{x + x} + \overline{x + \bar{x}} + \bar{x}} && (\mathrm{Ba}_1) \\ &= \overline{x + x} + \overline{\overline{x + \bar{x}} + \bar{x}} + \overline{\bar{x} + \bar{x}} && \mathbf{3}(\mathrm{iii}) \end{aligned}$$

$$= \overline{\overline{\overline{\overline{\overline{\overline{\overline{\overline{x+x+\bar{\bar{x}}}+\overline{\overline{x+\bar{\bar{x}}+\bar{x}}}+\bar{\bar{x}}+x}}}}}}} \quad \mathbf{3}(\mathrm{v})$$

$$= \overline{\overline{\bar{\bar{x}}+\bar{x}}+\overline{\overline{\overline{\overline{\bar{\bar{x}}+x}+\bar{x}+\overline{\bar{\bar{x}}+x}}}}+x} \quad (\mathrm{Ba}_2)$$

$$= \overline{\bar{\bar{x}}+\bar{x}}+\overline{\bar{\bar{x}}+x} \quad (\mathrm{Ba}_3)$$

$$= x \quad (\mathrm{Ba}_3).$$

3(vii): $x \cdot x = \overline{\bar{\bar{x}}+\bar{x}}$ (Ba_4)

$= \bar{\bar{\bar{x}}}$ **3**(vi).

$= x$ **3**(ii).

3(viii): $x \cdot y = \overline{\bar{\bar{x}}+\bar{\bar{y}}}$ (Ba_4)

$= \overline{\bar{\bar{y}}+\bar{x}}$ (Ba_2)

$= y \cdot x$ (Ba_4).

3(ix): $x \cdot y \cdot z = \overline{\overline{\overline{\bar{\bar{x}}+\bar{\bar{y}}}+\bar{z}}}$ (Ba_4)

$= \overline{\bar{\bar{x}}+\bar{\bar{y}}+\bar{\bar{z}}}$ **3**(ii)

$= \overline{\bar{\bar{x}}+(\bar{\bar{y}}+\bar{\bar{z}})}$ (Ba_1)

$= \overline{\bar{\bar{x}}+\overline{\overline{\bar{\bar{y}}+\bar{\bar{z}}}}}$ **3**(ii)

$= x \cdot (y \cdot z)$ (Ba_4).

3(x): $(x+y) \cdot x = \overline{\overline{\overline{x+\bar{\bar{y}}}+\bar{\bar{x}}}}$ (Ba_4)

$= \overline{\overline{x+\bar{\bar{y}}}+\overline{(x+\bar{\bar{y}}+\overline{x+\bar{\bar{y}}})}}$ **3**(iii)

$= \overline{\overline{x+\bar{\bar{y}}}+\overline{x+\bar{\bar{y}}}+\overline{x+\bar{\bar{y}}}}$ (Ba_1)

$= \overline{\overline{x+\bar{\bar{y}}}+\overline{x+\bar{\bar{y}}}}$ **3**(vi)

$= \bar{\bar{\bar{x}}}$ **3**(iii)

$= x$ **3**(ii).

3(xi): $x = \overline{\bar{\bar{x}}+\bar{\bar{y}}}+\overline{\bar{\bar{x}}+y}$ (Ba_3)

$= \overline{\bar{\bar{x}}+\bar{\bar{y}}}+\overline{x+\bar{\bar{y}}}$ **3**(ii)

$= x \cdot y + x \cdot \bar{y}$ (Ba_4).

3(xii): $x = \bar{\bar{\bar{x}}}$ **3**(ii)

$= \overline{\overline{x+\bar{\bar{y}}}+\overline{x+y}}$ **3**(iii), (Ba_2)

$= (x+\bar{y}) \cdot (x+y)$ (Ba_4).

3(xiii): $(x+y) \cdot \bar{x} = (x+y) \cdot ((\bar{x}+y) \cdot \bar{x})$ **3**(x)

$= (x+y) \cdot (\bar{x}+y) \cdot \bar{x}$ **3**(ix)

$= (y+\bar{x}) \cdot (y+x) \cdot \bar{x}$ **3**(viii), (Ba_2)

$= y \cdot \bar{x}$ **3**(xii).

3(xiv): $x + x \cdot y = x \cdot y + x \cdot \bar{y} + x \cdot y$ **3**(xi)

$= x \cdot y + x \cdot y + x \cdot \bar{y}$ (Ba_1), (Ba_2)

$= x \cdot y + x \cdot \bar{y}$ **3**(vi)

$= x$ **3**(xi).

3(xv): $x \cdot (y+z) = x \cdot (y+z) \cdot y + x \cdot (y+z) \cdot \overline{y}$ **3**(xi)
$= x \cdot ((y+z) \cdot y) + x \cdot ((y+z) \cdot \overline{y})$ **3**(ix)
$= x \cdot y + x \cdot ((y+z) \cdot \overline{y})$ **3**(x)
$= x \cdot y + x \cdot (z \cdot \overline{y})$ **3**(xiii)
$= x \cdot y + x \cdot y \cdot z + x \cdot (z \cdot \overline{y})$ **3**(xiv)
$= x \cdot y + (x \cdot z \cdot y + x \cdot z \cdot \overline{y})$ (Ba_1), **3**(viii)(ix)
$= x \cdot y + x \cdot z$ **3**(xi).

3(xvi): $\overline{x} \cdot \overline{y} = \overline{\overline{x} + \overline{y}}$ (Ba_4)
$= \overline{x + y}$ **3**(ii).

3(xvii): $\overline{x \cdot y} = \overline{\overline{x} + \overline{y}}$ (Ba_4)
$= \overline{x} + \overline{y}$ **3**(ii).

3(xviii): $x + y \cdot z = x + \overline{\overline{y} + \overline{z}}$ (Ba_4)
$= \overline{\overline{x}} + \overline{\overline{y} + \overline{z}}$ **3**(ii)
$= \overline{\overline{x} \cdot (\overline{y} + \overline{z})}$ **3**(xvii)
$= \overline{\overline{x} \cdot \overline{y} + \overline{x} \cdot \overline{z}}$ **3**(xv)
$= \overline{\overline{x + y} + \overline{x + z}}$ **3**(xvi)
$= (x + y) \cdot (x + z)$ (Ba_4).

3(xix): $(x + y) \cdot (\overline{x} + z)$
$= (x + y) \cdot \overline{x} + (x + y) \cdot z$ **3**(xv)
$= y \cdot \overline{x} + (x + y) \cdot z$ **3**(xiii)
$= y \cdot \overline{x} + x \cdot z + y \cdot z$ (Ba_2), **3**(xv), (Ba_1)
$= y \cdot \overline{x} + x \cdot z + y \cdot z \cdot x + y \cdot z \cdot \overline{x}$ **3**(xi), (Ba_1)
$= \overline{x} \cdot y + \overline{x} \cdot y \cdot z + (x \cdot z + x \cdot z \cdot y)$ **3**(viii)(ix), (Ba_1), (Ba_2)
$= \overline{x} \cdot y + x \cdot z$ **3**(xiv).

3(xx): $(v \cdot w + \overline{v} \cdot x) \cdot \overline{v \cdot y + \overline{v} \cdot z}$
$= (v \cdot w + \overline{v} \cdot x) \cdot (\overline{v} + \overline{y}) \cdot (v + \overline{z})$ **3**(ii)(viii)(xvi)(xvii)
$= (\overline{v} + w) \cdot (v + x) \cdot (\overline{v} + \overline{y}) \cdot (v + \overline{z})$ **3**(ii)(xix)
$= (\overline{v} + w) \cdot (\overline{v} + \overline{y}) \cdot (v + x) \cdot (v + \overline{z})$ **3**(viii)(ix)
$= (\overline{v} + w \cdot \overline{y}) \cdot (v + x \cdot \overline{z})$ **3**(xviii)
$= v \cdot w \cdot \overline{y} + \overline{v} \cdot x \cdot \overline{z}$ **3**(ii)(ix)(xix).

3(xxi): $x + y = x + y \cdot x + y \cdot \overline{x}$ **3**(xi), (Ba_1)
$= x + \overline{x} \cdot y$ **3**(viii)(xiv).

From **3**(i) it follows that, in every Boolean algebra $\mathfrak{B}$, each of the sets $\{x + \overline{x} : x \in B\}$ and $\{\overline{x + \overline{x}} : x \in B\}$ contains exactly one element. This observation justifies the next definition.

Definition 4. For every Boolean algebra $\mathfrak{B}$, the unique element in $\{x + \overline{x} : x \in B\}$ is denoted by 1, and the unique element in $\{\overline{x + \overline{x}} : x \in B\}$ is denoted by 0.

Theorem 5. *The following identities are satisfied in every Boolean algebra.*

(i) $1 = x + \bar{x}$.
(ii) $0 = x \cdot \bar{x}$.
(iii) $\bar{1} = 0$.
(iv) $\bar{0} = 1$.
(v) $x + 1 = 1$.
(vi) $x \cdot 0 = 0$.
(vii) $x + 0 = x$.
(viii) $x \cdot 1 = x$.

Proof. Using **4** and (Ba_4), we convert **5**(i)–**5**(viii) into equivalent identities, and indicate why each of them holds.

5(i) is equivalent to $y + \bar{y} = x + \bar{x}$, which holds by **3**(i).
5(ii) is equivalent to $\overline{y + \bar{y}} = \bar{x} + \bar{\bar{x}}$, which holds by **3**(i).
5(iii) is equivalent to $\overline{x + \bar{x}} = \overline{y + \bar{y}}$, which holds by **3**(i).
5(iv) is equivalent to $\overline{\overline{x + \bar{x}}} = y + \bar{y}$, which holds by **3**(i)(ii).
5(v) is equivalent to $x + (y + \bar{y}) = z + \bar{z}$, which holds by **3**(iv).
5(vi) is equivalent to $\bar{x} + \overline{\overline{y + \bar{y}}} = \overline{z + \bar{z}}$, which holds by **3**(ii)(iv).
5(vii) is equivalent to $x + \overline{y + \bar{y}} = x$, which holds by **3**(v)(vi).
5(viii) is equivalent to $\bar{x} + \overline{y + \bar{y}} = x$, which holds by **3**(ii)(v)(vi). □

Definition 6. For every Boolean algebra $\mathfrak{B}$, define binary relations $\leqslant$ and $\geqslant$ on B as follows: $x \leqslant y$ iff $x + y = y$, and $x \geqslant y$ iff $y \leqslant x$.

Theorem 7. *Let $\mathfrak{B}$ be a Boolean algebra.*

(i) *The relation $\leqslant$ is a partial ordering of B.*
(ii) *For every $x \in B$, $0 \leqslant x$ and $x \leqslant 1$.*
(iii) *For all $x, y, z \in B$, if $x \leqslant y$ then $x + z \leqslant y + z$ and $x \cdot z \leqslant y \cdot z$.*
(iv) *$\langle B, \leqslant \rangle$ is a lattice in which the join of $\{x, y\} \subseteq B$ is $x + y$ and the meet of $\{x, y\}$ is $x \cdot y$.*
(v) *The following statements are equivalent for all $x, y \in B$:*
  (a) $x \leqslant y$,
  (b) $\bar{y} \leqslant \bar{x}$,
  (c) $x + y = y$,
  (d) $x \cdot y = x$,
  (e) $\bar{x} + y = 1$,
  (f) $x \cdot \bar{y} = 0$.
(vi) *For all $x, y, z \in B$, $x \cdot y \leqslant z$ iff $y \leqslant \bar{x} + z$.*

Proof. **7**(i): Let $x, y, z \in B$. Then $x \leqslant x$ since $x + x = x$ by **3**(vi), so $\leqslant$ is reflexive over B. If $x \leqslant y$ and $y \leqslant z$, then $x + y = y$ and $y + z = z$, so, using these equations and (Ba_1), we have $x + z = x + (y + z) = x + y + z = y + z = z$, i.e., $x \leqslant z$. Thus $\leqslant$ is transitive. Finally, $\leqslant$ is antisymmetric, for if $x \leqslant y$ and $y \leqslant x$, then $x + y = y$ and $y + x = x$, so $x = y$ by (Ba_2). Thus $\leqslant$ is a partial ordering of B by **1**(i).

7(ii): We obtain $0 \leqslant x$ from **5**(vii), (Ba_2), and **6**, while $x \leqslant 1$ follows from **5**(v) and **6**.

7(iii): Suppose $x \leqslant y$, i.e., $x + y = y$. Then

$$\begin{aligned} x + z + (y + z) &= x + y + (z + z) && (Ba_1), (Ba_2) \\ &= x + y + z && \mathbf{3}(vi) \\ &= y + z && x + y = y, \end{aligned}$$

so $x + z \leqslant y + z$. Also,

$$\begin{aligned} x \cdot z + y \cdot z &= (x + y) \cdot z && \mathbf{3}(viii)(xv) \\ &= y \cdot z && x + y = y, \end{aligned}$$

so $x \cdot z \leqslant y \cdot z$.

7(iv): We have

$$\begin{aligned} x + (x + y) &= x + x + y && (Ba_1) \\ &= x + y && \mathbf{3}(vi), \end{aligned}$$

so $x \leqslant x + y$, and

$$\begin{aligned} y + (x + y) &= x + y + y && (Ba_2) \\ &= x + (y + y) && (Ba_1) \\ &= x + y && \mathbf{3}(vi), \end{aligned}$$

so $y \leqslant x + y$. Thus $x + y$ is an upper bound of $\{x, y\}$. Suppose z is an upper bound of $\{x, y\}$. Then $x \leqslant z$ and $y \leqslant z$, i.e., $x + z = z$ and $y + z = z$, so $x + y + z = x + (y + z) = x + z = z$ by (Ba_1). Thus $x + y \leqslant z$. This shows $x + y$ is the least upper bound of $\{x, y\}$.

We have $x \cdot y + x = x$ and $x \cdot y + y = y$ by **3**(viii)(xiv) and (Ba_2), so $x \cdot y \leqslant x$ and $x \cdot y \leqslant y$. Thus $x \cdot y$ is a lower bound of $\{x, y\}$. If $z \leqslant x$ and $z \leqslant y$, then $z + x = x$ and $z + y = y$, so, by **3**(xviii), $z + x \cdot y = (z + x) \cdot (z + y) = x \cdot y$, and therefore $z \leqslant x \cdot y$. Thus $x \cdot y$ is the greatest lower bound of $\{x, y\}$.

7(v): **7**(v)(a) and **7**(v)(c) are equivalent by **6**. Assume **7**(v)(c) holds. Then

$$\begin{aligned} 1 &= y + 1 && \mathbf{5}(v) \\ &= y + (x + \bar{x}) && \mathbf{5}(i) \\ &= \bar{x} + (x + y) && (Ba_1), (Ba_2) \\ &= \bar{x} + y && \mathbf{7}(v)(c), \end{aligned}$$

so **7**(v)(b) holds. Using (Ba_4) and **5**(iii), we see that **7**(v)(f) is equivalent to $\overline{\bar{x} + \bar{\bar{y}}} = \bar{1}$, but the latter statement is equivalent to **7**(v)(e) by **3**(ii). Assume **7**(v)(e) holds. Then

$$\begin{aligned} \bar{x} &= (\bar{x} + \bar{y}) \cdot (\bar{x} + y) && \mathbf{3}(xii) \\ &= (\bar{x} + \bar{y}) \cdot 1 && \mathbf{7}(v)(e) \\ &= \bar{x} + \bar{y} && \mathbf{5}(viii), \end{aligned}$$

so **7**(v)(b) holds by **6**. Assume **7**(v)(b) holds, i.e., $\bar{y}+\bar{x}=\bar{y}$ by **6**. Then

$$\begin{aligned} x\cdot y &= \overline{\bar{x}+\bar{y}} && (\mathrm{Ba}_4)\\ &= \overline{\bar{y}+\bar{\bar{x}}} && (\mathrm{Ba}_2)\\ &= \bar{\bar{x}} && \mathbf{7}(\mathrm{v})(\mathrm{b})\\ &= x && \mathbf{3}(\mathrm{ii}), \end{aligned}$$

so **7**(v)(d) holds. Assume **7**(v)(d) holds. Then

$$\begin{aligned} y &= y+y\cdot x && \mathbf{3}(\mathrm{xiv})\\ &= x\cdot y+x && (\mathrm{Ba}_2),\ \mathbf{3}(\mathrm{viii})\\ &= x+y && \mathbf{7}(\mathrm{v})(\mathrm{d}), \end{aligned}$$

so $x\leqslant y$, and

$$\begin{aligned} \bar{x}+y &= \bar{x}+x\cdot y && \mathbf{3}(\mathrm{ii})(\mathrm{xxi})\\ &= x+\bar{x} && \mathbf{7}(\mathrm{v})(\mathrm{d})\\ &= 1 && (\mathrm{Ba}_2),\ \mathbf{5}(\mathrm{i}). \end{aligned}$$

Thus, **7**(v)(d) implies **7**(v)(c) and **7**(v)(e).

7(vi):

$$\begin{aligned} & x\cdot y\leqslant z\\ \text{iff}\quad & x\cdot y\cdot\bar{z}=0 && \text{by } \mathbf{7}(\mathrm{v})\\ \text{iff}\quad & y\cdot(x\cdot\bar{z})=0 && \text{by } \mathbf{3}(\mathrm{viii})(\mathrm{ix})\\ \text{iff}\quad & y\cdot\overline{\bar{x}+z}=0 && \text{by } \mathbf{3}(\mathrm{ii})(\mathrm{xvi})\\ \text{iff}\quad & y\leqslant\bar{x}+z && \text{by } \mathbf{7}(\mathrm{v}). \end{aligned}$$

□

Theorem 8. *Let $\mathfrak{B}$ be a Boolean algebra. Let I be an arbitrary set. Suppose $x_i\in B$ for every $i\in I$, and $y\in B$.*

(i) *If $I=\emptyset$ then $\sum_{i\in I}x_i=0$ and $\prod_{i\in I}x_i=1$.*

(ii) *If $\sum_{i\in I}x_i$ exists then $\prod_{i\in I}\bar{x}_i$ also exists and $\overline{\sum_{i\in I}x_i}=\prod_{i\in I}\bar{x}_i$.*

(iii) *If $\prod_{i\in I}x_i$ exists then $\sum_{i\in I}\bar{x}_i$ also exists and $\overline{\prod_{i\in I}x_i}=\sum_{i\in I}\bar{x}_i$.*

(iv) *For every y, both $\prod\{x:x\geqslant y\}$ and $\sum\{x:x\leqslant y\}$ exist, and*

$$y=\prod\{x:x\geqslant y\}=\sum\{x:x\leqslant y\}.$$

Proof. 8(i): Assume $I=\emptyset$. Then $\{x_i:i\in I\}=\emptyset$. Every element of $\mathfrak{B}$ is an upper bound of $\emptyset$, so the least upper bound of $\emptyset$ is the least element of $\mathfrak{B}$, namely, by **7**(ii), 0. Similarly, every element of $\mathfrak{B}$ is a lower bound of $\emptyset$, so the greatest lower bound of $\emptyset$ is the greatest element of $\mathfrak{B}$, namely 1.

8(ii): Assume $\sum_{i\in I}x_i$ exists. We need to show that $\overline{\sum_{i\in I}x_i}$ is the greatest lower bound of $\{\bar{x}_i:i\in I\}$. For every $i\in I$, $x_i\leqslant\sum_{i\in I}x_i$, hence $\overline{\sum_{i\in I}x_i}\leqslant\bar{x}_i$ by **7**(v). Thus $\overline{\sum_{i\in I}x_i}$ is a lower bound of $\{\bar{x}_i:i\in I\}$. Let z be a lower bound of $\{\bar{x}_i:i\in I\}$. Then for every $i\in I$, we have $z\leqslant\bar{x}_i$, hence $x_i\leqslant\bar{z}$ by **7**(v) and **3**(ii). Thus $\bar{z}$ is an upper bound of $\{x_i:i\in I\}$. It follows that $\sum_{i\in I}x_i\leqslant\bar{z}$, so $z\leqslant\overline{\sum_{i\in I}x_i}$ by **7**(v).

8(iii): Similar to **8**(ii).

8(iv): If $z \in \{x : x \geqslant y\}$, then $z \geqslant y$. Therefore y is a lower bound of $\{x : x \geqslant y\}$. Suppose y' is also a lower bound of $\{x : x \geqslant y\}$. Then $y' \leqslant y$ since $y \in \{x : x \geqslant y\}$. Thus y contains every lower bound, so it is the greatest lower bound of $\{x : x \geqslant y\}$, i.e., $y = \prod \{x : x \geqslant y\}$. The other equation is proved similarly.

Theorem 9. *Let $\mathfrak{B}$ be a Boolean algebra. Let I be an arbitrary set and suppose $x_i, y_i \in B$ for every $i \in I$.*

(i) *If $\sum_{i\in I} x_i$ and $\sum_{i\in I} y_i$ exist, then $\sum_{i\in I}(x_i + y_i)$ also exists and $\sum_{i\in I}(x_i + y_i) = \sum_{i\in I} x_i + \sum_{i\in I} y_i$.*

(ii) *If $\prod_{i\in I} x_i$ and $\prod_{i\in I} y_i$ exist, then $\prod_{i\in I}(x_i \cdot y_i)$ also exists and $\prod_{i\in I}(x_i \cdot y_i) = \prod_{i\in I} x_i \cdot \prod_{i\in I} y_i$.*

(iii) *Suppose $x_i \leqslant y_i$ for every $i \in I$. If $\sum_{i\in I} x_i$ and $\sum_{i\in I} y_i$ exist, then $\sum_{i\in I} x_i \leqslant \sum_{i\in I} y_i$. If $\prod_{i\in I} x_i$ and $\prod_{i\in I} y_i$ exist, then $\prod_{i\in I} x_i \leqslant \prod_{i\in I} y_i$.*

Proof. **9**(i): Suppose $\sum_{i\in I} x_i$ and $\sum_{i\in I} y_i$ exist. For every $i \in I$, we have $x_i \leqslant \sum_{i\in I} x_i$ and $y_i \leqslant \sum_{i\in I} y_i$, hence also $x_i + y_i \leqslant \sum_{i\in I} x_i + \sum_{i\in I} y_i$ by **7**(iii)(iv). Thus, $\sum_{i\in I} x_i + \sum_{i\in I} y_i$ is an upper bound of $\{x_i + y_i : i \in I\}$. If z is an upper bound of $\{x_i + y_i : i \in I\}$, then z is an upper bound of $\{x_i : i \in I\}$, since $x_i \leqslant x_i + y_i \leqslant z$ for every $i \in I$, so $\sum_{i\in I} x_i \leqslant z$, and, similarly, $\sum_{i\in I} y_i \leqslant z$. It follows that $\sum_{i\in I} x_i + \sum_{i\in I} y_i \leqslant z$ by **7**(iii). This shows that $\sum_{i\in I} x_i + \sum_{i\in I} y_i$ is the least upper bound of $\{x_i + y_i : i \in I\}$, so the desired equation holds.

9(ii): Similar to **9**(i).

9(iii): Suppose $\sum_{i\in I} x_i$ and $\sum_{i\in I} y_i$ exist, and $x_i \leqslant y_i$ for every $i \in I$. Then $x_i + y_i = y_i$ and $x_i \cdot y_i = x_i$ for every $i \in I$ by **7**(v), so, by **9**(i), $\sum_{i\in I} x_i + \sum_{i\in I} y_i = \sum_{i\in I}(x_i + y_i) = \sum_{i\in I} y_i$, and, by **9**(ii), $\prod_{i\in I} x_i \cdot \prod_{i\in I} y_i = \prod_{i\in I}(x_i \cdot y_i) = \prod_{i\in I} x_i$. Thus, by **7**(v), $\sum_{i\in I} x_i \leqslant \sum_{i\in I} y_i$ and $\prod_{i\in I} x_i \leqslant \prod_{i\in I} y_i$. □

Theorem 10. *Let $\mathfrak{B}$ be a Boolean algebra. Let I and J be arbitrary sets. Suppose $x_i \in B$ for every $i \in I \cup J$.*

(i) *If $\sum_{i\in I} x_i$ and $\sum_{i\in J} x_i$ exist, then $\sum_{i\in I\cup J} x_i$ also exists, and $\sum_{i\in I\cup J} x_i = \sum_{i\in I} x_i + \sum_{i\in J} x_i$.*

(ii) *If $\prod_{i\in I} x_i$ and $\prod_{i\in J} x_i$ exist, then $\prod_{i\in I\cup J} x_i$ also exists, and $\prod_{i\in I\cup J} x_i = \prod_{i\in I} x_i \cdot \prod_{i\in J} x_i$.*

(iii) *If $\sum_{i\in I} x_i$ and $\sum_{i\in J} x_i$ exist and $I \subseteq J$, then $\sum_{i\in I} x_i \leqslant \sum_{i\in J} x_i$.*

(iv) *If $\prod_{i\in I} x_i$ and $\prod_{i\in J} x_i$ exist and $I \subseteq J$, then $\prod_{i\in J} x_i \leqslant \prod_{i\in I} x_i$.*

Proof. **10**(i): Suppose $\sum_{i\in I} x_i$ and $\sum_{i\in J} x_i$ exist. Then $\sum_{i\in I} x_i + \sum_{i\in J} x_i$ is an upper bound of $\{x_i : i \in I \cup J\}$, for if $i \in I \cup J$, then either $i \in I$ or $i \in J$. In case $i \in I$, we have $x_i \leqslant \sum_{i\in I} x_i \leqslant \sum_{i\in I} x_i + \sum_{i\in J} x_i$ by **7**(iv), and similarly, $x_i \leqslant \sum_{i\in I} x_i + \sum_{i\in J} x_i$ in case $i \in J$. If z is an upper bound of $\{x_i : i \in I \cup J\}$, then z is both an upper bound of $\{x_i : i \in I\}$ and an upper bound of $\{x_i : i \in J\}$. Hence $\sum_{i\in I} x_i \leqslant z$ and $\sum_{i\in J} x_i \leqslant z$,

so $\sum_{i\in I} x_i + \sum_{i\in J} x_i \leqslant z$ by (Ba_1) and **6**. We have shown that $\sum_{i\in I} x_i + \sum_{i\in J} x_i$ is the least upper bound of $\{x_i : i \in I \cup J\}$, so the desired equation holds.

10(ii): Similar to **10**(i).

10(iii): Assume $\sum_{i\in I} x_i$ and $\sum_{i\in J} x_i$ exist and $I \subseteq J$. If $i \in I$, then $i \in J$ since $I \subseteq J$, so $x_i \leqslant \sum_{i\in J} x_i$. Thus $\sum_{i\in J} x_i$ is an upper bound of $\{x_i : i \in I\}$. But $\sum_{i\in I} x_i$ is the least upper bound of $\{x_i : i \in I\}$, so $\sum_{i\in I} x_i \leqslant \sum_{i\in J} x_i$.

10(iv): Similar to **10**(iii). □

3. Operators on Boolean algebras

This is a brief exposition of part of the theory of operators on Boolean algebras. It is based on [26], and contains only material needed later applications. The treatment is restricted to unary operators, i.e., functions mapping a Boolean algebra to itself.

Definition 11. For every Boolean algebra $\mathfrak{B}$ and every function f mapping B to B, f^δ is the *dual of* f, defined for every $x \in B$ by $f^\delta(x) = \overline{f(\bar{x})}$.

Theorem 12. *Every function f on a Boolean algebra $\mathfrak{B}$ is the dual of its dual,* i.e., $f^{\delta\delta} = f$.

Proof. By **3**(ii) and **11**, $f^{\delta\delta}(x) = \overline{f^\delta(\bar{x})} = \overline{\overline{f(\bar{\bar{x}})}} = f(x)$ for every $x \in B$, so $f = f^{\delta\delta}$. □

Definition 13. Let f and g be functions on a Boolean algebra $\mathfrak{B}$. *g is a conjugate of f* just in case for all $x, y \in B$, $f(x) \cdot y = 0$ iff $x \cdot g(y) = 0$.

Theorem 14. *Let f, g, and h be functions on a Boolean algebra $\mathfrak{B}$.*

(i) *If g and h are conjugates of f, then $g = h$.*

(ii) *The following statements are equivalent:*

(a) *g is a conjugate of f,*

(b) *f is a conjugate of g.*

Proof. **14**(i): Assume g and h are conjugates of f. Then, for all $x, y \in B$, we have $f(x) \cdot y = 0$ iff $x \cdot g(y) = 0$, and $f(x) \cdot y = 0$ iff $x \cdot h(y) = 0$. Therefore,

$$x \cdot g(y) = 0 \text{ iff } x \cdot h(y) = 0. \tag{5}$$

Consider a fixed y. Set $x = \overline{g(y)}$. Then $x \cdot g(y) = \overline{g(y)} \cdot g(y) = 0$ by **5**(ii) and **3**(viii). By (5), $\overline{g(y)} \cdot h(y) = 0$, so $h(y) \leqslant g(y)$ by **3**(viii) and **7**(v). Similarly, set $x = \overline{h(y)}$ and get $g(y) \leqslant h(y)$ from (5). By **7**(i), $g(y) = h(y)$.

14(ii): This part follows immediately from **13** and **3**(viii). □

In view of the symmetry expressed by **14**(ii), we shall say "f and g are conjugate" instead of "f is a conjugate of g".

Definition 15. A function f on a Boolean algebra $\mathfrak{B}$ is

(i) *normal* if $f(0) = 0$,

(ii) *monotonic* (or *increasing*) if $x \leqslant y$ implies $f(x) \leqslant f(y)$ for all $x, y \in B$,

(iii) *additive* (or *finitely additive*) if $f(x + y) = f(x) + f(y)$ for all $x, y \in B$,

(iv) *multiplicative* (or *finitely multiplicative*) if $f(x \cdot y) = f(x) \cdot f(y)$ for all $x, y \in B$,

(v) *completely additive* (or *positively additive*) if, for every indexed set $\{x_i : i \in I\} \subseteq B$, if $\sum_{i\in I} x_i$ exists and I is not empty then $\sum_{i\in I} f(x_i)$ also exists and $f\left(\sum_{i\in I} x_i\right) = \sum_{i\in I} f(x_i)$,

(vi) *universally additive* if it is both normal and completely additive,

(vii) *completely multiplicative* (or *positively multiplicative*) if, for every indexed set $\{x_i : i \in I\} \subseteq B$, if $\prod_{i\in I} x_i$ exists and I is not empty then $\prod_{i\in I} f(x_i)$ also exists and $f\left(\prod_{i\in I} x_i\right) = \prod_{i\in I} f(x_i)$,

(viii) *universally multiplicative* if f is completely multiplicative and $f(1) = 1$.

Theorem 16 (Jónsson and Tarski [26, Theorem 1.2]). *For every Boolean algebra $\mathfrak{B}$ and every $x \in B$, the functions $x \cdot (-)$ and $(-) \cdot x$ are universally additive and completely multiplicative, and the functions $x + (-)$ and $(-) + x$ are universally multiplicative and completely additive.*

Proof. We only show that $x \cdot (-)$ is universally additive. First note that $x \cdot (-)$ is normal by **5**(vi). To show that $x \cdot (-)$ completely additive, assume $\sum_{i\in I} y_i$ exists and I is not empty. We wish to show $x \cdot \sum_{i\in I} y_i$ is the least upper bound of $\{x \cdot y_i : i \in I\}$. For every $j \in I$ we have $y_j \leqslant \sum_{i\in I} y_i$, so $x \cdot y_j \leqslant x \cdot \sum_{i\in I} y_i$ by **7**(iii) and **3**(viii). Therefore, $x \cdot \sum_{i\in I} y_i$ is an upper bound of $\{x \cdot y_i : i \in I\}$. Suppose z is an upper bound of $\{x \cdot y_i : i \in I\}$, i.e., , $x \cdot y_i \leqslant z$ for every $i \in I$. By **7**(vi), this implies $y_i \leqslant \bar{x} + z$ for every $i \in I$, hence $\sum_{i\in I} y_i \leqslant \bar{x} + z$, and finally, $x \cdot \sum_{i\in I} y_i \leqslant z$ by **7**(vi). □

If $\mathfrak{B}$ has more than one element then the function $x \cdot (-)$ is not universally multiplicative and $x + (-)$ is not universally additive since, for example, $0 \cdot \left(\prod_{i\in\emptyset} 1\right) = 0 \cdot 1 = 0 \neq 1 = \prod_{i\in\emptyset}\left(0 \cdot 1\right)$ and $1 + \left(\sum_{i\in\emptyset} 0\right) = 1 + 0 = 1 \neq 0 = \sum_{i\in\emptyset}\left(1 + 0\right)$.

Theorem 17. (i) [26, p. 898] *Every completely additive function on a Boolean algebra is additive and every additive function is monotonic.*

(ii) *Every completely multiplicative function on a Boolean algebra is multiplicative and every multiplicative function is monotonic.*

(iii) *A function on a Boolean algebra is universally, completely, or finitely additive iff its dual is universally, completely, or finitely multiplicative, respectively.*

Theorem 18 (Jónsson and Tarski [26, Theorems 1.13 and 1.14]). (i) *The conjugate g of a function f on a Boolean algebra $\mathfrak{B}$, if it exists, is given by $g(y) = \prod\{x : y \leqslant f^{\delta}(x)\}$ for every $y \in B$.*

(ii) *The function f has a conjugate iff the following conditions are satisfied:*
(a) *f is universally additive,*
(b) $\prod\{x : y \leqslant f^{\delta}(x)\}$ *exists for every* $y \in B$.

Proof. **18**(i): Assume g is a conjugate of f. Then

$$\begin{aligned} g(y) &= \prod\{x : x \geqslant g(y)\} && \textbf{8}(\text{iv}) \\ &= \prod\{x : g(y) \cdot \overline{x} = 0\} && \textbf{7}(\text{v}) \\ &= \prod\{x : y \cdot f(\overline{x}) = 0\} && f \text{ and } g \text{ are conjugate} \\ &= \prod\{x : y \leqslant f^{\delta}(x)\} && \textbf{3}(\text{ii}), \textbf{7}(\text{v}), \textbf{11}. \end{aligned}$$

18(ii): First assume f has a conjugate function, say g. Since $0 = 0 \cdot g(1)$, it follows that $0 = f(0) \cdot 1 = f(0)$, so f is normal. Assume $\{x_i : i \in I\} \subseteq B$, $I \neq \emptyset$, and $\sum_{i \in I} x_i$ exists. Then

$$\begin{aligned} & f\Big(\sum_{i \in I} x_i\Big) \leqslant y \\ \text{iff}\ & f\Big(\sum_{i \in I} x_i\Big) \cdot \overline{y} = 0 && \text{by } \textbf{7}(\text{v}) \\ \text{iff}\ & \sum_{i \in I} x_i \cdot g(\overline{y}) = 0 && \text{since } f \text{ and } g \text{ are conjugate} \\ \text{iff}\ & \sum_{i \in I} x_i \leqslant \overline{g(\overline{y})} && \text{by } \textbf{7}(\text{v}) \\ \text{iff}\ & x_i \leqslant \overline{g(\overline{y})} \text{ for every } i \in I && \text{by } \textbf{1}(\text{iii}), \textbf{7}(\text{i}) \\ \text{iff}\ & x_i \cdot g(\overline{y}) = 0 \text{ for every } i \in I && \text{by } \textbf{7}(\text{v}) \\ \text{iff}\ & f(x_i) \cdot \overline{y} = 0 \text{ for every } i \in I && \text{since } f \text{ and } g \text{ are conjugate} \\ \text{iff}\ & f(x_i) \leqslant y \text{ for every } i \in I && \text{by } \textbf{7}(\text{v}) \\ \text{iff}\ & y \text{ is an upper bound of } \{f(x_i) : i \in I\}. \end{aligned}$$

The first statement is true when $y = f\big(\sum_{i \in I} x_i\big)$, so $f\big(\sum_{i \in I} x_i\big)$ is an upper bound of $\{f(x_i) : i \in I\}$. Reading in the other direction, we see that $f\big(\sum_{i \in I} x_i\big)$ is included in all the upper bounds of $\{f(x_i) : i \in I\}$. Thus $f\big(\sum_{i \in I} x_i\big)$ is the least upper bound of $\{f(x_i) : i \in I\}$, i.e., $f\big(\sum_{i \in I} x_i\big) = \sum_{i \in I} f(x_i)$. This shows that f is completely additive. Since f is also normal, f is universally additive. Finally, $\prod\{x : y \leqslant f^{\delta}(x)\}$ exists for every $y \in B$ by **18**(i).

For the converse, assume that f is universally additive (hence also montonic) and that $\prod\{x : y \leqslant f^{\delta}(x)\}$ exists for every $y \in B$. We will prove that f has a conjugate. We may define a function g by setting $g(y) = \prod\{x : y \leqslant f^{\delta}(x)\}$ for every $y \in B$. From this it follows, by **11**, **8**(iii), and **3**(ii), that

$$\overline{g(y)} = \overline{\prod\{x : y \leqslant \overline{f(\overline{x})}\}} = \sum\{\overline{x} : y \leqslant \overline{f(\overline{x})}\} = \sum\{x : y \leqslant \overline{f(x)}\}. \tag{6}$$

According to (6), $\overline{g(y)}$ contains every x such that $y \leqslant \overline{f(x)}$. Consequently, if $f(x) \cdot y = 0$, then $y \leqslant \overline{f(x)}$, hence $x \leqslant \overline{g(y)}$ by (6), which implies $x \cdot g(y) = 0$.

Conversely, if $x \cdot g(y) = 0$, then $x \leqslant \overline{g(y)}$, hence

$$\begin{aligned}
f(x) &\leqslant f\left(\overline{g(y)}\right) && f \text{ is monotonic} \\
&= f\left(\sum\{x : y \leqslant \overline{f(x)}\}\right) && (6) \\
&= \sum\{f(x) : y \leqslant \overline{f(x)}\} && f \text{ is universally additive} \\
&= \sum\{f(x) : f(x) \leqslant \overline{y}\} && \mathbf{7}(\mathrm{v}), \mathbf{3}(\mathrm{ii}) \\
&\leqslant \overline{y} && \mathbf{1}(\mathrm{iii}),
\end{aligned}$$

so $f(x) \cdot y = 0$. This completes the proof that $f(z) \cdot y = 0$ iff $z \cdot g(y) = 0$, so g is a conjugate of f. □

Theorem 19 (Jonsson and Tarski [26, Theorem 1.15]). *Let f and g be functions on a Boolean algebra $\mathfrak{B}$. The following statements are equivalent:*

(i) *f and g are conjugate.*

(ii) *For all $x, y \in B$,*
  (a) $f\left(x \cdot \overline{g(y)}\right) \leqslant f(x) \cdot \overline{y}$,
  (b) $g\left(y \cdot \overline{f(x)}\right) \leqslant g(y) \cdot \overline{x}$.

(iii) $f(0) = 0$, $g(0) = 0$, *and, for all $y, z \in B$,*
  (a) $f(y) \cdot z \leqslant f(y \cdot g(z))$,
  (b) $g(z) \cdot y \leqslant g(z \cdot f(y))$.

Proof. **19**(i) iff **19**(ii): Suppose f and g are conjugate. Then f is monotonic by **17**(i) and **18**(ii), so $f(x \cdot \overline{g(y)}) \leqslant f(x)$. Furthermore, from $x \cdot \overline{g(y)} \cdot g(y) = 0$ we get $f(x \cdot \overline{g(y)}) \cdot y = 0$ since f and g are conjugate, so $f(x \cdot \overline{g(y)}) \leqslant \overline{y}$. Thus $f(x \cdot \overline{g(y)}) \leqslant f(x) \cdot \overline{y}$. By symmetry, we also have $g(x \cdot \overline{f(y)}) \leqslant g(x) \cdot \overline{y}$. Thus **19**(i) implies **19**(ii). For the converse, assume **19**(ii). If $x \cdot g(y) = 0$, then $x \cdot \overline{g(y)} = x$, hence $f(x) = f(x \cdot \overline{g(y)}) \leqslant f(x) \cdot \overline{y} \leqslant \overline{y}$ by **19**(ii)(a), so $f(x) \cdot y = 0$. Conversely, if $f(x) \cdot y = 0$, then $y = y \cdot \overline{f(x)}$, so $g(y) = g(y \cdot \overline{f(x)}) \leqslant \overline{x}$ by **19**(ii)(b), hence $x \cdot g(y) = 0$. Thus f and g are conjugate. □

19(i) iff **19**(iii): Suppose f and g are conjugate. Then f and g are normal by **18**(ii), i.e., $f(0) = 0 = g(0)$. To show that **19**(iii)(a) holds we first observe that f is additive by **18**(ii) and that **19**(ii)(a) holds by the first part of the proof. Then

$$\begin{aligned}
f(y) \cdot z &= f\left(y \cdot g(z) + y \cdot \overline{g(z)}\right) \cdot z && \mathbf{3}(\mathrm{xi}) \\
&= \left(f(y \cdot g(z)) + f(y \cdot \overline{g(z)})\right) \cdot z && f \text{ is additive} \\
&\leqslant \left(f(y \cdot g(z)) + f(y) \cdot \overline{z}\right) \cdot z && \mathbf{19}(\mathrm{ii})(\mathrm{a}), \mathbf{7}(\mathrm{iii}) \\
&\leqslant f(y \cdot g(z)) && \mathbf{3}(\mathrm{viii})(\mathrm{ix})(\mathrm{xv}), \mathbf{5}(\mathrm{ii})(\mathrm{vi})(\mathrm{vii}), \mathbf{7}(\mathrm{iv})
\end{aligned}$$

The proof of **19**(iii)(b) is similar. Thus **19**(i) implies **19**(iii). For the converse, assume **19**(iii). If $f(y) \cdot z = 0$, then, since g is normal and **19**(iii)(b) holds, $g(z) \cdot y \leqslant g(z \cdot f(y)) = g(0) = 0$. Conversely, if $g(z) \cdot y = 0$ then $f(y) \cdot z = 0$ by the normality of g and **19**(iii)(a). Thus f and g are conjugate. □

Definition 20. For any function f and any $i \in \omega$, f^i is the result of composing f with itself i times. More precisely, $f^0(x) = x$ and $f^{i+1} = f(f^i(x))$ for every x in the domain of f and every $i \in \omega$.

Theorem 21. *Let $\mathfrak{B}$ be Boolean algebra.*

(i) *Every constant function on $\mathfrak{B}$ is monotonic. The identity function on $\mathfrak{B}$ is monotonic. If f and g are monotonic functions on $\mathfrak{B}$, then the functions $f(\text{-}) \cdot g(\text{-})$ and $f(\text{-}) + g(\text{-})$ are also monotonic.*

(ii) *If $\mathfrak{B}$ is complete and f_i is a monotonic function on $\mathfrak{B}$ for every $i \in I$, then $\sum_{i\in I} f_i(\text{-})$ and $\prod_{i\in I} f_i(\text{-})$ are also monotonic.*

(iii) [10, Lemma 1.4.1] *If f is a binary operation on a complete Boolean algebra $\mathfrak{B}$ such that $f(\text{-},z)$ is monotonic for every $z \in B$, then $\prod\{z : z \geqslant f(\text{-},z)\}$ and $\sum\{z : z \leqslant f(\text{-},z)\}$ are monotonic unary functions on $\mathfrak{B}$.*

Proof. 21(iii): Assume $x \leqslant y$. Then $f(x,z) \leqslant f(y,z)$ for every $z \in B$ by assumption. It follows that $\{z : z \geqslant f(y,z)\} \subseteq \{z : z \geqslant f(x,z)\}$ and $\{z : z \leqslant f(x,z)\} \subseteq \{z : z \leqslant f(y,z)\}$. These inclusions imply that $\prod\{z : z \geqslant f(x,z)\} \leqslant \prod\{z : z \geqslant f(y,z)\}$ and $\sum\{z : z \leqslant f(x,z)\} \leqslant \sum\{z : z \leqslant f(y,z)\}$ by **10**(iii)(iv). Thus $\prod\{z : z \geqslant f(\text{-},z)\}$ and $\sum\{z : z \leqslant f(\text{-},z)\}$ are monotonic. □

4. Tarski's Fixed Point Theorem

In 1927 Knaster and Tarski [28] proved that if a function maps subsets of a set U to subsets of U and is increasing (with respect to set-theoretical inclusion), then it has at least one fixed point. In 1939 Tarski proved a lattice-theoretical generalization of this theorem. The generalization was published (along with many applications) in 1955 [53].

Theorem 22 ([53, Theorem 1]). *Assume that $\langle A, \leqslant\rangle$ is a complete lattice and that f is a monotonic function from A to A, that is, if $x, y \in A$ and $x \leqslant y$ then $f(x) \leqslant f(y)$. Then*

(i) $\langle \{x : x = f(x)\}, \leqslant\rangle$ *is a nonempty complete lattice.*

(ii) $\sum\{x : x \leqslant f(x)\} = \sum\{x : x = f(x)\} \in \{x : x = f(x)\}$.

(iii) $\prod\{x : x \geqslant f(x)\} = \prod\{x : x = f(x)\} \in \{x : x = f(x)\}$.

Proof. 22(ii): This proof follows Tarski's proof [53]. Let E, C, and F be the subsets of A that are expanded, contracted, and fixed by f, respectively, i.e.,

$$E = \{x : x \leqslant f(x)\}, \quad C = \{x : x \geqslant f(x)\}, \quad F = \{x : x = f(x)\}.$$

First we prove

$$\text{if } X \subseteq E \text{ then } x \leqslant f(\textstyle\sum X) \text{ for every } x \in X. \tag{7}$$

Assume $X \subseteq E$. Then $\sum X$ exists since $\langle A, \leqslant \rangle$ is complete. We prove the conclusion of (7) as follows.

(a)	$x \in X$	hypothesis
(b)	$x \leqslant f(x)$	(a), $X \subseteq E$, definition of E
(c)	$x \leqslant \sum X$	(a), definition of $\sum$
(d)	$f(x) \leqslant f(\sum X)$	(c), f is monotonic
(e)	$x \leqslant f(\sum X)$	(b), (d), $\leqslant$ is transitive.

According to (7), $f(\sum X)$ is a upper bound of X whenever $X \subseteq E$, so

$$\sum X \leqslant f(\sum X) \text{ for every } X \subseteq E. \tag{8}$$

From (8) and the definition of E we have

$$\sum X \in E \text{ for every } X \subseteq E. \tag{9}$$

Next we prove that

$$E \text{ is closed under } f \tag{10}$$

as follows.

(a)	$x \in E$	hypothesis
(b)	$x \leqslant f(x)$	(a), definition of E
(c)	$f(x) \leqslant f(f(x))$	(b), f is monotonic
(d)	$f(x) \in E$	(c), definition of E.

From (9) and (10) we see that

$$f(\sum E) \in E. \tag{11}$$

It follows from (11) that

$$f(\sum E) \leqslant \sum E. \tag{12}$$

From (8) and (12) we get

$$f(\sum E) = \sum E. \tag{13}$$

By (13) and the definition of F,

$$\sum E \in F, \tag{14}$$

so F is not empty. From (14) we have

$$\sum E \leqslant \sum F. \tag{15}$$

Note that $F = E \cap C \subseteq E$, hence $\sum F \leqslant \sum E$. Together with (15), this gives us

$$\sum E = \sum F. \tag{16}$$

In view of (14) and (16), we have completed the proof of **22**(ii). The proof of **22**(iii) is similar.

22(i): We have seen that F is nonempty, so what remains is to show that $\langle F, \leqslant \rangle$ is a complete lattice. For this it suffices to show that every $X \subseteq F$ has a join and meet in $\langle F, \leqslant \rangle$. Let $X \subseteq F$. Consider the complete sublattice $\langle \{x : \sum X \leqslant x\}, \leqslant \rangle$ of $\langle A, \leqslant \rangle$. We prove that

$$\{x : \sum X \leqslant x\} \text{ is closed under } f \tag{17}$$

as follows.

(a)	$\sum X \leqslant x$	hypothesis
(b)	$f(\sum X) \leqslant f(x)$	(a), f is monotonic
(c)	$\sum X \leqslant f(\sum X)$	(8), $X \subseteq F \subseteq E$
(d)	$\sum X \leqslant f(x)$	(b), (c), $\leqslant$ is transitive.

Let f' be the restriction of f to $\{x : \sum X \leqslant x\}$. Let $F' = \{x : \sum X \leqslant x = f(x)\}$. Thus, F' is the set of fixed points of f that are upper bounds of X. When **22**(ii) is applied to $\langle \{x : \sum X \leqslant x\}, \leqslant \rangle$ and f', the conclusion is that $\sum F' \in F'$. Hence, $\sum F' \in F$ since $F' \subseteq F$, and $\sum F'$ is an upper bound of X since $\sum X \leqslant \sum F'$. $\sum F'$ is the least upper bound of the set of fixed points of f that are upper bounds of X, so $\sum F'$ is the least upper bound of X in $\langle F, \leqslant \rangle$. Similarly, the greatest lower bound of X in $\langle F, \leqslant \rangle$ exists, so $\langle F, \leqslant \rangle$ is a complete lattice. □

It may happen that the least upper bound of $X \subseteq F$ in the lattice $\langle F, \leqslant \rangle$ of fixed points may differ from the least upper bound of X in the original lattice $\langle A, \leqslant \rangle$. For an example, let A be the set of all subsets of $\{a, b, c\}$, ordered by inclusion. For each $S \subseteq \{a, b, c\}$, let $f(S) = \{a, b, c\}$ if S has two or more elements and let $f(S) = S$ if S has fewer than two elements. Let F be the set of fixed points of f, and let $X = \{\{a\}, \{b\}\}$. Note that $X \subseteq F$. The least upper bound of X in $\langle A, \leqslant \rangle$ is $\{a, b\}$, but the least upper bound of X in $\langle F, \leqslant \rangle$ is $\{a, b, c\}$.

5. Relation algebras

Peirce [42, 43], and especially [44], combined the work of Boole [4] and De Morgan [35, 36] to create a calculus of relations that was extensively developed by Schröder [50]. A fragment of this calculus was axiomatized by Tarski [52]. Tarski's axiomatization, in a slightly altered form, became the definition of relation algebras [6, 25, 27]. For further introductory and historical material on relation algebras, see [6, 23, 24, 27, 32, 33],

and [54]. This section contains just enough basic definitions and results for the applications given later. Most of the material in this section can be found in [6] or [27].

Definition 23. A *relation algebra* is an algebraic structure of the form

$$\mathfrak{A} = \langle A, +, {}^{-}, ;, {}^{\smile}, 1' \rangle,$$

where $\langle A, +, {}^{-} \rangle$ is a Boolean algebra, ; is a binary operation on A, ${}^{\smile}$ is a unary operation on A, and 1' is an element of A, such that the following axioms are satisfied for all $x, y, z \in A$:

(Ra_1) $x;y;z = x;(y;z)$,
(Ra_2) $(x + y);z = x;z + y;z$,
(Ra_3) $x;1' = x$,
(Ra_4) $\breve{\breve{x}} = x$,
(Ra_5) $(x + y)\breve{} = \breve{x} + \breve{y}$,
(Ra_6) $(x;y)\breve{} = \breve{y};\breve{x}$,
(Ra_7) $\breve{x};\overline{x;y} + \overline{y} = \overline{y}$.

An additional binary operation $\dagger$ on A is defined by

(Ra_8) $x \dagger y = \overline{\breve{x};\overline{y}}$.

Note that (Ra_7) is equivalent to $\breve{x};\overline{x;y} \leqslant \overline{y}$ and to $\breve{x};\overline{x;y} \cdot y = 0$, by **7**(v).

Let U be an arbitrary set, called "the universe". Let $\mathrm{Re}(U)$ be the set of all binary relations on the universe U, i.e., $\mathrm{Re}(U) = \{ x : x \subseteq U \times U \}$. We obtain a relation algebra

$$\mathfrak{Re}\,(U) = \langle \mathrm{Re}(U), +, {}^{-}, ;, {}^{\smile}, 1' \rangle$$

by defining 1' and the operations $+$, ${}^{-}$, ;, and ${}^{\smile}$ as follows. Let 1' be the identity relation on U, that is,

- $1' = \{ \langle u, u \rangle : u \in U \}$.

For any binary relations $x, y \in \mathrm{Re}(U)$, let

- $x + y = \{ \langle u, v \rangle : \langle u, v \rangle \in x \text{ or } \langle u, v \rangle \in y \}$,
- $\bar{x} = \{ \langle u, v \rangle : \langle u, v \rangle \in U \text{ and } \langle u, v \rangle \notin x \}$,
- $x;y = \{ \langle u, w \rangle : \text{there is some } v \in U \text{ such that } \langle u, v \rangle \in x \text{ and } \langle v, w \rangle \in y \}$,
- $\breve{x} = \{ \langle v, u \rangle : \langle u, v \rangle \in U \}$.

Thus, $x + y$ is the *union* of x and y, $\bar{x}$ is the *complement* of x with respect to $U \times U$, $x;y$ is the *relative product* of x and y, and $\breve{x}$ is the *converse* of x. It is a straightforward exercise to verify that $\mathfrak{Re}\,(U)$ satisfies axioms (Ba_1)–(Ba_3) and (Ra_1)–(Ra_7). Therefore, $\mathfrak{Re}\,(U)$ is a relation algebra. By definition (Ba_4), $x \cdot y$ is the *intersection* of x and y. The relation $x \dagger y$, defined by (Ra_8), is called the *relative sum* of x and y.

If U is empty, then $\mathfrak{Re}\,(U)$ is an algebra with just one element in it. If U contains exactly one element, then $\mathfrak{Re}\,(U)$ is *Boolean*, that is, it satisfies the identity $1' = 1$. On the other hand, if $\mathfrak{Re}\,(U)$ satisfies $1' = 1$, then U is either empty or has exactly

one element. If U is finite, so is $\mathfrak{Re}(U)$. If U is a countable infinite set, then $\mathfrak{Re}(U)$ is an uncountable algebra.

Axioms (Ra_1)–(Ra_7) are equations, so relation algebras form a variety, that is, the class of relation algebras is closed under the formation of subalgebras, homomorphic images, and direct products. We can therefore construct other examples of relation algebras by applying these operations to algebras of the form $\mathfrak{Re}(U)$. For example, $\mathfrak{Re}(U_0) \times \mathfrak{Re}(U_1)$ is a relation algebra whose elements are pairs of relations on U_0 and U_1, respectively. If U_0 and U_1 are disjoint, then the maximum element 1 of $\mathfrak{Re}(U_0) \times \mathfrak{Re}(U_1)$ is an equivalence relation with exactly two equivalence classes, namely U_0 and U_1.

Relation algebras whose elements are actually binary relations and whose operations are the set-theoretic ones defined above are called *proper*. A relation algebra is *representable* if it is isomorphic to a proper relation algebra. There are many relation algebras that are not representable. For an example, take a finite Boolean algebra $\mathfrak{B}$ with four atoms (16 elements altogether), define 1' to be one of the atoms, and let a, b, and c be the other three atoms. Define $\breve{}$ of $\mathfrak{B}$ by $\breve{x} = x$ for every $x \in B$. Define ; on the atoms of $\mathfrak{B}$ as follows. Let y and z be distinct atoms in $\{a,b,c\}$. Set $1';y = y = y;1'$, $y;y = \overline{y}$, and $y;z = y + z$. There is exactly one way to extend ; to a binary operation on all of $\mathfrak{B}$ that satisfies the distributivity conditions (Ra_2) and **24**(ix). This produces a finite nonrepresentable relation algebra $\mathfrak{A}$ [30]. One way to show that $\mathfrak{A}$ is not representable is to note first that the equation

$$t \cdot (u;v \cdot w);(x \cdot y;z)) \leqslant u;[(\breve{u};t \cdot v;x);\breve{z} \cdot v;y \cdot \breve{u};(t;\breve{z} \cdot w;y)];z. \tag{18}$$

holds in every representable relation algebra. (It suffices to check that (18) is true in every $\mathfrak{Re}(U)$.) Then check that (18) fails in $\mathfrak{A}$ when $t = a$, $u = c$, $v = c$, $w = a$, $x = b$, $y = b$, and $x = c$. Finite nonrepresentable relation algebras are quite numerous. The number of such algebras with n atoms is roughly 2^{n^3} when n is large [31]. See [32, p. 384]; [33, p. 448] for historical remarks concerning nonrepresentable relation algebras.

Theorem 24. *The following statements hold in every relation algebra.*

(i) $x \leqslant y$ *iff* $\breve{x} \leqslant \breve{y}$.
(ii) $\breve{0} = 0$.
(iii) $\breve{1} = 1$.
(iv) $\breve{\breve{x}} = \overline{\breve{x}}$.
(v) $(x \cdot y)\breve{} = \breve{x} \cdot \breve{y}$.
(vi) $0 = \breve{x} \cdot y$ *iff* $0 = x \cdot \breve{y}$.
(vii) *The function* $\breve{}$ *is universally additive and universally multiplicative.*
(viii) $\breve{1}' = 1'$.
(ix) $x;(y + z) = x;y + x;z$.
(x) *If* $x \leqslant y$ *then* $z;x \leqslant z;y$ *and* $x;z \leqslant y;z$.
(xi) *The functions* $x;(\text{-})$ *and* $\breve{x};(\text{-})$ *are conjugate.*

(xii) $\overline{y;x};\check{x} \leqslant \overline{y}$.
(xiii) *The functions* $(\text{-});x$ *and* $(\text{-});\check{x}$ *are conjugate.*
(xiv) $x;y \cdot z = 0$ *iff* $\check{x};z \cdot y = 0$ *iff* $z;\check{y} \cdot x = 0$.
(xv) *The functions* $x;(\text{-})$ *and* $(\text{-});x$ *are universally additive.*
(xvi) $x;y \cdot z \leqslant x;(y \cdot \check{x};z)$.
(xvii) $y;x \cdot z \leqslant (y \cdot z;\check{x});x$.
(xviii) $x;0 = 0 = 0;x$.
(xix) $x;1' = x = 1';x$.
(xx) $x \leqslant x;1$.
(xxi) $x \leqslant 1;x$.
(xxii) $1;1 = 1$.
(xxiii) $x;y \cdot \overline{x;z} = x;(y \cdot \overline{z}) \cdot \overline{x;z}$.
(xxiv) $\overline{x;y} + x;z = \overline{x;(y \cdot \overline{z})} + x;z$.
(xxv) *If* $x;1 = x$ *then* $\overline{x};1 = \overline{x}$.
(xxvi) *If* $x;1 = x$ *then* $(x \cdot y);z = x \cdot y;z$.
(xxvii) *If* $x;1 = x$ *and* $y;1 = y$ *then* $(x \cdot y);1 = x \cdot y$.
(xxviii) *If* $x;1 = x$ *then* $(x \cdot 1');y = x \cdot y$.
(xxix) *If* $x;1 = x$ *then* $(y \cdot \check{x});z = y;(x \cdot z) = (y \cdot \check{x});(x \cdot z)$.
(xxx) *If* $x \leqslant 1'$ *then* $\check{x} = x$.
(xxxi) *If* $x \leqslant 1'$ *then* $x;1 \cdot y = x;y$.
(xxxii) *If* $x \leqslant 1'$ *then* $\overline{x;1} \cdot 1' = \overline{x} \cdot 1'$.
(xxxiii) *If* $x \leqslant 1'$ *and* $y \leqslant 1'$ *then* $x;y = x \cdot y$.
(xxxiv) *If* $x \leqslant 1'$ *and* $y \leqslant 1'$ *then* $x;z \cdot x;y = (x \cdot y);z$.
(xxxv) *If* $x \leqslant 1'$ *then* $x;y \cdot \overline{z} = x;y \cdot \overline{x;z}$.

Proof. **24**(i): Suppose $x \leqslant y$, i.e., $x + y = y$. Then $\check{y} = (x + y)\check{} = \check{x} + \check{y}$ by (Ra_5), so $\check{x} \leqslant \check{y}$. Conversely, if $\check{x} \leqslant \check{y}$, then $\check{x} + \check{y} = \check{y}$, so, by (Ra_4) and (Ra_5), $x + y = \check{\check{x}} + \check{\check{y}} = (\check{x} + \check{y})\check{} = (\check{y})\check{} = y$, hence $\check{x} \leqslant \check{y}$.

24(ii):
$$\begin{aligned} \check{0} &= 0 + \check{0} && \textbf{5}(\mathrm{vii}),\ (\mathrm{Ba}_2) \\ &= \check{\check{0}} + \check{0} && (\mathrm{Ra}_4) \\ &= (\check{0} + 0)\check{} && (\mathrm{Ra}_5) \\ &= (\check{0})\check{} && \textbf{5}(\mathrm{vii}) \\ &= 0 && (\mathrm{Ra}_4). \end{aligned}$$

24(iii):
$$\begin{aligned} \check{1} &= (1 + \check{1})\check{} && \textbf{5}(\mathrm{v}),\ (\mathrm{Ba}_2) \\ &= \check{1} + \check{\check{1}} && (\mathrm{Ra}_5) \\ &= \check{1} + 1 && (\mathrm{Ra}_4) \\ &= 1 && \textbf{5}(\mathrm{v}). \end{aligned}$$

24(iv): For every y, $\check{y} + \check{\overline{y}} = (y + \overline{y})\check{} = \check{1} = 1$ by (Ra_5), **5**(i), and **24**(iii), so

$$\overline{\check{y}} + \check{\overline{y}} = \check{\overline{y}} \tag{19}$$

by **3**(ii) and **7**(v). Then

$$\begin{aligned}
\breve{\bar{x}} &= \bar{\breve{x}} + \breve{\bar{x}} && (19)\\
&= \breve{\bar{\breve{x}}} + \bar{\breve{\breve{x}}} && (\mathrm{Ra}_4)\\
&= \left(\bar{\breve{\breve{x}}} + \breve{\bar{\breve{x}}}\right)\breve{} && (\mathrm{Ra}_5)\\
&= \left(\bar{\breve{\breve{x}}}\right)\breve{} && (\mathrm{Ba}_2),\ (19)\\
&= \bar{\breve{x}} && (\mathrm{Ra}_4).
\end{aligned}$$

24(v): $$\begin{aligned}
(x \cdot y)\breve{} &= \overline{(\bar{x} + \bar{y})\breve{}} && (\mathrm{Ba}_4)\\
&= \overline{(\bar{x} + \bar{y})\breve{}} && \mathbf{24}(\mathrm{iv})\\
&= \bar{\breve{\bar{x}}} + \bar{\breve{\bar{y}}} && (\mathrm{Ra}_5)\\
&= \bar{\breve{\bar{x}}} + \bar{\breve{\bar{y}}} && \mathbf{24}(\mathrm{iv})\\
&= \breve{x} \cdot \breve{y} && (\mathrm{Ba}_4).
\end{aligned}$$

24(vi): Assume $0 = \breve{x} \cdot y$. Then

$$\begin{aligned}
0 &= \breve{0} && \mathbf{24}(\mathrm{ii})\\
&= (\breve{x} \cdot y)\breve{} && 0 = \breve{x} \cdot y\\
&= \breve{\breve{x}} \cdot \breve{y} && \mathbf{24}(\mathrm{v})\\
&= x \cdot \breve{y} && (\mathrm{Ra}_4).
\end{aligned}$$

The proof of the converse is similar.

24(vii): By **24**(vi), $\breve{}$ is a conjugate of $\breve{}$. It follows that $\breve{}$ is universally additive by **18**(ii). By **24**(iv) and **3**(ii), $\breve{}$ is the dual of $\breve{}$, so $\breve{}$ is also universally multiplicative by **17**(iii).

24(viii): $$\begin{aligned}
\breve{1}' &= \breve{1}';1' && (\mathrm{Ra}_3)\\
&= \breve{1}';\breve{1}' && (\mathrm{Ra}_4)\\
&= \left(\breve{1}';1'\right)\breve{} && (\mathrm{Ra}_6)\\
&= \left(\breve{1}'\right)\breve{} && (\mathrm{Ra}_3)\\
&= 1' && (\mathrm{Ra}_4).
\end{aligned}$$

24(ix): $$\begin{aligned}
x;(y+z) &= \breve{\breve{x}};\left(\breve{\breve{y}} + \breve{\breve{z}}\right) && (\mathrm{Ra}_4)\\
&= \breve{\breve{x}};(\breve{y} + \breve{z})\breve{} && (\mathrm{Ra}_5)\\
&= ((\breve{y} + \breve{z});\breve{x})\breve{} && (\mathrm{Ra}_6)\\
&= (\breve{y};\breve{x} + \breve{z};\breve{x})\breve{} && (\mathrm{Ra}_2)\\
&= (\breve{y};\breve{x})\breve{} + (\breve{z};\breve{x})\breve{} && (\mathrm{Ra}_5)\\
&= \breve{\breve{x}};\breve{\breve{y}} + \breve{\breve{x}};\breve{\breve{z}} && (\mathrm{Ra}_6)\\
&= x;y + x;z && (\mathrm{Ra}_4).
\end{aligned}$$

24(x): Suppose $x \leqslant y$, i.e., $x + y = y$. Then, by **24**(ix), $z;x + z;y = z;(x + y) = z;y$, so $z;x \leqslant z;y$, and $x;z + y;z = (x + y);z = y;z$ by (Ra_2), so $x;z \leqslant y;z$ as well.

24(xi): Let x be fixed. Define functions f and g by $f(y) = x;y$ and $g(y) = \breve{x};y$ for every y. By **24**(x), f and g are monotonic. Then

$$\begin{aligned} g\left(y \cdot \overline{f(z)}\right) &\leqslant g(y) \cdot g\left(\overline{f(z)}\right) && g \text{ is monotonic, } \mathbf{7}(\text{iv}) \\ &= g(y) \cdot \breve{x};\overline{x;z} && \\ &\leqslant g(y) \cdot \bar{z} && (\text{Ra}_7),\ \mathbf{3}(\text{viii}),\ \mathbf{7}(\text{iii}), \end{aligned}$$

so **19**ii(b) holds, and

$$\begin{aligned} f\left(z \cdot \overline{g(y)}\right) &\leqslant f(z) \cdot f\left(\overline{g(y)}\right) && f \text{ is monotonic, } \mathbf{7}(\text{iv}) \\ &= f(z) \cdot x;\breve{\overline{x;y}} && \\ &= f(z) \cdot \breve{x};\breve{\overline{x;y}} && (\text{Ra}_4) \\ &\leqslant f(z) \cdot \bar{y} && (\text{Ra}_7),\ \mathbf{3}(\text{viii}),\ \mathbf{7}(\text{iii}), \end{aligned}$$

so **19**(ii)(a) holds as well. It follows by **19** that f and g are conjugate, as desired.

$$\begin{aligned} \mathbf{24}(\text{xii}):\quad \overline{y;x};\breve{x} &= (\overline{y;x};\breve{x})\breve{} && (\text{Ra}_4) \\ &= \left(\breve{x};(\overline{y;x})\breve{}\right)\breve{} && (\text{Ra}_6) \\ &= \left(\breve{x};\overline{(y;x)\breve{}}\right)\breve{} && \mathbf{24}(\text{iv}) \\ &= \left(\breve{x};\breve{\overline{x};\bar{y}}\right)\breve{} && (\text{Ra}_6) \\ &\leqslant \left(\breve{\bar{y}}\right)\breve{} && (\text{Ra}_7),\ \mathbf{24}(\text{i}) \\ &= \left(\breve{\bar{y}}\right)\breve{} && \mathbf{24}(\text{iv}) \\ &= \bar{y} && (\text{Ra}_4). \end{aligned}$$

24(xiii): Let x be fixed. Define functions f and g by $f(y) = y;x$ and $g(y) = y;\breve{x}$ for every y. By **24**(x), f and g are monotonic. Then

$$\begin{aligned} g\left(y \cdot \overline{f(z)}\right) &\leqslant g(y) \cdot g\left(\overline{f(z)}\right) && g \text{ is monotonic, } \mathbf{7}(\text{iv}) \\ &\leqslant g(y) \cdot \bar{z} && \mathbf{24}(\text{xii}),\ \mathbf{3}(\text{viii}),\ \mathbf{7}(\text{iii}), \end{aligned}$$

so **19**(ii)(b) holds, and

$$\begin{aligned} f\left(z \cdot \overline{g(y)}\right) &\leqslant f(z) \cdot f\left(\overline{g(y)}\right) && f \text{ is monotonic, } \mathbf{7}(\text{iv}) \\ &\leqslant f(z) \cdot \bar{y} && (\text{Ra}_4),\ \mathbf{24}(\text{xii}),\ \mathbf{3}(\text{viii}),\ \mathbf{7}(\text{iii}), \end{aligned}$$

so **19**(ii)(a) holds as well. Therefore, f and g are conjugate by **19**.

24(xiv): This part follows immediately from **24**(xi) and **24**(xiii). In fact, **24**(xiv) is equivalent to the conjunction of **24**(xi) and **24**(xiii).

24(xv): This part follows immediately from **24**(xi) and **24**(xiii) by **18**(ii).

24(xvi): The desired equation is identical to equation **19**(iii)(a) with $f = x;(\text{-})$ and $g = \breve{x};(\text{-})$, and it therefore holds by **24**(xi) and **19**.

24(xvii): The desired equation is identical to equation **19**(iii)(a) with $f = (\text{-});x$ and $g = (\text{-});\breve{x}$, and it therefore holds by **24**(xiii) and **19**.

24(xviii): By **24**(xv) and **15**(vi), $x;(\text{-})$ and $(\text{-});x$ are normal, i.e., $x;0 = 0 = 0;x$.

24(xix): $x;1' = x \quad (Ra_3)$
$= \breve{\breve{x}} \quad (Ra_4)$
$= (\breve{x};1')\breve{} \quad (Ra_3)$
$= \breve{1}';\breve{\breve{x}} \quad (Ra_6)$
$= \breve{1}';x \quad (Ra_4)$
$= 1';x \quad$ **24**(viii).

24(xx): $x = x;1' \quad (Ra_3)$
$\leqslant x;1 \quad$ **24**(x).

24(xxi): $x = 1';x \quad$ **24**(xix)
$\leqslant 1;x \quad$ **24**(x).

24(xxii): $1 \leqslant 1;1 \quad$ **24**(xx)
$\leqslant 1 \quad$ **7**(ii),

so $1 = 1;1$.

24(xxiii): We have

$$x;y \cdot \overline{x;z} \leqslant x;(y \cdot \breve{x};\overline{x;z}) \quad \textbf{24}(\text{xvi})$$
$$\leqslant x;(y \cdot \bar{z}) \quad \textbf{24}(\text{x})(\text{xii}).$$

So $x;y \cdot \overline{x;z} = x;(y \cdot \bar{z}) \cdot \overline{x;z}$ by **7**.

24(xxiv): This follows from **24**(xxiii) by **3**(ii)(xvi)(xvii).

24(xxv): Assume $x;1 = x$. Then

$\bar{x};1 = \overline{x;1};1 \quad x;1 = x$
$= \overline{x;1};\breve{1} \quad$ **24**(iii)
$\leqslant \bar{x} \quad$ **24**(xii)
$\leqslant \bar{x};1 \quad$ **24**(xx),

so $\bar{x} = \bar{x};1$.

24(xxvi): Assume $x;1 = x$. Then

$(x \cdot y);z \leqslant x;1 \cdot y;z \quad$ **24**(x), **7**(iv)
$= x \cdot y;z \quad x;1 = x$
$\leqslant (y \cdot x;\breve{z});z \quad$ **24**(xvii)
$\leqslant (y \cdot x;1);z \quad$ **24**(x)
$= (x \cdot y);z \quad x;1 = x,$ **3**(viii),

so $(x \cdot y);z = (y \cdot x;\breve{z});z$.

24(xxvii): If $x;1 = x$ and $y;1 = y$ then $(x \cdot y);1 = x \cdot y;1 = x \cdot y$ by **24**(xxvi).

24(xxviii): If $x;1 = x$ then $(x \cdot 1');y = x \cdot 1';y = x \cdot y$ by **24**(xxvi)(xix).

24(xxix): Assume $x;1 = x$. We get $(y \cdot \breve{x});(x \cdot z) \leqslant (y \cdot \breve{x});z$ and $(y \cdot \breve{x});(x \cdot z) \leqslant y;(x \cdot z)$ by **24**(x). For the opposite inclusions, we argue as follows.

$$\begin{aligned}
(y \cdot \breve{x});z &= (y \cdot \breve{x});z \cdot 1 && \textbf{5}(\text{viii}) \\
&\leqslant (y \cdot \breve{x});(z \cdot (y \cdot \breve{x})\breve{\ });1) && \textbf{24}(\text{xvi}) \\
&= (y \cdot \breve{x});(z \cdot (\breve{y} \cdot x);1) && \textbf{24}(\text{v}), (\text{Ra}_4) \\
&\leqslant (y \cdot \breve{x});(z \cdot x;1) && \textbf{24}(\text{x}) \\
&= (y \cdot \breve{x});(z \cdot x) && x;1 = x,
\end{aligned}$$

$$\begin{aligned}
y;(x \cdot z) &= y;(x \cdot z) \cdot 1 && \textbf{5}(\text{viii}) \\
&\leqslant (y \cdot 1;(x \cdot z)\breve{\ });(x \cdot z) && \textbf{24}(\text{xvii}) \\
&\leqslant (y \cdot 1;\breve{x});(x \cdot z) && \textbf{24}(\text{i})(\text{x}) \\
&= (y \cdot (x;1)\breve{\ });(x \cdot z) && \textbf{24}(\text{iii})(\text{v}) \\
&= (y \cdot \breve{x});(x \cdot z) && x;1 = x.
\end{aligned}$$

24(xxx): Assume $x \leqslant 1'$. First we show $x \leqslant \breve{x}$ as follows.

$$\begin{aligned}
x &= x;1' \cdot 1' && (\text{Ra}_3),\ x \leqslant 1' \\
&\leqslant x;(1' \cdot \breve{x};1') && \textbf{24}(\text{xvi}) \\
&\leqslant 1';(\breve{x};1') && \textbf{24}(\text{x}),\ x \leqslant 1' \\
&= \breve{x} && \textbf{24}(\text{xix}).
\end{aligned}$$

From this we get $\breve{x} \leqslant \breve{\breve{x}} = x$ by **24**(i) and (Ra_4), so $x = \breve{x}$ by **7**(i).

24(xxxi): Assume $x \leqslant 1'$. Then $\breve{x} \leqslant 1'$ by **24**(i)(viii), so

$$\begin{aligned}
x;1 \cdot y &\leqslant x;(1 \cdot \breve{x};y) && \textbf{24}(\text{xvi}) \\
&= x;\breve{x};y && \textbf{5}(\text{viii}), (\text{Ra}_1) \\
&\leqslant x;y && \breve{x} \leqslant 1',\ \textbf{24}(\text{x})(\text{xix}) \\
&\leqslant x;1 \cdot 1';y && x \leqslant 1',\ \textbf{24}(\text{xx}),\ \textbf{7}(\text{ii})(\text{iv}) \\
&= x;1 \cdot y && \textbf{24}(\text{xix}).
\end{aligned}$$

Therefore $x;1 \cdot y = x;y$.

24(xxxii): Assume $x \leqslant 1'$. We have $\overline{x;1} \cdot 1' \leqslant \overline{x} \cdot 1'$ by **24**(xx) and **7**(v). For the opposite inclusion, first note that $\breve{x} \leqslant 1'$ by **24**(i)(viii). Then

$$\begin{aligned}
\overline{x} \cdot 1' \cdot x;1 &\leqslant x;(1 \cdot \breve{x};(\overline{x} \cdot 1')) && \textbf{24}(\text{xvi}) \\
&= x;\breve{x};(\overline{x} \cdot 1') && \textbf{5}(\text{viii}), (\text{Ra}_1) \\
&\leqslant 1';1';\overline{x} \cdot x;1';1' && x \leqslant 1',\ \breve{x} \leqslant 1',\ \textbf{24}(\text{x}) \\
&= \overline{x} \cdot x && \textbf{24}(\text{xix}) \\
&= 0 && \textbf{5}(\text{ii}),
\end{aligned}$$

so $\overline{x} \cdot 1' \leqslant \overline{x;1}$ by **7**(v) and **3**(ii). It follows that $\overline{x;1} \cdot 1' = \overline{x} \cdot 1'$.

24(xxxiii): Assume $x \leqslant 1'$ and $y \leqslant 1'$. Then

$$\begin{aligned} x;y &\leqslant x;1' \cdot 1';y && \textbf{24}(x),\ x \leqslant 1',\ y \leqslant 1' \\ &= x \cdot y && \textbf{24}(xix) \\ &= x;1' \cdot y && \textbf{24}(xix) \\ &\leqslant x;(1' \cdot \breve{x};y) && \textbf{24}(xvi) \\ &\leqslant x;(\breve{1}';y) && \textbf{24}(i)(x),\ x \leqslant 1' \\ &= x;y && \textbf{24}(viii)(xix), \end{aligned}$$

so $x;y = x \cdot y$.

24(xxxiv): If $x \leqslant 1'$ and $y \leqslant 1'$ then

$$\begin{aligned} x;z \cdot y;z &\leqslant x;1 \cdot y;z && \textbf{24}(x) \\ &= x;y;z && \textbf{24}(xxxi), (Ra_1) \\ &= (x \cdot y);z && \textbf{24}(xxxiii), x \leqslant 1',\ y \leqslant 1' \\ &\leqslant x;z \cdot y;z && \textbf{24}(x) \end{aligned}$$

so $x;z \cdot y;z = (x \cdot y);z$.

24(xxxv): Assume $x \leqslant 1'$. We have $x;z \leqslant 1';z = z$ by **24**(x)(xix), so $\bar{z} \leqslant \overline{x;z}$ by **7**(v). Then

$$\begin{aligned} x;y \cdot \bar{z} &\leqslant x;y \cdot \overline{x;z} && \bar{z} \leqslant \overline{x;z},\ \textbf{16} \\ &= x;(y \cdot \breve{x};\overline{x;z}) && \textbf{24}(xvi) \\ &\leqslant x;(y \cdot \bar{z}) && (Ra_7), \textbf{24}(x) \\ &\leqslant x;y \cdot 1';\bar{z} && \textbf{24}(x), x \leqslant 1' \\ &= x;y \cdot \bar{z} && \textbf{24}(xix), \end{aligned}$$

so $x;y \cdot \bar{z} = x;y \cdot \overline{x;z}$. □

Definition 25. An element x of a relation algebra $\mathfrak{A}$ is a *domain element* if $x;1 = x$.

For every set U, the domain elements of $\mathfrak{Re}\ (U)$ are the relations of the form $W \times U$ where $W \subseteq U$. The next theorem shows that the set of domain elements in a complete relation algebra forms a complete Boolean algebra. For example, the Boolean algebra of all subsets of U is isomorphic to the Boolean algebra of domain elements of the complete relation algebra $\mathfrak{Re}\ (U)$.

Theorem 26. *Let $\mathfrak{A}$ be a relation algebra and let D be the set of domain elements of $\mathfrak{A}$. Then*

(i) $x;1 \in D$ *for every* $x \in A$.
(ii) D *is closed under* $^-$, $+$, *and* $\cdot$.
(iii) D *is closed under* $x;(\text{-})$ *for every* $x \in A$.
(iv) *If* $\{x_i : i \in I\} \subseteq D$ *and* $\sum_{i \in I} x_i$ *exists, then* $\sum_{i \in I} x_i \in D$.
(v) *If* $\{x_i : i \in I\} \subseteq D$ *and* $\prod_{i \in I} x_i$ *exists, then* $\prod_{i \in I} x_i \in D$.
(vi) *If* $x \in D$ *and* $\sum\{y : y \leqslant x + z;y\}$ *exists, then* $\sum\{y : y \leqslant x + z;y\} \in D$.

Proof. **26**(i): $(x;1);1 = x;(1;1) = x;1$ by (Ra_1) and **24**(xxii), so $x;1 \in D$.

26(ii): Assume $x \in D$, i.e., $x;1 = x$. Then $\bar{x};1 = \bar{x}$ by **24**(xxv), so $\bar{x} \in D$. If $x, y \in D$ then $(x+y);1 = x;1 + y;1 = x + y$ by (Ra_2), so $x + y \in D$, and $x \cdot y \in D$ by **24**(xxvii).

26(iii): Let $x \in A$ and $y \in D$. Then $y;1 = y$, so, by (Ra_1), $x;y;1 = x;(y;1) = x;y$, and hence $x;y \in D$.

26(iv): Assume $\{x_i : i \in I\} \subseteq D$ and $\sum_{i\in I} x_i$ exists. Then $\sum_{i\in I} x_i = \sum_{i\in I}(x_i;1) = \left(\sum_{i\in I} x_i\right);1$ by **24**(xv), so $\sum_{i\in I} x_i \in D$.

26(v): This part follows from **26**(ii)(iv) by **8**(iii) and **3**(ii).

26(vi): Assume $x;1 = x$ and $\sum\{y : y \leqslant x+z;y\}$ exists. For every y, if $y \leqslant x+z;y$ then

$$\begin{aligned} y;1 &\leqslant (x+z;y);1 && \textbf{24}(\mathrm{x}) \\ &= x;1 + z;y;1 && (\mathrm{Ra}_2) \\ &= x + z;(y;1) && (\mathrm{Ra}_1),\ x;1 = x. \end{aligned}$$

This shows that $\{y : y \leqslant x+z;y\}$ is closed under $(\text{-});1$. It follows that $\{y;1 : y \leqslant x+z;y\} \subseteq \{y : y \leqslant x+z;y\}$, so, by **10**(iii),

$$\sum\{y;1 : y \leqslant x+z;y\} \leqslant \sum\{y : y \leqslant x+z;y\}. \tag{20}$$

But $\sum\{y : y \leqslant x+z;y\} \leqslant \left(\sum\{y : y \leqslant x+z;y\}\right);1 = \sum\{y;1 : y \leqslant x+z;y\}$ by **24**(xx)(xv), so, together with (20), this gives us $\sum\{y;1 : y \leqslant x+z;y\} = \sum\{y : y \leqslant x+z;y\}$. Since $\sum\{y : y \leqslant x+z;y\}$ is a join of elements of the form $y;1$, each of which is a domain element by **26**(i), it follows that $\sum\{y : y \leqslant x+z;y\}$ is a domain element by **26**(iv). □

Definition 27. An element x of a relation algebra $\mathfrak{A}$ is a *functional element* if $\breve{x};x \leqslant 1'$.

The functional elements of $\mathfrak{Re}(U)$ are the partial functions from U to U.

Theorem 28. *Let $\mathfrak{A}$ be a relation algebra.*

(i) [6, Theorem 3.39] *If x and y are functional elements of $\mathfrak{A}$, then so is $x;y$.*

(ii) [6, Theorem 4.2] *If x is a functional element of $\mathfrak{A}$, then $x;(y \cdot z) = x;y \cdot x;z$ for all $y,z \in A$.*

(iii) [6, Theorem 4.2] *An element x of $\mathfrak{A}$ is functional iff $x;y \cdot x;\bar{y} = 0$ for every element $y \in A$.*

(iv) *If $x \leqslant 1'$ then x is functional.*

Proof. **28**(i): Suppose x and y are functional elements of $\mathfrak{A}$. Then

$$\begin{aligned} (x;y)\breve{}\,;(x;y) &= \breve{y};\breve{x};(x;y) && (\mathrm{Ra}_6) \\ &= \breve{y};(\breve{x};x);y && (\mathrm{Ra}_1) \\ &\leqslant \breve{y};1';y && x \text{ is functional, } \textbf{24}(\mathrm{x}) \\ &= \breve{y};y && (\mathrm{Ra}_3) \\ &\leqslant 1' && y \text{ is functional,} \end{aligned}$$

so $x;y$ is functional as well.

$$\begin{aligned}
\textbf{28(ii)}: \quad x;y\cdot x;z &\leqslant x;(z\cdot \breve{x};(x;y)) && \textbf{24}(\text{xvi})\\
&= x;(z\cdot \breve{x};x;y) && (\text{Ra}_1)\\
&\leqslant x;(z\cdot 1';y) && x \text{ is functional}, \textbf{24}(\text{x}), \textbf{7}(\text{iii})\\
&= x;(z\cdot y) && \textbf{24}(\text{xix})\\
&\leqslant x;z\cdot x;y && \textbf{24}(\text{x}), \textbf{7}(\text{iv}).
\end{aligned}$$

28(iii): Assume first that x is functional. Let $y \in A$. Then $x;y\cdot x;\overline{y} = x;(y\cdot \overline{y}) = x;0 = 0$ by **28**(ii), **5**(ii), **24**(xviii). For the converse, suppose $x;y\cdot x;\overline{y} = 0$ for every element y. Take $y = 1'$ and get $0 = x;1'\cdot x;\overline{1'} = x\cdot x;\overline{1'}$ by (Ra_3). Then $0 = \overline{1'}\cdot \breve{x};x$ by **24**(xiv), so $\breve{x};x \leqslant 1'$. Thus x is functional.

28(iv): If $x \leqslant 1'$ then $\breve{x};x \leqslant \breve{1}';1' = 1'$, so x is functional. □

Definition 29. For every element x of a relation algebra let $x^0 = 1'$, and, for every $i \in \omega$, let $x^{i+1} = x;x^i$. Let $x^\omega = \sum \{x^i : i \in \omega\}$ whenever the join exists.

Theorem 30. *Let $\mathfrak{A}$ be a complete relation algebra with elements $p,q,y \in A$. Then*

(i) $\prod \{x : x \geqslant p+q;x\} = q^\omega;p$.

(ii) $\sum \{x : x \leqslant p\cdot \overline{q;\overline{x}}\} = \overline{q^\omega;\overline{p}}$.

(iii) $\prod \{x : x \geqslant p+q;x\};y = \prod \{x : x \geqslant p;y+q;x\}$.

Proof. 30(i): $\langle A, \leqslant\rangle$ is a complete lattice (with additional but irrelevant properties) and $p+q;(\text{-})$ is a monotonic function, so by Tarski's Theorem **22** it has a least fixed point, namely $\prod \{x : x \geqslant p+q;x\}$. We must show this is equal to $q^\omega;p$. First note that $q^\omega;p$ is a fixed point of $p+q;(\text{-})$, since

$$\begin{aligned}
p+q;\left(q^\omega;p\right) &= p+\left(q;q^\omega\right);p && (\text{Ra}_1)\\
&= p+\left(q;\left(\sum_{i\in\omega} q^i\right)\right);p && \textbf{29}\\
&= p+\left(\sum_{i\in\omega}\left(q;q^i\right)\right);p && \textbf{24}(\text{xv})\\
&= 1';p+\left(\sum_{i\in\omega} q^{i+1}\right);p && \textbf{29}, \textbf{24}(\text{xix})\\
&= \left(1'+\sum_{i\in\omega} q^{i+1}\right);p && (\text{Ra}_2)\\
&= \left(q^0+\sum_{i\in\omega} q^{i+1}\right);p && \textbf{29}\\
&= \left(\sum_{i\in\omega} q^i\right);p && \textbf{10}(\text{i})\\
&= q^\omega;p && \textbf{29}.
\end{aligned}$$

Since $q^\omega;p$ is a fixed point of $p+q;(\text{-})$, it includes the least fixed point of that function, hence $q^\omega;p \geqslant \prod \{x : x \geqslant p+q;x\}$. For the inclusion in the other direction we must show that $q^\omega;p$ is included in every x such that $x \geqslant p+q;x$. Assume $x \geqslant p+q;x$. We show $q^\omega;p \leqslant x$ by induction. The base case is that $q^0;p = 1';p = p \leqslant p+q;x \leqslant x$. For the inductive case, assume $q^i;p \leqslant x$. Then $q^{i+1};p = q;q^i;p = q;(q^i;p) \leqslant q;x \leqslant p+q;x \leqslant x$. Thus, x is an upper bound of $\{q^i;p : i \in \omega\}$, hence $x \geqslant \sum_{i\in\omega}(q^i;p) = \left(\sum_{i\in\omega} q^i\right);p = q^\omega;p$.

$$\begin{aligned}
\textbf{30}(\text{ii}): \quad \overline{q^{\omega};\overline{p}} &= \overline{\prod\{x : x \geqslant \overline{p}+q;x\}} && \textbf{30}(\text{i})\\
&= \sum\{\bar{x} : x \geqslant \overline{p}+q;x\} && \textbf{8}(\text{iii})\\
&= \sum\{x : \bar{x} \geqslant \overline{p}+q;\bar{x}\} && \textbf{3}(\text{ii})\\
&= \sum\{x : x \leqslant \overline{\overline{p}+q;\bar{x}}\} && \textbf{3}(\text{ii}), \textbf{7}(\text{v})\\
&= \sum\{x : x \leqslant p \cdot \overline{q;\bar{x}}\} && \textbf{3}(\text{ii})(\text{xvii}).
\end{aligned}$$

$$\begin{aligned}
\textbf{30}(\text{iii}): \quad \prod\{x : x \geqslant p+q;x\};y &= q^{\omega};p;y && \textbf{30}(\text{i})\\
&= q^{\omega};(p;y) && (\text{Ra}_1)\\
&= \prod\{x : x \geqslant p;y+q;x\} && \textbf{30}(\text{i}). \quad \square
\end{aligned}$$

Lemma 4.4 of [10] is obtained from **30**(iii) by setting $p = 1'$.

Theorem 31. *Let $\mathfrak{A}$ be a complete relation algebra with elements p, q, t, and c.*

(i) *If $c = q + t;c$, then $\sum\{x : x \leqslant p+q+t;x\} = \sum\{x : x \leqslant p+t;x\} + c$*

(ii) $\sum\{x : x \leqslant p+q+t;x\} = \sum\{x : x \leqslant p+t;x\} + \prod\{x : x \geqslant q+t;x\}$.

(iii) $\prod\{x : x \geqslant p \cdot q \cdot \overline{t;\bar{x}}\} = \prod\{x : x \geqslant p \cdot \overline{t;\bar{x}}\} \cdot \sum\{x : x \leqslant q \cdot \overline{t;\bar{x}}\}$.

Proof. **31**(i): Assume $c = q + t;c$, and let

$$a := \sum\{x : x \leqslant p+q+t;x\},$$
$$b := \sum\{x : x \leqslant p+t;x\}.$$

We want to show $a = b + c$. Note that b is a fixed point of $p + t;(\text{-})$ by **22**, so

$$b + c = (p + t;b) + (q + t;c) = p + q + t;(b + c).$$

Thus $b + c$ is a fixed point of $p + q + t;(\text{-})$. By **22**, the greatest such fixed point is a, so $b + c \leqslant a$. To prove $a \leqslant b + c$, it suffices to assume $x \leqslant p + q + t;x$ and show $x \leqslant b + c$. First note that from $c = q + t;c$ we may conclude that $\bar{c} \cdot q = 0$ and $\bar{c} \leqslant \overline{t;c}$. Then

$$\begin{aligned}
x \cdot \bar{c} &\leqslant (p+q+t;x) \cdot \bar{c} && x \leqslant p+q+t;x\\
&= p \cdot \bar{c} + q \cdot \bar{c} + t;x \cdot \bar{c} && \textbf{3}(\text{viii})(\text{xv})\\
&= p \cdot \bar{c} + t;x \cdot \bar{c} && \bar{c} \cdot q = 0\\
&\leqslant p + t;(x \cdot \breve{t};\bar{c}) && \textbf{24}(\text{xvi})\\
&\leqslant p + t;(x \cdot \breve{t};\overline{t;c}) && \bar{c} \leqslant \overline{t;c},\ \textbf{24}(\text{x})\\
&\leqslant p + t;(x \cdot \bar{c}) && (\text{Ra}_7),\ \textbf{24}(\text{x})
\end{aligned}$$

so from the definition of b we get $x \cdot \bar{c} \leqslant b$, hence $x \leqslant b + c$ by **7**(v), as desired.

31(ii): Let $c := \prod\{x : x \geqslant q + t;x\}$. Then $c = q + t;c$, so the desired conlusion follows by **31**(i).

31(iii): This follows from **31**(ii) by **3**(ii)(xvi), **8**(ii)(iii), and **7**(v). $\square$

6. Arbitrary interpretations

Let $\mathscr{S}tat$, with typical elements S, T, S', T', S'', ..., S_i, ..., be the set of statements of a programming language $\mathscr{L}$. Note that $\mathscr{S}tat$ can be an arbitrary set. The idea behind the following definition is explained in the Introduction.

Definition 32. Let $\mathfrak{A}$ be a relation algebra. An $\mathfrak{A}$-*interpretation* of $\mathscr{L}$ is a pair $\langle \mathsf{r}, \mathsf{e} \rangle$ of functions that map the statements $\mathscr{S}tat$ of the language $\mathscr{L}$ to elements of the algebra $\mathfrak{A}$ (in symbols, $\mathsf{r}, \mathsf{e} : \mathscr{S}tat \to A$), such that $\mathsf{e}_S ; 1 = \mathsf{e}_S$ for every $S \in \mathscr{S}tat$.

If $\mathfrak{A}$ is any relation algebra whatsoever, then an $\mathfrak{A}$-interpretation is obtained by setting $\mathsf{r}_S = \mathsf{e}_S = 0$ for every $S \in \mathscr{S}tat$, and another $\mathfrak{A}$-interpretation is obtained by setting $\mathsf{r}_S = \mathsf{e}_S = 1$. A slightly more interesting interpretation results from setting $\mathsf{r}_S = 1'$ and $\mathsf{e}_S = 0$. This is tantamount to saying that every program statement does nothing (leaves every state unchanged) and always terminates. These examples obviously may not conform to the intended meanings of the statements, but such conformity is not needed for many initial results. In the remainder of this section we prove several general results applicable to any set of statements $\mathscr{S}tat$ in a programming language $\mathscr{L}$ and any $\mathfrak{A}$-interpretation of those statements.

6.1. Predicate transformers and their laws

Definition 33. Let $\mathfrak{A}$ be a relation algebra and let $\langle \mathsf{r}, \mathsf{e} \rangle$ be an $\mathfrak{A}$-interpretation of $\mathscr{L}$. For every statement $S \in \mathscr{S}tat$ define two unary operators on $\mathfrak{A}$, namely $\mathrm{wlp}_S(\text{-}) : A \to A$ and $\mathrm{wp}_S(\text{-}) : A \to A$, as follows:

(i) $\mathrm{wlp}_S(x) = \overline{\mathsf{r}_S ; \bar{x}}$,

(ii) $\mathrm{wp}_S(x) = \overline{\mathsf{r}_S ; \bar{x}} \cdot \overline{\mathsf{e}_S}$.

In case x is a domain element, $\mathrm{wlp}_S(x)$ is called the "weakest liberal precondition guaranteeing x", and $\mathrm{wp}_S(x)$ is called the "weakest precondition guaranteeing x". We will usually apply the functions $\mathrm{wlp}_S(\text{-})$ and $\mathrm{wp}_S(\text{-})$ only to domain elements, but they are defined for all elements of the relation algebra $\mathfrak{A}$. This definition allows the recovery of r_S from $\mathrm{wlp}_S(\text{-})$ since, as is shown below, $\mathsf{r}_S = \mathrm{wlp}_S^{\delta}(1')$. It allows something more. Suppose we consider two statements $S, S' \in \mathscr{S}tat$, and we wish to construct from them a statement S'' such that $\mathsf{r}_{S''} ; \mathsf{r}_{S'} \leqslant \mathsf{r}_S$. We can achieve this by using any S'' such that

$$\mathsf{r}_{S''} \leqslant (\mathrm{wlp}_{S'}(\breve{\mathsf{r}}_S))\breve{} \tag{21}$$

for if (21) holds, then $\mathsf{r}_{S''} \leqslant (\mathrm{wlp}_{S'}(\breve{\mathsf{r}}_S))\breve{} = \left(\overline{\mathsf{r}_{S'} ; \bar{\mathsf{r}}_S}\right)\breve{} = \overline{\mathsf{r}_S ; \breve{\mathsf{r}}_{S'}}$ by **33**(i), **24**(iv),(Ra_6), and (Ra_4), hence $\mathsf{r}_{S''} ; \mathsf{r}_{S'} \leqslant \overline{\mathsf{r}_S ; \breve{\mathsf{r}}_{S'}} ; \mathsf{r}_{S'} \leqslant \mathsf{r}_S$ by (Ra_4), **24**(xii), and **3**(ii). Conversely, if $\mathsf{r}_{S''} ; \mathsf{r}_{S'} \leqslant \mathsf{r}_S$, then $\mathsf{r}_{S''} ; \mathsf{r}_{S'} \cdot \overline{\mathsf{r}_S} = 0$ by **7**(v), hence $\overline{\mathsf{r}_S} ; \breve{\mathsf{r}}_{S'} \cdot \mathsf{r}_{S''} = 0$ by **24**(xiv), so $\mathsf{r}_{S''} \leqslant \overline{\overline{\mathsf{r}_S} ; \breve{\mathsf{r}}_{S'}} = (\mathrm{wlp}_{S'}(\breve{\mathsf{r}}_S))\breve{}$ by **24**(xiv) by **7**(v). The relation $\overline{\overline{\mathsf{r}_S} ; \breve{\mathsf{r}}_{S'}} = (\mathrm{wlp}_{S'}(\breve{\mathsf{r}}_S))\breve{}$ is called the "weakest prespecification" of S and S' (see [18, p. 684]).

Peirce's "progressive involution", the converse-dual of the weakest prespecification, namely $\overline{\overline{x};y}$, was introduced by De Morgan [36]. The weakest prespecification was explicitly mentioned by Peirce [43] (under a different name, of course). Many algebraic laws governing this operation can be found in [50], and some of them are proved in [19, 20] from a different axiomatization of relation algebras.

From a given intepretation $\langle \mathrm{r}, \mathrm{e} \rangle$ it is possible to create others with interesting properties. For example, if $\mathrm{r}'_S = \mathrm{r}_S \cdot \overline{\mathrm{e}_S}$ for every $S \in \mathscr{S}tat$, then $\langle \mathrm{r}', \mathrm{e} \rangle$ is an interpretation whose weakest precondition transformer $\mathrm{wp}'_S(\text{-})$ is the same as the weakest precondition transformer $\mathrm{wp}_S(\text{-})$ of the interpretation $\langle \mathrm{r}, \mathrm{e} \rangle$, because

$$\begin{aligned}
\mathrm{wp}'_S(x) &= \overline{\mathrm{r}'_S;\overline{x} \cdot \overline{\mathrm{e}_S}} && \textbf{33}(\mathrm{ii}) \\
&= \overline{(\mathrm{r}_S \cdot \overline{\mathrm{e}_S});\overline{x} \cdot \overline{\mathrm{e}_S}} && \mathrm{r}'_S = \mathrm{r}_S \cdot \overline{\mathrm{e}_S} \\
&= \overline{\overline{\mathrm{e}_S} \cdot \mathrm{r}_S;\overline{x}} \cdot \overline{\mathrm{e}_S} && \mathrm{e}_S;1 = \mathrm{e}_S,\ \textbf{26}(\mathrm{ii}),\ \textbf{24}(\mathrm{xxvi}) \\
&= \left(\mathrm{e}_S + \overline{\mathrm{r}_S;\overline{x}}\right) \cdot \overline{\mathrm{e}_S} && \textbf{3}(\mathrm{ii})(\mathrm{xvii}) \\
&= \overline{\mathrm{r}_S;\overline{x}} \cdot \overline{\mathrm{e}_S} && \textbf{3}(\mathrm{xiii}) \\
&= \mathrm{wp}_S(x) && \textbf{33}(\mathrm{ii}).
\end{aligned}$$

Theorem 34. *Let* $\mathfrak{A}$ *be a relation algebra and let* $\langle \mathrm{r}, \mathrm{e} \rangle$ *be an* $\mathfrak{A}$*-interpretation of* $\mathscr{L}$.

(i) *If* x *is a domain element then* $\mathrm{wlp}_S(x)$ *and* $\mathrm{wp}_S(x)$ *are also domain elements.*
(ii) $\mathrm{wp}_S(x) = \mathrm{wlp}_S(x) \cdot \overline{\mathrm{e}_S}$.
(iii) $\mathrm{wlp}_S(1) = 1$.
(iv) $\mathrm{wp}_S(1) = \overline{\mathrm{e}_S}$.
(v) $\mathrm{wp}_S(x) = \mathrm{wlp}_S(x) \cdot \mathrm{wp}_S(1)$.
(vi) $\mathrm{wlp}^{\delta}_S(x) = \mathrm{r}_S;x$.
(vii) $\mathrm{wp}^{\delta}_S(x) = \mathrm{r}_S;x + \mathrm{e}_S$.
(viii) $\mathrm{wlp}^{\delta}_S(1') = \mathrm{r}_S$.
(ix) $\mathrm{wp}^{\delta}_S(0) = \mathrm{e}_S$.
(x) $\mathrm{wlp}^{\delta}_S(\text{-})$ *is universally additive.*
(xi) $\mathrm{wlp}_S(\text{-})$ *is universally multiplicative.*
(xii) $\mathrm{wp}_S(\text{-})$ *is completely multiplicative.*
(xiii) $\mathrm{wp}^{\delta}_S(\text{-})$ *is completely additive.*
(xiv) $\mathrm{wlp}_S(x) \cdot \mathrm{wlp}_S(y) = \mathrm{wlp}_S(x \cdot y)$.
(xv) $\mathrm{wp}_S(x) \cdot \mathrm{wp}_S(y) = \mathrm{wp}_S(x \cdot y)$.
(xvi) $\mathrm{wp}_S(x) \cdot \mathrm{wlp}_S(y) = \mathrm{wp}_S(x \cdot y)$.
(xvii) If $\mathrm{wp}_S(0) = 0$ *then* $\mathrm{wp}_S(x) \leqslant \mathrm{wlp}^{\delta}_S(x)$.

Proof. **34**(i): This part is an immediate consequence of **26**(ii)(iii) and **33**.
34(ii): This part follows immediately from **33**.
34(iii): $\mathrm{wlp}_S(1) = \overline{\mathrm{r}_S;\overline{1}} = \overline{\mathrm{r}_S;\overline{0}} = \overline{0} = 1$ by **33**(i), **5**(iii), **24**(xviii), and **5**(iv).
34(iv): $\mathrm{wp}_S(1) = \mathrm{wlp}_S(1) \cdot \overline{\mathrm{e}_S} = 1 \cdot \overline{\mathrm{e}_S} = \overline{\mathrm{e}_S}$ by **34**(ii),(iii), **3**(viii), and **5**(viii).
34(v): This part follows from **34**(ii) and **34**(iv).
34(vi): Using **11**, **33**(i) and **3**(ii), we get $\mathrm{wlp}^{\delta}_S(x) = \overline{\mathrm{wlp}_S(\overline{x})} = \overline{\overline{\mathrm{r}_S;\overline{x}}} = \mathrm{r}_S;x$.

34(vii): $\mathrm{wp}_S^\delta(x) = \overline{\mathrm{wp}_S(\bar{x})} = \overline{\mathrm{r}_S;\bar{\bar{x}} \cdot \overline{\mathrm{e}_S}} = \mathrm{r}_S;x + \mathrm{e}_S$ by **11**, **33**(ii), and **3**(ii)(xvii).

34(viii): This part follows from **34**(vi) by **24**(xix).

34(ix): This part follows from **34**(vii) by **24**(xviii).

34(x): Since $\mathrm{r}_S;(\text{-})$ is universally additive by **24**(xv), it follows from **34**(vi) that $\mathrm{wlp}_S^\delta(\text{-})$ is also universally additive.

34(xi): $\mathrm{wlp}_S(\text{-})$ is universally multiplicative by **17**(iii) and **34**(x).

34(xii): For every nonempty indexed set $\{x_i : i \in I\} \subseteq A$, if $\prod_{i\in I} x_i$ exists, then

$$\begin{aligned}
\mathrm{wp}_S\Big(\prod_{i\in I} x_i\Big) &= \mathrm{wlp}_S\Big(\prod_{i\in I} x_i\Big) \cdot \overline{\mathrm{e}_S} && \textbf{34}(\mathrm{ii})\\
&= \Big(\prod_{i\in I} \mathrm{wlp}_S(x_i)\Big) \cdot \overline{\mathrm{e}_S} && \textbf{34}(\mathrm{xi})\\
&= \prod_{i\in I} \Big(\mathrm{wlp}_S(x_i) \cdot \overline{\mathrm{e}_S}\Big) && I \neq \emptyset,\ \textbf{16}\\
&= \prod_{i\in I} \mathrm{wp}_S(x_i) && \textbf{34}(\mathrm{ii})
\end{aligned}$$

Thus, $\mathrm{wp}_S(\text{-})$ is completely multiplicative.

34(xiii): It follows from **34**(xii) by **17**(iii) that $\mathrm{wp}_S^\delta(\text{-})$ is completely additive.

34(xiv) and **34**(xv): These parts follow from **34**(xi) and **34**(xii) by **17**(ii).

34(xvi):
$$\begin{aligned}
\mathrm{wp}_S(x) \cdot \mathrm{wlp}_S(y) &= \mathrm{wlp}_S(x) \cdot \overline{\mathrm{e}_S} \cdot \mathrm{wlp}_S(y) && \textbf{34}(\mathrm{ii})\\
&= \mathrm{wlp}_S(x) \cdot \mathrm{wlp}_S(y) \cdot \overline{\mathrm{e}_S} && \textbf{3}(\mathrm{viii})(\mathrm{ix})\\
&= \mathrm{wlp}_S(x \cdot y) \cdot \overline{\mathrm{e}_S} && \textbf{34}(\mathrm{xiv})\\
&= \mathrm{wp}_S(x \cdot y) && \textbf{34}(\mathrm{ii}).
\end{aligned}$$

34(xvii): Assume $\mathrm{wp}_S(0) = 0$. Then

$$\begin{aligned}
0 &= \mathrm{wp}_S(0) && \text{hypothesis}\\
&= \mathrm{wp}_S(x \cdot \bar{x}) && \textbf{5}(\mathrm{ii})\\
&= \mathrm{wp}_S(x) \cdot \mathrm{wlp}_S(\bar{x}) && \textbf{34}(\mathrm{xvi}),
\end{aligned}$$

so $\mathrm{wp}_S(x) \leqslant \overline{\mathrm{wlp}_S(\bar{x})} = \mathrm{wlp}_S^\delta(x)$ by **3**(ii), **7**(v), **11**. □

6.2. *Determinism for arbitrary interpretations*

Definition 35. Let $\mathfrak{A}$ be a relation algebra and let $\langle \mathrm{r}, \mathrm{e}\rangle$ be an $\mathfrak{A}$-interpretation of $\mathscr{L}$. A statement S is *deterministic* if $\mathrm{wlp}_S^\delta(x) \leqslant \mathrm{wp}_S(x)$ for all $x \in A$.

Definition **35** is based on the remarks in [15, p. 137]. What is actually used as a definition of "S is deterministic" in [15] depends on the assumption that $\mathrm{wp}_S(0) = 0$, and is expressed in the first part of the following theorem.

Theorem 36. *Let $\mathfrak{A}$ be a relation algebra and let $\langle \mathrm{r}, \mathrm{e}\rangle$ be an $\mathfrak{A}$-interpretation of $\mathscr{L}$.*

(i) *Assume* $\mathrm{wp}_S(0) = 0$. *Then S is deterministic iff* $\mathrm{wp}_S(x) = \mathrm{wlp}_S^\delta(x)$ *for all* $x \in A$.

(ii) $S \in \mathscr{S}tat$ *is deterministic iff* $\check{\mathrm{r}}_S;\mathrm{r}_S \leqslant 1'$ *and* $\mathrm{r}_S \cdot \mathrm{e}_S = 0$.

Proof. **36**(i): This parts follows immediately from **34**(xvii) and **35**.

36(ii): The following statements are equivalent.

S is deterministic	
For all x, $\mathrm{wlp}_S^{\delta}(x) \leqslant \mathrm{wp}_S(x)$	**35**
For all x, $\mathrm{r}_S;x \leqslant \overline{\mathrm{r}_S;\bar{x}} \cdot \overline{\mathrm{e}_S}$	**34**(vi), **33**(ii)
For all x, $\mathrm{r}_S;x \cdot (\mathrm{r}_S;\bar{x} + \mathrm{e}_S) = 0$	**7**(v), **3**(xvii)(ii)
For all x, $\mathrm{r}_S;x \cdot \mathrm{r}_S;\bar{x} + \mathrm{r}_S;x \cdot \mathrm{e}_S = 0$	**3**(xv)
For all x, $\mathrm{r}_S;x \cdot \mathrm{r}_S;\bar{x} = 0$ and for all x, $\mathrm{r}_S;x \cdot \mathrm{e}_S = 0$	**7**(ii)(iv)
r_S is functional and $\mathrm{r}_S \cdot \mathrm{e}_S = 0$	(see next paragraph).

The equivalence of the last two statements comes from the following observations. By **28**(iii), r_S is functional iff for all x, $\mathrm{r}_S;x \cdot \mathrm{r}_S;\bar{x} = 0$. If for all $x \in A$, $\mathrm{r}_S;x \cdot \mathrm{e}_S = 0$, then, taking $x = 1$, we have $\mathrm{r}_S \cdot \mathrm{e}_S \leqslant \mathrm{r}_S;1 \cdot \mathrm{e}_S = 0$ by **24**(xx) and **7**(iii). Conversely, if $\mathrm{r}_S \cdot \mathrm{e}_S = 0$, then for every $x \in A$,

$\mathrm{r}_S;x \cdot \mathrm{e}_S = (\mathrm{r}_S \cdot \mathrm{e}_S);x$	**3**(viii), $\mathrm{e}_S;1 = \mathrm{e}_S$, **24**(xxvi)
$= 0;x$	hypothesis
$= 0$	**24**(xviii). □

7. Correct interpretations

Let $\mathscr{L}$ be a programming language whose set of statements $\mathscr{S}tat$ contains two kinds of statements, called *basic* and *compound*. Let $\mathscr{B}asic$ be the set of basic statements, containing

- skip, abort, havoc,
- assignment statements,
- Boolean statements $B, \ldots, B_i, \ldots$,
- variable statements $X, Y, Z, \ldots$,
- and other statements.

Assume that no basic statement belongs to more than one of the types listed above. Let $\mathscr{V}ar$ be the set of variable statements, usually called simply 'variables'. We assume that $\mathscr{V}ar$ is well-ordered. The compound statements $S, T, S', T', S'', \ldots, S_i, \ldots$, are obtained from the basic statements by repeated use of the following operations:

$S;T$	sequential composition ("do S, then do T")
S or T	binary nondeterministic choice ("do either S or T")
$\mathsf{OR}_{i \in I} S_i$	I-indexed nondeterministic choice ("do S_i for some $i \in I$")
if B then S else T	binary deterministic choice ("do S if B holds, otherwise do T")
$B \to S$	guarded command ("if B holds, do S")

$\mathsf{IF}_{i\in I}(B_i \to S_i)$	I-indexed guarded nondeterministic choice ("do some S_i for which B_i holds")
while B **do** S	while-loop ("if B holds, do S, otherwise do nothing; repeat")
$\mu X\,[S]$	single recursion ("do S, interpreting X as $\mu X\,[S]$").

Single recursion is part of the μ-calculus of Scott and de Bakker [51]. That multiple (simultaneous) recursion can be eliminated in favor of single recursion is proved in [2, 29, 51].

We assume that there are enough variables so that for every statement S there is a variable X that does not occur in S. Since $\mathscr{V}ar$ is well-ordered, there is a first such variable. In case the I-indexed operations are applicable only when I is finite, it suffices to let $\mathscr{V}ar$ be a countably infinite set. If I is allowed to range over all sets up to a given cardinality, then $\mathscr{V}ar$ will have to be appropriately larger.

7.1. *Definition of correct interpretations*

Let $\mathfrak{A}$ be a relation algebra and let $\langle \mathrm{r}, \mathrm{e}\rangle$ be an $\mathfrak{A}$-interpretation. The interpretation $\langle \mathrm{r}, \mathrm{e}\rangle$ is "correct" if it is a correct mathematical translation of the intended intuitive (or operational) meanings of the program constructs. Correctness lies at two levels. First, the basic statements must be interpreted correctly. Second, the interpretation of a compound statement should be computed from the interpretations of the constituent parts in the correct way. Thus, to motivate Definition **39** below, it is necessary to describe the intuitive meaning of a program construct using only the input/output relations and domains of nontermination of the parts and to see that such descriptions can be successfully written as relation-algebraic terms.

Start with the Boolean statements. These are supposed to represent conditions that may or may not be true of a given state. Each Boolean statement B determines the set of states that satisfy B, so B should be assigned by a correct interpretation to an element of $\mathfrak{A}$ that corresponds to a set. Domain elements are used this way, but in the computations that follow it is more convenient to use identity elements instead. We choose to let a correct interpretation satisfy $\mathrm{r}_B \leqslant 1'$ for every Boolean statement B.

Below we will have something to say about **havoc**, **abort**, **skip**, and variable statements, but the structure of assignment statements and other basic statements will not be relevant for the rest of this paper, so we have no requirements concerning them to impose on a correct interpretation.

Every computation of **havoc** terminates; upon termination the machine may be in any state. Thus, every state is connected to every other state by a terminating computation of **havoc**, and **havoc** has no nonterminating computations. Therefore, a correct interpretation should satisfy the conditions $\mathrm{r}_{\mathsf{havoc}} = 1$ and $\mathrm{e}_{\mathsf{havoc}} = 0$. For every

initial state the computation of **abort** fails to terminate, that is, every state initiates a nonterminating computation of **abort**, and **abort** has no terminating computations. So a correct interpretation should satisfy $r_{\mathbf{abort}} = 0$ and $e_{\mathbf{abort}} = 1$. From every state there should be a terminating computation of **skip** that leaves the state of the machine unchanged and there should be no nonterminating computations of **skip**. Hence, we want $r_{\mathbf{skip}} = 1'$ and $e_{\mathbf{skip}} = 0$.

The operational interpretation of $S;T$ is "first do S, then do T". Thus, a terminating computation of $S;T$ starts at the initial state of a terminating computation of S that ends at the initial state of a terminating computation of T that ends at the final state of the computation of $S;T$. The equation which asserts this is $r_{S;T} = r_S;r_T$. A state initiates a nonterminating computation of $S;T$ if it either initiates a nonterminating computation of S, or else initiates a terminating computation of S that ends at a state that starts a nonterminating computation of T. This is expressed by the equation $e_{S;T} = e_S + r_S;e_T$. Another way to read this equation is that nontermination of $S;T$ either occurs in the attempt to execute S, or else the execution of S terminates, but nontermination occurs in the subsequent execution of T.

S **or** T means "do either S or T", with no preference for either alternative. Its terminating computations are the terminating computations of S together with the terminating computations of T, i.e., $r_{S \text{ or } T} = r_S + r_T$, and a nonterminating computation of S **or** T is available iff one is available for either S or T, i.e., $e_{S \text{ or } T} = e_S + e_T$. Generalizing from the binary case to $\mathbf{OR}_{i\in I}S_i$ ("do S_i for some $i \in I$") yields $r_{\mathbf{OR}_{i\in I}S_i} = \sum_{i\in I} r_{S_i}$ and $e_{\mathbf{OR}_{i\in I}S_i} = \sum_{i\in I} e_{S_i}$.

The terminating computations of the guarded command $B \to S$ ("if B holds, do S") are just those terminating computations of S whose initial states satisfy B. Since r_B is to be an identity relation, this requirement is correctly expressed by $r_{B\to S} = r_B;r_S$. (If r_B were taken to be a domain element, the proper equation would be $r_{B\to S} = r_B \cdot r_S$.) All the nonterminating computations of S should be included among the nonterminating computations of $B \to S$. In addition, we imagine that there is a nonterminating computation of $B \to S$ starting at every state where B fails, so that $e_{B\to S} = \overline{r_B;1} + e_S$. (Note that $\overline{r_B;1}$ is a domain element whose domain is the complement of the domain of r_B. If we took r_B to be a domain element, then we could use $\overline{r_B}$ instead of $\overline{r_B;1}$.)

The terminating computations of the binary deterministic choice statement **if** B **then** S **else** T ("do S if B holds, otherwise do T") should be those terminating computations of S that start in states satisfying B plus those terminating computations of T that start in states not satisfying B. Hence, correct interpretations should satisfy $r_{\mathbf{if}\,B\,\mathbf{then}\,S\,\mathbf{else}\,T} = r_B;r_S + \overline{r_B;1} \cdot r_T$. Nontermination of **if** B **then** S **else** T should be possible from a state satisfying B if there is a nonterminating computation of S starting there, and it should be possible from a state not satisfying B if there is a nonterminating computation of T starting there, i.e., $e_{\mathbf{if}\,B\,\mathbf{then}\,S\,\mathbf{else}\,T} = r_B;e_S + \overline{r_B;1} \cdot e_T$.

A computation is a terminating computation of $\mathbf{IF}_{i\in I}(B_i \to S_i)$ iff, for some $i \in I$, it is a terminating computation of S_i whose initial state satisfies B_i. This is expressed by $r_{\mathbf{IF}_{i\in I}(B_i\to S_i)} = \sum_{i\in I}(r_{B_i};r_{S_i})$. The states initiating nonterminating computations of $\mathbf{IF}_{i\in I}(B_i \to S_i)$ are those in which no B_i is satisfied, together with those which, for some

$i \in I$, satisfy B_i and initiate a nonterminating computation of S_i, that is, $e_{\mathsf{IF}_{i\in I}(B_i \to S_i)} = \prod_{i\in I} \overline{r_{B_i}} + \sum_{i\in I} (r_{B_i}; e_{S_i})$. Note that if $r_{B_i} = 0$ for every $i \in I$, then $r_{\mathsf{IF}_{i\in I}(B_i \to S_i)} = \sum_{i\in I} 0 = 0 = r_{\mathsf{abort}}$ and $e_{\mathsf{IF}_{i\in I}(B_i \to S_i)} = \prod_{i\in I} 1 + \sum_{i\in I} 0 = 1 = e_{\mathsf{abort}}$. So if no B_i is satisfied, then $\mathsf{IF}_{i\in I}(B_i \to S_i)$ is semantically equivalent to **abort**, assuming **abort** is interpreted correctly.

Here is a more detailed version of the operational meaning of **while** B **do** S:

Step 0. Start with an initial state σ. Let the current state be the initial state.

Step 1. Check the current state. If B holds in the current state, then terminate without changing state and put the pair $\langle \sigma, \text{current state} \rangle$ into the input/output relation of **while** B **do** S. If B does not hold in the current state, then go on to Step 2.

Step 2. B fails in the current state. Do S, i.e., try to select a computation of S. If the current state does not initiate any computation of S or initiates a nonterminating computation of S, then put σ into the domain of nontermination of **while** B **do** S. If the current state initiates a terminating computation of S then let the new current state be the final state of any one of those terminating computations of S. Go back to Step 1.

Roughly speaking, a terminating computation for **while** B **do** S is a finite (possibly empty) sequence of terminating computations of $B \to S$, such that the last computation terminates at a state not satisfying B. This is expressed by $r_{\mathsf{while}\, B\, \mathsf{do}\, S} = \sum_{i\in\omega} ((r_B; r_S)^i; (\overline{r_B} \cdot 1'))$. But $\sum_{i\in\omega} ((r_B; r_S)^i; (\overline{r_B} \cdot 1'))$ is the least fixed point of $\overline{r_B} \cdot 1' + r_B; r_S; (\text{-})$, so we will use $r_{\mathsf{while}\, B\, \mathsf{do}\, S} = \prod \{x : x \geqslant \overline{r_B} \cdot 1' + r_B; r_S; x\}$.

Consider a state σ in the domain of $e_{\mathsf{while}\, B\, \mathsf{do}\, S}$. First, B must hold at σ, since otherwise the computation of **while** B **do** S would terminate immediately and $\langle \sigma, \sigma \rangle$ would be put into the input/output relation. Therefore, σ is in the domain of r_B. Since B holds, S is executed. This either leads to a nonterminating computation of S, that is, σ is in the domain of e_S, or else there is no such nonterminating computation. Therefore, σ must initiate a terminating computation of S, for if not, we would have a state satisfying B from which no computation of S is possible, contradicting our assumption that σ does initiate a computation of **while** B **do** S. Thus, σ initiates no nonterminating computations of S, but does initiate a nonterminating computation of **while** B **do** S, so at least one of the terminating computations of S must end in a state from which a nonterminating computation of **while** B **do** S is possible. This conclusion is equivalent to asserting that σ is in the domain of $r_S; e_{\mathsf{while}\, B\, \mathsf{do}\, S}$. Putting these inclusions together, we conclude that any state in the domain of $e_{\mathsf{while}\, B\, \mathsf{do}\, S}$ must be in the domain of $r_B; (e_S + r_S; e_{\mathsf{while}\, B\, \mathsf{do}\, S})$, that is, $e_{\mathsf{while}\, B\, \mathsf{do}\, S} \leqslant r_B; (e_S + r_S; e_{\mathsf{while}\, B\, \mathsf{do}\, S})$. Conversely, we can argue that if $y \leqslant r_B; (e_S + r_S; y)$ then $y \leqslant e_{\mathsf{while}\, B\, \mathsf{do}\, S}$. Indeed, a state σ in the domain of y must satisfy B, and either a nonterminating computation of S is possible from σ, in which case σ initiates a nonterminating computation of **while** B **do** S, or else σ initiates a terminating computation of S that ends in a state σ' which is again in the domain of y. Either σ' initiates a nonterminating computation of S or a terminating computation of S that ends at a state σ'' in the domain of y, and so on. We either eventually get into a nonterminating computation of S, or else create an infinite sequence of terminating computations of S. Either way we get a nonterminating computation of **while** B **do** S, so σ is in the domain of

$e_{\text{while } B \text{ do } S}$. Since $e_{\text{while } B \text{ do } S}$ is a domain relation, this argument is enough to show $y \leqslant e_{\text{while } B \text{ do } S}$. Thus, $e_{\text{while } B \text{ do } S}$ is, in fact, the greatest solution of $y \leqslant r_B ; (e_S + r_S ; y)$, i.e.,

$$e_{\text{while } B \text{ do } S} = \sum\{y : y \leqslant r_B ; (e_S + r_S ; y)\} = \sum\{y : y \leqslant r_B ; e_S + r_B ; r_S ; y\}.$$

A description of the operational meaning of $\mu X[S]$ is "execute S, but whenever a free occurrence of X is encountered (one that is not inside a substatement of S of the form $\mu X[T]$), that occurrence should be replaced by $\mu X[S]$, and execution should continue, beginning with the newly created occurrence of $\mu X[S]$." A consequence of this description is that the elements of $\mathfrak{A}$ assigned to $\mu X[S]$ should coincide with the elements assigned to the statement obtained from S by replacing free occurrences of X with $\mu X[S]$. Thus, $r_{\mu X[S]}$ and $e_{\mu X[S]}$ are completely independent of r_X and e_X. Indeed, to compute $r_{\mu X[S]}$ and $e_{\mu X[S]}$ we must consider other interpretations that differ from $\langle r, e \rangle$ on X. We need to able to find, given two elements x and y of $\mathfrak{A}$, a correct interpretation $\langle r', e' \rangle$, satisfying $r'_X = x$ and $e'_X = y$, that does not differ from $\langle r, e \rangle$ any more than necessary. This can be done by splitting correctness into two parts: correctness on basic statements, and correctness in the way that elements are assigned to compound statements. We compute $\langle r', e' \rangle$ from $\langle r, e \rangle$ by restricting $\langle r, e \rangle$ to the basic statements, obtaining ρ and ε, two maps on basic statements that are "basically correct" (defined below according to the remarks above), changing the values of ρ and ε at X to x and y, respectively, and then recomputing the assignments of elements to the compound statements. For this process we need, first, the notion of basic correctness for maps from basic statements to elements of $\mathfrak{A}$, and, second, a "correct" method of computing elements of $\mathfrak{A}$ for compound statements that starts from basically correct maps ρ and ε and is in accordance with the intuition regarding correctness for compound statements. The remarks above concerning $\mu X[S]$ lead to the conclusion that $r_{\mu X[S]}$ should be a fixed point of the function f, determined from S, that assigns input element x to the output element r'_S obtained by reassigning X to x. More thoughts along the lines indicated above for $\textsf{while}\, B \,\textsf{do}\, S$ lead to the further conclusion, arising already in [2, 40, 51], that r'_S should be the *least* fixed point of this function. If f is monotonic then this least fixed point is $\prod\{x : x \geqslant f(x)\}$ by **22**. (Note, however, that in a complete relation algebra $\prod\{x : x \geqslant f(x)\}$ always exists for *every* function f.)

Similarly, by imitating and generalizing the remarks concerning the nontermination domain of $\textsf{while}\, B \,\textsf{do}\, S$, one eventually gets to the conclusion that $e_{\mu X[S]}$ should be the *greatest* fixed point of the function g, determined from S, that assigns input element y to the output element e'_S, where $\langle r', e' \rangle$ is the interpretation obtained by reassigning r_X and e_X to $r_{\mu X[S]}$ and y, respectively. This analysis is the same as that which justifies the definition of the Hitchcock–Park [17] coderivative (the lower derivative of de Bakker [9]). Indeed, the definition of lower derivative from [9] is part of **39** below. Consult [17, 9] for more explanation.

Definition 37. Let ρ and ε be functions mapping $\mathscr{Basic}$ to elements of a relation algebra $\mathfrak{A}$. Then ρ and ε are *basically correct* if

(i) $\rho_{\mathsf{skip}} = 1'$,
(ii) $\varepsilon_{\mathsf{skip}} = 0$,
(iii) $\rho_{\mathsf{abort}} = 0$,
(iv) $\varepsilon_{\mathsf{abort}} = 1$,
(v) $\rho_{\mathsf{havoc}} = 1$,
(vi) $\varepsilon_{\mathsf{havoc}} = 0$,
(vii) $\rho_B \leqslant 1'$ for every Boolean statement B,
(viii) ε_R is a domain element for every $R \in \mathscr{Basic}$.

Definition 38. For any relation algebra $\mathfrak{A}$, any pair of maps $\rho, \varepsilon : \mathscr{Basic} \to A$, any variable X, and any two elements $x, y \in A$, define a new pair of maps $\rho\left(X_y^x\right), \varepsilon\left(X_y^x\right) : \mathscr{Basic} \to A$ as follows:

$$\rho\left(X_y^x\right)_R = \begin{cases} \rho_R \text{ if } \mathrm{X} \neq \mathrm{R} \in \mathscr{Basic}, \\ x \quad \text{if } \mathrm{X} = \mathrm{R}, \end{cases}$$

$$\varepsilon\left(X_y^x\right)_R = \begin{cases} \varepsilon_R \text{ if } \mathrm{X} \neq \mathrm{R} \in \mathscr{Basic}, \\ y \quad \text{if } \mathrm{X} = \mathrm{R}. \end{cases}$$

In discussing correctness we freely formed joins which, in case $\mathfrak{A}$ is the algebra of all binary relations on a set, are simply unions and certainly do exist. In the next definition, however, we need to know that the various joins exist, and so, in order to avoid lengthy formulations of results, we ask that $\mathfrak{A}$ be complete.

Definition 39. Let $\mathfrak{A}$ be a complete relation algebra. For every pair of maps $\rho, \varepsilon : \mathscr{Basic} \to A$, let $\mathbf{r}^{\rho,\varepsilon}, \mathbf{e}^{\rho,\varepsilon} : \mathscr{Stat} \to A$ be the unique pair of maps that satisfy the following conditions:

$$\begin{aligned}
\mathbf{r}_R^{\rho,\varepsilon} &= \rho_R \qquad \text{if } \mathrm{R} \in \mathscr{Basic}, \\
\mathbf{r}_{S;T}^{\rho,\varepsilon} &= \mathbf{r}_S^{\rho,\varepsilon};\mathbf{r}_T^{\rho,\varepsilon}, \\
\mathbf{r}_{S \text{ or } T}^{\rho,\varepsilon} &= \mathbf{r}_S^{\rho,\varepsilon} + \mathbf{r}_T^{\rho,\varepsilon}, \\
\mathbf{r}_{\mathsf{OR}_{i\in I} S_i}^{\rho,\varepsilon} &= \sum_{i\in I} \mathbf{r}_{S_i}^{\rho,\varepsilon}, \\
\mathbf{r}_{\mathsf{if}\, B \,\mathsf{then}\, S \,\mathsf{else}\, T}^{\rho,\varepsilon} &= \rho_B;\mathbf{r}_S^{\rho,\varepsilon} + \overline{\rho_B;1} \cdot \mathbf{r}_T^{\rho,\varepsilon}, \\
\mathbf{r}_{B\to S}^{\rho,\varepsilon} &= \rho_B;\mathbf{r}_S^{\rho,\varepsilon}, \\
\mathbf{r}_{\mathsf{IF}_{i\in I}(B_i\to S_i)}^{\rho,\varepsilon} &= \sum_{i\in I} \left(\rho_{B_i};\mathbf{r}_{S_i}^{\rho,\varepsilon}\right), \\
\mathbf{r}_{\mathsf{while}\, B \,\mathsf{do}\, S}^{\rho,\varepsilon} &= \prod \left\{ x : x \geqslant \overline{\rho_B} \cdot 1' + \rho_B;\mathbf{r}_S^{\rho,\varepsilon};x \right\}, \\
\mathbf{r}_{\mu X[S]}^{\rho,\varepsilon} &= \prod \left\{ x : x \geqslant \mathbf{r}_S^{\rho\left(X_0^x\right),\varepsilon\left(X_0^x\right)} \right\},
\end{aligned}$$

$$
\begin{aligned}
\mathbf{e}_R^{\rho,\varepsilon} &= \varepsilon_R \qquad \text{if } \mathrm{R} \in \mathscr{Basic},\\
\mathbf{e}_{S;T}^{\rho,\varepsilon} &= \mathbf{e}_S^{\rho,\varepsilon} + \mathbf{r}_S^{\rho,\varepsilon};\mathbf{e}_T^{\rho,\varepsilon},\\
\mathbf{e}_{S \text{ or } T}^{\rho,\varepsilon} &= \mathbf{e}_S^{\rho,\varepsilon} + \mathbf{e}_T^{\rho,\varepsilon},\\
\mathbf{e}_{\mathsf{OR}_{i\in I}S_i}^{\rho,\varepsilon} &= \sum_{i\in I} \mathbf{e}_{S_i}^{\rho,\varepsilon},\\
\mathbf{e}_{\text{if } B \text{ then } S \text{ else } T}^{\rho,\varepsilon} &= \rho_B;\mathbf{e}_S^{\rho,\varepsilon} + \overline{\rho_B;1}\cdot\mathbf{e}_T^{\rho,\varepsilon},\\
\mathbf{e}_{B\to S}^{\rho,\varepsilon} &= \overline{\rho_B;1} + \mathbf{e}_S^{\rho,\varepsilon},\\
\mathbf{e}_{\mathsf{IF}_{i\in I}(B_i\to S_i)}^{\rho,\varepsilon} &= \prod_{i\in I} \overline{\rho_{B_i};1} + \sum_{i\in I} \left(\rho_{B_i};\mathbf{e}_{S_i}^{\rho,\varepsilon}\right),\\
\mathbf{e}_{\text{while } B \text{ do } S}^{\rho,\varepsilon} &= \sum \left\{ y : y \leqslant \rho_B;\mathbf{e}_S^{\rho,\varepsilon} + \rho_B;\mathbf{r}_S^{\rho,\varepsilon};y \right\},\\
\mathbf{e}_{\mu X[S]}^{\rho,\varepsilon} &= \sum \left\{ y : y \leqslant \mathbf{e}_S^{\rho\left(X_y^{\mathbf{r}_{\mu X[S]}^{\rho,\varepsilon}}\right),\varepsilon\left(X_y^{\mathbf{r}_{\mu X[S]}^{\rho,\varepsilon}}\right)} \right\}.
\end{aligned}
$$

A *correct interpretation* is any pair of extensions $\langle \mathbf{r}^{\rho,\varepsilon}, \mathbf{e}^{\rho,\varepsilon}\rangle$ obtained from a basically correct pair of maps $\rho,\varepsilon : \mathscr{Basic} \to A$.

Suppose we have a complete relation algebra $\mathfrak{A}$ and a correct interpretation $\langle \mathbf{r}^{\rho,\varepsilon}, \mathbf{e}^{\rho,\varepsilon}\rangle$. We do not yet know $\langle \mathbf{r}^{\rho,\varepsilon}, \mathbf{e}^{\rho,\varepsilon}\rangle$ is an $\mathfrak{A}$-interpretation. From the basic correctness of ρ and ε we do know that $\mathbf{e}_R^{\rho,\varepsilon}$ is a domain element for every $R \in \mathscr{Basic}$, but to conclude that $\langle \mathbf{r}^{\rho,\varepsilon}, \mathbf{e}^{\rho,\varepsilon}\rangle$ is an $\mathfrak{A}$-interpretation we must prove that $\mathbf{e}_S^{\rho,\varepsilon}$ is a domain element for every $S \in \mathscr{Stat}$. This is done in Theorem 53.

Definition 40. For every relation algebra $\mathfrak{A}$, every pair of maps $\rho,\varepsilon : \mathscr{Basic} \to A$, every variable X, and all elements $x, y \in A$, let

$$
\begin{aligned}
\mathbf{r}^{\rho,\varepsilon}\left(X_y^x\right) &= \mathbf{r}^{\rho\left(X_y^x\right),\varepsilon\left(X_y^x\right)},\\
\mathbf{e}^{\rho,\varepsilon}\left(X_y^x\right) &= \mathbf{e}^{\rho\left(X_y^x\right),\varepsilon\left(X_y^x\right)}.
\end{aligned}
$$

$\mathbf{r}^{\rho}\left(X_y^x\right)$ and $\mathbf{e}^{\rho,\varepsilon}\left(X_y^x\right)$ are the new extensions obtained from previous extensions $\mathbf{r}^{\rho,\varepsilon}$ and $\mathbf{e}^{\rho,\varepsilon}$ by changing the value of $\mathbf{r}^{\rho,\varepsilon}$ and $\mathbf{e}^{\rho,\varepsilon}$ at X to x and y, respectively.

Theorem 41. *If $\mathfrak{A}$ is a complete relation algebra and $\rho,\varepsilon,\varepsilon' : \mathscr{Basic} \to A$, then $\mathbf{r}^{\rho,\varepsilon} = \mathbf{r}^{\rho,\varepsilon'}$.*

Proof. The definition of $\mathbf{r}^{\rho,\varepsilon}$ and $\mathbf{e}^{\rho,\varepsilon}$ shows that the values of ε and $\mathbf{e}^{\rho,\varepsilon}$ are irrelevant to the computation of $\mathbf{r}^{\rho,\varepsilon}$. □

In view of **41**, we will write $\mathbf{r}^{\rho}$ instead of $\mathbf{r}^{\rho,\varepsilon}$. Consequently the first part of **40** can be restated more simply as $\mathbf{r}^{\rho}\left(X_y^x\right) = \mathbf{r}^{\rho(X_y^x)}$. With these notational changes, **39** becomes

$$
\begin{aligned}
\mathbf{r}_R^{\rho} &= \rho_R \qquad \text{if } \mathrm{R} \in \mathscr{Basic},\\
\mathbf{r}_{S;T}^{\rho} &= \mathbf{r}_S^{\rho};\mathbf{r}_T^{\rho},\\
\mathbf{r}_{S\text{ or }T}^{\rho} &= \mathbf{r}_S^{\rho} + \mathbf{r}_T^{\rho},\\
\mathbf{r}_{\mathsf{OR}_{i\in I}S_i}^{\rho} &= \sum_{i\in I} \mathbf{r}_{S_i}^{\rho},\\
\mathbf{r}_{\text{if } B \text{ then } S \text{ else } T}^{\rho} &= \rho_B;\mathbf{r}_S^{\rho} + \overline{\rho_B;1}\cdot\mathbf{r}_T^{\rho},\\
\mathbf{r}_{B\to S}^{\rho} &= \rho_B;\mathbf{r}_S^{\rho},\\
\mathbf{r}_{\mathsf{IF}_{i\in I}(B_i\to S_i)}^{\rho} &= \sum_{i\in I}\left(\rho_{B_i};\mathbf{r}_{S_i}^{\rho}\right),\\
\mathbf{r}_{\text{while } B \text{ do } S}^{\rho} &= \prod\left\{x : x \geqslant \overline{\rho_B}\cdot 1' + \rho_B;\mathbf{r}_S^{\rho};x\right\},\\
\mathbf{r}_{\mu X[S]}^{\rho} &= \prod\left\{x : x \geqslant \mathbf{r}_S^{\rho}(X_0^x)\right\},\\
\mathbf{e}_R^{\rho,\varepsilon} &= \varepsilon_R \qquad \text{if } R \in \mathscr{Basic},\\
\mathbf{e}_{S;T}^{\rho,\varepsilon} &= \mathbf{e}_S^{\rho,\varepsilon} + \mathbf{r}_S^{\rho};\mathbf{e}_T^{\rho,\varepsilon},\\
\mathbf{e}_{S\text{ or }T}^{\rho,\varepsilon} &= \mathbf{e}_S^{\rho,\varepsilon} + \mathbf{e}_T^{\rho,\varepsilon},\\
\mathbf{e}_{\mathsf{OR}_{i\in I}S_i}^{\rho,\varepsilon} &= \sum_{i\in I}\mathbf{e}_{S_i}^{\rho,\varepsilon},\\
\mathbf{e}_{\text{if } B \text{ then } S \text{ else } T}^{\rho,\varepsilon} &= \rho_B;\mathbf{e}_S^{\rho,\varepsilon} + \overline{\rho_B;1}\cdot\mathbf{e}_T^{\rho,\varepsilon},\\
\mathbf{e}_{B\to S}^{\rho,\varepsilon} &= \overline{\rho_B;1} + \mathbf{e}_S^{\rho,\varepsilon},\\
\mathbf{e}_{\mathsf{IF}_{i\in I}(B_i\to S_i)}^{\rho,\varepsilon} &= \prod_{i\in I}\overline{\rho_{B_i};1} + \sum_{i\in I}\left(\rho_{B_i};\mathbf{e}_{S_i}^{\rho,\varepsilon}\right),\\
\mathbf{e}_{\text{while } B \text{ do } S}^{\rho,\varepsilon} &= \sum\left\{y : y \leqslant \rho_B;\mathbf{e}_S^{\rho,\varepsilon} + \rho_B;\mathbf{r}_S^{\rho};y\right\},\\
\mathbf{e}_{\mu X[S]}^{\rho,\varepsilon} &= \sum\left\{y : y \leqslant \mathbf{e}^{\rho,\varepsilon}\left(X_y^{\mathbf{r}_{\mu X[S]}^{\rho}}\right)_S\right\}.
\end{aligned}
$$

Lemma 42. *Suppose* $\mathfrak{A}$ *is a complete relation algebra,* $\rho,\varepsilon : \mathscr{Basic} \to A$, $v,w,x,y \in A$, *and* $X \neq Y$. *Then*

(i) $\mathbf{r}^{\rho}\left(X_y^x\right)\left(Y_w^v\right) = \mathbf{r}^{\rho}\left(Y_w^v\right)\left(X_y^x\right)$ *and* $\mathbf{e}^{\rho,\varepsilon}\left(X_y^x\right)\left(Y_w^v\right) = \mathbf{e}^{\rho,\varepsilon}\left(Y_w^v\right)\left(X_y^x\right)$,

(ii) $\mathbf{r}^{\rho}\left(X_y^x\right)\left(X_w^v\right) = \mathbf{r}^{\rho}\left(X_w^v\right)$ *and* $\mathbf{e}^{\rho,\varepsilon}\left(X_y^x\right)\left(X_w^v\right) = \mathbf{e}^{\rho,\varepsilon}\left(X_w^v\right)$.

Proof. **42**(i): It follows immediately from **38** and the assumption that $X \neq Y$ that $\rho\left(X_y^x\right)\left(Y_w^v\right) = \rho\left(Y_w^v\right)\left(X_y^x\right)$ and $\varepsilon\left(X_y^x\right)\left(Y_w^v\right) = \varepsilon\left(Y_w^v\right)\left(X_y^x\right)$, so by **40** we have

$$
\begin{aligned}
\mathbf{r}^{\rho}\left(X_y^x\right)\left(Y_w^v\right) &= \mathbf{r}^{\rho(X_y^x)}\left(Y_w^v\right)\\
&= \mathbf{r}^{\rho(X_y^x)(Y_w^v)}\\
&= \mathbf{r}^{\rho(Y_w^v)(X_y^x)}\\
&= \mathbf{r}^{\rho(Y_w^v)}\left(X_y^x\right)\\
&= \mathbf{r}^{\rho}\left(Y_w^v\right)\left(X_y^x\right).
\end{aligned}
$$

For the other equation, we have a similar proof:

$$\begin{aligned}
\mathbf{e}^{\rho,\varepsilon}\left(X_y^x\right)\left(Y_w^v\right) &= \mathbf{e}^{\rho(X_y^x),\varepsilon(X_y^x)}\left(Y_w^v\right)\\
&= \mathbf{e}^{\rho(X_y^x)(Y_w^v),\varepsilon(X_y^x)(Y_w^v)}\\
&= \mathbf{e}^{\rho(Y_w^v)(X_y^x),\varepsilon(Y_w^v)(X_y^x)}\\
&= \mathbf{e}^{\rho(Y_w^v),\varepsilon(Y_w^v)}\left(X_y^x\right)\\
&= \mathbf{e}^{\rho,\varepsilon}\left(Y_w^v\right)\left(X_y^x\right).
\end{aligned}$$

42(ii): The proof is similar to that of **42**(i), but uses the observation that $\rho\left(X_y^x\right)\left(X_w^v\right) = \rho\left(X_w^v\right)$ and $\varepsilon\left(X_y^x\right)\left(X_w^v\right) = \varepsilon\left(X_w^v\right)$. □

Lemma 43. *Suppose* $\mathfrak{A}$ *is a complete relation algebra,* $\rho, \varepsilon : \mathscr{B}asic \to A$, *and* $x, y \in A$. *Then* $\mathbf{r}^{\rho}\left(X_y^x\right) = \mathbf{r}^{\rho}\left(X_0^x\right)$.

Proof. Nothing that $\rho(X_y^x) = \rho(X_0^x)$, we have $\mathbf{r}^{\rho}(X_y^x) = \mathbf{r}^{\rho(X_y^x)} = \mathbf{r}^{\rho(X_0^x)} = \mathbf{r}^{\rho}\left(X_0^x\right)$. □

Definition 44. The free-variable function Free(-) is the unique function mapping $\mathscr{S}tat$ to subsets of $\mathscr{V}ar$ that satisfies the following conditions:

(i) $\mathrm{Free}(\mathrm{S}) = \begin{cases} \{S\} \text{ if } \mathrm{S} \in \mathscr{V}ar, \\ \emptyset \text{ if } \mathrm{S} \in \mathscr{B}asic \sim \mathscr{V}ar. \end{cases}$

(ii) $\mathrm{Free}(\mathrm{S};\mathrm{T}) = \mathrm{Free}(\mathrm{S}\ \mathsf{or}\ \mathrm{T}) = \mathrm{Free}(\mathsf{if}\ \mathrm{B}\ \mathsf{then}\ \mathrm{S}\ \mathsf{else}\ \mathrm{T}) = \mathrm{Free}(\mathrm{S}) \cup \mathrm{Free}(\mathrm{T})$.

(iii) $\mathrm{Free}(\mathsf{OR}_{i\in I}\mathrm{S}_i) = \mathrm{Free}(\mathsf{IF}_{i\in I}(\mathrm{B}_i \to \mathrm{S}_i)) = \bigcup_{i\in I}\mathrm{Free}(\mathrm{S}_i)$.

(iv) $\mathrm{Free}(\mathrm{B} \to \mathrm{S}) = \mathrm{Free}(\mathsf{while}\ \mathrm{B}\ \mathsf{do}\ \mathrm{S}) = \mathrm{Free}(\mathrm{S})$.

(v) $\mathrm{Free}(\mu\mathrm{X}[\mathrm{S}]) = \mathrm{Free}(\mathrm{S}) \sim \{\mathrm{X}\}$.

A variable X **occurs free in** a statement S iff $X \in \mathrm{Free}(\mathrm{S})$.

Lemma 45. *Suppose* $\mathfrak{A}$ *is a complete relation algebra,* $\rho, \varepsilon : \mathscr{B}asic \to A$, *and* $x, y \in A$. *If* X *does not occur free in* S, *then* $\mathbf{r}^{\rho}\left(X_y^x\right)_S = \mathbf{r}_S^{\rho}$ *and* $\mathbf{e}^{\rho,\varepsilon}\left(X_y^x\right)_S = \mathbf{e}_S^{\rho,\varepsilon}$.

Proof. The proof is by induction on the complexity of statements. The only interesting case is the one involving $\mu Y[S]$. First we handle the case in which $Y \neq X$. To prove the result for $\mu Y[S]$, we assume that X does not occur free in $\mu Y[S]$. Then X also does not occur free in S and S has lower complexity than $\mu Y[S]$. Our induction hypothesis is that **45** applies to S with $\mathbf{r}^{\rho}\left(Y_0^z\right)$ in place of $\mathbf{r}^{\rho}$, i.e., $\mathbf{r}^{\rho}\left(Y_0^z\right)\left(X_y^x\right)_S = \mathbf{r}^{\rho}\left(Y_0^z\right)_S$. Then

$$\begin{aligned}
\mathbf{r}^{\rho}\left(X_y^x\right)_{\mu Y[S]} &= \prod\left\{z : z \geqslant \mathbf{r}^{\rho}\left(X_y^x\right)\left(Y_0^z\right)_S\right\} && \mathbf{39}\\
&= \prod\left\{z : z \geqslant \mathbf{r}^{\rho}\left(Y_0^z\right)\left(X_y^x\right)_S\right\} && \mathbf{42}(\mathrm{i})\\
&= \prod\left\{z : z \geqslant \mathbf{r}^{\rho}\left(Y_0^z\right)_S\right\} && \text{induction hypothesis}\\
&= \mathbf{r}^{\rho}_{\mu Y[S]} && \mathbf{39}.
\end{aligned}$$

The second case is when $Y = X$ and $\mu Y[S] = \mu X[S]$. X does not occur free in $\mu X[S]$, although it may occur free in S. Note that $\mathbf{r}^\rho\left(X_y^x\right)\left(X_0^z\right) = \mathbf{r}^\rho\left(X_0^z\right)$ by **42**(ii). No induction hypothesis is needed:

$$\begin{aligned}\mathbf{r}^\rho\left(X_y^x\right)_{\mu X[S]} &= \prod\left\{z : z \geqslant \mathbf{r}^\rho\left(X_y^x\right)\left(X_0^z\right)_S\right\} && \textbf{39}\\ &= \prod\left\{z : z \geqslant \mathbf{r}^\rho\left(X_0^z\right)_S\right\} && \textbf{42}(\text{ii})\\ &= \mathbf{r}^\rho_{\mu X[S]} && \textbf{39}.\end{aligned}$$

Similar arguments apply to $\mathbf{e}^{\rho,\varepsilon}_{\mu Y[S]}$. The other cases are easy. For example, if **45** holds for S and T then it also holds for $S;T$, for if $X \notin \mathrm{Free}(\mathrm{S};\mathrm{T})$ then $X \notin \mathrm{Free}(\mathrm{S})$ and $X \notin \mathrm{Free}(\mathrm{T})$, so $\mathbf{r}^\rho\left(X_y^x\right)_{S;T} = \mathbf{r}^\rho\left(X_y^x\right)_S;\mathbf{r}^\rho\left(X_y^x\right)_T = \mathbf{r}^\rho_S;\mathbf{r}^\rho_T = \mathbf{r}^\rho_{S;T}$ and $\mathbf{e}^{\rho,\varepsilon}\left(X_y^x\right)_{S;T} = \mathbf{e}^{\rho,\varepsilon}\left(X_y^x\right)_S + \mathbf{r}^\rho\left(X_y^x\right)_S;\mathbf{e}^{\rho,\varepsilon}\left(X_y^x\right)_T = \mathbf{e}^{\rho,\varepsilon}_S + \mathbf{r}^\rho_S;\mathbf{e}^{\rho,\varepsilon}_T = \mathbf{e}^{\rho,\varepsilon}_{S;T}$. □

Theorem 46. *Suppose* $\mathfrak{A}$ *is a complete relation algebra,* $\rho, \varepsilon : \mathscr{B}asic \to A$, *and* $z \in A$. *Then* $\mathbf{r}^\rho\left(X_z^{(\cdot)}\right)_S$ *and* $\mathbf{e}^{\rho,\varepsilon}\left(X^z_{(\cdot)}\right)_S$ *are monotonic functions.*

Proof. It follows from **24**(x) that if f and g are monotonic operations on $\mathfrak{A}$, then the function $f(\cdot);g(\cdot)$ is also monotonic. Using this together with **21**, it is easy to complete the proof by induction on the complexity of statements. □

Definition 47. The substitution function $\mathrm{sub}^S_X[\cdot] : \mathscr{S}tat \to \mathscr{S}tat$ (of statement S for variable X) is the unique function that satisfies the following conditions:

(i) $\mathrm{sub}^S_X[T] = \begin{cases} T & \text{if } \mathrm{X} \neq \mathrm{T} \in \mathscr{B}asic \\ S & \text{if } \mathrm{X} = \mathrm{T} \end{cases}$

(ii) $\mathrm{sub}^S_X[S;T] = \mathrm{sub}^S_X[S];\mathrm{sub}^S_X[T]$.

(iii) $\mathrm{sub}^S_X[S \text{ or } T] = \mathrm{sub}^S_X[S] \text{ or } \mathrm{sub}^S_X[T]$.

(iv) $\mathrm{sub}^S_X\left[\mathsf{OR}_{i\in I}S_i\right] = \mathsf{OR}_{i\in I}\mathrm{sub}^S_X[S_i]$.

(v) $\mathrm{sub}^S_X\left[\mathsf{if}\,B\,\mathsf{then}\,T\,\mathsf{else}\,T'\right] = \mathsf{if}\,B\,\mathsf{then}\,\mathrm{sub}^S_X[T]\,\mathsf{else}\,\mathrm{sub}^S_X\left[T'\right]$.

(vi) $\mathrm{sub}^S_X[B \to T] = B \to \mathrm{sub}^S_X[T]$.

(vii) $\mathrm{sub}^S_X\left[\mathsf{IF}_{i\in I}(B_i \to S_i)\right] = \mathsf{IF}_{i\in I}(B_i \to \mathrm{sub}^S_X[S_i])$.

(viii) $\mathrm{sub}^S_X[\mathsf{while}\,B\,\mathsf{do}\,T] = \mathsf{while}\,B\,\mathsf{do}\,\mathrm{sub}^S_X[T]$.

(ix) $\mathrm{sub}^S_X[\mu Y[T]] = \mu Z\left[\mathrm{sub}^S_X\left[\mathrm{sub}^Z_Y[T]\right]\right]$ where Z is the first variable distinct from X that does not occur free in S and does not occur free in T.

Theorem 48. *Suppose* $\mathfrak{A}$ *is a complete relation algebra and* $\rho, \varepsilon : \mathscr{B}asic \to A$. *Then* $\mathbf{r}^\rho_{\mathrm{sub}^S_X[T]} = \mathbf{r}^\rho\left(X_0^{\mathbf{r}^\rho_S}\right)_T$ *and* $\mathbf{e}^{\rho,\varepsilon}_{\mathrm{sub}^S_X[T]} = \mathbf{e}^{\rho,\varepsilon}\left(X^{\mathbf{r}^\rho_S}_{\mathbf{e}^{\rho,\varepsilon}_S}\right)_T$.

Proof. The proof is by induction on the complexity of statements. The most complicated case is the μ-case. We assume **48** is true for all statements with complexity less than that of $\mu Y[T]$, and prove **48** for $\mu Y[T]$ itself. We have

$$\mathrm{sub}^S_X[\mu Y[T]] = \mu Z\left[\mathrm{sub}^S_X\left[\mathrm{sub}^Z_Y[T]\right]\right], \tag{22}$$

where Z is the first variable distinct from X that does not occur free in either S or T. Both T and $\mathrm{sub}_Y^Z[T]$ have complexity less than that of $\mu Y[T]$, so we can apply **48** to both of them. We must show

$$\mathbf{r}^{\rho}_{\mathrm{sub}_X^S[\mu Y[T]]} = \mathbf{r}^{\rho}\left(X_0^{\mathbf{r}^{\rho}_S}\right)_{\mu Y[T]} \tag{23}$$

$$\mathbf{e}^{\rho,\varepsilon}_{\mathrm{sub}_X^S[\mu Y[T]]} = \mathbf{e}^{\rho,\varepsilon}\left(X^{\mathbf{r}^{\rho}_S}_{\mathbf{e}^{\rho,\varepsilon}_S}\right)_{\mu Y[T]}. \tag{24}$$

Eq. (23) is proved as follows:

$$\begin{aligned}
\mathbf{r}^{\rho}_{\mathrm{sub}_X^S[\mu Y[T]]} &= \mathbf{r}^{\rho}_{\mu Z[\mathrm{sub}_X^S[\mathrm{sub}_Y^Z[T]]]} \\
&\qquad (22) \\
&= \prod\left\{z : z \geqslant \mathbf{r}^{\rho}\left(Z_0^z\right)_{\mathrm{sub}_X^S[\mathrm{sub}_Y^Z[T]]}\right\} \\
&\qquad \mathbf{39} \\
&= \prod\left\{z : z \geqslant \mathbf{r}^{\rho}\left(Z_0^z\right)\left(X_0^{\mathbf{r}^{\rho}(Z_0^z)_S}\right)_{\mathrm{sub}_Y^Z[T]}\right\} \\
&\qquad \text{induction hypothesis for } \mathrm{sub}_Y^Z[T] \\
&= \prod\left\{z : z \geqslant \mathbf{r}^{\rho}\left(Z_0^z\right)\left(X_0^{\mathbf{r}^{\rho}_S}\right)_{\mathrm{sub}_Y^Z[T]}\right\} \\
&\qquad Z \notin \mathrm{Free}(S),\ \mathbf{45} \\
&= \prod\left\{z : z \geqslant \mathbf{r}^{\rho}\left(Z_0^z\right)\left(X_0^{\mathbf{r}^{\rho}_S}\right)\left(Y_0^{\mathbf{r}^{\rho}(Z_0^z)\left(X_0^{\mathbf{r}^{\rho}_S}\right)_z}\right)_T\right\} \\
&\qquad \text{induction hypothesis for } T \\
&= \prod\left\{z : z \geqslant \mathbf{r}^{\rho}\left(Z_0^z\right)\left(X_0^{\mathbf{r}^{\rho}_S}\right)\left(Y_0^z\right)_T\right\} \\
&\qquad \mathbf{42}(\mathrm{i}),\ \mathbf{39},\ \mathbf{38} \\
&= \prod\left\{z : z \geqslant \mathbf{r}^{\rho}\left(X_0^{\mathbf{r}^{\rho}_S}\right)\left(Y_0^z\right)_T\right\} \\
&\qquad \mathbf{42}(i),\ Z \notin \mathrm{Free}(S),\ \mathbf{45} \\
&= \mathbf{r}^{\rho}\left(X_0^{\mathbf{r}^{\rho}_S}\right)_{\mu Y[T]} \\
&\qquad \mathbf{39}.
\end{aligned}$$

For the proof of (24), let $r' = \mathbf{r}^{\rho}_{\mu Z[\mathrm{sub}_X^S[\mathrm{sub}_Y^Z[T]]]}$. By (22), (23), and **43**, we have

$$r' = \mathbf{r}^{\rho}\left(X^{\mathbf{r}^{\rho}_S}_{\mathbf{e}^{\rho,\varepsilon}_S}\right)_{\mu Y[T]}. \tag{25}$$

Then proceed as follows.

$$\mathbf{e}^{\rho,\varepsilon}_{\mathrm{sub}^S_X[\mu Y[T]]} = \mathbf{e}^{\rho,\varepsilon}_{\mu Z[\mathrm{sub}^S_X[\mathrm{sub}^Z_Y[T]]]}$$

(22)

$$= \sum \left\{ z : z \leqslant \mathbf{e}^{\rho,\varepsilon} \left(Z_z^{\mathbf{r}^\rho_{\mu Z[\mathrm{sub}^S_X[\mathrm{sub}^Z_Y[T]]]}} \right)_{\mathrm{sub}^S_X[\mathrm{sub}^Z_Y[T]]} \right\}$$

39

$$= \sum \left\{ z : z \leqslant \mathbf{e}^{\rho,\varepsilon} \left(Z_z^{r'} \right)_{\mathrm{sub}^S_X[\mathrm{sub}^Z_Y[T]]} \right\}$$

definition of r'

$$= \sum \left\{ z : z \leqslant \mathbf{e}^{\rho,\varepsilon} \left(Z_z^{r'} \right) \left(X^{\mathbf{r}^\rho(Z_z^{r'})_S}_{\mathbf{e}^{\rho,\varepsilon}(Z_z^{r'})_S} \right)_{\mathrm{sub}^Z_Y[T]} \right\}$$

induction hypothesis on $\mathrm{sub}^Z_Y[T]$

$$= \sum \left\{ z : z \leqslant \mathbf{e}^{\rho,\varepsilon} \left(Z_z^{r'} \right) \left(X^{\mathbf{r}^\rho_S}_{\mathbf{e}^{\rho,\varepsilon}_S} \right)_{\mathrm{sub}^Z_Y[T]} \right\}$$

$Z \notin \mathrm{Free}(S)$, **45**

$$= \sum \left\{ z : z \leqslant \mathbf{e}^{\rho,\varepsilon} \left(Z_z^{r'} \right) \left(X^{\mathbf{r}^\rho_S}_{\mathbf{e}^{\rho,\varepsilon}_S} \right) \left(Y^{\mathbf{r}^\rho(Z_z^{r'})\left(X^{\mathbf{r}^\rho_S}_{\mathbf{e}^{\rho,\varepsilon}_S}\right)_Z}_{\mathbf{e}^{\rho,\varepsilon}(Z_z^{r'})\left(X^{\mathbf{r}^\rho_S}_{\mathbf{e}^{\rho,\varepsilon}_S}\right)_Z} \right)_T \right\}$$

induction hypothesis on T

$$= \sum \left\{ z : z \leqslant \mathbf{e}^{\rho,\varepsilon} \left(Z_z^{r'} \right) \left(X^{\mathbf{r}^\rho_S}_{\mathbf{e}^{\rho,\varepsilon}_S} \right) \left(Y_z^{r'} \right)_T \right\}$$

42(i), **39**, **38**

$$= \sum \left\{ z : z \leqslant \mathbf{e}^{\rho,\varepsilon} \left(X^{\mathbf{r}^\rho_S}_{\mathbf{e}^{\rho,\varepsilon}_S} \right) \left(Y_z^{r'} \right)_T \right\}$$

42(i), $Z \notin \mathrm{Free}(T)$, **45**

$$= \sum \left\{ z : z \leqslant \mathbf{e}^{\rho,\varepsilon} \left(X^{\mathbf{r}^\rho_S}_{\mathbf{e}^{\rho,\varepsilon}_S} \right) \left(Y_z^{\mathbf{r}^\rho\left(X^{r^\rho_S}_{\mathbf{e}^{\rho,\varepsilon}_S}\right)_{\mu Y[T]}} \right)_T \right\}$$

(25)

$$= \mathbf{e}^{\rho,\varepsilon} \left(X^{\mathbf{r}^\rho_S}_{\mathbf{e}^{\rho,\varepsilon}_S} \right)_{\mu Y[T]}$$

39.

We will not worry about the other cases. □

7.2. *Derivatives and the Hitchcock–Park-de Bakker theorem*

The derivative $\mathbf{d}X[S]$ of a statement S with respect to a variable X is another statement with the following intuitive meaning. Suppose we execute statement S from state σ_1. We pass through many intermediate states while executing the substatements of S. Suppose we arrive at state σ_2 just before executing the variable X. Then the pair $\langle \sigma_1, \sigma_2 \rangle$ belongs to $\mathbf{r}^\rho_{\mathbf{d}X[S]}$. See [17, 9, 48] for more such remarks.

The definition of derivative has been extended here to cover some additional language contructs; in particular, $\mathsf{d}X\,[\mathsf{while}\,B\,\mathsf{do}\,S]$ is defined according the fact that, under the right hypotheses, $\mathsf{while}\,B\,\mathsf{do}\,S$ and $\mu X\,\left[\mathsf{if}\,B\,\mathsf{then}\,S;X\,\mathsf{else\ skip}\right]$ are semantically equivalent.

Definition 49. The derivative $\mathsf{d}X\,[\text{-}] : \mathscr{S}tat \to \mathscr{S}tat$ (with respect to variable $X \in \mathscr{V}ar$) is the unique function that satisfies the following conditions:

(i) $\mathsf{d}X\,[S] = \begin{cases} \mathsf{abort} \text{ if } X \neq S \in \mathscr{B}asic, \\ \mathsf{skip} \text{ if } X = S \end{cases}$

(ii) $\mathsf{d}X\,[S;T] = \mathsf{d}X\,[S]\,\mathsf{or}\,S;\mathsf{d}X\,[T]$.

(iii) $\mathsf{d}X\,[S\,\mathsf{or}\,T] = \mathsf{d}X\,[S]\,\mathsf{or}\,\mathsf{d}X\,[T]$.

(iv) $\mathsf{d}X\,\left[\mathsf{OR}_{i\in I}S_i\right] = \mathsf{OR}_{i\in I}\mathsf{d}X\,[S_i]$.

(v) $\mathsf{d}X\,\left[\mathsf{if}\,B\,\mathsf{then}\,S\,\mathsf{else}\,T\right] = \mathsf{if}\,B\,\mathsf{then}\,\mathsf{d}X\,[S]\,\mathsf{else}\,\mathsf{d}X\,[T]$.

(vi) $\mathsf{d}X\,[B \to S] = B \to \mathsf{d}X\,[S]$.

(vii) $\mathsf{d}X\,[\mathsf{IF}_{i\in I}(B_i \to S_i)] = \mathsf{IF}_{i\in I}(B_i \to \mathsf{d}X\,[S_i])$.

(viii) $\mathsf{d}X\,[\mathsf{while}\,B\,\mathsf{do}\,S] = \mu Z[(\mathsf{if}\,B\,\mathsf{then}\,\mathsf{d}X\,[S]\,\mathsf{else\ abort})\,\mathsf{or}((\mathsf{if}\,B\,\mathsf{then}\,S\,\mathsf{else\ abort});Z)]$, where Z is the first variable distinct from X that does not occur free in S.

(ix) $\mathsf{d}X\,[\mu X\,[S]] = \mathsf{abort}$.

(x) If $X \neq Y$ then $\mathsf{d}X\,[\mu Y\,[S]] = \mu Z\left[\mathrm{sub}_Y^{\mu Y[S]}\,[\mathsf{d}X\,[S]\,\mathsf{or}\,\mathsf{d}Y\,[S]\,;Z]\right]$, where Z is the first variable that does not occur free in S and is distinct from X and Y.

Theorem **51** below is the main result of this subsection. It corresponds to Theorem 8.43 and Corollary 8.42 of [9]. First we need a lemma.

Lemma 50. *If $\mathfrak{A}$ is a complete relation algebra, $\rho, \varepsilon : \mathscr{B}asic \to A$, and $X \neq Y$, then, for every $S \in \mathscr{S}tat$,*

$$\mathbf{r}^{\rho}_{\mathsf{d}X[\mu Y[S]]} = \prod\left\{ z : z \geqslant \mathbf{r}^{\rho}_{\mathrm{sub}_Y^{\mu Y[S]}[\mathsf{d}X[S]]} + \mathbf{r}^{\rho}_{\mathrm{sub}_Y^{\mu Y[S]}[\mathsf{d}Y[S]]};z \right\}.$$

Proof. Let Z be the first variable that does not occur free in S and is distinct from X and Y. Then Z does not occur free in either $\mathrm{sub}_Y^{\mu Y[S]}\,[\mathsf{d}X\,[S]]$ or $\mathrm{sub}_Y^{\mu Y[S]}\,[\mathsf{d}Y\,[S]]$, so

$$\begin{aligned}
&\mathbf{r}^{\rho}_{\mathsf{d}X[\mu Y[S]]} \\
&= \mathbf{r}^{\rho}_{\mu Z\left[\mathrm{sub}_Y^{\mu Y[S]}[\mathsf{d}X[S]\,\mathsf{or}\,\mathsf{d}Y[S];Z]\right]} && \textbf{49(x)} \\
&= \mathbf{r}^{\rho}_{\mu Z\left[\mathrm{sub}_Y^{\mu Y[S]}[\mathsf{d}X[S]]\,\mathsf{or}\,\mathrm{sub}_Y^{\mu Y[S]}[\mathsf{d}Y[S]];Z\right]} && \textbf{47(i)(ii)(iii)} \\
&= \prod\left\{ z : z \geqslant \mathbf{r}^{\rho}\left(Z_0^z\right)_{\mathrm{sub}_Y^{\mu Y[S]}[\mathsf{d}X[S]]\,\mathsf{or}\,\mathrm{sub}_Y^{\mu Y[S]}[\mathsf{d}Y[S]];Z} \right\} && \textbf{39} \\
&= \prod\left\{ z : z \geqslant \mathbf{r}^{\rho}_{\mathrm{sub}_Y^{\mu Y[S]}[\mathsf{d}X[S]]} + \mathbf{r}^{\rho}_{\mathrm{sub}_Y^{\mu Y[S]}[\mathsf{d}Y[S]]};z \right\} && \textbf{38, 39, 45.}
\end{aligned}$$

□

Theorem 51. *Assume* $\mathfrak{A}$ *is a complete relation algebra,* $\rho, \varepsilon : \mathscr{Basic} \to A$, $x, y \in A$, $\rho_{\mathsf{abort}} = 0$, *and* $\rho_{\mathsf{skip}} = 1'$. *Then, for every* $S \in \mathscr{Stat}$,

$$\mathbf{e}^{\rho,\varepsilon}\left(X_y^x\right)_S = \mathbf{e}^{\rho,\varepsilon}\left(X_0^x\right)_S + \mathbf{r}^{\rho}\left(X_0^x\right)_{\mathsf{d}X[S]} ; y.$$

Proof. The proof is by induction on the complexity of statements. Suppose first that $S \in \mathscr{Basic}$. If $X \neq S$, then

$$\begin{aligned}
&\mathbf{e}^{\rho,\varepsilon}\left(X_0^x\right)_S + \mathbf{r}^{\rho}\left(X_0^x\right)_{\mathsf{d}X[S]} ; y \\
&\quad = \mathbf{e}_S^{\rho,\varepsilon} + \mathbf{r}^{\rho}\left(X_0^x\right)_{\mathsf{abort}} ; y && \textbf{45}, X \neq S, \textbf{49}(\mathrm{i}) \\
&\quad = \mathbf{e}_S^{\rho,\varepsilon} + 0 ; y && \textbf{39}, \textbf{45}, \rho_{\mathsf{abort}} = 0 \\
&\quad = \mathbf{e}_S^{\rho,\varepsilon} && \textbf{24}(\mathrm{xviii}), \textbf{5}(\mathrm{vii}) \\
&\quad = \mathbf{e}^{\rho,\varepsilon}\left(X_y^x\right)_S && \textbf{45}, X \neq S.
\end{aligned}$$

If $X = S$, then

$$\begin{aligned}
&\mathbf{e}^{\rho,\varepsilon}\left(X_0^x\right)_S + \mathbf{r}^{\rho}\left(X_0^x\right)_{\mathsf{d}X[S]} ; y \\
&\quad = \mathbf{e}^{\rho,\varepsilon}\left(X_0^x\right)_X + \mathbf{r}^{\rho}\left(X_0^x\right)_{\mathsf{d}X[X]} ; y && X = S \\
&\quad = 0 + \mathbf{r}^{\rho}\left(X_0^x\right)_{\mathsf{skip}} ; y && \textbf{38}, \textbf{39}, \textbf{49}(\mathrm{i}) \\
&\quad = 1' ; y && (\mathrm{Ba}_1), \textbf{5}(\mathrm{vii}), \textbf{39}, \textbf{45}, \rho_{\mathsf{skip}} = 1' \\
&\quad = y && \textbf{24}(\mathrm{xix}) \\
&\quad = \mathbf{e}^{\rho,\varepsilon}\left(X_y^x\right)_X && \textbf{38}, \textbf{39}
\end{aligned}$$

Thus, the result holds for every basic statement $S \in \mathscr{Basic}$.

For the rest of the proof we assume that the theorem holds for statements S, T, and S_i for every $i \in I$, and we show that the theorem also holds for the compound statements built up from these statements.

Proof for $S;T$:

$$\begin{aligned}
&\mathbf{e}^{\rho,\varepsilon}\left(X_y^x\right)_{S;T} \\
&\quad = \mathbf{e}^{\rho,\varepsilon}\left(X_y^x\right)_S + \mathbf{r}^{\rho}\left(X_y^x\right)_S ; \mathbf{e}^{\rho,\varepsilon}\left(X_y^x\right)_T \\
&\qquad\qquad \textbf{39} \\
&\quad = \left(\mathbf{e}^{\rho,\varepsilon}\left(X_0^x\right)_S + \mathbf{r}^{\rho}\left(X_0^x\right)_{\mathsf{d}X[S]} ; y\right) + \mathbf{r}^{\rho}\left(X_0^x\right)_S ; \left(\mathbf{e}^{\rho,\varepsilon}\left(X_0^x\right)_T + \mathbf{r}^{\rho}\left(X_0^x\right)_{\mathsf{d}X[T]} ; y\right) \\
&\qquad\qquad \text{induction hypothesis} \\
&\quad = \mathbf{e}^{\rho,\varepsilon}\left(X_0^x\right)_S + \mathbf{r}^{\rho}\left(X_0^x\right)_S ; \mathbf{e}^{\rho,\varepsilon}\left(X_0^x\right)_T + \left(\mathbf{r}^{\rho}\left(X_0^x\right)_{\mathsf{d}X[S]} + \mathbf{r}^{\rho}\left(X_0^x\right)_S ; \mathbf{r}^{\rho}\left(X_0^x\right)_{\mathsf{d}X[T]}\right) ; y \\
&\qquad\qquad (\mathrm{Ba}_1), (\mathrm{Ba}_2), \textbf{24}(\mathrm{xv}) \\
&\quad = \mathbf{e}^{\rho,\varepsilon}\left(X_0^x\right)_{S;T} + \mathbf{r}^{\rho}\left(X_0^x\right)_{\mathsf{d}X[S]\,\mathsf{or}\,S;\mathsf{d}X[T]} ; y \\
&\qquad\qquad \textbf{39} \\
&\quad = \mathbf{e}^{\rho,\varepsilon}\left(X_0^x\right)_{S;T} + \mathbf{r}^{\rho}\left(X_0^x\right)_{\mathsf{d}X[S;T]} ; y \\
&\qquad\qquad \textbf{49}(\mathrm{ii})
\end{aligned}$$

Proof for S or T:

$$\begin{aligned}
&\mathbf{e}^{\rho,\varepsilon}\left(X_y^x\right)_{S \text{ or } T}\\
&= \mathbf{e}^{\rho,\varepsilon}\left(X_y^x\right)_S + \mathbf{e}^{\rho,\varepsilon}\left(X_y^x\right)_T\\
&\qquad\qquad \mathbf{39}\\
&= \mathbf{e}^{\rho,\varepsilon}\left(X_0^x\right)_S + \mathbf{r}^{\rho}\left(X_0^x\right)_{\mathrm{d}X[S]};y + \mathbf{e}^{\rho,\varepsilon}\left(X_0^x\right)_T + \mathbf{r}^{\rho}\left(X_0^x\right)_{\mathrm{d}X[T]};y\\
&\qquad\qquad \text{induction hypothesis}\\
&= \mathbf{e}^{\rho,\varepsilon}\left(X_0^x\right)_S + \mathbf{e}^{\rho,\varepsilon}\left(X_0^x\right)_T + \left(\mathbf{r}^{\rho}\left(X_0^x\right)_{\mathrm{d}X[S]} + \mathbf{r}^{\rho}\left(X_0^x\right)_{\mathrm{d}X[T]}\right);y\\
&\qquad\qquad (\mathrm{Ba}_1),\ (\mathrm{Ba}_2),\ (\mathrm{Ra}_2)\\
&= \mathbf{e}^{\rho,\varepsilon}\left(X_0^x\right)_{S \text{ or } T} + \mathbf{r}^{\rho}\left(X_0^x\right)_{\mathrm{d}X[S] \text{ or } \mathrm{d}X[T]};y\\
&\qquad\qquad \mathbf{39}\\
&= \mathbf{e}^{\rho,\varepsilon}\left(X_0^x\right)_{S \text{ or } T} + \mathbf{r}^{\rho}\left(X_0^x\right)_{\mathrm{d}X[S \text{ or } T]};y\\
&\qquad\qquad \mathbf{49}(\mathrm{iii}).
\end{aligned}$$

Proof for $\mathsf{OR}_{i\in I}S_i$:

$$\begin{aligned}
&\mathbf{e}^{\rho,\varepsilon}\left(X_y^x\right)_{\mathsf{OR}_{i\in I}S_i}\\
&= \sum_{i\in I}\mathbf{e}^{\rho,\varepsilon}\left(X_y^x\right)_{S_i} && \mathbf{39}\\
&= \sum_{i\in I}\left(\mathbf{e}^{\rho,\varepsilon}\left(X_0^x\right)_{S_i} + \mathbf{r}^{\rho}\left(X_0^x\right)_{\mathrm{d}X[S_i]};y\right) && \text{induction hypothesis}\\
&= \sum_{i\in I}\mathbf{e}^{\rho,\varepsilon}\left(X_0^x\right)_{S_i} + \sum_{i\in I}\mathbf{r}^{\rho}\left(X_0^x\right)_{\mathrm{d}X[S_i]};y && \mathbf{9}(\mathrm{i}),\ \mathbf{24}(\mathrm{xv})\\
&= \mathbf{e}^{\rho,\varepsilon}\left(X_0^x\right)_{\mathsf{OR}_{i\in I}S_i} + \mathbf{r}^{\rho}\left(X_0^x\right)_{\mathsf{OR}_{i\in I}\mathrm{d}X[S_i]};y && \mathbf{39}\\
&= \mathbf{e}^{\rho,\varepsilon}\left(X_0^x\right)_{\mathsf{OR}_{i\in I}S_i} + \mathbf{r}^{\rho}\left(X_0^x\right)_{\mathrm{d}X[\mathsf{OR}_{i\in I}S_i]};y && \mathbf{49}(\mathrm{iv})
\end{aligned}$$

Proof for if B then S else T:

$$\begin{aligned}
&\mathbf{e}^{\rho,\varepsilon}\left(X_y^x\right)_{\text{if } B \text{ then } S \text{ else } T}\\
&= \rho_B;\mathbf{e}^{\rho,\varepsilon}\left(X_y^x\right)_S + \overline{\rho_B;1}\cdot\mathbf{e}^{\rho,\varepsilon}\left(X_y^x\right)_T\\
&\qquad\qquad \mathbf{39}\\
&= \rho_B;\left(\mathbf{e}^{\rho,\varepsilon}\left(X_0^x\right)_S + \mathbf{r}^{\rho}\left(X_0^x\right)_{\mathrm{d}X[S]};y\right)\\
&\quad +\overline{\rho_B;1}\cdot\left(\mathbf{e}^{\rho,\varepsilon}\left(X_0^x\right)_T + \mathbf{r}^{\rho}\left(X_0^x\right)_{\mathrm{d}X[T]};y\right)\\
&\qquad\qquad \text{induction hypothesis}\\
&= \rho_B;\mathbf{e}^{\rho,\varepsilon}\left(X_0^x\right)_S + \overline{\rho_B;1}\cdot\mathbf{e}^{\rho,\varepsilon}\left(X_0^x\right)_T\\
&\quad +\rho_B;\mathbf{r}^{\rho}\left(X_0^x\right)_{\mathrm{d}X[S]};y + \overline{\rho_B;1}\cdot\mathbf{r}^{\rho}\left(X_0^x\right)_{\mathrm{d}X[T]};y\\
&\qquad\qquad \mathbf{3}(\mathrm{xv}),\ \mathbf{24}(\mathrm{xv}),\ (\mathrm{Ba}_1),\ (\mathrm{Ba}_2)\\
&= \rho_B;\mathbf{e}^{\rho,\varepsilon}\left(X_0^x\right)_S + \overline{\rho_B;1}\cdot\mathbf{e}^{\rho,\varepsilon}\left(X_0^x\right)_T\\
&\quad +\left(\rho_B;\mathbf{r}^{\rho}\left(X_0^x\right)_{\mathrm{d}X[S]} + \overline{\rho_B;1}\cdot\mathbf{r}^{\rho}\left(X_0^x\right)_{\mathrm{d}X[T]}\right);y\\
&\qquad\qquad \mathbf{26}(\mathrm{i})(\mathrm{ii}),\ \mathbf{24}(\mathrm{xxviii}),\ (\mathrm{Ra}_2)\\
&= \mathbf{e}^{\rho,\varepsilon}\left(X_0^x\right)_{\text{if } B \text{ then } S \text{ else } T} + \mathbf{e}^{\rho,\varepsilon}\left(X_0^x\right)_{\text{if } B \text{ then } \mathrm{d}X[S] \text{ else } \mathrm{d}X[T]};y\\
&\qquad\qquad \mathbf{39}\\
&= \mathbf{e}^{\rho,\varepsilon}\left(X_0^x\right)_{\text{if } B \text{ then } S \text{ else } T} + \mathbf{e}^{\rho,\varepsilon}\left(X_0^x\right)_{\mathrm{d}X[\text{if } B \text{ then } S \text{ else } T]};y\\
&\qquad\qquad \mathbf{49}(\mathrm{v}).
\end{aligned}$$

Proof for $B \to S$:

$$\begin{aligned}
&\mathbf{e}^{\rho,\varepsilon}\left(X_y^x\right)_{B\to S}\\
&= \overline{\rho_B;1} + \rho_B;\mathbf{e}^{\rho,\varepsilon}\left(X_y^x\right)_S\\
&\qquad\qquad \textbf{39}\\
&= \overline{\rho_B;1} + \rho_B;\left(\mathbf{e}^{\rho,\varepsilon}\left(X_0^x\right)_S + \mathbf{r}^{\rho}\left(X_0^x\right)_{\mathrm{d}X[S]};y\right)\\
&\qquad\qquad \text{induction hypothesis}\\
&= \overline{\rho_B;1} + \rho_B;\mathbf{e}^{\rho,\varepsilon}\left(X_0^x\right)_S + \rho_B;\mathbf{r}^{\rho}\left(X_0^x\right)_{\mathrm{d}X[S]};y\\
&\qquad\qquad \textbf{24}(\mathrm{ix}),\ (\mathrm{Ba}_1),\ (\mathrm{Ra}_1)\\
&= \mathbf{e}^{\rho,\varepsilon}\left(X_0^x\right)_{B\to S} + \mathbf{r}^{\rho}\left(X_0^x\right)_{B\to \mathrm{d}X[S]};y\\
&\qquad\qquad \textbf{39}\\
&= \mathbf{e}^{\rho,\varepsilon}\left(X_0^x\right)_{B\to S} + \mathbf{r}^{\rho}\left(X_0^x\right)_{\mathrm{d}X[B\to S]};y\\
&\qquad\qquad \textbf{49}(\mathrm{vi}).
\end{aligned}$$

Proof for $\mathsf{IF}_{i\in I}(B_i \to S_i)$:

$$\begin{aligned}
&\mathbf{e}^{\rho,\varepsilon}\left(X_y^x\right)_{\mathsf{IF}_{i\in I}(B_i\to S_i)}\\
&= \prod_{i\in I}\overline{\rho_{B_i};1} + \sum_{i\in I}\left(\rho_{B_i};\mathbf{e}^{\rho,\varepsilon}\left(X_y^x\right)_{S_i}\right)\\
&\qquad\qquad \textbf{39}\\
&= \prod_{i\in I}\overline{\rho_{B_i};1} + \sum_{i\in I}\left(\rho_{B_i};\left(\mathbf{e}^{\rho,\varepsilon}\left(X_0^x\right)_{S_i} + \mathbf{r}^{\rho}\left(X_0^x\right)_{\mathrm{d}X[S_i]};y\right)\right)\\
&\qquad\qquad \text{induction hypothesis}\\
&= \prod_{i\in I}\overline{\rho_{B_i};1} + \sum_{i\in I}\left(\rho_{B_i};\mathbf{e}^{\rho,\varepsilon}\left(X_0^x\right)_{S_i}\right) + \sum_{i\in I}\left(\rho_{B_i};\mathbf{r}^{\rho}\left(X_0^x\right)_{\mathrm{d}X[S_i]}\right);y\\
&\qquad\qquad \textbf{24}(\mathrm{xv}),\ \textbf{9}(\mathrm{i}),\ (\mathrm{Ba}_1),\ (\mathrm{Ra}_1)\\
&= \mathbf{e}^{\rho,\varepsilon}\left(X_0^x\right)_{\mathsf{IF}_{i\in I}(B_i\to S_i)} + \mathbf{r}^{\rho}\left(X_0^x\right)_{\mathsf{IF}_{i\in I}(B_i\to \mathrm{d}X[S_i])};y\\
&\qquad\qquad \textbf{39}\\
&= \mathbf{e}^{\rho,\varepsilon}\left(X_0^x\right)_{\mathsf{IF}_{i\in I}(B_i\to S_i)} + \mathbf{r}^{\rho}\left(X_0^x\right)_{\mathrm{d}X[\mathsf{IF}_{i\in I}(B_i\to S_i)]};y\\
&\qquad\qquad \textbf{49}(\mathrm{vii}).
\end{aligned}$$

Proof for $\mathsf{while}\,B\,\mathsf{do}\,S$: We wish to show

$$\mathbf{e}^{\rho,\varepsilon}\left(X_y^x\right)_{\mathsf{while}\,B\,\mathsf{do}\,S} = \mathbf{e}^{\rho,\varepsilon}\left(X_0^x\right)_{\mathsf{while}\,B\,\mathsf{do}\,S} + \mathbf{r}^{\rho}\left(X_0^x\right)_{\mathrm{d}X[\mathsf{while}\,B\,\mathsf{do}\,S]};y \tag{26}$$

Let

$$\begin{aligned}
p &:= \rho_B;\mathbf{e}^{\rho,\varepsilon}\left(X_0^x\right)_S\\
s &:= \rho_B;\mathbf{r}^{\rho}\left(X_0^x\right)_{\mathrm{d}X[S]}\\
t &:= \rho_B;\mathbf{r}^{\rho}\left(X_0^x\right)_S.
\end{aligned}$$

Expand the left-hand side of (26):

$$\begin{aligned}
&\mathbf{e}^{\rho,\varepsilon}\left(X_y^x\right)_{\text{while } B \text{ do } S} \\
&\quad = \sum\left\{ z : z \leqslant \rho_B ; \mathbf{e}^{\rho,\varepsilon}\left(X_y^x\right)_S + \rho_B ; \mathbf{r}^{\rho}\left(X_y^x\right)_S ; z \right\} \\
&\qquad\qquad \mathbf{39} \\
&\quad = \sum\left\{ z : z \leqslant \rho_B ; \left(\mathbf{e}^{\rho,\varepsilon}\left(X_0^x\right)_S + \mathbf{r}^{\rho}\left(X_0^x\right)_{\mathrm{d}X[S]} ; y\right) + \rho_B ; \mathbf{r}^{\rho}\left(X_0^x\right)_S ; z \right\} \\
&\qquad\qquad \text{induction hypothesis, } \mathbf{43} \\
&\quad = \sum\{ z : z \leqslant p + s ; y + t ; z \} \\
&\qquad\qquad \mathbf{24}(\mathrm{ix}),\ (\mathrm{Ra}_1),\ \text{definitions of } p,\ s,\ t.
\end{aligned}$$

Consider the first term on the right-hand side of (26):

$$\begin{aligned}
&\mathbf{e}^{\rho,\varepsilon}\left(X_0^x\right)_{\text{while } B \text{ do } S} \\
&\quad = \sum\left\{ z : z \leqslant \rho_B ; \mathbf{e}^{\rho,\varepsilon}\left(X_0^x\right)_S + \rho_B ; \mathbf{r}^{\rho}\left(X_0^x\right)_S ; z \right\} \\
&\qquad\qquad \mathbf{39} \\
&\quad = \sum\{ z : z \leqslant p + t ; z \} \\
&\qquad\qquad \text{definitions of } p,\ t.
\end{aligned}$$

For the second term on the right-hand side of (26), first note that

$$\begin{aligned}
\mathrm{d}X\,[\textsf{while } B \textsf{ do } S] = \mu Z\,[&(\textsf{if } B \textsf{ then } \mathrm{d}X\,[S] \textsf{ else abort}) \\
&\textsf{or } ((\textsf{if } B \textsf{ then } S \textsf{ else abort}) ; Z)]
\end{aligned}$$

where Z is the first variable distinct from X that does not occur free in S. Furthermore,

$$\begin{aligned}
&\mathbf{r}^{\rho}\left(X_0^x\right)\left(Z_0^z\right)_{\text{if } B \text{ then } S \text{ else abort}} \\
&\quad = \rho_B ; \mathbf{r}^{\rho}\left(X_0^x\right)\left(Z_0^z\right)_S + \overline{\rho_B ; 1} \cdot \rho_{\textsf{abort}} && \mathbf{38},\ \mathbf{39} \\
&\quad = \rho_B ; \mathbf{r}^{\rho}\left(X_0^x\right)\left(Z_0^z\right)_S + \overline{\rho_B ; 1} \cdot 0 && \rho_{\textsf{abort}} = 0 \\
&\quad = \rho_B ; \mathbf{r}^{\rho}\left(X_0^x\right)\left(Z_0^z\right)_S && \mathbf{5}(\mathrm{vi})(\mathrm{vii}) \\
&\quad = \rho_B ; \mathbf{r}^{\rho}\left(X_0^x\right)_S && Z \notin \mathrm{Free}(S),\ \mathbf{45} \\
&\quad = t && \text{definition of } t
\end{aligned}$$

so

$$\mathbf{r}^{\rho}\left(X_0^x\right)\left(Z_0^z\right)_{\text{if } B \text{ then } S \text{ else abort}} = t, \tag{27}$$

and, similarly,

$$\mathbf{r}^{\rho}\left(X_0^x\right)\left(Z_0^z\right)_{\text{if } B \text{ then } \mathrm{d}X[S] \text{ else abort}} = \rho_B ; \mathbf{r}^{\rho}\left(X_0^x\right)_{\mathrm{d}X[S]} = s, \tag{28}$$

since $Z \notin \mathrm{Free}(\mathrm{d}X[S])$. Then we get

$$\begin{aligned}
&\mathbf{r}^{\rho}\left(X_0^x\right)_{\mathrm{d}X[\mathsf{while}\,B\,\mathsf{do}\,S]} \\
&= \mathbf{r}^{\rho}\left(X_0^x\right)_{\mu Z[(\mathsf{if}\,B\,\mathsf{then}\,\mathrm{d}X[S]\,\mathsf{else\,abort})\,\mathsf{or}((\mathsf{if}\,B\,\mathsf{then}\,S\,\mathsf{else\,abort});Z)]} \\
&\qquad\qquad\qquad\textbf{49}(\mathrm{viii}) \\
&= \prod\left\{z : z \geqslant \mathbf{r}^{\rho}\left(X_0^x\right)\left(Z_0^z\right)_{(\mathsf{if}\,B\,\mathsf{then}\,\mathrm{d}X[S]\,\mathsf{else\,abort})\,\mathsf{or}((\mathsf{if}\,B\,\mathsf{then}\,S\,\mathsf{else\,abort});Z)}\right\} \\
&\qquad\qquad\qquad\textbf{39} \\
&= \prod\Big\{z : z \geqslant \mathbf{r}^{\rho}\left(X_0^x\right)\left(Z_0^z\right)_{\mathsf{if}\,B\,\mathsf{then}\,\mathrm{d}X[S]\,\mathsf{else\,abort}} \\
&\quad + \mathbf{r}^{\rho}\left(X_0^x\right)\left(Z_0^z\right)_{\mathsf{if}\,B\,\mathsf{then}\,S\,\mathsf{else\,abort}} ; \mathbf{r}^{\rho}\left(X_0^x\right)\left(Z_0^z\right)_Z\Big\} \\
&\qquad\qquad\qquad\textbf{39} \\
&= \prod\{z : z \geqslant s + t;z\}
\end{aligned}$$

(27), (28), $Z \notin \mathrm{Free}(S)$, **45**, definitions of s, t,

so, by **30**(iii),

$$\mathbf{r}^{\rho}\left(X_0^x\right)_{\mathrm{d}X[\mathsf{while}\,B\,\mathsf{do}\,S]} ; y = \prod\{z : z \geqslant s + t;z\} ; y = \prod\{z : z \geqslant s;y + t;z\}.$$

In summary, we have

$$\mathbf{e}^{\rho,\varepsilon}\left(X_y^x\right)_{\mathsf{while}\,B\,\mathsf{do}\,S} = \sum\{z : z \leqslant p + s;y + t;z\}$$

$$\mathbf{e}^{\rho,\varepsilon}\left(X_0^x\right)_{\mathsf{while}\,B\,\mathsf{do}\,S} = \sum\{z : z \leqslant p + t;z\}$$

$$\mathbf{r}^{\rho}\left(X_0^x\right)_{\mathrm{d}X[\mathsf{while}\,B\,\mathsf{do}\,S]} ; y = \prod\{z : z \geqslant s;y + t;z\},$$

so (26) follows by **31**(ii).

The proof for $\mu Y[S]$ is similar to the proof for $\mathsf{while}\,B\,\mathsf{do}\,S$. We wish to prove that

$$\mathbf{e}^{\rho,\varepsilon}\left(X_y^x\right)_{\mu Y[S]} = \mathbf{e}^{\rho,\varepsilon}\left(X_0^x\right)_{\mu Y[S]} + \mathbf{r}^{\rho}\left(X_0^x\right)_{\mathrm{d}X[\mu Y[S]]} ; y \tag{29}$$

If $Y = X$ then

$$\mathbf{e}^{\rho,\varepsilon}\left(X_y^x\right)_{\mu Y[S]} = \mathbf{e}^{\rho,\varepsilon}_{\mu Y[S]} = \mathbf{e}^{\rho,\varepsilon}\left(X_0^x\right)_{\mu Y[S]}$$

by **44**(v) and **45**, and

$$\mathbf{r}^{\rho}\left(X_0^x\right)_{\mathrm{d}X[\mu Y[S]]} ; y = \mathbf{r}^{\rho}_{\mathsf{abort}} ; y = 0;y = 0$$

by hypothesis and **24**(xviii), so (29) holds. Assume $Y \neq X$. Let

$$\begin{aligned}
q &:= \mathbf{r}^{\rho}\left(X_y^x\right)_{\mu Y[S]}, \\
p &:= \mathbf{e}^{\rho,\varepsilon}\left(X_0^x\right)\left(Y_0^q\right)_S, \\
s &:= \mathbf{r}^{\rho}\left(X_0^x\right)\left(Y_0^q\right)_{\mathrm{d}X[S]}, \\
t &:= \mathbf{r}^{\rho}\left(X_0^x\right)\left(Y_0^q\right)_{\mathrm{d}Y[S]}.
\end{aligned}$$

Expand the left-hand-side of (29):

$$
\begin{aligned}
&\mathbf{e}^{\rho,\varepsilon}\left(X_y^x\right)_{\mu Y[S]} \\
&\quad = \sum\left\{ w : w \leqslant \mathbf{e}^{\rho,\varepsilon}\left(X_y^x\right)\left(Y_w^{\mathbf{r}^\rho(X_y^x)_{\mu Y[S]}}\right)_S \right\} \\
&\qquad\qquad \mathbf{39} \\
&\quad = \sum\left\{ w : w \leqslant \mathbf{e}^{\rho,\varepsilon}\left(X_y^x\right)\left(Y_w^q\right)_S \right\} \\
&\qquad\qquad \text{definition of } q \\
&\quad = \sum\left\{ w : w \leqslant \mathbf{e}^{\rho,\varepsilon}\left(X_y^x\right)\left(Y_0^q\right)_S + \mathbf{r}^\rho\left(X_y^x\right)\left(Y_0^q\right)_{\mathsf{d}Y[S]} ; w \right\} \\
&\qquad\qquad \text{induction hypothesis} \\
&\quad = \sum\left\{ w : w \leqslant \mathbf{e}^{\rho,\varepsilon}\left(Y_0^q\right)\left(X_y^x\right)_S + \mathbf{r}^\rho\left(Y_0^q\right)\left(X_y^x\right)_{\mathsf{d}Y[S]} ; w \right\} \\
&\qquad\qquad \mathbf{42}(\mathrm{i}) \\
&\quad = \sum\left\{ w : w \leqslant \mathbf{e}^{\rho,\varepsilon}\left(Y_0^q\right)\left(X_0^x\right)_S + \mathbf{r}^\rho\left(Y_0^q\right)\left(X_0^x\right)_{\mathsf{d}X[S]} ; y \right. \\
&\qquad \left. + \mathbf{r}^\rho\left(Y_0^q\right)\left(X_0^x\right)_{\mathsf{d}Y[S]} ; w \right\} \\
&\qquad\qquad \text{induction hypothesis, } \mathbf{43} \\
&\quad = \sum\{ w : w \leqslant p + s ; y + t ; w \} \\
&\qquad\qquad \mathbf{42}(\mathrm{i}), \text{ definitions of } p, s, t.
\end{aligned}
$$

Expand the first term on the right-hand side of (29):

$$
\begin{aligned}
&\mathbf{e}^{\rho,\varepsilon}\left(X_0^x\right)_{\mu Y[S]} \\
&\quad = \sum\left\{ w : w \leqslant \mathbf{e}^{\rho,\varepsilon}\left(X_0^x\right)\left(Y_w^{\mathbf{r}^\rho(X_0^x)_{\mu Y[S]}}\right)_S \right\} && \mathbf{39} \\
&\quad = \sum\left\{ w : w \leqslant \mathbf{e}^{\rho,\varepsilon}\left(X_0^x\right)\left(Y_w^q\right)_S \right\} && \text{definition of } q, \mathbf{43} \\
&\quad = \sum\left\{ w : w \leqslant \mathbf{e}^{\rho,\varepsilon}\left(X_0^x\right)\left(Y_0^q\right)_S + \mathbf{r}^\rho\left(X_0^x\right)\left(Y_0^q\right)_{\mathsf{d}Y[S]} ; w \right\} && \text{induction hypothesis} \\
&\quad = \sum\{ w : w \leqslant p + t ; w \} && \text{definitions of } p \text{ and } t.
\end{aligned}
$$

Next, expand the second term on the right-hand side of (29):

$$
\begin{aligned}
&\mathbf{r}^\rho\left(X_0^x\right)_{\mathsf{d}X[\mu Y[S]]} ; y \\
&\quad = \prod\left\{ w : w \geqslant \mathbf{r}^\rho\left(X_0^x\right)_{\mathrm{sub}_Y^{\mu Y[S]}[\mathsf{d}X[S]]} ; y + \mathbf{r}^\rho\left(X_0^x\right)_{\mathrm{sub}_Y^{\mu Y[S]}[\mathsf{d}Y[S]]} ; w \right\} \\
&\qquad\qquad \mathbf{50},\ \mathbf{30}(\mathrm{iii}) \\
&\quad = \prod\left\{ w : w \geqslant \mathbf{r}^\rho\left(X_0^x\right)\left(Y_0^{\mathbf{r}^\rho(X_0^x)_{\mu Y[S]}}\right)_{\mathsf{d}X[S]} ; y + \mathbf{r}^\rho\left(X_0^x\right)\left(Y_0^{\mathbf{r}^\rho(X_0^x)_{\mu Y[S]}}\right)_{\mathsf{d}Y[S]} ; w \right\} \\
&\qquad\qquad \mathbf{48} \\
&\quad = \prod\left\{ w : w \geqslant \mathbf{r}^\rho\left(X_0^x\right)\left(Y_0^q\right)_{\mathsf{d}X[S]} ; y + \mathbf{r}^\rho\left(X_0^x\right)\left(Y_0^q\right)_{\mathsf{d}Y[S]} ; w \right\} \\
&\qquad\qquad \text{definition of } q \\
&\quad = \prod\{ w : w \geqslant s ; y + t ; w \} \\
&\qquad\qquad \text{definitions of } s \text{ and } t.
\end{aligned}
$$

We have shown

$$\mathbf{e}^{\rho,\varepsilon}\left(X_y^x\right)_{\mu Y[S]} = \sum\{w : w \leqslant p+s; y+t; w\}$$

$$\mathbf{e}^{\rho,\varepsilon}\left(X_0^x\right)_{\mu Y[S]} = \sum\{w : w \leqslant p+t; w\}$$

$$\mathbf{r}^{\rho}\left(X_0^x\right)_{\mathrm{d}X[\mu Y[S]]}; y = \prod\{w : w \geqslant s; y+t; w\},$$

so the desired conclusion now follows by **31**(ii). □

Theorem 8.47 of [9] concerns "well-foundedness" (see pp. 339–340): a statement S is **well-founded with respect to** a condition B if there are no infinite $\mathbf{r}_S^{\rho}$-chains and no finite $\mathbf{r}_S^{\rho}$-chains that end in states satisfying B. If x is a domain relation in $\mathfrak{Re}(U)$ whose domain is the set of states satisfying B, then this is equivalent to $0 = \sum\{y : y \leqslant x + \mathbf{r}_S^{\rho}; y\}$.

The following theorem contains a relation-algebraic formulation of Theorem 8.47 of [9]. A different relation-algebraic version of the Hitchcock–Park theorem can be found in [48].

Corollary 52. *Assume* $\mathfrak{A}$ *is a complete relation algebra,* $\rho, \varepsilon : \mathscr{Basic} \to A$, $\rho_{\mathsf{abort}} = 0$, *and* $\rho_{\mathsf{skip}} = 1'$. *Then*

(i) $\mathbf{e}^{\rho,\varepsilon}_{\mu X[S]} = \sum\left\{ y : y \leqslant \mathbf{e}^{\rho,\varepsilon}\left(X_0^{\mathbf{r}^{\rho}_{\mu X[S]}}\right)_S + \mathbf{r}^{\rho}\left(X_0^{\mathbf{r}^{\rho}_{\mu X[S]}}\right)_{dX[S]}; y \right\}$.

(ii) $\mathbf{e}^{\rho,\varepsilon}_{\mu X[S]} = \sum\left\{ y : y \leqslant \mathbf{e}^{\rho,\varepsilon}\left(X_0^{\mathbf{r}^{\rho}_{\mu X[S]}}\right)_S + \mathbf{r}^{\rho}_{\mathrm{sub}_X^{\mu X[S]}[\mathrm{d}X[S]]}; y \right\}$.

(iii) *The following statements are equivalent.*

(a) $\mathbf{e}^{\rho,\varepsilon}_{\mu X[S]} = 0$.

(b) $\mathrm{wp}_{\mu X[S]}(1) = 1$.

(c) $\mathrm{sub}_X^{\mu X[S]}[\mathrm{d}X[S]]$ *is well-founded with respect to* $\mathbf{e}^{\rho,\varepsilon}\left(X_0^{\mathbf{r}^{\rho}_{\mu X[S]}}\right)_S$.

(d) $0 = \mathbf{e}^{\rho,\varepsilon}\left(X_0^{\mathbf{r}^{\rho}_{\mu X[S]}}\right)_S$ *and* $0 = \sum\{y : y \leqslant \mathbf{r}^{\rho}_S; y\}$.

Proof. **52**(i), (ii): These parts follow immediately from **51** with $x = \mathbf{r}^{\rho}_{\mu X[S]}$ and **48**. **52**(iii): Use **52**(ii), **34**(iv), parts of **3** and **24**. □

Theorem 53. *Assume* $\mathfrak{A}$ *is a complete relation algebra,* $\rho, \varepsilon : \mathscr{Basic} \to A$, $\rho_{\mathsf{abort}} = 0$, $\rho_{\mathsf{skip}} = 1'$, *and* ε_R *is a domain element for every basic statement* $R \in \mathscr{Basic}$. *Then* $\mathbf{e}^{\rho,\varepsilon}_S$ *is a domain element for every statement* $S \in \mathscr{Stat}$.

Proof. Assume $\rho_{\mathsf{abort}} = 0$ and $\rho_{\mathsf{skip}} = 1'$. We prove by induction on the complexity of statements S that

if ε maps $\mathscr{Basic}$ to domain elements, then $\mathbf{e}^{\rho,\varepsilon}_S$ is a domain element. (30)

Since ε and $\mathbf{e}^{\rho,\varepsilon}$ agree on basic statements, it follows that (30) holds whenever $S \in \mathscr{Basic}$. Suppose (30) is true for S, T, and S_i for every $i \in I$. Assume ε maps $\mathscr{Basic}$ to domain elements. Then $\mathbf{e}^{\rho,\varepsilon}_S$, $\mathbf{e}^{\rho,\varepsilon}_T$, and $\mathbf{e}^{\rho,\varepsilon}_{S_i}$ are domain elements for every $i \in I$. It follows by **39** and **26**(i)(ii)(iii)(iv)(v) that $\mathbf{e}^{\rho,\varepsilon}_{S;T}$, $\mathbf{e}^{\rho,\varepsilon}_{S \text{ or } T}$, $\mathbf{e}^{\rho,\varepsilon}_{\mathsf{OR}_{i\in I}S_i}$, $\mathbf{e}^{\rho,\varepsilon}_{\mathsf{if}\,B\,\mathsf{then}\,S\,\mathsf{else}\,T}$, $\mathbf{e}^{\rho,\varepsilon}_{B\to S}$, and $\mathbf{e}^{\rho,\varepsilon}_{\mathsf{IF}_{i\in I}(B_i\to S_i)}$ are domain elements. To see that $\mathbf{e}^{\rho,\varepsilon}_{\mathsf{while}\,B\,\mathsf{do}\,S}$ is a domain element we also need **26**(vi). From our assumption that ε maps $\mathscr{Basic}$ to domain elements and the fact that 0 is a domain element it follows that $\varepsilon\left(X_0^{\mathbf{r}^\rho_{\mu X[S]}}\right)$ also maps $\mathscr{Basic}$ to domain elements. From the assumption that (30) is true for S it follows that $\mathbf{e}^{\rho,\varepsilon}\left(X_0^{\mathbf{r}^\rho_{\mu X[S]}}\right)_S$ is a domain element. Consequently, by **52**(i) and **26**(vi), $\mathbf{e}^{\rho,\varepsilon}_{\mu X[S]}$ is a domain element. □

Corollary 54. *Assume* $\mathfrak{A}$ *is a complete relation algebra and* $\rho, \varepsilon : \mathscr{Basic} \to A$. *If* $\langle \mathbf{r}^\rho, \mathbf{e}^{\rho,\varepsilon}\rangle$ *is a correct interpretation, then* $\langle \mathbf{r}^\rho, \mathbf{e}^{\rho,\varepsilon}\rangle$ *is an* $\mathfrak{A}$*-interpretation.*

Proof. This is a consequence of **32**, **53**, and **37**(viii). □

7.3. Semantic equivalence

Much could be said in this section, but we will only make one definition, prove one expected theorem, and give a few examples.

Definition 55. S and T are *semantically equivalent* iff $\mathbf{r}^\rho_S = \mathbf{r}^\rho_T$ and $\mathbf{e}^{\rho,\varepsilon}_S = \mathbf{e}^{\rho,\varepsilon}_T$ for every complete relation algebra $\mathfrak{A}$ and every correct $\mathfrak{A}$-interpretation $\langle \mathbf{r}^\rho, \mathbf{e}^{\rho,\varepsilon}\rangle$.

Theorem 56. *If* $X \notin \mathrm{Free}(S)$, *then* $\mathsf{while}\,B\,\mathsf{do}\,S$ *and* $\mu X\,[\mathsf{if}\,B\,\mathsf{then}\,S;X\,\mathsf{else}\,\mathsf{skip}]$ *are semantically equivalent.*

Proof. Let $\mathfrak{A}$ be a complete relation algebra and let $\langle \mathbf{r}^\rho, \mathbf{e}^{\rho,\varepsilon}\rangle$ be a correct $\mathfrak{A}$-interpretation. Then

$$
\begin{aligned}
&\mathbf{r}^\rho_{\mu X[\mathsf{if}\,B\,\mathsf{then}\,S;X\,\mathsf{else}\,\mathsf{skip}]} \\
&\quad = \prod\left\{ x : x \geqslant \mathbf{r}^\rho\left(X_0^x\right)_{\mathsf{if}\,B\,\mathsf{then}\,S;X\,\mathsf{else}\,\mathsf{skip}} \right\} && \textbf{39} \\
&\quad = \prod\left\{ x : x \geqslant \rho_B;\mathbf{r}^\rho\left(X_0^x\right)_S;\mathbf{r}^\rho\left(X_0^x\right)_X + \overline{\rho_B;1}\cdot\mathbf{r}^\rho\left(X_0^x\right)_{\mathsf{skip}} \right\} && \textbf{39} \\
&\quad = \prod\left\{ x : x \geqslant \rho_B;\mathbf{r}^\rho_S;x + \overline{\rho_B;1}\cdot 1' \right\} && \textbf{39}, \textbf{37}(\mathrm{i}) \\
&\quad = \prod\left\{ x : x \geqslant \overline{\rho_B}\cdot 1' + \rho_B;\mathbf{r}^\rho_S;x \right\} && \textbf{37}(\mathrm{vii}), \textbf{24}(\mathrm{xxxii}) \\
&\quad = \mathbf{r}^\rho_{\mathsf{while}\,B\,\mathsf{do}\,S} && \textbf{39}.
\end{aligned}
$$

and, letting $r = \mathbf{r}^{\rho}_{\mu X[\text{if } B \text{ then } S;X \text{ else skip}]} = \mathbf{r}^{\rho}_{\text{while } B \text{ do } S}$,

$$
\begin{aligned}
&\mathbf{e}^{\rho,\varepsilon}_{\mu X[\text{if } B \text{ then } S;X \text{ else skip}]} \\
&= \sum \left\{ y : y \leqslant \mathbf{e}^{\rho,\varepsilon}\left(X^r_y\right)_{\text{if } B \text{ then } S;X \text{ else skip}} \right\} \\
&\qquad\qquad \mathbf{39} \\
&= \sum \left\{ y : y \leqslant \rho_B ; \mathbf{e}^{\rho,\varepsilon}\left(X^r_y\right)_{S;X} + \overline{\rho_B ; 1} \cdot \mathbf{e}^{\rho,\varepsilon}\left(X^r_y\right)_{\text{skip}} \right\} \\
&\qquad\qquad \mathbf{39} \\
&= \sum \left\{ y : y \leqslant \rho_B ; \left(\mathbf{e}^{\rho,\varepsilon}\left(X^r_y\right)_S + \mathbf{r}^{\rho}\left(X^r_y\right)_S ; \mathbf{e}^{\rho,\varepsilon}\left(X^r_y\right)_X \right) + \overline{\rho_B ; 1} \cdot 0 \right\} \\
&\qquad\qquad \mathbf{39},\ \mathbf{37}(\text{ii}) \\
&= \sum \left\{ y : y \leqslant \rho_B ; \mathbf{e}^{\rho,\varepsilon}\left(X^r_y\right)_S + \rho_B ; \mathbf{r}^{\rho}\left(X^r_y\right)_S ; \mathbf{e}^{\rho,\varepsilon}\left(X^r_y\right)_X \right\} \\
&\qquad\qquad \mathbf{3},\ \mathbf{24}(\text{ix}) \\
&= \sum \left\{ y : y \leqslant \rho_B ; \mathbf{e}^{\rho,\varepsilon}_S + \rho_B ; \mathbf{r}^{\rho}_S ; y \right\} \\
&\qquad\qquad X \notin \text{Free}(S),\ \mathbf{45},\ \mathbf{39} \\
&= \mathbf{e}^{\rho,\varepsilon}_{\text{while } B \text{ do } S} \\
&\qquad\qquad \mathbf{39}. \qquad \square
\end{aligned}
$$

Examples. Let $\mathfrak{A}$ be complete relation algebra and let $\langle \mathbf{r}^{\rho}, \mathbf{e}^{\rho,\varepsilon} \rangle$ be a correct $\mathfrak{A}$-interpretation. Note that

$$
\begin{aligned}
\mathbf{r}^{\rho}_{\mu X[X]} &= \prod \{ x : x \geqslant x \} = 0, \\
\mathbf{e}^{\rho,\varepsilon}_{\mu X[X]} &= \sum \{ y : y \leqslant y \} = 1.
\end{aligned}
$$

Thus, $\mu X[X]$ is semantically equivalent to **havoc**. Assume $X \notin \text{Free}(S)$. Then

$$
\begin{aligned}
\mathbf{r}^{\rho}_{\mu X[X;S]} &= \prod \{ x : x \geqslant x ; \mathbf{r}^{\rho}_S \} = 0, \\
\mathbf{e}^{\rho,\varepsilon}_{\mu X[X;S]} &= \sum \{ y : y \leqslant y + 0 ; \mathbf{e}^{\rho,\varepsilon}_S \} = 1.
\end{aligned}
$$

Thus, $\mu X[X;S]$ is also semantically equivalent to **havoc**. On the other hand, $\mathbf{r}^{\rho}_{\mu X[S;X]}$ is not semantically equivalent to **havoc**, since

$$
\begin{aligned}
\mathbf{r}^{\rho}_{\mu X[S;X]} &= \prod \{ x : x \geqslant \mathbf{r}^{\rho}_S ; x \} = 0, \\
\mathbf{e}^{\rho,\varepsilon}_{\mu X[S;X]} &= \sum \{ y : y \leqslant \mathbf{e}^{\rho,\varepsilon}_S + \mathbf{r}^{\rho}_S ; y \} = \sum \{ y : y \leqslant \mathbf{r}^{\rho}_S ; y \} + \left(\mathbf{r}^{\rho}_S\right)^{\omega} ; \mathbf{e}^{\rho,\varepsilon}_S.
\end{aligned}
$$

by **31**(ii) and **30**(i). Thus, in case $\mathfrak{A} = \mathfrak{Re}(U)$, the domain of nontermination of $\mathbf{r}^{\rho}_{\mu X[S;X]}$ is the set of states that belong to infinite $\mathbf{r}^{\rho}_S$-chains or initiate finite $\mathbf{r}^{\rho}_S$-chains that end at a state in the domain of nontermination of S.

Suppose there is a basic statement **true** such that $\rho_{\text{true}} = 1'$ ("**true** is true in all states"). Then **while true do skip** is semantically equivalent to **abort**, since

$$
\begin{aligned}
\mathbf{r}^{\rho}_{\text{while true do skip}} &= \prod \left\{ x : x \geqslant \overline{\rho_{\text{true}}} \cdot 1' + \rho_{\text{true}} ; \mathbf{r}^{\rho}_{\text{skip}} ; x \right\} = \prod \{ x : x \geqslant x \} = 0, \\
\mathbf{e}^{\rho,\varepsilon}_{\text{while true do skip}} &= \sum \left\{ y : y \leqslant \rho_{\text{true}} ; \mathbf{e}^{\rho,\varepsilon}_{\text{skip}} + \rho_{\text{true}} ; \mathbf{r}^{\rho}_{\text{skip}} ; y \right\} = \sum \{ y : y \leqslant y \} = 1.
\end{aligned}
$$

Consider a somewhat less trivial example [7, p. 858]. Suppose we have a language with exactly one integer variable. Machine states can be identified with integer assignments to that variable, so we simply let the set of machine states be $\mathbb{Z} = \{\ldots,-3,-2,-1,0,1,2,3,\ldots\}$. Let S be an assignment statement that always terminates and sets the variable equal to 0: $\mathbf{r}_S^\rho = \{\langle n,0\rangle : n \in \mathbb{Z}\}$ and $\mathbf{e}_S^{\rho,\varepsilon} = 0$. Let B be a Boolean statement that says "the value of the variable is nonzero": $\rho_B = \{\langle n,n\rangle : 0 \neq n \in \mathbb{Z}\}$. Let P be the statement that always terminates and subtracts 1 from the value assigned to the variable: $\mathbf{r}_P^\rho = \{\langle n,n-1\rangle : n \in \mathbb{Z}\}$ and $\mathbf{e}_P^{\rho,\varepsilon} = 0$. Then S and $\mathsf{havoc};\mathsf{while}\,B\,\mathsf{do}\,P$ have the same input/output relation, since

$$
\begin{aligned}
&\mathbf{r}^\rho_{\mathsf{havoc};\mathsf{while}\,B\,\mathsf{do}\,P}\\
&\quad = 1;\prod\{x : x \geqslant \overline{\rho_B}\cdot 1' + \rho_B;\mathbf{r}_P^\rho;x\}\\
&\quad = 1;\prod\Big\{x : x \geqslant \overline{\{\langle n,n\rangle : 0 \neq n \in \mathbb{Z}\}}\cdot 1'\\
&\qquad + \{\langle n,n\rangle : 0 \neq n \in \mathbb{Z}\};\{\langle n,n-1\rangle : n \in \mathbb{Z}\};x\Big\}\\
&\quad = 1;\prod\{x : x \geqslant \{\langle 0,0\rangle\} + \{\langle n,n-1\rangle : 0 \neq n \in \mathbb{Z}\};x\}\\
&\quad = 1;(\{\langle n,n-1\rangle : 0 \neq n \in \mathbb{Z}\})^\omega;\{\langle 0,0\rangle\}\\
&\quad = \{\langle n,0\rangle : n \in \mathbb{Z}\}\\
&\quad = \mathbf{r}_S^\rho,
\end{aligned}
$$

but they are not semantically equivalent since

$$
\begin{aligned}
\mathbf{e}^{\rho,\varepsilon}_{\mathsf{havoc};\mathsf{while}\,B\,\mathsf{do}\,P} &= \mathbf{e}^{\rho,\varepsilon}_{\mathsf{havoc}} + \mathbf{r}^\rho_{\mathsf{havoc}};\sum\{y : y \leqslant \rho_B;\mathbf{e}_P^{\rho,\varepsilon} + \rho_B;\mathbf{r}_P^\rho;y\}\\
&= 0 + 1;\sum\{y : y \leqslant \{\langle n,n\rangle : 0 \neq n \in \mathbb{Z}\};0\\
&\qquad + \{\langle n,n\rangle : 0 \neq n \in \mathbb{Z}\};\{\langle n,n-1\rangle : n \in \mathbb{Z}\};y\}\\
&= 1;\sum\{y : y \leqslant \{\langle n,n-1\rangle : 0 \neq n \in \mathbb{Z}\};y\}\\
&= 1 \neq 0 = \mathbf{e}_S^{\rho,\varepsilon}.
\end{aligned}
$$

7.4. Laws of predicate transformers for correct interpretations

In this section we show that the weakest-precondition predicate transformer $\mathrm{wp}_{(\cdot)}(\cdot)$ and the weakest-liberal-precondition predicate transformer $\mathrm{wlp}_{(\cdot)}(\cdot)$ associated with a correct intepretation obey all the standard laws, except for the "law of the excluded miracle". Suppose $\mathfrak{A}$ is a complete relation algebra and $\langle \mathbf{r}^\rho, \mathbf{e}^{\rho,\varepsilon}\rangle$ is a correct interpretation. Then for every statement $S \in \mathscr{S}tat$, $\mathrm{wlp}_S(\cdot)$ and $\mathrm{wp}_S(\cdot)$ are functions that map the complete Boolean algebra of domain elements to itself (by **54**). The functions therefore transform (denotations of) predicates to (denotations of) predicates, and hence are properly called "predicate transformers". Theorem **57** below is almost enough to show

that $\mathrm{wlp}_{(\cdot)}(\cdot)$ and $\mathrm{wp}_{(\cdot)}(\cdot)$ qualify as predicate transformer semantics according to the requirements of [15]. First, the requirement R0, p. 132, that $\mathrm{wlp}_S(\cdot)$ be universally multiplicative (which also appears as (0), p. 129), holds by **34**(xi). Note that correctness of the interpretation is not needed for R0. Definitions (10)–(18), pp. 133–136, that specify $\mathrm{wlp}_S(\cdot)$ and $\mathrm{wp}_S(\cdot)$ in case S is **havoc**, **abort**, or **skip**, hold by **57**(i)–**57**(vii). Definitions (23)–(25), p. 137, that specify the predicate transformers for the composition of statements, hold by **57**(viii)(ix). Definitions (27)–(29), p. 137, for guarded nondeterministic choice, hold by **57**(xviii)(xix). Finally, Definitions (1)–(2), p. 171, for the `while`-statement, hold by **57**(xxii)(xxv). However, we do not know, and cannot prove, that every statement S satisfies the "law of the excluded miracle". This "law" is treated in the next section.

Theorem 57. *Assume* $\mathfrak{A}$ *is a complete relation algebra,* $\rho, \varepsilon : \mathscr{B}asic \to A$, *and* $\langle \mathbf{r}^\rho, \mathbf{e}^{\rho,\varepsilon} \rangle$ *is a correct* $\mathfrak{A}$*-interpretation. Then*

(i) $\mathrm{wlp}_{\mathsf{skip}}(x) = x.$

(ii) $\mathrm{wp}_{\mathsf{skip}}(x) = x.$

(iii) $\mathrm{wlp}_{\mathsf{abort}}(x) = 1.$

(iv) $\mathrm{wp}_{\mathsf{abort}}(x) = 0.$

(v) $\mathrm{wlp}_{\mathsf{havoc}}(x) = 0 \dagger x.$

(vi) $\mathrm{wp}_{\mathsf{havoc}}(x) = 0 \dagger x.$

(vii) $\mathrm{wp}_{\mathsf{havoc}}(1) = 1.$

(viii) $\mathrm{wlp}_{S;T}(x) = \mathrm{wlp}_S(\mathrm{wlp}_T(x)).$

(ix) $\mathrm{wp}_{S;T}(x) = \mathrm{wp}_S(\mathrm{wp}_T(x)).$

(x) $\mathrm{wlp}_{S \text{ or } T}(x) = \mathrm{wlp}_S(x) \cdot \mathrm{wlp}_T(x).$

(xi) $\mathrm{wp}_{S \text{ or } T}(x) = \mathrm{wp}_S(x) \cdot \mathrm{wp}_T(x).$

(xii) $\mathrm{wlp}_{\mathsf{OR}_{i\in I} S_i}(x) = \prod_{i\in I} \mathrm{wlp}_{S_i}(x).$

(xiii) $\mathrm{wp}_{\mathsf{OR}_{i\in I} S_i}(x) = \prod_{i\in I} \mathrm{wp}_{S_i}(x).$

(xiv) $\mathrm{wlp}_{\mathsf{if}\ B\ \mathsf{then}\ S\ \mathsf{else}\ T}(x) = \rho_B;\mathrm{wlp}_S(x) + \overline{\rho_B;1} \cdot \mathrm{wlp}_T(x).$

(xv) $\mathrm{wp}_{\mathsf{if}\ B\ \mathsf{then}\ S\ \mathsf{else}\ T}(x) = \rho_B;\mathrm{wp}_S(x) + \overline{\rho_B;1} \cdot \mathrm{wp}_T(x).$

(xvi) $\mathrm{wlp}_{B\to S}(x) = \overline{\rho_B;1} + \mathrm{wlp}_S(x).$

(xvii) $\mathrm{wp}_{B\to S}(x) = \rho_B;\mathrm{wp}_S(x).$

(xviii) $\mathrm{wlp}_{\mathsf{IF}_{i\in I}(B_i\to S_i)}(x) = \prod_{i\in I}\left(\overline{\rho_{B_i};1} + \mathrm{wlp}_{S_i}(x)\right).$

(xix) $\mathrm{wp}_{\mathsf{IF}_{i\in I}(B_i\to S_i)}(x) = \prod_{i\in I}\left(\overline{\rho_{B_i};1} + \mathrm{wp}_{S_i}(x)\right) \cdot \sum_{i\in I}(\rho_{B_i};1).$

(xx) $(\mathrm{wlp}_S)^i(x) = \overline{(\mathbf{r}_S^\rho)^i};\bar{x}$ *for every* $i \in \omega$.

(xxi) $\mathrm{wlp}_{\mathsf{while}\ B\ \mathsf{do}\ S}(x) = \prod_{i\in\omega}(\mathrm{wlp}_{B\to S})^i(\rho_B;1+x).$

(xxii) $\mathrm{wlp}_{\mathsf{while}\ B\ \mathsf{do}\ S}(x) = \sum\{\, y : y \leqslant (\rho_B;1+x) \cdot (\overline{\rho_B;1} + \mathrm{wlp}_S(y)) \,\}.$

(xxiii) $\mathrm{wlp}_{\mathsf{while}\ B\ \mathsf{do}\ S}(x) = \sum\{\, y : y \leqslant (\rho_B;1+x) \cdot \mathrm{wlp}_{B\to S}(y) \,\}.$

(xxiv) $\mathrm{wlp}_{\mathsf{while}\ B\ \mathsf{do}\ S}(x) = \sum\{\, y : y \leqslant \overline{\rho_B;1} \cdot x + \rho_B;\mathrm{wlp}_S(y) \,\}.$

(xxv) $\mathrm{wp}_{\mathsf{while}\ B\ \mathsf{do}\ S}(x) = \prod\{\, y : y \geqslant (\rho_B;1+x) \cdot (\overline{\rho_B;1} + \mathrm{wp}_S(y)) \,\}.$

(xxvi) $\mathrm{wp}_{\mathsf{while}\ B\ \mathsf{do}\ S}(x) = \prod\{\, y : y \geqslant \overline{\rho_B;1} \cdot x + \rho_B;\mathrm{wp}_S(y) \,\}.$

Proof. **57**(i): $\mathrm{wlp}_{\mathsf{skip}}(x) = \overline{\mathbf{r}^{\rho}_{\mathsf{skip}};\bar{x}} = \overline{1';\bar{x}} = \bar{\bar{x}} = x$, by **33**(i), **37**(i), **39**, **24**(xix), and **3**(ii).

57(ii): $\mathrm{wp}_{\mathsf{skip}}(x) = \mathrm{wlp}_{\mathsf{skip}}(x)\cdot\overline{\mathbf{e}^{\rho,\varepsilon}_{\mathsf{skip}}} = x\cdot\bar{0} = x$, by **34**(ii), **37**(ii), **39**, and **5**(iv)(viii).

57(iii): $\mathrm{wlp}_{\mathsf{abort}}(x) = \overline{\mathbf{r}^{\rho}_{\mathsf{abort}};\bar{x}} = \overline{0;\bar{x}} = \bar{0} = 1$, by **33**(i), **37**(iii), **39**, **24**(xviii), and **5**(iv).

57(iv): $\mathrm{wp}_{\mathsf{abort}}(x) = \mathrm{wlp}_{\mathsf{abort}}(x)\cdot\overline{\mathbf{e}^{\rho,\varepsilon}_{\mathsf{abort}}} = \mathrm{wlp}_{\mathsf{abort}}(x)\cdot\bar{1} = 0$, by **34**(ii), **37**(iv), **39**, and **5**(iii)(vi).

57(v):
$$\begin{aligned}
\mathrm{wlp}_{\mathsf{havoc}}(x) &= \overline{\mathbf{r}^{\rho}_{\mathsf{havoc}};\bar{x}} && \textbf{33}(\mathrm{i})\\
&= \overline{1;\bar{x}} && \textbf{37}(\mathrm{v}),\ \textbf{39}\\
&= 0\dagger x && \textbf{5}(\mathrm{iv}),\ (\mathrm{Ra}_8).
\end{aligned}$$

57(vi):
$$\begin{aligned}
\mathrm{wp}_{\mathsf{havoc}}(x) &= \mathrm{wlp}_{\mathsf{havoc}}(x)\cdot\overline{\mathbf{e}^{\rho,\varepsilon}_{\mathsf{havoc}}} && \textbf{34}(\mathrm{ii})\\
&= 0\dagger x\cdot\bar{0} && \textbf{57}(\mathrm{i}),\ \textbf{37}(\mathrm{vi}),\ \textbf{39}\\
&= 0\dagger x && \textbf{5}(\mathrm{iv})(\mathrm{viii}).
\end{aligned}$$

57(vii):
$$\begin{aligned}
\mathrm{wp}_{\mathsf{havoc}}(1) &= 0\dagger 1 && \textbf{57}(\mathrm{vi})\\
&= \bar{\bar{0}};\bar{\bar{1}} && (\mathrm{Ra}_8)\\
&= \bar{\bar{0}};0 && \textbf{5}(\mathrm{iii})\\
&= \bar{0} && \textbf{24}(\mathrm{xviii})\\
&= 1 && \textbf{5}(\mathrm{iv}).
\end{aligned}$$

57(viii):
$$\begin{aligned}
\mathrm{wlp}_{S;T}(x) &= \overline{\mathbf{r}^{\rho}_{S;T};\bar{x}} && \textbf{33}(\mathrm{i})\\
&= \overline{(\mathbf{r}^{\rho}_{S};\mathbf{r}^{\rho}_{T});\bar{x}} && \textbf{39}\\
&= \overline{\mathbf{r}^{\rho}_{S};(\mathbf{r}^{\rho}_{T};\bar{x})} && (\mathrm{Ra}_1)\\
&= \overline{\mathbf{r}^{\rho}_{S};\bar{\bar{\mathbf{r}}}^{\rho}_{T};\bar{x}} && \textbf{3}(\mathrm{ii})\\
&= \overline{\mathbf{r}^{\rho}_{S};\overline{\mathrm{wlp}_{T}(x)}} && \textbf{33}(\mathrm{i})\\
&= \mathrm{wlp}_{S}(\mathrm{wlp}_{T}(x)) && \textbf{33}(\mathrm{i}).
\end{aligned}$$

57(ix):
$$\begin{aligned}
\mathrm{wp}_{S;T}(x) &= \mathrm{wlp}_{S;T}(x)\cdot\overline{\mathbf{e}^{\rho,\varepsilon}_{S;T}} && \textbf{34}(\mathrm{ii})\\
&= \mathrm{wlp}_{S}(\mathrm{wlp}_{T}(x))\cdot\overline{\mathbf{e}^{\rho,\varepsilon}_{S;T}} && \textbf{57}(\mathrm{viii})\\
&= \mathrm{wlp}_{S}(\mathrm{wlp}_{T}(x))\cdot\overline{\mathbf{e}^{\rho,\varepsilon}_{S}+\mathbf{r}^{\rho}_{S};\mathbf{e}^{\rho,\varepsilon}_{T}} && \textbf{39}\\
&= \mathrm{wlp}_{S}(\mathrm{wlp}_{T}(x))\cdot\overline{\mathbf{e}^{\rho,\varepsilon}_{S}}\cdot\overline{\mathbf{r}^{\rho}_{S};\mathbf{e}^{\rho,\varepsilon}_{T}} && \textbf{3}(\mathrm{xvi})\\
&= \mathrm{wlp}_{S}(\mathrm{wlp}_{T}(x))\cdot\mathbf{r}^{\rho}_{S};\bar{\bar{\mathbf{e}}}^{\rho,\varepsilon}_{T}\cdot\overline{\mathbf{e}^{\rho,\varepsilon}_{S}} && \textbf{3}(\mathrm{ii})(\mathrm{viii})(\mathrm{ix})\\
&= \mathrm{wlp}_{S}(\mathrm{wlp}_{T}(x))\cdot\mathrm{wlp}_{S}\left(\overline{\mathbf{e}^{\rho,\varepsilon}_{T}}\right)\cdot\overline{\mathbf{e}^{\rho,\varepsilon}_{S}} && \textbf{33}(\mathrm{i})\\
&= \mathrm{wlp}_{S}\left(\mathrm{wlp}_{T}(x)\cdot\overline{\mathbf{e}^{\rho,\varepsilon}_{T}}\right)\cdot\overline{\mathbf{e}^{\rho,\varepsilon}_{S}} && \textbf{34}(\mathrm{xiv})\\
&= \mathrm{wp}_{S}(\mathrm{wp}_{T}(x)) && \textbf{34}(\mathrm{ii}).
\end{aligned}$$

57(xxv) and **57**(xxvi):

$$
\begin{aligned}
&\mathrm{wp}_{\text{while } B \text{ do } S}(x)\\
&= \mathrm{wlp}_{\text{while } B \text{ do } S}(x) \cdot \overline{\mathbf{e}^{\rho,\varepsilon}_{\text{while } B \text{ do } S}}\\
&\qquad\qquad \mathbf{34}(\mathrm{ii})\\
&= \sum \left\{ y : y \leqslant (\rho_B;1+x) \cdot \overline{\rho_B;\mathbf{r}^{\rho}_S;\overline{y}} \right\} \cdot \overline{\sum \left\{ y : y \leqslant \rho_B;\mathbf{e}^{\rho,\varepsilon}_S + \rho_B;\mathbf{r}^{\rho}_S;y \right\}}\\
&\qquad\qquad (31),\ \mathbf{39}\\
&= \sum \left\{ y : y \leqslant (\rho_B;1+x) \cdot \overline{\rho_B;\mathbf{r}^{\rho}_S;\overline{y}} \right\} \cdot \prod \left\{ y : y \geqslant \overline{\rho_B;\mathbf{e}^{\rho,\varepsilon}_S} \cdot \overline{\rho_B;\mathbf{r}^{\rho}_S;\overline{y}} \right\}\\
&\qquad\qquad \mathbf{8}(\mathrm{ii}),\mathbf{3}(\mathrm{ii})(\mathrm{xvi})(\mathrm{xvii}),\mathbf{37}(\mathrm{v})\\
&= \prod \left\{ y : y \geqslant (\rho_B;1+x) \cdot \overline{\rho_B;\mathbf{e}^{\rho,\varepsilon}_S} \cdot \overline{\rho_B;\mathbf{r}^{\rho}_S;\overline{y}} \right\}\\
&\qquad\qquad \mathbf{31}(\mathrm{iii}),\mathbf{3}(\mathrm{viii})\\
&= \prod \left\{ y : y \geqslant (\rho_B;1+x) \cdot \overline{\rho_B;\mathbf{e}^{\rho,\varepsilon}_S + \rho_B;\mathbf{r}^{\rho}_S;\overline{y}} \right\}\\
&\qquad\qquad \mathbf{3}(\mathrm{xvi})\\
&= \prod \left\{ y : y \geqslant (\rho_B;1+x) \cdot \overline{\rho_B;\left(\mathbf{e}^{\rho,\varepsilon}_S + \mathbf{r}^{\rho}_S;\overline{y}\right)} \right\}\\
&\qquad\qquad \mathbf{24}(\mathrm{ix})\\
&= \prod \left\{ y : y \geqslant (\rho_B;1+x) \cdot \overline{\rho_B;1 \cdot \left(\mathbf{e}^{\rho,\varepsilon}_S + \mathbf{r}^{\rho}_S;\overline{y}\right)} \right\}\\
&\qquad\qquad \mathbf{37}(\mathrm{vii}),\mathbf{24}(\mathrm{xxviii})\\
&= \prod \left\{ y : y \geqslant (\rho_B;1+x) \cdot \left(\overline{\rho_B;1} + \overline{\mathbf{e}^{\rho,\varepsilon}_S} \cdot \overline{\mathbf{r}^{\rho}_S;\overline{y}}\right) \right\}\\
&\qquad\qquad \mathbf{3}(\mathrm{xvi})(\mathrm{xvii})\\
&= \prod \left\{ y : y \geqslant (\rho_B;1+x) \cdot \left(\overline{\rho_B;1} + \mathrm{wp}_S(y)\right) \right\}\\
&\qquad\qquad \mathbf{33}(\mathrm{ii}),\mathbf{3}(\mathrm{viii})\\
&= \prod \left\{ y : y \geqslant \overline{\rho_B;1} \cdot x + \rho_B;1 \cdot \mathrm{wp}_S(y) \right\}\\
&\qquad\qquad \mathbf{3}(\mathrm{xix})\\
&= \prod \left\{ y : y \geqslant \overline{\rho_B;1} \cdot x + \rho_B;\mathrm{wp}_S(y) \right\}\\
&\qquad\qquad \mathbf{37}(\mathrm{vii}),\mathbf{24}(\mathrm{xxxi}). \quad \square
\end{aligned}
$$

7.5. The "law of the excluded miracle"

Let $\mathfrak{A}$ be a complete relation algebra. Consider an arbitrary $\mathfrak{A}$-interpretation $\langle \mathrm{r}, \mathrm{e} \rangle$. We say that a statement S satisfies the "law of the excluded miracle" (so called by Dijkstra) if $\mathrm{wp}_S(0) = 0$. Equivalent forms of this "law" are $\mathrm{r}_S;1+\mathrm{e}_S = 1$ and $\overline{\mathrm{r}_S;1} \leqslant \mathrm{e}_S$.

Definition 58. An interpretation is *miracle-free* if $\mathrm{wp}_S(0) = 0$ for every $S \in \mathscr{S}tat$.

Interpretations (even correct ones) may not be miracle-free simply because some basic statements fail to obey the "law". For example, the results in this paper apply to correct interpretations in which, for every assignment statement S, $\mathbf{r}^{\rho}_S = \mathbf{e}^{\rho,\varepsilon}_S = 0$ (S has no

57(xv): $\mathrm{wp}_{\text{if } B \text{ then } S \text{ else } T}(x)$

$= \mathrm{wlp}_{\text{if } B \text{ then } S \text{ else } T}(x) \cdot \overline{\mathbf{e}^{\rho,\varepsilon}_{\text{if } B \text{ then } S \text{ else } T}}$ **34**(ii)

$= \left(\rho_B;\mathrm{wlp}_S(x) + \overline{\rho_B;1} \cdot \mathrm{wlp}_T(x)\right) \cdot \overline{\rho_B;\mathbf{e}^{\rho,\varepsilon}_S + \overline{\rho_B;1} \cdot \mathbf{e}^{\rho,\varepsilon}_T}$ **57**(xiv), **39**

$= \left(\rho_B;1 \cdot \mathrm{wlp}_S(x) + \overline{\rho_B;1} \cdot \mathrm{wlp}_T(x)\right) \cdot \overline{\rho_B;1 \cdot \mathbf{e}^{\rho,\varepsilon}_S + \overline{\rho_B;1} \cdot \mathbf{e}^{\rho,\varepsilon}_T}$ **37**(vii), **24**(xxxi)

$= \rho_B;1 \cdot \mathrm{wlp}_S(x) \cdot \overline{\mathbf{e}^{\rho,\varepsilon}_S} + \overline{\rho_B;1} \cdot \left(\mathrm{wlp}_T(x) \cdot \overline{\mathbf{e}^{\rho,\varepsilon}_T}\right)$ **3**(xx)(ix)

$= \rho_B;1 \cdot \mathrm{wp}_S(x) + \overline{\rho_B;1} \cdot \mathrm{wp}_T(x)$ **34**(ii)

$= \rho_B;\mathrm{wp}_S(x) + \overline{\rho_B;1} \cdot \mathrm{wp}_T(x)$ **37**(vii), **24**(xxxi).

57(xvi): $\mathrm{wlp}_{B\to S}(x)$

$= \overline{\mathbf{r}^{\rho}_{B\to S};\bar{x}}$ **33**(i)

$= \overline{\rho_B;\mathbf{r}^{\rho}_S;\bar{x}}$ **39**

$= \overline{\rho_B;1 \cdot \mathbf{r}^{\rho}_S;\bar{x}}$ **37**(vii), **24**(xxxi)

$= \overline{\rho_B;1} + \mathbf{r}^{\rho}_S;\bar{x}$ **3**(xvii)

$= \overline{\rho_B;1} + \mathrm{wlp}_S(x)$ **33**(i).

57(xvii): $\mathrm{wp}_{B\to S}(x)$

$= \mathrm{wlp}_{B\to S}(x) \cdot \overline{\mathbf{e}^{\rho,\varepsilon}_{B\to S}}$ **34**(ii)

$= \left(\overline{\rho_B;1} + \mathrm{wlp}_S(x)\right) \cdot \left(\overline{\overline{\rho_B;1} + \mathbf{e}^{\rho,\varepsilon}_S}\right)$ **57**(xvi), **39**

$= \left(\overline{\rho_B;1} + \mathrm{wlp}_S(x)\right) \cdot \left(\rho_B;1 \cdot \overline{\mathbf{e}^{\rho,\varepsilon}_S}\right)$ **3**(ii)(xvi)

$= \rho_B;1 \cdot \mathrm{wlp}_S(x) \cdot \overline{\mathbf{e}^{\rho,\varepsilon}_S}$ **3**(ii)(viii)(ix)(xiii)

$= \rho_B;\mathrm{wp}_S(x)$ **37**(vii), **24**(xxxi), **34**(ii).

57(xviii): $\mathrm{wlp}_{\mathsf{IF}_{i\in I}(B_i\to S_i)}(x)$

$= \overline{\mathbf{r}^{\rho}_{\mathsf{IF}_{i\in I}(B_i\to S_i)};\bar{x}}$ **33**(i)

$= \overline{\sum_{i\in I}\left(\rho_{B_i};\mathbf{r}^{\rho}_{S_i}\right);\bar{x}}$ **39**

$= \overline{\sum_{i\in I}\left(\rho_{B_i};\mathbf{r}^{\rho}_{S_i};\bar{x}\right)}$ **24**(xv)

$= \overline{\sum_{i\in I}\left(\rho_{B_i};1 \cdot \mathbf{r}^{\rho}_{S_i};\bar{x}\right)}$ **37**(vii), **24**(xxxi)

$= \prod_{i\in I}\left(\overline{\rho_{B_i};1} + \overline{\mathbf{r}^{\rho}_{S_i};\bar{x}}\right)$ **8**(ii), **3**(xvii)

$= \prod_{i\in I}\left(\overline{\rho_{B_i};1} + \mathrm{wlp}_{S_i}(x)\right)$ **33**(i).

57(xix): $\mathrm{wp}_{\mathsf{IF}_{i\in I}(B_i\to S_i)}(x)$

$$= \mathrm{wlp}_{\mathsf{IF}_{i\in I}(B_i\to S_i)}(x)\cdot \overline{\mathbf{e}^{\rho,\varepsilon}_{\mathsf{IF}_{i\in I}(B_i\to S_i)}}$$

34(ii)

$$= \prod_{i\in I}\left(\overline{\rho_{B_i};1} + \mathrm{wlp}_{S_i}(x)\right)\cdot \overline{\prod_{i\in I}\overline{\rho_{B_i};1} + \sum_{i\in I}\left(\rho_{B_i};1\cdot \mathbf{e}^{\rho,\varepsilon}_{S_i}\right)}$$

57(xviii), **39**, **37**(vii), **24**(xxxi)

$$= \prod_{i\in I}\left(\overline{\rho_{B_i};1} + \mathrm{wlp}_{S_i}(x)\right)\cdot \left(\sum_{i\in I}(\rho_{B_i};1)\cdot \prod_{i\in I}\left(\overline{\rho_{B_i};1} + \overline{\mathbf{e}^{\rho,\varepsilon}_{S_i}}\right)\right)$$

3(ii)(xvi)(xvii), **8**(ii)(iii)

$$= \prod_{i\in I}\left(\left(\overline{\rho_{B_i};1} + \mathrm{wlp}_{S_i}(x)\right)\cdot \left(\overline{\rho_{B_i};1} + \overline{\mathbf{e}^{\rho,\varepsilon}_{S_i}}\right)\right)\cdot \sum_{i\in I}(\rho_{B_i};1)$$

3(viii)(ix), **9**(ii)

$$= \prod_{i\in I}\left(\overline{\rho_{B_i};1} + \mathrm{wlp}_{S_i}(x)\cdot \overline{\mathbf{e}^{\rho,\varepsilon}_{S_i}}\right)\cdot \sum_{i\in I}(\rho_{B_i};1)$$

3(xviii)

$$= \prod_{i\in I}\left(\overline{\rho_{B_i};1} + \mathrm{wp}_{S_i}(x)\right)\cdot \sum_{i\in I}(\rho_{B_i};1)$$

34(ii).

57(xx): We prove this by induction. First note that $(\mathrm{wlp}_S)^0(x) = x = \overline{1';\bar{x}} = \overline{(\mathbf{r}^\rho_S)^0;\bar{x}}$ by **20**, **3**(ii), **24**(xix), and **29**. Next, assume that $(\mathrm{wlp}_S)^i(x) = \overline{(\mathbf{r}^\rho_S)^i;\bar{x}}$. Then we have

$$\begin{aligned}
(\mathrm{wlp}_S)^{i+1}(x) &= \mathrm{wlp}_S\left((\mathrm{wlp}_S)^i(x)\right) && \textbf{20}\\
&= \mathrm{wlp}_S\left(\overline{(\mathbf{r}^\rho_S)^i;\bar{x}}\right) && \text{induction hypothesis}\\
&= \overline{\overline{\mathbf{r}^\rho_S;(\mathbf{r}^\rho_S)^i};\bar{x}} && \textbf{33}(\mathrm{i})\\
&= \overline{\mathbf{r}^\rho_S;\left(\overline{(\mathbf{r}^\rho_S)^i;\bar{x}}\right)} && \textbf{3}(\mathrm{ii})\\
&= \overline{\mathbf{r}^\rho_S;(\mathbf{r}^\rho_S)^i;\bar{x}} && (\mathrm{Ra}_1)\\
&= \overline{(\mathbf{r}^\rho_S)^{i+1};\bar{x}} && \textbf{29}.
\end{aligned}$$

57(xxi)-**57**(xxiv): First we prove

$$\mathrm{wlp}_{\mathsf{while}\,B\,\mathsf{do}\,S}(x) = \sum\left\{\, y : y \leqslant (\rho_B;1+x)\cdot \overline{\rho_B;\mathbf{r}^\rho_S;\bar{y}}\,\right\} \tag{31}$$

Applying the hypothesis of (32) to these altered maps, we conclude that

$$\overline{\mathbf{r}^{\rho}\left(X^{r}_{\overline{r;1}}\right)_S;1} \leqslant \mathbf{e}^{\rho,\varepsilon}\left(X^{r}_{\overline{r;1}}\right)_S.$$

Combining this with (33) yields

$$\overline{r;1} \leqslant \mathbf{e}^{\rho,\varepsilon}\left(X^{r}_{\overline{r;1}}\right)_S.$$

By **39**, **46**, and **22**, $\mathbf{e}^{\rho,\varepsilon}_{\mu X[S]}$ is the greatest element y of A such that

$$y \leqslant \mathbf{e}^{\rho,\varepsilon}\left(X^{r}_{y}\right)_S.$$

We have just seen that $\overline{r;1}$ is itself such an element, so it follows that

$$\overline{r;1} \leqslant \mathbf{e}^{\rho,\varepsilon}_{\mu X[S]}.$$

as desired. □

7.6. Determinism for correct interpretations

From their operational interpretation it is natural to expect that **skip** and **abort** would be deterministic under a correct interpretation. It is also natural to say that **havoc** is not deterministic, since, in the operational interpretation, a computation of **havoc** can start at any machine state and end at any other. However, even under the operational interpretation there is one case in which **havoc** really *is* deterministic, namely, when there is only one machine state. An obviously sufficient (but not necessary) condition for $S;T$ to be deterministic is that S and T are deterministic. These ideas are included in various parts of the following theorem.

Theorem 61. *Suppose* $\mathfrak{A}$ *is a complete relation algebra and* $\langle \mathbf{r}^{\rho}, \mathbf{e}^{\rho,\varepsilon}\rangle$ *is a correct* $\mathfrak{A}$*-interpretation.*

(i) **skip** *and* **abort** *are deterministic.*

(ii) **havoc** *is deterministic iff* $1' = 1$, i.e., $\mathfrak{A}$ *is a Boolean relation algebra.*

(iii) *If* S *and* T *are deterministic, then so is* $S;T$.

(iv) S **or** T *is deterministic iff* S *and* T *are deterministic,* $(\mathbf{r}^{\rho}_S)^{\smile};\ \mathbf{r}^{\rho}_T \leqslant 1'$, *and* $\mathbf{r}^{\rho}_S \cdot \mathbf{e}^{\rho,\varepsilon}_T + \mathbf{r}^{\rho}_T \cdot \mathbf{e}^{\rho,\varepsilon}_S = 0$.

(v) $\mathbf{OR}_{i\in I}S_i$ *is deterministic iff* $(\mathbf{r}^{\rho}_S)^{\smile};\mathbf{r}^{\rho}_{S_j} \leqslant 1'$ *and* $\mathbf{r}^{\rho}_{S_i} \cdot \mathbf{e}^{\rho,\varepsilon}_{S_j} = 0$ *for all* $i,j \in S$.

(vi) *If* S *and* T *are deterministic, then so is* **if** B **then** S **else** T.

(vii) *If* S *is deterministic then so is* $B \to S$.

(viii) *If* S_i *is deterministic for every* $i \in I$ *and* $\rho_{B_i} \cdot \rho_{B_j} = 0$ *whenever* $i \neq j$ *and* $i,j \in I$, *then* $\mathbf{IF}_{i\in I}(B_i \to S_i)$ *is deterministic.*

(ix) *If* S *is deterministic, then so is* **while** B **do** S.

57(x): $\mathrm{wlp}_{S \text{ or } T}(x) = \overline{\mathbf{r}^{\rho}_{S \text{ or } T}; \bar{x}}$ **33**(i)
$= \overline{(\mathbf{r}^{\rho}_{S} + \mathbf{r}^{\rho}_{T}); \bar{x}}$ **39**
$= \overline{\mathbf{r}^{\rho}_{S}; \bar{x} + \mathbf{r}^{\rho}_{T}; \bar{x}}$ (Ra_2)
$= \overline{\mathbf{r}^{\rho}_{S}; \bar{x}} \cdot \overline{\mathbf{r}^{\rho}_{T}; \bar{x}}$ **3**(xvi)
$= \mathrm{wlp}_S(x) \cdot \mathrm{wlp}_T(x)$ **33**(i).

57(xi): $\mathrm{wp}_{S \text{ or } T}(x) = \mathrm{wlp}_{S \text{ or } T}(x) \cdot \overline{\mathbf{e}^{\rho,\varepsilon}_{S \text{ or } T}}$ **34**(ii)
$= (\mathrm{wlp}_S(x) \cdot \mathrm{wlp}_T(x)) \cdot \overline{\mathbf{e}^{\rho,\varepsilon}_{S \text{ or } T}}$ **57**(x)
$= (\mathrm{wlp}_S(x) \cdot \mathrm{wlp}_T(x)) \cdot \overline{\mathbf{e}^{\rho,\varepsilon}_{S} + \mathbf{e}^{\rho,\varepsilon}_{T}}$ **39**
$= \mathrm{wlp}_S(x) \cdot \overline{\mathbf{e}^{\rho,\varepsilon}_{S}} \cdot \left(\mathrm{wlp}_T(x) \cdot \overline{\mathbf{e}^{\rho,\varepsilon}_{T}}\right)$ **3**(viii)(ix)(xvi)
$= \mathrm{wp}_S(x) \cdot \mathrm{wp}_T(x)$ **34**(ii).

57(xii): $\mathrm{wlp}_{\mathsf{OR}_{i\in I} S_i}(x) = \overline{\mathbf{r}^{\rho}_{\mathsf{OR}_{i\in I} S_i}; \bar{x}}$ **33**(i)
$= \overline{\sum_{i\in I} \mathbf{r}^{\rho}_{S_i}; \bar{x}}$ **39**
$= \overline{\sum_{i\in I} (\mathbf{r}^{\rho}_{S_i}; \bar{x})}$ **24**(xv)
$= \prod_{i\in I} \overline{\mathbf{r}^{\rho}_{S_i}; \bar{x}}$ **8**(ii)
$= \prod_{i\in I} \mathrm{wlp}_{S_i}(x)$ **33**(i).

57(xiii): $\mathrm{wp}_{\mathsf{OR}_{i\in I} S_i}(x)$
$= \mathrm{wlp}_{\mathsf{OR}_{i\in I} S_i}(x) \cdot \overline{\mathbf{e}^{\rho,\varepsilon}_{\mathsf{OR}_{i\in I} S_i}}$ **34**(ii)
$= \prod_{i\in I} \mathrm{wlp}_{S_i}(x) \cdot \overline{\sum_{i\in I} \mathbf{e}^{\rho,\varepsilon}_{S_i}}$ **57**(xii), **39**
$= \prod_{i\in I} \mathrm{wlp}_{S_i}(x) \cdot \prod_{i\in I} \overline{\mathbf{e}^{\rho,\varepsilon}_{S_i}}$ **8**(ii)
$= \prod_{i\in I} \left(\mathrm{wlp}_{S_i}(x) \cdot \overline{\mathbf{e}^{\rho,\varepsilon}_{S_i}}\right)$ **9**(ii)
$= \prod_{i\in I} \mathrm{wp}_{S_i}(x)$ **34**(ii).

57(xiv): $\mathrm{wlp}_{\mathsf{if}\ B\ \mathsf{then}\ S\ \mathsf{else}\ T}(x)$
$= \overline{\mathbf{r}^{\rho}_{\mathsf{if}\ B\ \mathsf{then}\ S\ \mathsf{else}\ T}; \bar{x}}$ **33**(i)
$= \overline{(\rho_B; \mathbf{r}^{\rho}_{S} + \overline{\rho_B; 1} \cdot \mathbf{r}^{\rho}_{T}); \bar{x}}$ **39**
$= \overline{\rho_B; \mathbf{r}^{\rho}_{S}; \bar{x} + (\overline{\rho_B; 1} \cdot \mathbf{r}^{\rho}_{T}); \bar{x}}$ (Ra_2)
$= \overline{\rho_B; \mathbf{r}^{\rho}_{S}; \bar{x}} \cdot \overline{\overline{\rho_B; 1} \cdot \mathbf{r}^{\rho}_{T}; \bar{x}}$ **3**(xvi), **26**(i)(ii), **24**(xxvi)
$= \left(\overline{\rho_B; 1} + \overline{\mathbf{r}^{\rho}_{S}; \bar{x}}\right) \cdot \left(\rho_B; 1 + \overline{\mathbf{r}^{\rho}_{T}; \bar{x}}\right)$ **37**(vii), **24**(xxxi), **3**(ii)(xvii)
$= \rho_B; 1 \cdot \overline{\mathbf{r}^{\rho}_{S}; \bar{x}} + \overline{\rho_B; 1} \cdot \overline{\mathbf{r}^{\rho}_{T}; \bar{x}}$ **3**(ii)(xix)
$= \rho_B; \mathrm{wlp}_S(x) + \overline{\rho_B; 1} \cdot \mathrm{wlp}_T(x)$ **37**(vii), **24**(xxxi), **33**(i).

computations at all). However, correct interpretations do have the property that if the basic statements obey the law, then all statements do so.

Theorem 59. *Suppose* $\mathfrak{A}$ *is a complete relation algebra and* $\langle \mathbf{r}^\rho, \mathbf{e}^{\rho,\varepsilon} \rangle$ *is a correct* $\mathfrak{A}$*-interpretation. Then*

(i) $\mathrm{wp}_S(0) = 0$ *whenever* $S \in \{\mathsf{havoc}, \mathsf{abort}, \mathsf{skip}\}$.
(ii) *If* $\mathrm{wp}_S(0) = 0$ *and* $\mathrm{wp}_T(0) = 0$, *then* $\mathrm{wp}_{S;T}(0) = 0$.
(iii) *If* $\mathrm{wp}_S(0) = 0$ *or* $\mathrm{wp}_T(0) = 0$, *then* $\mathrm{wp}_{S \text{ or } T}(0) = 0$.
(iv) *If* $\mathrm{wp}_{S_j}(0) = 0$ *for some* $j \in I$, *then* $\mathrm{wp}_{\mathsf{OR}_{i\in I} S_i}(0) = 0$.
(v) *If* $\mathrm{wp}_S(0) = 0$ *and* $\mathrm{wp}_T(0) = 0$, *then* $\mathrm{wp}_{\mathsf{if}\ B\ \mathsf{then}\ S\ \mathsf{else}\ T}(0) = 0$.
(vi) *If* $\mathrm{wp}_S(0) = 0$ *then* $\mathrm{wp}_{B\to S}(0) = 0$.
(vii) *If* $\mathrm{wp}_{S_i}(0) = 0$ *for every* $i \in I$, *then* $\mathrm{wp}_{\mathsf{IF}_{i\in I}(B_i \to S_i)}(0) = 0$.
(viii) *If* $\mathrm{wp}_S(0) = 0$, *then* $\mathrm{wp}_{\mathsf{while}\ B\ \mathsf{do}\ S}(0) = 0$.

Proof. **59**(i): We have $\mathrm{wp}_{\mathsf{havoc}}(0) = 0 \dagger 0 = \overline{\overline{0};\overline{0}} = \overline{1;1} = \overline{1} = 0$ by **57**(vi), (Ra_8), **5**(iii)(iv), and **24**(xxii), $\mathrm{wp}_{\mathsf{abort}}(0) = 0$ by **57**(iv), and $\mathrm{wp}_{\mathsf{skip}}(0) = 0$ by **57**(ii).

59(ii): If $\mathrm{wp}_S(0) = 0$ and $\mathrm{wp}_T(0) = 0$ then $\mathrm{wp}_{S;T}(0) = \mathrm{wp}_S(\mathrm{wp}_T(0)) = \mathrm{wp}_S(0) = 0$ by **57**(ix).

59(iii): If $\mathrm{wp}_S(0) = 0$ then $\mathrm{wp}_{S \text{ or } T}(0) = \mathrm{wp}_S(0) \cdot \mathrm{wp}_T(0) = 0 \cdot \mathrm{wp}_T(0) = 0$ by **57**(xi). Similarly, if $\mathrm{wp}_T(0) = 0$, then $\mathrm{wp}_{S \text{ or } T}(0) = 0$.

59(iv): If $\mathrm{wp}_{S_j}(0) = 0$ for some $j \in I$, then $\mathrm{wp}_{\mathsf{OR}_{i\in I} S_i}(0) = \prod_{i\in I} \mathrm{wp}_{S_i}(0) \leqslant \mathrm{wp}_{S_j}(0) = 0$ by **57**(xiii).

59(v): If $\mathrm{wp}_S(0) = 0$ and $\mathrm{wp}_T(0) = 0$ then $\mathrm{wp}_{\mathsf{if}\ B\ \mathsf{then}\ S\ \mathsf{else}\ T}(0) = \rho_B;\mathrm{wp}_S(0) + \overline{\rho_B;1} \cdot \mathrm{wp}_T(0) = \rho_B;0 + \overline{\rho_B;1} \cdot 0 = 0 + 0 = 0$ by **57**(xv).

59(vi): If $\mathrm{wp}_S(0) = 0$ then $\mathrm{wp}_{B\to S}(0) = \rho_B;\mathrm{wp}_S(0) = \rho_B;0 = 0$ by **57**(xvii).

59(vii): Assume $\mathrm{wp}_{S_i}(0) = 0$ for every $i \in I$. Then

$$\begin{aligned}
\mathrm{wp}_{\mathsf{IF}_{i\in I}(B_i\to S_i)}(0) &= \prod_{i\in I} \left(\overline{\rho_{B_i}} + \mathrm{wp}_{S_i}(0)\right) \cdot \sum_{i\in I} \rho_{B_i} && \textbf{57}(\mathrm{xix}) \\
&= \prod_{i\in I} \overline{\rho_{B_i}} \cdot \sum_{i\in I} \rho_{B_i} && \text{hypothesis, } \textbf{5}(\mathrm{vii}) \\
&= 0 && \textbf{8}(\mathrm{ii}), \textbf{5}(\mathrm{ii}), \textbf{3}(\mathrm{viii}).
\end{aligned}$$

59(viii): If $\mathrm{wp}_S(0) = 0$ then

$$\begin{aligned}
\mathrm{wp}_{\mathsf{while}\ B\ \mathsf{do}\ S}(0) &= \prod \{\, y : y \geqslant \overline{\rho_B;1} \cdot 0 + \rho_B;\mathrm{wp}_S(0) \,\} && \textbf{57}(\mathrm{xxvi}) \\
&= \prod \{\, y : y \geqslant 0 \,\} && \mathrm{wp}_S(0) = 0,\ \textbf{5}(\mathrm{vi})(\mathrm{vii}), \\
& && \textbf{24}(\mathrm{xviii}) \\
&= 0 && \textbf{8}(\mathrm{iv}) \quad \square
\end{aligned}$$

Theorem 60. *Suppose* $\mathfrak{A}$ *is a complete relation algebra,* $\langle \mathbf{r}^\rho, \mathbf{e}^{\rho,\varepsilon} \rangle$ *is a correct* $\mathfrak{A}$*-interpretation, and* $\mathrm{wp}_R(0) = 0$ *for every basic statement* R *distinct from* **havoc**, **abort**, *and* **skip**. *Then* $\langle \mathbf{r}^\rho, \mathbf{e}^{\rho,\varepsilon} \rangle$ *is miracle-free.*

Proof. It suffices to prove that, for every $S \in \mathscr{S}tat$,

$$\text{if } \rho \text{ and } \varepsilon \text{ are basically correct and } \mathrm{wp}_R(0) = 0 \text{ for every } R \in \mathscr{B}asic \sim \{\mathsf{havoc}, \mathsf{abort}, \mathsf{skip}\}, \text{ then } \mathrm{wp}_S(0) = 0. \tag{32}$$

We prove this by induction on the complexity of statements S. Suppose that $R \in \mathscr{B}asic$ and that the hypothesis of (32) holds. If R is distinct from **havoc**, **abort**, and **skip**, then $\mathrm{wp}_R(0) = 0$ by the hypothesis of (32). On the other hand, if R is either **havoc**, **abort**, or **skip**, then we get $\mathrm{wp}_R(0) = 0$ by **59**(i). Suppose that (32) is true of both S and T, and that the hypothesis of (32) holds. It follows immediately that $\mathrm{wp}_S(0) = 0$ and $\mathrm{wp}_T(0) = 0$. By **59**(ii), we conclude that $\mathrm{wp}_{S;T}(0) = 0$. Thus, (32) holds for $S;T$ whenever it holds for S and T. If follows from **59**(iii) and **59**(v) that if (32) holds for S and T, then it holds for S or T and if B then S else T. By **59**(vi) and **59**(viii), if (32) holds for S, then it holds for $B \to S$ and while B do S. By **59**(iv) and **59**(vii), if (32) is true of S_i for every $i \in I$ then (32) holds for both $\mathsf{OR}_{i\in I} S_i$ and $\mathsf{IF}_{i\in I}(B_i \to S_i)$. For the final case, we assume that (32) is true of S. We will show that (32) holds for $\mu X\,[S]$. We have shown in **46** that the function $\mathbf{r}^\rho\left(X_0^{(\cdot)}\right)_S$ is monotonic. Let $r = \mathbf{r}^\rho_{\mu X[S]}$ and recall that $r = \prod\{x : x \geqslant \mathbf{r}^\rho\left(X_0^x\right)_S\}$. It follows, by **22**, that r is the least fixed point of $\mathbf{r}^\rho\left(X_0^{(\cdot)}\right)_S$, hence $r = \mathbf{r}^\rho\left(X_0^r\right)_S$. From this and **43** we get $r = \mathbf{r}^\rho\left(X^r_{\overline{r;1}}\right)_S$, so

$$\overline{r;1} = \overline{\mathbf{r}^\rho\left(X^r_{\overline{r;1}}\right)_S;1}. \tag{33}$$

We have assumed that ρ and ε are basically correct and $\overline{\mathbf{r}^\rho_R;1} \leqslant \mathbf{e}^{\rho,\varepsilon}_R$ for every $R \in \mathscr{B}asic \sim \{\mathsf{havoc}, \mathsf{abort}, \mathsf{skip}\}$. It follows easily from this assumption that $\rho\left(X^r_{\overline{r;1}}\right)$ and $\varepsilon\left(X^r_{\overline{r;1}}\right)$ are also basically correct and also satisfy

$$\overline{\mathbf{r}^\rho\left(X^r_{\overline{r;1}}\right)_R;1} \leqslant \mathbf{e}^{\rho,\varepsilon}\left(X^r_{\overline{r;1}}\right)_R$$

for every $R \in \mathscr{B}asic \sim \{\mathsf{havoc}, \mathsf{abort}, \mathsf{skip}\}$. Indeed, since ρ and ε agree with $\rho\left(X^r_{\overline{r;1}}\right)$ and $\varepsilon\left(X^r_{\overline{r;1}}\right)$ everywhere except possibly at X, we need only note that $\overline{r;1}$ is a domain element of $\mathfrak{A}$ and

$$\overline{\mathbf{r}^\rho\left(X^r_{\overline{r;1}}\right)_X;1} = \overline{r;1} = \mathbf{e}^{\rho,\varepsilon}\left(X^r_{\overline{r;1}}\right)_X.$$

as follows.

$$
\begin{aligned}
&\mathrm{wlp}_{\text{while } B \text{ do } S}.(x)\\
&= \overline{\mathbf{r}^{\rho}_{\text{while } B \text{ do } S}; \bar{x}} && \textbf{33}(\mathrm{i})\\
&= \overline{\prod \left\{ y : y \geqslant \overline{\rho_B} \cdot 1' + \rho_B; \mathbf{r}^{\rho}_S; y \right\}; \bar{x}} && \textbf{39}\\
&= \overline{\prod \left\{ y : y \geqslant \overline{\rho_B; \overline{1}} \cdot 1' + \rho_B; \mathbf{r}^{\rho}_S; y \right\}; \bar{x}} && \textbf{37}(\mathrm{vii}), \textbf{24}(\mathrm{xxxii})\\
&= \overline{\prod \left\{ y : y \geqslant \left(\overline{\rho_B; \overline{1}} \cdot 1'\right); \bar{x} + \rho_B; \mathbf{r}^{\rho}_S; y \right\}} && \textbf{30}(\mathrm{iii})\\
&= \overline{\prod \left\{ y : y \geqslant \overline{\rho_B; \overline{1}} \cdot \bar{x} + \rho_B; \mathbf{r}^{\rho}_S; y \right\}} && \textbf{26}(\mathrm{i})(\mathrm{ii}), \textbf{24}(\mathrm{xxvii})\\
&= \sum \left\{ \bar{y} : y \geqslant \overline{\rho_B; \overline{1}} \cdot \bar{x} + \rho_B; \mathbf{r}^{\rho}_S; y \right\} && \textbf{8}(\mathrm{iii})\\
&= \sum \left\{ y : \bar{y} \geqslant \overline{\rho_B; \overline{1}} \cdot \bar{x} + \rho_B; \mathbf{r}^{\rho}_S; \bar{y} \right\} && \textbf{3}(\mathrm{ii})\\
&= \sum \left\{ y : y \leqslant \overline{\overline{\rho_B; \overline{1}} \cdot \bar{x} + \rho_B; \mathbf{r}^{\rho}_S; \bar{y}} \right\} && \textbf{3}(\mathrm{ii}), \textbf{7}(\mathrm{v})\\
&= \sum \left\{ y : y \leqslant (\rho_B; 1 + x) \cdot \overline{\rho_B; \mathbf{r}^{\rho}_S; \bar{y}} \right\} && \textbf{3}(\mathrm{ii})(\mathrm{xvi})(\mathrm{xvii}).
\end{aligned}
$$

Starting from (31), we first obtain **57**(xxi):

$$
\begin{aligned}
\mathrm{wlp}_{\text{while } B \text{ do } S}(x) &= \sum \left\{ y : y \leqslant (\rho_B; 1 + x) \cdot \overline{\mathbf{r}^{\rho}_{B \to S}; \bar{y}} \right\} && (31),\ \textbf{39}\\
&= \overline{\left(\mathbf{r}^{\rho}_{B \to S}\right)^{\omega}; \overline{\rho_B; \overline{1 + x}}} && \textbf{30}(\mathrm{ii})\\
&= \overline{\sum_{i \in \omega} \left(\mathbf{r}^{\rho}_{B \to S}\right)^{i}; \overline{\rho_B; \overline{1 + x}}} && \textbf{29}\\
&= \prod_{i \in \omega} \overline{\left(\mathbf{r}^{\rho}_{B \to S}\right)^{i}; \overline{\rho_B; \overline{1 + x}}} && \textbf{8}(\mathrm{ii})\\
&= \prod_{i \in \omega} (\mathrm{wlp}_{B \to S})^{i} (\rho_B; 1 + x) && \textbf{57}(\mathrm{xx})
\end{aligned}
$$

and then **57**(xxii)-**57**(xxiv):

$$
\begin{aligned}
\mathrm{wlp}_{\text{while } B \text{ do } S}(x) &= \sum \left\{ y : y \leqslant (\rho_B; 1 + x) \cdot \overline{\mathbf{r}^{\rho}_{B \to S}; \bar{y}} \right\} && (31),\ \textbf{39}\\
&= \sum \left\{ y : y \leqslant (\rho_B; 1 + x) \cdot \mathrm{wlp}_{B \to S}(y) \right\} && \textbf{33}(\mathrm{ii})\\
&= \sum \left\{ y : y \leqslant (\rho_B; 1 + x) \cdot \left(\overline{\rho_B; \overline{1}} + \mathrm{wlp}_S(y)\right) \right\} && \textbf{57}(\mathrm{xvi})\\
&= \sum \left\{ y : y \leqslant \overline{\rho_B; \overline{1}} \cdot x + \rho_B; 1 \cdot \mathrm{wlp}_S(y) \right\} && \textbf{3}(\mathrm{xix})\\
&= \sum \left\{ y : y \leqslant \overline{\rho_B; \overline{1}} \cdot x + \rho_B; \mathrm{wlp}_S(y) \right\} && \textbf{37}(\mathrm{vii}), \textbf{24}(\mathrm{xxxi}).
\end{aligned}
$$

Proof. **61**(i): By **36**(ii) and **37**(i)–(iv), **skip** is deterministic because 1' is functional and $1' \cdot 0 = 0$, while **abort** is deterministic because 0 is functional and $0 \cdot 1 = 0$.

61(ii): By **36**(ii) and **37**(v)(vi), **havoc** is deterministic iff 1 is functional, i.e., iff $\check{1};1 \leqslant 1'$. But $\check{1};1 = 1$, so **havoc** is deterministic iff $1' = 1$.

61(iii): Assume S and T are deterministic. By **36**(ii) we get

$$\mathbf{r}_S^\rho \text{ and } \mathbf{r}_T^\rho \text{are functional,} \tag{34}$$

$$\mathbf{r}_S^\rho \cdot \mathbf{e}_S^{\rho,\varepsilon} = 0 \quad \text{and} \quad \mathbf{r}_T^\rho \cdot \mathbf{e}_T^{\rho,\varepsilon} = 0. \tag{35}$$

From (34) it follows that $\mathbf{r}_{S;T}^\rho$ is functional by **28**(i) and **39**. Also,

$$\begin{aligned}
\mathbf{r}_{S;T}^\rho \cdot \mathbf{e}_{S;T}^{\rho,\varepsilon} &= \mathbf{r}_S^\rho;\mathbf{r}_T^\rho \cdot (\mathbf{e}_S^{\rho,\varepsilon} + \mathbf{r}_S^\rho;\mathbf{e}_T^{\rho,\varepsilon}) && \textbf{39}\\
&= \mathbf{r}_S^\rho;\mathbf{r}_T^\rho \cdot \mathbf{e}_S^{\rho,\varepsilon} + \mathbf{r}_S^\rho;\mathbf{r}_T^\rho \cdot \mathbf{r}_S^\rho;\mathbf{e}_T^{\rho,\varepsilon} && \textbf{3}(\text{xv})\\
&= (\mathbf{e}_S^{\rho,\varepsilon} \cdot \mathbf{r}_S^\rho);\mathbf{r}_T^\rho + \mathbf{r}_S^\rho;\mathbf{r}_T^\rho \cdot \mathbf{r}_S^\rho;\mathbf{e}_T^{\rho,\varepsilon} && \textbf{3}(\text{viii}), \textbf{37}(\text{viii}), \textbf{24}(\text{xxvi})\\
&= (\mathbf{e}_S^{\rho,\varepsilon} \cdot \mathbf{r}_S^\rho);\mathbf{r}_T^\rho + \mathbf{r}_S^\rho;(\mathbf{r}_T^\rho \cdot \mathbf{e}_T^{\rho,\varepsilon}) && (34), \textbf{28}(\text{ii})\\
&= 0;\mathbf{r}_T^\rho + \mathbf{r}_S^\rho;0 && (35), \textbf{3}(\text{viii})\\
&= 0 && \textbf{24}(\text{xviii}).
\end{aligned}$$

Therefore, $\mathbf{r}_{S;T}^\rho$ is deterministic by **36**(ii).

61(iv): By **36**(ii), S or T is deterministic iff

$$\mathbf{r}_{S \text{ or } T}^\rho \text{ is functional,} \tag{36}$$

$$\mathbf{r}_{S \text{ or } T}^{\rho,\varepsilon} \cdot S \text{ or } T = 0. \tag{37}$$

By **27**, **39**, **24**(xv), and **7**(iv), (36) is equivalent to

$$(\mathbf{r}_S^\rho)\check{};\mathbf{r}_S^\rho \leqslant 1' \text{ and } (\mathbf{r}_T^\rho)\check{};\mathbf{r}_S^\rho \leqslant 1' \text{ and } (\mathbf{r}_S^\rho)\check{};\mathbf{r}_T^\rho \leqslant 1' \text{ and } (\mathbf{r}_T^\rho)\check{};\mathbf{r}_T^\rho \leqslant 1'. \tag{38}$$

Similarly, (37) is equivalent to

$$\mathbf{r}_S^\rho \cdot \mathbf{e}_S^{\rho,\varepsilon} = 0 \text{ and } \mathbf{r}_T^\rho \cdot \mathbf{e}_S^{\rho,\varepsilon} = 0 \text{ and } \mathbf{r}_S^\rho \cdot \mathbf{e}_T^{\rho,\varepsilon} = 0 \text{ and } \mathbf{r}_T^\rho \cdot \mathbf{e}_T^{\rho,\varepsilon} = 0. \tag{39}$$

Four of the statements in (38) and (39) are equivalent to the assertion that S and T are deterministic. Three of the others are explicitly included in the statement of **61**(iv), so it suffices to observe that the second and third statements of (38) are equivalent to each other by **24**(i)(viii), (Ra_6), and (Ra_4).

61(v): This part follows from the relevant definitions by **16** and **24**(vii)(x).

61(vi): Suppose S and T are deterministic, i. e., $\mathbf{r}_S^\rho$ and $\mathbf{r}_T^\rho$ are functional and $\mathbf{r}_S^\rho \cdot \mathbf{e}_S^{\rho,\varepsilon} = 0 = \mathbf{r}_T^\rho \cdot \mathbf{e}_T^{\rho,\varepsilon}$. Then

$$
\begin{aligned}
&\left(\mathbf{r}^\rho_{\text{if } B \text{ then } S \text{ else } T}\right)^\smile ; \mathbf{r}^\rho_{\text{if } B \text{ then } S \text{ else } T} \\
&\quad = \left(\rho_B;1 \cdot \mathbf{r}_S^\rho + \overline{\rho_B;1} \cdot \mathbf{r}_T^\rho\right)^\smile ; \left(\rho_B;1 \cdot \mathbf{r}_S^\rho + \overline{\rho_B;1} \cdot \mathbf{r}_T^\rho\right) \\
&\qquad\qquad \textbf{39}, \textbf{37}(\text{vii}), \textbf{24}(\text{xxx}) \\
&\quad = \left(1;\rho_B \cdot \left(\mathbf{r}_S^\rho\right)^\smile + \overline{1;\rho_B} \cdot \left(\mathbf{r}_T^\rho\right)^\smile\right) ; \left(\rho_B;1 \cdot \mathbf{r}_S^\rho + \overline{\rho_B;1} \cdot \mathbf{r}_T^\rho\right) \\
&\qquad\qquad \textbf{37}(\text{vii}), (\text{Ra}_5), (\text{Ra}_6), \textbf{24}(\text{iii})(\text{iv})(\text{v}) \\
&\quad = \left(1;\rho_B \cdot \left(\mathbf{r}_S^\rho\right)^\smile\right) ; \left(\rho_B;1 \cdot \mathbf{r}_S^\rho\right) + \left(\overline{1;\rho_B} \cdot \left(\mathbf{r}_T^\rho\right)^\smile\right) ; \left(\rho_B;1 \cdot \mathbf{r}_S^\rho\right) \\
&\quad + \left(1;\rho_B \cdot \left(\mathbf{r}_S^\rho\right)^\smile\right) ; \left(\overline{\rho_B;1} \cdot \mathbf{r}_T^\rho\right) + \left(\overline{1;\rho_B} \cdot \left(\mathbf{r}_T^\rho\right)^\smile\right) ; \left(\overline{\rho_B;1} \cdot \mathbf{r}_T^\rho\right) \\
&\qquad\qquad \textbf{24}(\text{xv}) \\
&\quad \leqslant \left(\mathbf{r}_S^\rho\right)^\smile ; \mathbf{r}_S^\rho + \overline{1;\rho_B};(\rho_B;1) + (1;\rho_B);\overline{\rho_B;1} + \left(\mathbf{r}_T^\rho\right)^\smile ; \mathbf{r}_T^\rho \\
&\qquad\qquad \textbf{24}(\text{x}) \\
&\quad \leqslant 1' \\
&\qquad\qquad \text{(see below).}
\end{aligned}
$$

For the last step we need only note that $\mathbf{r}_S^\rho$ and $\mathbf{r}_T^\rho$ are functional, that

$$\overline{1;\rho_B};(\rho_B;1) = \overline{1;\rho_B};\rho_B;1 = \overline{1;\rho_B};\breve{\rho_B};1 \leqslant \overline{1};1 = 0;1 = 0$$

by (Ra_1), **37**(vii), **24**(xxx)(xii)(xviii), and **5**(iii), and, similarly, $(1;\rho_B);\overline{\rho_B;1} = 0$. From these observations and the assumption that $\mathbf{r}_S^\rho \cdot \mathbf{e}_S^{\rho,\varepsilon} = 0 = \mathbf{r}_T^\rho \cdot \mathbf{e}_T^{\rho,\varepsilon}$, we also get

$$
\begin{aligned}
&\mathbf{r}^\rho_{\text{if } B \text{ then } S \text{ else } T} \cdot \mathbf{e}^{\rho,\varepsilon}_{\text{if } B \text{ then } S \text{ else } T} \\
&\quad = \left(\rho_B;1 \cdot \mathbf{r}_S^\rho + \overline{\rho_B;1} \cdot \mathbf{r}_T^\rho\right) \cdot \left(\rho_B;1 \cdot \mathbf{e}_S^{\rho,\varepsilon} + \overline{\rho_B;1} \cdot \mathbf{e}_T^{\rho,\varepsilon}\right) \\
&\quad = \mathbf{r}_S^\rho \cdot \mathbf{e}_S^{\rho,\varepsilon} + \overline{1;\rho_B};(\rho_B;1) + (1;\rho_B);\overline{\rho_B;1} + \mathbf{r}_T^\rho \cdot \mathbf{e}_T^{\rho,\varepsilon} \\
&\quad = 0.
\end{aligned}
$$

Therefore, **if** B **then** S **else** T is deterministic.

61(vii): Assume S is deterministic, i.e., $\mathbf{r}_S^\rho$ is functional and $\mathbf{r}_S^\rho \cdot \mathbf{e}_S^{\rho,\varepsilon} = 0$. Then

$$
\begin{aligned}
\left(\mathbf{r}^\rho_{B\to S}\right)^\smile ; \mathbf{r}^\rho_{B\to S} &= \left(\rho_B;\mathbf{r}_S^\rho\right)^\smile ; \left(\rho_B;\mathbf{r}_S^\rho\right) && \textbf{39} \\
&\leqslant \left(\mathbf{r}_S^\rho\right)^\smile ; \mathbf{r}_S^\rho && \textbf{37}(\text{vii}), \textbf{24}(\text{i})(\text{x})(\text{xix}) \\
&\leqslant 1' && S \text{ is functional}
\end{aligned}
$$

and

$$
\begin{aligned}
\mathbf{r}^\rho_{B\to S} \cdot \mathbf{e}^{\rho,\varepsilon}_{B\to S} &= \rho_B;1 \cdot \mathbf{r}_S^\rho \cdot \left(\overline{\rho_B;1} + \mathbf{e}_S^{\rho,\varepsilon}\right) && \textbf{39}, \textbf{37}(\text{vii}), \textbf{24}(\text{xxxi}) \\
&\leqslant 0 && \textbf{3}, \textbf{5}, \mathbf{r}_S^\rho \cdot \mathbf{e}_S^{\rho,\varepsilon} = 0,
\end{aligned}
$$

so $B \to S$ is also deterministic.

61(viii): From the assumptions we get, by **36**(ii),

$$\rho_{B_i} \cdot \rho_{B_j} = 0 \text{ when ever } i \neq j \text{ and } i,j \in I, \tag{40}$$

$$\mathbf{r}_{S_i}^\rho \text{ is functional and } \mathbf{r}_{S_i}^\rho \cdot \mathbf{e}_{S_i}^{\rho,\varepsilon} = 0 \text{ for every } i \in I. \tag{41}$$

Then

$$
\begin{aligned}
&\left(\mathbf{r}^{\rho}_{\mathsf{IF}_{i\in I}(B_i\to S_i)}\right)\breve{}\ ;\mathbf{r}^{\rho}_{\mathsf{IF}_{i\in I}(B_i\to S_i)}\\
&= \left(\sum_{i\in I}\rho_{B_i};\mathbf{r}^{\rho}_{S_i}\right)\breve{}\ ;\sum_{j\in I}\left(\rho_{B_j};\mathbf{r}^{\rho}_{S_j}\right)\\
&\qquad\qquad\qquad\qquad \mathbf{39}\\
&= \sum_{i\in I}\left(\left(\mathbf{r}^{\rho}_{S_i}\right)\breve{}\ ;\left(\rho_{B_i}\right)\breve{}\right);\sum_{j\in I}\left(\rho_{B_j};\mathbf{r}^{\rho}_{S_j}\right)\\
&\qquad\qquad\qquad\qquad \mathbf{24}(\text{vii}),(\text{Ra}_6)\\
&= \sum_{i\in I}\sum_{j\in I}\left(\left(\left(\mathbf{r}^{\rho}_{S_i}\right)\breve{}\ ;\left(\rho_{B_i}\right)\breve{}\right);\left(\rho_{B_j};\mathbf{r}^{\rho}_{S_j}\right)\right)\\
&\qquad\qquad\qquad\qquad \mathbf{24}(\text{xv})\\
&= \sum_{i\in I}\sum_{j\in I}\left(\left(\mathbf{r}^{\rho}_{S_i}\right)\breve{}\ ;\left(\rho_{B_i}\cdot\rho_{B_j}\right);\mathbf{r}^{\rho}_{S_j}\right)\\
&\qquad\qquad\qquad\qquad \mathbf{37}(\text{vii}),\ \mathbf{24}(\text{xxx})(\text{xxxiii}),\ (\text{Ra}_1)\\
&= \sum_{i\in I}\left(\left(\mathbf{r}^{\rho}_{S_i}\right)\breve{}\ ;\left(\rho_{B_i}\cdot\rho_{B_i}\right);\mathbf{r}^{\rho}_{S_i}+\sum_{i\neq j\in I}\left(\left(\mathbf{r}^{\rho}_{S_i}\right)\breve{}\ ;\left(\rho_{B_i}\cdot\rho_{B_j}\right);\mathbf{r}^{\rho}_{S_j}\right)\right)\\
&\qquad\qquad\qquad\qquad \mathbf{10}(\text{i})\\
&= \sum_{i\in I}\left(\left(\mathbf{r}^{\rho}_{S_i}\right)\breve{}\ ;\rho_{B_i};\mathbf{r}^{\rho}_{S_i}+\sum_{i\neq j\in I}\left(\left(\mathbf{r}^{\rho}_{S_i}\right)\breve{}\ ;0;\mathbf{r}^{\rho}_{S_j}\right)\right)\\
&\qquad\qquad\qquad\qquad \mathbf{3}(\text{vii}),\ (40)\\
&= \sum_{i\in I}\left(\left(\mathbf{r}^{\rho}_{S_i}\right)\breve{}\ ;\rho_{B_i};\mathbf{r}^{\rho}_{S_i}\right)\\
&\qquad\qquad\qquad\qquad \mathbf{5}(\text{vii}),\ \mathbf{24}(\text{xviii}),\ \mathbf{1}(\text{iii})\\
&\leqslant \sum_{i\in I}\left(\left(\mathbf{r}^{\rho}_{S_i}\right)\breve{}\ ;\mathbf{r}^{\rho}_{S_i}\right)\\
&\qquad\qquad\qquad\qquad \mathbf{37}(\text{vii}),\ \mathbf{24}(\text{x})(\text{xix}),\ \mathbf{9}(\text{iii})\\
&\leqslant \sum_{i\in I}1'\\
&\qquad\qquad\qquad\qquad (41),\ \mathbf{9}(\text{iii})\\
&= 1'\\
&\qquad\qquad\qquad\qquad \mathbf{1}(\text{iii}).
\end{aligned}
$$

Therefore, $\mathbf{r}^{\rho}_{\mathsf{IF}_{i\in I}(B_i\to S_i)}$ is functional. We have

$$\sum_{i\in I}\left(\rho_{B_i};\mathbf{r}^{\rho}_{S_i}\right)\leqslant\sum_{i\in I}\rho_{B_i}=\overline{\prod_{i\in I}\overline{\rho_{B_i}}}$$

by **9**(iii), **8**(ii), and **3**(ii), so

$$\sum_{i\in I}(\rho_{B_i};\mathbf{r}^{\rho}_{S_i})\cdot\prod_{i\in I}\overline{\rho_{B_i}}=0 \tag{42}$$

by **7**(v) and **3**(ii). Next we prove

$$\sum_{i\in I}(\rho_{B_i};\mathbf{r}^{\rho}_{S_i})\cdot\sum_{j\in I}(\rho_{B_j};\mathbf{e}^{\rho,\varepsilon}_{S_j})=0 \tag{43}$$

as follows:

$$\begin{aligned}
&\sum_{i\in I}\left(\rho_{B_i};\mathbf{r}^{\rho}_{S_i}\right)\cdot\sum_{j\in I}\left(\rho_{B_j};\mathbf{e}^{\rho,\varepsilon}_{S_j}\right)\\
&=\sum_{i\in I}\sum_{j\in I}(\rho_{B_i};\mathbf{r}^{\rho}_{S_i}\cdot\rho_{B_j};\mathbf{e}^{\rho,\varepsilon}_{S_j})\\
&\qquad\qquad\textbf{16, 3}(\text{ix})\\
&=\sum_{i\in I}\left(\left(\rho_{B_i};\mathbf{r}^{\rho}_{S_i}\cdot\rho_{B_i};\mathbf{e}^{\rho,\varepsilon}_{S_i}\right)+\sum_{i\neq j\in I}\left(\rho_{B_i};\mathbf{r}^{\rho}_{S_i}\cdot\rho_{B_j};\mathbf{e}^{\rho,\varepsilon}_{S_j}\right)\right)\\
&\qquad\qquad\textbf{10}(\text{i})\\
&=\sum_{i\in I}\left(\rho_{B_i};\left(\mathbf{r}^{\rho}_{S_i}\cdot\ \mathbf{e}^{\rho,\varepsilon}\right)\right)+\sum_{i\neq j\in I}\left(\left(\rho_{B_i}\cdot\rho_{B_j}\right);\left(\mathbf{r}^{\rho}_{S_i}\cdot\mathbf{e}^{\rho,\varepsilon}_{S_j}\right)\right)\\
&\qquad\qquad\textbf{37}(\text{vii}),\ \textbf{24}(\text{xxxiv}),\ \textbf{28}(\text{ii})(\text{iv})\\
&=\sum_{i\in I}(\rho_{B_i};0)+\sum_{i\neq j\in I}\left(0;\left(\mathbf{r}^{\rho}_{S_i}\cdot\mathbf{e}^{\rho,\varepsilon}_{S_j}\right)\right)\\
&\qquad\qquad(40),\ (41)\\
&=0\\
&\qquad\qquad\textbf{24}(\text{xviii}).
\end{aligned}$$

Using (42) and (43), we have

$$\begin{aligned}
&\mathbf{r}^{\rho}_{\mathsf{IF}_{i\in I}(B_i\to S_i)}\cdot\mathbf{e}^{\rho,\varepsilon}_{\mathsf{IF}_{i\in I}(B_i\to S_i)}\\
&\quad=\sum_{i\in I}\left(\rho_{B_i};\mathbf{r}^{\rho}_{S_i}\right)\cdot\left(\prod_{i\in I}\overline{\rho_{B_i};1}+\sum_{j\in I}\left(\rho_{B_j};\mathbf{e}^{\rho,\varepsilon}_{S_j}\right)\right) && \textbf{39}\\
&\quad=\sum_{i\in I}\left(\rho_{B_i};\mathbf{r}^{\rho}_{S_i}\right)\cdot\prod_{i\in I}\overline{\rho_{B_i};1}+\sum_{i\in I}\left(\rho_{B_i};\mathbf{r}^{\rho}_{S_i}\right)\cdot\sum_{j\in I}\left(\rho_{B_j};\mathbf{e}^{\rho,\varepsilon}_{S_j}\right) && \textbf{3}(\text{xv})\\
&\quad=0 && (42),\ (43),
\end{aligned}$$

so we conclude that $\mathsf{IF}_{i\in I}(B_i\to S_i)$ is deterministic.

61(ix): Assume S is deterministic. By **35** we know that

$$\mathrm{wlp}^{\delta}_{S}(y)\leqslant\mathrm{wp}_{S}(y)\ \text{ for all } y\in A, \tag{44}$$

and we need only show $\mathrm{wlp}^{\delta}_{\textsf{while}\,B\,\textsf{do}\,S}(x)\leqslant\mathrm{wp}_{\textsf{while}\,B\,\textsf{do}\,S}(x)$ for every x.

$$\begin{aligned}
&\mathrm{wlp}^{\delta}_{\textsf{while}\,B\,\textsf{do}\,S}x\\
&\quad=\overline{\mathrm{wlp}_{\textsf{while}\,B\,\textsf{do}\,S}(\bar{x})} && \textbf{11}\\
&\quad=\overline{\sum\left\{\,y:y\leqslant(\rho_B;1+\bar{x})\cdot(\overline{\rho_B;1}+\mathrm{wlp}_S(y))\,\right\}} && \textbf{57}(\text{xxii})\\
&\quad=\prod\left\{\,y:y\geqslant\overline{\rho_B;1}\cdot x+\rho_B;1\cdot\mathrm{wlp}^{\delta}_{S}(y)\,\right\} && \textbf{3}(\text{ii})(\text{xvi})(\text{xvii}),\ \textbf{8}(\text{ii}),\ \textbf{11}\\
&\quad=\prod\left\{\,y:y\geqslant(\rho_B;1+x)\cdot(\overline{\rho_B;1}+\mathrm{wlp}^{\delta}_{S}(y))\,\right\} && \textbf{3}(\text{xix})\\
&\quad\leqslant\prod\left\{\,y:y\geqslant(\rho_B;1+x)\cdot(\overline{\rho_B;1}+\mathrm{wp}_S(y))\,\right\} && (44),\ \textbf{10}(\text{iv})\\
&\quad=\mathrm{wp}_{\textsf{while}\,B\,\textsf{do}\,S}(y) && \textbf{57}(\text{xxv}).\quad\square
\end{aligned}$$

7.7. *The invariance theorem for* `while`*-statements*

The theorem presented in this section is a generalization of what is called "the Main Repetition Theorem" in [15]. An informal statement of this result runs as follows. Assume

(i) P is a predicate,

(ii) if P and B hold at a state then no nonterminating computation of S is possible from that state,

(iii) if P and B hold at the initial state σ_1 of a terminating computation of S, then P holds at the final state σ_2, and the initial state σ_1 is in the relation G to (say, is "greater than") the final state σ_2, i.e., $\langle \sigma_1, \sigma_2 \rangle \in G$,

(iv) there is no infinite sequence of states such that P and B hold at every state in the sequence, and each state is in relation G to the next state.

It follows from these assumptions that P is a sufficient (but usually not necessary) condition for the guaranteed termination of $\mathsf{while}\, B\, \mathsf{do}\, S$ at a state satisfying P. Theorem **62** generalizes the Main Repetition Theorem in two ways. First, it does not include the assumption that G is transitive, a possibility noted in [15, pp. 174–175]. Second, as is the case for all the results in this paper, it applies to interpretations over arbitrary complete relation algebras, not just the proper relation algebras built from binary relations on a set. (For a similar algebraic generalization, see [55].)

Theorem 62. *Suppose* $\mathfrak{A}$ *is a complete relation algebra,* $\rho, S \in A$ *and* $\langle \mathbf{r}^\rho, \mathbf{e}^{\rho,\varepsilon} \rangle$ *is a correct* $\mathfrak{A}$*-interpretation. If*

(i) $p \leqslant 1'$,

(ii) $p;\rho_B;\mathbf{e}_S^{\rho,\varepsilon} = 0$,

(iii) $p;\rho_B;\mathbf{r}_S^\rho \leqslant s;p$,

(iv) $\sum\{z : z \leqslant p;\rho_B;s;p;\rho_B;z\} = 0$,

then $p;1 \leqslant \mathrm{wp}_{\mathsf{while}\, B\, \mathsf{do}\, S}(p;1)$.

Proof. First we prove that

$$\text{if } y \leqslant \rho_B;\ \left(\mathbf{e}_S^{\rho,\varepsilon} + \mathbf{r}_S^\rho;y\right) \text{ then } p;y = 0. \tag{45}$$

Assume $y \leqslant \rho_B;(\mathbf{e}_S^{\rho,\varepsilon} + \mathbf{r}_S^\rho;y)$. Notice first that $y \leqslant \rho_B;1$, hence $y = \rho_B;y$ by **24**(xxxi). Then

$$\begin{aligned}
p;y &\leqslant p;\rho_B;\left(\mathbf{e}_S^{\rho,\varepsilon} + \mathbf{r}_S^\rho;y\right) && \text{hypothesis, } \mathbf{24}(\mathrm{x}) \\
&= p;\rho_B;\mathbf{e}_S^{\rho,\varepsilon} + p;\rho_B;\mathbf{r}_S^\rho;y && \mathbf{24}(\mathrm{ix}) \\
&= p;\rho_B;\mathbf{r}_S^\rho;(\rho_B;y) && \mathbf{62}(\mathrm{ii}),\ (\mathrm{Ba}_2),\ \mathbf{5}(\mathrm{vii}),\ y = \rho_B;y \\
&= \left(p;\rho_B;\mathbf{r}_S^\rho \cdot s;p\right);\rho_B;y && \mathbf{62}(\mathrm{iii}),\ (\mathrm{Ra}_1) \\
&= \left(\mathbf{r}_S^\rho \cdot p;\rho_B;s;p\right);\rho_B;y && \mathbf{62}(\mathrm{i}),\ \mathbf{24}(\mathrm{xxxi}),\ \mathbf{37}(\mathrm{vii}),\ \mathbf{3}(\mathrm{viii})(\mathrm{ix}) \\
&\leqslant p;\rho_B;s;p;\rho_B;(p;y) && \mathbf{24}(\mathrm{x}),\ \mathbf{62}(\mathrm{i}),\ \mathbf{37}(\mathrm{vii}),\ (\mathrm{Ra}_1),\ \mathbf{3}(\mathrm{vii})(\mathrm{viii}),\ \mathbf{24}(\mathrm{xxxiii}).
\end{aligned}$$

Since $p;y$ belongs to a set whose join is 0 by **62**(iv), we conclude that $p;y = 0$, finishing the proof of (45). Next,

$$\begin{aligned} p;\mathbf{e}^{\rho,\varepsilon}_{\text{while } B \text{ do } S} &= p;\sum\{y : y \leqslant \rho_B;(\mathbf{e}^{\rho,\varepsilon}_S + \mathbf{r}^{\rho}_S;y)\} && \textbf{39}, \textbf{24}(\text{ix}), (\text{Ra}_1) \\ &= \sum\{p;y : y \leqslant \rho_B;(\mathbf{e}^{\rho,\varepsilon}_S + \mathbf{r}^{\rho}_S;y)\} && \textbf{24}(\text{xv}) \\ &= \sum\{0\} && (45) \\ &= 0. \end{aligned}$$

It follows that

$$p;1 \leqslant \overline{\mathbf{e}^{\rho,\varepsilon}_{\text{while } B \text{ do } S}} \tag{46}$$

by **62**(i), **24**(xxxi), **3**(ii), and **7**(v). From hypothesis **62**(iii), that $s \leqslant 1'$, we derive $s;p;\overline{p;1} = 0$ as in the proof of **61**(vi), so

$$\begin{aligned} p;1 &= \overline{\rho_B;1} \cdot p;1 + \rho_B;1 \cdot p;1 && \textbf{3}(\text{viii})(\text{xi}) \\ &= \overline{\rho_B;1} \cdot p;1 + p;\rho_B;\left(\mathbf{r}^{\rho}_S;\overline{p;1} + \overline{\mathbf{r}^{\rho}_S;\overline{p;1}}\right) && \textbf{5}(\text{i}), \textbf{62}(\text{i}), \textbf{24}(\text{xxxi}) \\ &= \overline{\rho_B;1} \cdot p;1 + p;\rho_B;\mathbf{r}^{\rho}_S;\overline{p;1} + p;\rho_B;\overline{\mathbf{r}^{\rho}_S;\overline{p;1}} && \textbf{24}(\text{ix}) \\ &\leqslant \overline{\rho_B;1} \cdot p;1 + s;p;\overline{p;1} + p;\rho_B;\overline{\mathbf{r}^{\rho}_S;\overline{p;1}} && \textbf{62}(\text{iii}), \textbf{24}(\text{x}) \\ &= \overline{\rho_B;1} \cdot p;1 + p;\rho_B;\overline{\mathbf{r}^{\rho}_S;\overline{p;1}} && s;p;\overline{p;1} = 0 \end{aligned}$$

Since $\text{wlp}_{\text{while } B \text{ do } S}(p;1)$ is the greatest fixed point of $\overline{\rho_B;1} \cdot p;1 + p;\rho_B;\overline{\mathbf{r}^{\rho}_S;\overline{(\cdot)}}$, and we have just seen that $p;1$ is expanded by $\overline{\rho_B;1} \cdot p;1 + p;\rho_B;\overline{\mathbf{r}^{\rho}_S;\overline{(\cdot)}}$, it follows that

$$p;1 \leqslant \text{wlp}_{\text{while } B \text{ do } S}(p;1). \tag{47}$$

From (46) and (47) we conclude by **34**(ii) and **7**(iv) that $p;1 \leqslant \text{wp}_{\text{while } B \text{ do } S}(p;1)$, as desired.

8. Demonic interpretations

Let $\mathfrak{A}$ be a complete relation algebra. Consider maps $\rho, \varepsilon : \mathscr{B}asic \to A$ and their extensions $\mathbf{r}^{\rho}, \mathbf{e}^{\rho,\varepsilon} : \mathscr{S}tat \to A$. Let us say that S is *demon-proof under* $\langle \rho, \varepsilon \rangle$ if $\rho_S;1 \cdot \varepsilon_S = 0$ and *demon-proof under* $\langle \mathbf{r}^{\rho}, \mathbf{e}^{\rho,\varepsilon} \rangle$ if $\mathbf{r}^{\rho}_S;1 \cdot \mathbf{e}^{\rho,\varepsilon}_S = 0$. The informal idea behind this terminology is that a statement is demon-proof if there are no states from which both terminating and nonterminating computations are possible, so a demon that would choose a nonterminating computation whenever any computation is possible would have no chance to cause nontermination when termination is available. Suppose S satisfies $\mathbf{r}^{\rho}_S;1 + \mathbf{e}^{\rho,\varepsilon}_S = 1$ (the "law of the excluded miracle" for the interpretation $\langle \mathbf{r}^{\rho}, \mathbf{e}^{\rho,\varepsilon} \rangle$, that every state initiates some computation). Then S is demon-proof under $\mathbf{r}^{\rho}$ and $\mathbf{e}^{\rho,\varepsilon}$ iff $\overline{\mathbf{r}^{\rho}_S;1} = \mathbf{e}^{\rho,\varepsilon}_S$, i.e., nonterminating computations start from exactly those states from which no terminating computation is possible.

Let us say that an interpretation is demon-proof if all statements are demon-proof under that interpretation. We consider the problem of creating a miracle-free demon-proof interpretation. Recall that ρ and ε are basically correct if

$$\begin{aligned} \rho_{\mathsf{skip}} &= 1', \quad \varepsilon_{\mathsf{skip}} = 0, \\ \rho_{\mathsf{abort}} &= 0, \quad \varepsilon_{\mathsf{abort}} = 1, \\ \rho_{\mathsf{havoc}} &= 1, \quad \varepsilon_{\mathsf{havoc}} = 0, \end{aligned}$$

$\rho_B \leqslant 1'$ for every Boolean statement $B \in \mathscr{Basic}$, $\varepsilon_R ; 1 = \varepsilon_R$ for every $R \in \mathscr{Basic}$,

Suppose we have a single map $\rho : \mathscr{Basic} \to A$ satisfying the items above that refer only to ρ, that is, $\rho_{\mathsf{skip}} = 1'$, $\rho_{\mathsf{abort}} = 0$, $\rho_{\mathsf{havoc}} = 1$, and $\rho_B \leqslant 1'$ for every Boolean statement $B \in \mathscr{Basic}$. From ρ we can create an additional map $\varepsilon : \mathscr{Basic} \to A$ by setting $\varepsilon_R = \overline{\rho_R ; 1}$ for every $R \in \mathscr{Basic}$. Notice that ε_R is a domain element for every $R \in \mathscr{Basic}$, and

$$\begin{aligned} \varepsilon_{\mathsf{skip}} &= \overline{\rho_{\mathsf{skip}} ; 1} = \overline{1' ; 1} = \overline{1} = 0, \\ \varepsilon_{\mathsf{abort}} &= \overline{\rho_{\mathsf{abort}} ; 1} = \overline{0 ; 1} = 1, \\ \varepsilon_{\mathsf{havoc}} &= \overline{\rho_{\mathsf{havoc}} ; 1} = \overline{1 ; 1} = 0. \end{aligned}$$

It follows that ρ and ε are basically correct and $\langle \mathbf{r}^\rho, \mathbf{e}^{\rho,\varepsilon} \rangle$ is a correct $\mathfrak{A}$-interpretation. We have $\rho_R ; 1 + \varepsilon_R = \rho_R ; 1 + \overline{\rho_R ; 1} = 1$ for every $R \in \mathscr{Basic}$, so $\langle \mathbf{r}^\rho, \mathbf{e}^{\rho,\varepsilon} \rangle$ is miracle-free by **60**. We have defined ε so that every $R \in \mathscr{Basic}$ is demon-proof under ρ and ε. But it does not follow that every $S \in \mathscr{Stat}$ is demon-proof under $\mathbf{r}^\rho$ and $\mathbf{e}^{\rho,\varepsilon}$. Here is an example that shows this. Suppose there are exactly two machine states, $\top$ and $\bot$, called "turmoil" and "repose", respectively. Choose two distinct variables X and Y and choose ρ so that $\rho_X = \{\langle \bot, \bot \rangle, \langle \bot, \top \rangle\}$ and $\rho_Y = \{\langle \bot, \bot \rangle\}$. Thus X says, "from repose go to any state", and Y says, "if in repose, then stay in repose". From ρ and ε we get the miracle-free correct interpretation $\langle \mathbf{r}^\rho, \mathbf{e}^{\rho,\varepsilon} \rangle$. Let $S = X ; Y$. Then

$$\overline{\mathbf{r}_S^\rho ; 1} = \overline{\mathbf{r}_{X;Y}^\rho ; 1} = \overline{\rho_X ; \rho_Y ; 1} = \overline{\{\langle \bot, \bot \rangle, \langle \bot, \top \rangle\} ; \{\langle \bot, \bot \rangle\} ; 1} = \{\langle \top, \bot \rangle, \langle \top, \top \rangle\},$$

so $\overline{\mathbf{r}_S^\rho ; 1}$ says "turmoil is the only state lacking terminating computations", while $\mathbf{e}_S^{\rho,\varepsilon}$ says "all states have nonterminating computations", since

$$\begin{aligned} \mathbf{e}_S^{\rho,\varepsilon} &= \mathbf{e}_{X;Y}^{\rho,\varepsilon} = \mathbf{e}_X^{\rho,\varepsilon} + \mathbf{r}_X^\rho ; \mathbf{e}_Y^{\rho,\varepsilon} = \varepsilon_X + \rho_X ; \varepsilon_Y \\ &= \overline{\{\langle \bot, \bot \rangle, \langle \bot, \top \rangle\} ; 1} + \{\langle \bot, \bot \rangle, \langle \bot, \top \rangle\} ; \overline{\{\langle \bot, \bot \rangle\} ; 1} = 1. \end{aligned}$$

Thus $\overline{\mathbf{r}_S^\rho ; 1} \neq \mathbf{e}_S^{\rho,\varepsilon}$, so $\langle \mathbf{r}^\rho, \mathbf{e}^{\rho,\varepsilon} \rangle$ is correct and miracle-free but not demon-proof.

Now there is a trivial way to start with any miracle-free interpretation $\langle \mathbf{r}^\rho, \mathbf{e}^{\rho,\varepsilon} \rangle$ and create one that is both miracle-free and demon-proof. For every $S \in \mathscr{Stat}$ define

$$\mathbf{s}_S^{\rho,\varepsilon} = \mathbf{r}_S^\rho \cdot \overline{\mathbf{e}_S^{\rho,\varepsilon}} \tag{48}$$

and consider $\langle \mathbf{s}^{\rho,\varepsilon}, \mathbf{e}^{\rho,\varepsilon} \rangle$. Then, for every $S \in \mathscr{Stat}$, $\mathbf{e}_S^{\rho,\varepsilon}$ is a domain element, so $\langle \mathbf{s}^{\rho,\varepsilon}, \mathbf{e}^{\rho,\varepsilon} \rangle$ is an interpretation,

$$1 = \mathbf{r}_S^\rho ; 1 + \mathbf{e}_S^{\rho,\varepsilon} = \mathbf{r}_S^\rho ; 1 \cdot \overline{\mathbf{e}_S^{\rho,\varepsilon}} + \mathbf{e}_S^{\rho,\varepsilon} = \left(\mathbf{r}_S^\rho \cdot \overline{\mathbf{e}_S^{\rho,\varepsilon}} \right) ; 1 + \mathbf{e}_S^{\rho,\varepsilon} = \mathbf{s}_S^{\rho,\varepsilon} ; 1 + \mathbf{e}_S^{\rho,\varepsilon},$$

so $\langle \mathbf{s}^{\rho,\varepsilon}, \mathbf{e}^{\rho,\varepsilon} \rangle$ is miracle-free, and

$$\mathbf{s}_S^{\rho,\varepsilon};1 \cdot \mathbf{e}_S^{\rho,\varepsilon} = \left(\mathbf{r}_S^{\rho} \cdot \overline{\mathbf{e}_S^{\rho,\varepsilon}}\right);1 \cdot \mathbf{e}_S^{\rho,\varepsilon} = \mathbf{r}_S^{\rho};1 \cdot \overline{\mathbf{e}_S^{\rho,\varepsilon}} \cdot \mathbf{e}_S^{\rho,\varepsilon} = 0,$$

so $\langle \mathbf{s}^{\rho,\varepsilon}, \mathbf{e}^{\rho,\varepsilon} \rangle$ is demon-proof. Furthermore, because $\langle \mathbf{s}^{\rho,\varepsilon}, \mathbf{e}^{\rho,\varepsilon} \rangle$ is miracle-free, the non-termination domain is entirely determined by the input–output element:

$$\mathbf{e}_S^{\rho,\varepsilon} = \overline{\mathbf{r}_S^{\rho};1} + \mathbf{e}_S^{\rho,\varepsilon} = \overline{\mathbf{r}_S^{\rho};1 \cdot \overline{\mathbf{e}_S^{\rho,\varepsilon}}} = \overline{\left(\mathbf{r}_S^{\rho} \cdot \overline{\mathbf{e}_S^{\rho,\varepsilon}}\right);1} = \overline{\mathbf{s}_S^{\rho,\varepsilon};1}. \tag{49}$$

But now the trouble is that $\langle \mathbf{s}^{\rho,\varepsilon}, \mathbf{e}^{\rho,\varepsilon} \rangle$ may not be correct, because $\mathbf{s}_{S;T}^{\rho,\varepsilon}$ and $\mathbf{s}_{S \text{ or } T}^{\rho,\varepsilon}$ are not determined from $\mathbf{s}_S^{\rho,\varepsilon}$ and $\mathbf{s}_T^{\rho,\varepsilon}$ by ordinary relative multiplication and union. Instead, we have

$$\mathbf{s}_{S;T}^{\rho,\varepsilon} = \mathbf{s}_S^{\rho,\varepsilon};\mathbf{s}_T^{\rho,\varepsilon} \cdot \overline{\mathbf{s}_S^{\rho,\varepsilon};\overline{\mathbf{s}_T^{\rho,\varepsilon};1}}, \tag{50}$$

$$\mathbf{s}_{S \text{ or } T}^{\rho,\varepsilon} = \left(\mathbf{s}_S^{\rho,\varepsilon} + \mathbf{s}_T^{\rho,\varepsilon}\right) \cdot \mathbf{s}_S^{\rho,\varepsilon};1 \cdot \mathbf{s}_T^{\rho,\varepsilon};1, \tag{51}$$

since

$$\begin{aligned}
\mathbf{s}_{S;T}^{\rho,\varepsilon} &= \mathbf{r}_{S;T}^{\rho} \cdot \overline{\mathbf{e}_{S;T}^{\rho,\varepsilon}} && (48)\\
&= \mathbf{r}_S^{\rho};\mathbf{r}_T^{\rho} \cdot \overline{\mathbf{e}_S^{\rho,\varepsilon} + \mathbf{r}_S^{\rho};\mathbf{e}_T^{\rho,\varepsilon}} && \mathbf{39}\\
&= \mathbf{r}_S^{\rho};\mathbf{r}_T^{\rho} \cdot \overline{\mathbf{e}_S^{\rho,\varepsilon}} \cdot \overline{\mathbf{e}_S^{\rho,\varepsilon} \cdot \mathbf{r}_S^{\rho};\mathbf{e}_T^{\rho,\varepsilon}} && \mathbf{3}(\text{xxi})\\
&= \mathbf{r}_S^{\rho};\mathbf{r}_T^{\rho} \cdot \overline{\mathbf{e}_S^{\rho,\varepsilon}} \cdot \overline{\overline{\mathbf{e}_S^{\rho,\varepsilon}} \cdot \mathbf{r}_S^{\rho};\mathbf{e}_T^{\rho,\varepsilon}} && \mathbf{3}(\text{xvi})\\
&= (\mathbf{r}_S^{\rho} \cdot \overline{\mathbf{e}_S^{\rho,\varepsilon}});\mathbf{r}_T^{\rho} \cdot (\mathbf{r}_S^{\rho} \cdot \overline{\mathbf{e}_S^{\rho,\varepsilon}});\mathbf{e}_T^{\rho,\varepsilon} && \mathbf{24}(\text{xxviii})\\
&= (\mathbf{r}_S^{\rho} \cdot \overline{\mathbf{e}_S^{\rho,\varepsilon}});(\mathbf{r}_T^{\rho} \cdot \overline{\mathbf{e}_T^{\rho,\varepsilon}}) \cdot \overline{(\mathbf{r}_S^{\rho} \cdot \overline{\mathbf{e}_S^{\rho,\varepsilon}});\mathbf{e}_T^{\rho,\varepsilon}} && \mathbf{24}(\text{xxiii})\\
&= \mathbf{s}_S^{\rho,\varepsilon};\mathbf{s}_T^{\rho,\varepsilon} \cdot \overline{\mathbf{s}_S^{\rho,\varepsilon};\mathbf{e}_T^{\rho,\varepsilon}} && (48)\\
&= \mathbf{s}_S^{\rho,\varepsilon};\mathbf{s}_T^{\rho,\varepsilon} \cdot \overline{\mathbf{s}_S^{\rho,\varepsilon};\overline{\mathbf{s}_T^{\rho,\varepsilon};1}} && (49)
\end{aligned}$$

and

$$\begin{aligned}
\mathbf{s}_{S \text{ or } T}^{\rho,\varepsilon} &= \mathbf{r}_{S \text{ or } T}^{\rho} \cdot \overline{\mathbf{e}_{S \text{ or } T}^{\rho,\varepsilon}} && (48)\\
&= \left(\mathbf{r}_S^{\rho} + \mathbf{r}_T^{\rho}\right) \cdot \overline{\mathbf{e}_S^{\rho,\varepsilon}} \cdot \overline{\mathbf{e}_T^{\rho,\varepsilon}} && \mathbf{39},\ \mathbf{3}(\text{xvi})\\
&= \left(\mathbf{r}_S^{\rho} \cdot \overline{\mathbf{e}_S^{\rho,\varepsilon}} + \mathbf{r}_T^{\rho} \cdot \overline{\mathbf{e}_T^{\rho,\varepsilon}}\right) \cdot \overline{\mathbf{e}_S^{\rho,\varepsilon}} \cdot \overline{\mathbf{e}_T^{\rho,\varepsilon}} && \mathbf{3}(\text{vii})(\text{viii})(\text{ix})(\text{xv})(\text{xvi})\\
&= \left(\mathbf{s}_S^{\rho,\varepsilon} + \mathbf{s}_T^{\rho,\varepsilon}\right) \cdot \mathbf{s}_S^{\rho,\varepsilon};1 \cdot \mathbf{s}_T^{\rho,\varepsilon};1 && (49),\ (48),\ \mathbf{3}(\text{ii}).
\end{aligned}$$

(The parts of **3** in the third step show that $(x+y)\cdot z = (x+y)\cdot z\cdot z = (x\cdot z + y\cdot z)\cdot z = (x\cdot z\cdot z + y\cdot z)\cdot z = (x\cdot z + y)\cdot z$.)

Formulas (50) and (51) use the "demonic" versions of composition and union (see [1, 3, 38, 39, 55]). The "demonic composition" of x and y is $x;y \cdot \overline{x;\overline{y;1}}$ and the "demonic union" of x and y is $(x+y)\cdot x;1 \cdot y;1$. A similar formula can be derived involving $\mathsf{OR}_{i\in I} S_i$ and the "demonic join" of $\{x_i : i \in I\}$, namely $\sum_{i\in I} x_i \cdot \prod_{i\in I}(x_i;1)$. These formulas suggest it may be possible to start from an arbitrary $\rho : \mathit{Basic} \to A$ and obtain $\mathbf{s}^{\rho,\varepsilon}$ directly by a single inductive definition employing demonic operations in place of ordinary ones, instead of passing first to ε via the definition $\varepsilon_R = \overline{\rho_R;1}$ for every basic $R \in \mathit{Basic}$, thence to $\langle \mathbf{r}^{\rho}, \mathbf{e}^{\rho,\varepsilon} \rangle$ via **39**, and finally to $\mathbf{s}^{\rho,\varepsilon}$ via (48). This may

be true, but it is not yet completely proved. The missing part involves recursion. We only consider languages without recursion. The incorporation of recursion is an open problem discussed at the end of the paper. For all other languages constructs, such a "demonic semantics" [3, 38] is given in the following definition.

Definition 63. For every complete relation algebra $\mathfrak{A}$ and every map $\rho : \mathscr{B}asic \to A$, let $\mathbf{d}^\rho : \mathscr{S}tat(\text{without } \mu) \to A$ be the unique map that satisfies the following conditions:

$$\mathbf{d}^\rho_R = \rho_R \qquad \text{if } R \in \mathscr{B}asic,$$
$$\mathbf{d}^\rho_{S;T} = \mathbf{d}^\rho_S;\mathbf{d}^\rho_T \cdot \overline{\mathbf{d}^\rho_S;\overline{\mathbf{d}^\rho_T;1}},$$
$$\mathbf{d}^\rho_{S \text{ or } T} = (\mathbf{d}^\rho_S + \mathbf{d}^\rho_T) \cdot \mathbf{d}^\rho_S;1 \cdot \mathbf{d}^\rho_T;1,$$
$$\mathbf{d}^\rho_{\mathsf{OR}_{i\in I}S_i} = \sum_{i\in I} \mathbf{d}^\rho_{S_i} \cdot \prod_{i\in I} (\mathbf{d}^\rho_{S_i};1),$$
$$\mathbf{d}^\rho_{\mathsf{if}\ B\ \mathsf{then}\ S\ \mathsf{else}\ T} = \rho_B;\mathbf{d}^\rho_S + \overline{\rho_B;1} \cdot \mathbf{d}^\rho_T,$$
$$\mathbf{d}^\rho_{B\to S} = \rho_B;\mathbf{d}^\rho_S,$$
$$\mathbf{d}^\rho_{\mathsf{IF}_{i\in I}(B_i\to S_i)} = \sum_{i\in I} (\rho_{B_i};\mathbf{d}^\rho_{S_i}) \cdot \prod_{i\in I} (\overline{\rho_{B_i};1} \cdot \mathbf{d}^\rho_{S_i};1),$$
$$\mathbf{d}^\rho_{\mathsf{while}\ B\ \mathsf{do}\ S} = \prod \left\{ x : x \geqslant \overline{\rho_B} \cdot 1' + \rho_B;\mathbf{d}^\rho_S;x \cdot \overline{\rho_B;\mathbf{d}^\rho_S;\overline{x;1}} \right\}.$$

A *demonic interpretation* is any extension $\mathbf{d}^\rho : \mathscr{S}tat(\text{without } \mu) \to A$ obtained from a map $\rho : \mathscr{B}asic \to A$.

Theorem 64. *Let $\mathfrak{A}$ be a complete relation algebra and let $\rho : \mathscr{B}asic \to A$. Define $\varepsilon : \mathscr{B}asic \to A$ by $\varepsilon_R = \overline{\rho_R;1}$ for every $R \in \mathscr{B}asic$. Then $\mathbf{r}^\rho_S \cdot \overline{\mathbf{e}^{\rho,\varepsilon}_S} = \mathbf{d}^\rho_S$ for every $S \in \mathscr{S}tat(\text{without } \mu)$.*

Proof. Define $\mathbf{s}^{\rho,\varepsilon}_S = \mathbf{r}^\rho_S \cdot \overline{\mathbf{e}^{\rho,\varepsilon}_S}$ as in (48) above. By the remarks at the beginning of this section, $\langle \mathbf{r}^\rho, \mathbf{e}^{\rho,\varepsilon} \rangle$ is a miracle-free correct interpretation and (49) holds, i.e., $\mathbf{e}^{\rho,\varepsilon}_S = \overline{\mathbf{s}^{\rho,\varepsilon}_S;1}$ for every S. We will prove, by induction on the complexity of statements, that $\mathbf{s}^{\rho,\varepsilon}_S = \mathbf{d}^\rho_S$ for every S. First suppose S is basic. Then

$$\begin{aligned}
\mathbf{s}^{\rho,\varepsilon}_S &= \mathbf{r}^\rho_S \cdot \overline{\mathbf{e}^{\rho,\varepsilon}_S} && (48)\\
&= \rho_S \cdot \overline{\varepsilon_S} && \mathbf{39}\\
&= \rho_S \cdot \rho_S;1 && \text{definition of } \varepsilon,\ \mathbf{3}(\text{ii})\\
&= \rho_S && \mathbf{24}(\text{xx}),\ \mathbf{7}(\text{v})\\
&= \mathbf{d}^\rho_S && \mathbf{63}.
\end{aligned}$$

As inductive hypotheses for the remaining cases, assume

$$\mathbf{s}^{\rho,\varepsilon}_S = \mathbf{d}^\rho_S, \qquad \mathbf{s}^{\rho,\varepsilon}_T = \mathbf{d}^\rho_T \qquad \mathbf{s}^{\rho,\varepsilon}_{S_i} = \mathbf{d}^\rho_{S_i} \quad \text{for every } i \in I \tag{52}$$

Proof that $\mathbf{s}^{\rho,\varepsilon}_{S;T} = \mathbf{d}^\rho_{S;T}$:

$$\begin{aligned}
\mathbf{s}^{\rho,\varepsilon}_{S;T} &= \mathbf{s}^{\rho,\varepsilon}_S;\mathbf{s}^{\rho,\varepsilon}_T \cdot \overline{\mathbf{s}^{\rho,\varepsilon}_S;\overline{\mathbf{s}^{\rho,\varepsilon}_T;1}} && (50)\\
&= \mathbf{d}^\rho_S;\mathbf{d}^\rho_T \cdot \overline{\mathbf{d}^\rho_S;\overline{\mathbf{d}^\rho_T;1}} && (52)\\
&= \mathbf{d}^\rho_{S;T} && \mathbf{63}.
\end{aligned}$$

Proof that $\mathbf{s}^{\rho,\varepsilon}_{S \text{ or } T} = \mathbf{d}^{\rho}_{S \text{ or } T}$:

$$\begin{aligned}
\mathbf{s}^{\rho,\varepsilon}_{S \text{ or } T} &= \left(\mathbf{s}^{\rho,\varepsilon}_{S} + \mathbf{s}^{\rho,\varepsilon}_{T}\right) \cdot \mathbf{s}^{\rho,\varepsilon}_{S}; 1 \cdot \mathbf{s}^{\rho,\varepsilon}_{T}; 1 && (51)\\
&= \left(\mathbf{d}^{\rho}_{S} + \mathbf{d}^{\rho}_{T}\right) \cdot \mathbf{d}^{\rho}_{S}; 1 \cdot \mathbf{d}^{\rho}_{T}; 1 && (52)\\
&= \mathbf{d}^{\rho}_{S \text{ or } T} && \mathbf{63}.
\end{aligned}$$

To prove that $\mathbf{s}^{\rho,\varepsilon}_{\mathsf{OR}_{i\in I} S_i} = \mathbf{d}^{\rho}_{\mathsf{OR}_{i\in I} S_i}$, first note that

$$\sum_{i\in I} \mathbf{r}^{\rho}_{S_i} \cdot \prod_{i\in I} \overline{\mathbf{e}^{\rho,\varepsilon}_{S_i}} = \sum_{i\in I} \left(\mathbf{r}^{\rho}_{S_i} \cdot \overline{\mathbf{e}^{\rho,\varepsilon}_{S_i}}\right) \cdot \prod_{i\in I} \overline{\mathbf{e}^{\rho,\varepsilon}_{S_i}} \tag{53}$$

since

$$\begin{aligned}
\sum_{i\in I} \mathbf{r}^{\rho}_{S_i} \cdot \prod_{i\in I} \overline{\mathbf{e}^{\rho,\varepsilon}_{S_i}} &= \sum_{i\in I} \left(\mathbf{r}^{\rho}_{S_i} \cdot \prod_{j\in I} \overline{\mathbf{e}^{\rho,\varepsilon}_{S_j}}\right) \cdot \prod_{i\in I} \overline{\mathbf{e}^{\rho,\varepsilon}_{S_i}} && \mathbf{3}(\text{vii}),\ \mathbf{16}\\
&\leqslant \sum_{i\in I} \left(\mathbf{r}^{\rho}_{S_i} \cdot \overline{\mathbf{e}^{\rho,\varepsilon}_{S_i}}\right) \cdot \prod_{i\in I} \overline{\mathbf{e}^{\rho,\varepsilon}_{S_i}} && \mathbf{1}(\text{v}),\ \mathbf{7}(\text{iii})(\text{iv}),\ \mathbf{9}(\text{iii})\\
&\leqslant \sum_{i\in I} \mathbf{r}^{\rho}_{S_i} \cdot \prod_{i\in I} \overline{\mathbf{e}^{\rho,\varepsilon}_{S_i}} && \mathbf{7}(\text{iii})(\text{iv}),\ \mathbf{9}(\text{iii})
\end{aligned}$$

so

$$\begin{aligned}
\mathbf{s}^{\rho,\varepsilon}_{\mathsf{OR}_{i\in I} S_i} &= \mathbf{r}^{\rho}_{\mathsf{OR}_{i\in I} S_i} \cdot \overline{\mathbf{e}^{\rho,\varepsilon}_{\mathsf{OR}_{i\in I} S_i}} && (48)\\
&= \sum_{i\in I} \mathbf{r}^{\rho}_{S_i} \cdot \overline{\sum_{i\in I} \mathbf{e}^{\rho,\varepsilon}_{S_i}} && \mathbf{39}\\
&= \sum_{i\in I} \mathbf{r}^{\rho}_{S_i} \cdot \prod_{i\in I} \overline{\mathbf{e}^{\rho,\varepsilon}_{S_i}} && \mathbf{8}(\text{ii})\\
&= \sum_{i\in I} \left(\mathbf{r}^{\rho}_{S_i} \cdot \overline{\mathbf{e}^{\rho,\varepsilon}_{S_i}}\right) \cdot \prod_{i\in I} \overline{\mathbf{e}^{\rho,\varepsilon}_{S_i}} && (53)\\
&= \sum_{i\in I} \mathbf{d}^{\rho}_{S_i} \cdot \prod_{i\in I} \left(\mathbf{d}^{\rho}_{S_i}; 1\right) && (48),\ (49),\ (52),\ \mathbf{3}(\text{ii})\\
&= \mathbf{d}^{\rho}_{\mathsf{OR}_{i\in I} S_i} && \mathbf{63}.
\end{aligned}$$

Proof that $\mathbf{s}^{\rho,\varepsilon}_{\mathsf{if}\, B \,\mathsf{then}\, S \,\mathsf{else}\, T} = \mathbf{d}^{\rho}_{\mathsf{if}\, B \,\mathsf{then}\, S \,\mathsf{else}\, T}$:

$$\begin{aligned}
\mathbf{s}^{\rho,\varepsilon}_{\mathsf{if}\, B \,\mathsf{then}\, S \,\mathsf{else}\, T} &= \mathbf{r}^{\rho}_{\mathsf{if}\, B \,\mathsf{then}\, S \,\mathsf{else}\, T} \cdot \overline{\mathbf{e}^{\rho,\varepsilon}_{\mathsf{if}\, B \,\mathsf{then}\, S \,\mathsf{else}\, T}} && (48)\\
&= \left(\rho_B; \mathbf{r}^{\rho}_{S} + \overline{\rho_B; 1} \cdot \mathbf{r}^{\rho}_{T}\right) \cdot \rho_B; \overline{\mathbf{e}^{\rho,\varepsilon}_{S} + \overline{\rho_B; 1} \cdot \mathbf{e}^{\rho,\varepsilon}_{T}} && \mathbf{39}\\
&= \left(\rho_B; 1 \cdot \mathbf{r}^{\rho}_{S} + \overline{\rho_B; 1} \cdot \mathbf{r}^{\rho}_{T}\right) \cdot \rho_B; 1 \cdot \overline{\mathbf{e}^{\rho,\varepsilon}_{S} + \overline{\rho_B; 1} \cdot \mathbf{e}^{\rho,\varepsilon}_{T}} && \rho_B \leqslant 1',\ \mathbf{24}(\text{xxxi})\\
&= \rho_B; 1 \cdot \left(\mathbf{r}^{\rho}_{S} \cdot \overline{\mathbf{e}^{\rho,\varepsilon}_{S}}\right) + \overline{\rho_B; 1} \cdot \left(\mathbf{r}^{\rho}_{T} \cdot \overline{\mathbf{e}^{\rho,\varepsilon}_{T}}\right) && \mathbf{3}(\text{ix})(\text{xx})\\
&= \rho_B; 1 \cdot \mathbf{s}^{\rho,\varepsilon}_{S} + \overline{\rho_B; 1} \cdot \mathbf{s}^{\rho,\varepsilon}_{T} && (48)\\
&= \rho_B; \mathbf{s}^{\rho,\varepsilon}_{S} + \overline{\rho_B; 1} \cdot \mathbf{s}^{\rho,\varepsilon}_{T} && \rho_B \leqslant 1',\ \mathbf{24}(\text{xxxi})\\
&= \rho_B; \mathbf{d}^{\rho}_{S} + \overline{\rho_B; 1} \cdot \mathbf{d}^{\rho}_{T} && (52)\\
&= \mathbf{d}^{\rho}_{\mathsf{if}\, B \,\mathsf{then}\, S \,\mathsf{else}\, T} && \mathbf{63}
\end{aligned}$$

Proof that $\mathbf{s}^{\rho,\varepsilon}_{B\to S} = \mathbf{d}^{\rho}_{B\to S}$:

$$\begin{aligned}
\mathbf{s}^{\rho,\varepsilon}_{B\to S} &= \mathbf{r}^{\rho}_{B\to S} \cdot \overline{\mathbf{e}^{\rho,\varepsilon}_{B\to S}} && (48)\\
&= \rho_B ; \mathbf{r}^{\rho}_{S} \cdot \overline{\overline{\rho_B ; 1} + \mathbf{e}^{\rho,\varepsilon}_{S}} && \mathbf{39}\\
&= \rho_B ; \mathbf{r}^{\rho}_{S} \cdot \left(\rho_B ; 1 \cdot \overline{\mathbf{e}^{\rho,\varepsilon}_{S}}\right) && \mathbf{3}(\mathrm{ii})(\mathrm{xvi})\\
&= \rho_B ; \left(\mathbf{r}^{\rho}_{S} \cdot \overline{\mathbf{e}^{\rho,\varepsilon}_{S}}\right) && \rho_B \leqslant 1', \ \mathbf{24}(\mathrm{xxxi})(\mathrm{xxxiv})\\
&= \rho_B ; \mathbf{s}^{\rho,\varepsilon}_{S} && (48)\\
&= \rho_B ; \mathbf{d}^{\rho}_{S} && (52)\\
&= \mathbf{d}^{\rho}_{B\to S} && \mathbf{63}.
\end{aligned}$$

Proof that $\mathbf{s}^{\rho,\varepsilon}_{\mathsf{IF}_{i\in I}(B_i\to S_i)} = \mathbf{d}^{\rho}_{\mathsf{IF}_{i\in I}(B_i\to S_i)}$:

$$\begin{aligned}
\mathbf{s}^{\rho,\varepsilon}_{\mathsf{IF}_{i\in I}(B_i\to S_i)} &= \mathbf{r}^{\rho}_{\mathsf{IF}_{i\in I}(B_i\to S_i)} \cdot \overline{\mathbf{e}^{\rho,\varepsilon}_{\mathsf{IF}_{i\in I}(B_i\to S_i)}}\\
&\qquad (48)\\
&= \sum_{i\in I} \left(\rho_{B_i} ; \mathbf{r}^{\rho}_{S_i}\right) \cdot \overline{\prod_{i\in I} \overline{\rho_{B_i} ; 1} + \sum_{i\in I} \left(\rho_{B_i} ; \mathbf{e}^{\rho,\varepsilon}_{S_i}\right)}\\
&\qquad \mathbf{39}\\
&= \sum_{i\in I} \left(\rho_{B_i} ; \mathbf{r}^{\rho}_{S_i}\right) \cdot \sum_{i\in I} \left(\rho_{B_i} ; 1\right) \cdot \prod_{i\in I} \overline{\rho_{B_i} ; \mathbf{e}^{\rho,\varepsilon}_{S_i}}\\
&\qquad \mathbf{3}(\mathrm{ii})(\mathrm{ix})(\mathrm{xvi}),\ \mathbf{8}(\mathrm{ii})(\mathrm{iii})\\
&= \sum_{i\in I} \left(\rho_{B_i} ; \mathbf{r}^{\rho}_{S_i}\right) \cdot \prod_{i\in I} \overline{\rho_{B_i} ; \mathbf{e}^{\rho,\varepsilon}_{S_i}}\\
&\qquad \mathbf{7}(\mathrm{ii})(\mathrm{v}),\ \mathbf{24}(\mathrm{x}),\ \mathbf{9}(\mathrm{iii})\\
&= \sum_{i\in I} \left(\rho_{B_i} ; \mathbf{r}^{\rho}_{S_i} \cdot \overline{\rho_{B_i} ; \mathbf{e}^{\rho,\varepsilon}_{S_i}}\right) \cdot \prod_{i\in I} \overline{\rho_{B_i} ; \mathbf{e}^{\rho,\varepsilon}_{S_i}}\\
&\qquad \text{see proof of (53)}\\
&= \sum_{i\in I} \left(\rho_{B_i} ; \mathbf{r}^{\rho}_{S_i} \cdot \overline{\mathbf{e}^{\rho,\varepsilon}_{S_i}}\right) \cdot \prod_{i\in I} \overline{\rho_{B_i} ; \mathbf{e}^{\rho,\varepsilon}_{S_i}}\\
&\qquad \rho_{B_i} \leqslant 1', \ \mathbf{24}(\mathrm{xxxv})\\
&= \sum_{i\in I} \left(\rho_{B_i} ; \left(\mathbf{r}^{\rho}_{S_i} \cdot \overline{\mathbf{e}^{\rho,\varepsilon}_{S_i}}\right)\right) \cdot \prod_{i\in I} \left(\overline{\rho_{B_i} ; 1} + \overline{\mathbf{e}^{\rho,\varepsilon}_{S_i}}\right)\\
&\qquad \rho_{B_i} \leqslant 1', \ \mathbf{24}(\mathrm{xxxi}),\ \mathbf{3}(\mathrm{ix})(\mathrm{xvii})\\
&= \sum_{i\in I} \left(\rho_{B_i} ; \mathbf{d}^{\rho}_{S_i}\right) \cdot \prod_{i\in I} \left(\overline{\rho_{B_i} ; 1} + \mathbf{d}^{\rho}_{S_i} ; 1\right)\\
&\qquad (48),\ (49),\ (52),\ \mathbf{3}(\mathrm{ii})\\
&= \mathbf{d}^{\rho}_{\mathsf{IF}_{i\in I}(B_i\to S_i)}\\
&\qquad \mathbf{63}.
\end{aligned}$$

Next we prove $\mathbf{s}^{\rho,\varepsilon}_{\mathsf{while}\,B\,\mathsf{do}\,S} = \mathbf{d}^{\rho}_{\mathsf{while}\,B\,\mathsf{do}\,S}$. To cut the amount of notation involved, introduce some abbreviations. Let

$$\begin{aligned}
b &= \rho_B, & r &= \mathbf{r}^{\rho}_{S}, & w &= \mathbf{r}^{\rho}_{\mathsf{while}\,B\,\mathsf{do}\,S},\\
d &= \mathbf{d}^{\rho}_{\mathsf{while}\,B\,\mathsf{do}\,S}, & e &= \mathbf{e}^{\rho,\varepsilon}_{S}, & n &= \mathbf{e}^{\rho,\varepsilon}_{\mathsf{while}\,B\,\mathsf{do}\,S}.
\end{aligned}$$

Then $\mathbf{s}^{\rho,\varepsilon}_{\mathsf{while}\,B\,\mathsf{do}\,S} = w \cdot \overline{n}$ and the inductive hypotheses (52) yield

$$\mathbf{d}^{\rho}_{S} = r \cdot \overline{e}. \tag{54}$$

We wish to show that $w \cdot \bar{n} = d$. By **39**, **63**, and (54) we have

$$w = \prod \{ x : x \geqslant \bar{b} \cdot 1' + b;r;x \}, \tag{55}$$

$$n = \sum \{ y : y \leqslant b;e + b;r;y \}, \tag{56}$$

$$d = \prod \left\{ x : x \geqslant \bar{b} \cdot 1' + b;(r \cdot \bar{e});x \cdot \overline{b;(r \cdot \bar{e});\overline{x;1}} \right\}. \tag{57}$$

Let h be the function $\overline{b;e} \cdot \overline{b;r;(\text{-})}$. Note that h is monotonic. It follows from (56) by **3**(ii)(xvi) and **8**(ii) that

$$\bar{n} = \prod \{ y : y \geqslant \overline{b;e} \cdot \overline{b;r;\bar{y}} \} = \prod \{ y : y \geqslant h(y) \},$$

so $\bar{n}$ is the least fixed point of h by **22**. In particular,

$$h(\bar{n}) = \bar{n}. \tag{58}$$

The interpretation is miracle-free, so $\bar{e} \leqslant r;1$ and $\bar{n} \leqslant w;1$. We derive a different form for h.

$$\begin{aligned}
h(x) &= \overline{b;e} \cdot \overline{b;r;\bar{x}} && \text{definition of } h \\
&= \overline{b;e + b;r;\bar{x}} && \mathbf{3}(\text{xvi}) \\
&= \overline{b;1 \cdot (e + b;r;\bar{x})} && b \leqslant 1', \ \mathbf{24}(\text{xxxi}), \ \mathbf{3}(\text{xv}) \\
&= \overline{b;1} + \bar{e} \cdot \overline{b;r;\bar{x}} && \mathbf{3}(\text{xvi})(\text{xvii}) \\
&= \overline{b;1} + \bar{e} \cdot b;1 \cdot r;1 \cdot \overline{b;r;\bar{x}} && \mathbf{3}(\text{viii})(\text{ix})(\text{xxi}), \ \bar{e} \leqslant r;1, \ \mathbf{7}(\text{v}) \\
&= \overline{b;1} + \bar{e} \cdot b;r;1 \cdot \overline{b;r;\bar{x}} && b \leqslant 1', \ \mathbf{24}(\text{xxxi}) \\
&= \overline{b;1} + \bar{e} \cdot b;r;x \cdot \overline{b;r;\bar{x}} && \mathbf{24}(\text{xxiii})
\end{aligned}$$

so

$$h(x) = \overline{b;1} + \bar{e} \cdot b;r;x \cdot \overline{b;r;\bar{x}}. \tag{59}$$

Let f be the function $\bar{b} \cdot 1' + b;(r \cdot \bar{e});(\text{-}) \cdot \overline{b;(r \cdot \bar{e});\overline{(\text{-});1}}$. Note that f is monotonic, $d = \prod \{ x : x \geqslant f(x) \}$, d is the least fixed point of f by **22**, and

$$\begin{aligned}
f(x) &= \bar{b} \cdot 1' + b;(r \cdot \bar{e});x \cdot \overline{b;(r \cdot \bar{e});\overline{x;1}} && \text{definition of } f \\
&= \bar{b} \cdot 1' + (b;r \cdot \bar{e});x \cdot \overline{(b;r \cdot \bar{e});\overline{x;1}} && b \leqslant 1', \ \mathbf{24}(\text{xxxi}), \ \mathbf{3}(\text{ix}) \\
&= \bar{b} \cdot 1' + \bar{e} \cdot b;r;x \cdot \overline{\bar{e} \cdot b;r;\overline{x;1}} && \mathbf{53}, \ \mathbf{26}(\text{ii}), \ \mathbf{24}(\text{xxvi}) \\
&= \bar{b} \cdot 1' + \bar{e} \cdot b;r;x \cdot \overline{b;r;\overline{x;1}} && \mathbf{3}(\text{viii})(\text{ix})(\text{xiii})(\text{xvii})
\end{aligned}$$

so

$$f(x) = \bar{b} \cdot 1' + \bar{e} \cdot b;r;x \cdot \overline{b;r;\overline{x;1}}, \tag{60}$$

$$f(d) = d. \tag{61}$$

We get $w \geqslant f(w \cdot \overline{n})$ as follows. By **22**, w is the least fixed point of the monotonic function $\overline{b} \cdot 1' + b;r;(\text{-})$, so

$$w = \overline{b} \cdot 1' + b;r;w, \tag{62}$$

$f(w \cdot \overline{n})$	$\leqslant f(w)$	f is monotonic
	$= \overline{b} \cdot 1' + \overline{e} \cdot b;r;w \cdot \overline{b;r;\overline{w;1}}$	(60)
	$\leqslant \overline{b} \cdot 1' + b;r;w$	**7**(iv)
	$= w$	(62),

and we get $\overline{n} \geqslant f(w \cdot \overline{n})$ as follows:

$f(w \cdot \overline{n})$	$\leqslant f(\overline{n})$	f is monotonic
	$= \overline{b;1} \cdot 1' + \overline{e} \cdot b;r;\overline{n} \cdot \overline{b;r;\overline{\overline{n};1}}$	(60), $b \leqslant 1'$, **24**(xxxii)
	$\leqslant \overline{b;1} + \overline{e} \cdot b;r;\overline{n} \cdot \overline{b;r;\overline{\overline{n}}}$	**53**, **26**(iii), **7**(ii)
	$= h(\overline{n})$	(59)
	$= \overline{n}$	(58).

Thus, we conclude that $d \leqslant w \cdot \overline{n}$. From this we get $d;1 \leqslant (w \cdot \overline{n});1 \leqslant \overline{n};1 = \overline{n}$. Therefore $\overline{n} = d;1$ and $\overline{d;1} = n$. Next, observe that

$d;1$	$= f(d);1$	(61)
	$= \left(\overline{b} \cdot 1' + \overline{e} \cdot b;r;d \cdot \overline{b;r;\overline{d;1}}\right);1$	(60)
	$= (\overline{b} \cdot 1');1 + \left(\overline{e} \cdot b;r;d \cdot \overline{b;r;\overline{d;1}}\right);1$	(Ra_2)
	$= \overline{b;1} + \overline{e} \cdot b;r;d;1 \cdot \overline{b;r;\overline{d;1}}$	$b \leqslant 1'$, **53**, **24**(xxvi)(xxviii)(xxxii), **26**(i)–(iii)
	$= h(d;1)$	(59).

Thus $d;1$ is a fixed point of h, but $\overline{n}$ is the least fixed point of h, so we have $\overline{n} \leqslant d;1$. For the final step, first recall that $n = b;e + b;r;n$. Then $\overline{n} = \overline{b;e} \cdot \overline{b;r;n} = \overline{b;e} \cdot \overline{b;r;\overline{d;1}}$, so

$\overline{b} \cdot 1' + b;r;(d+n)$	$= \overline{b} \cdot 1' + b;r;d + b;r;n$	**24**(ix)
	$\leqslant \overline{b} \cdot 1' + b;r;d + n$	since $b;r;n \leqslant n$
	$= \overline{b} \cdot 1' + b;r;d \cdot \overline{n} + n$	**3**(xxi)
	$= \overline{b} \cdot 1' + b;r;d \cdot \overline{b;r;\overline{d;1}} \cdot \overline{b;e} + n$	remark above
	$= \overline{b} \cdot 1' + \overline{e} \cdot b;r;d \cdot \overline{b;r;\overline{d;1}} + n$	$b \leqslant 1'$, **24**(xxxv), **3**(viii)(ix
	$= f(d) + n$	(60)
	$= d + n$	(61).

Thus $d + n$ is contracted by the function $\overline{b} \cdot 1' + b;r;(\text{-})$, but w is the least such element, so $w \leqslant d + n$, which implies $w \cdot \overline{n} \leqslant d$. Combined with $d \leqslant w \cdot \overline{n}$, this gives us $w \cdot \overline{n} = d$, as desired. □

Most of the following corollary is proved for $\mathfrak{A} = \mathfrak{Re}(U)$ in [38]. A proof of part (v) appears in [48, p. 175].

Corollary 65. *Assume $\mathfrak{A}$ is a complete relation algebra, $\rho : \mathit{Basic} \to A$, and $\mathbf{d}^\rho$ is a demonic $\mathfrak{A}$-interpretation of Stat(without μ). Define $\mathrm{wp}'_S(\text{-}) : A \to A$ by $\mathrm{wp}'_S(x) = \overline{\mathbf{d}^\rho_S;\bar{x} \cdot \mathbf{d}^\rho_S;1}$ for every $S \in \mathit{Stat}$(without μ). Then*

(i) $\mathrm{wp}'_{\mathsf{skip}}(x) = x$.
(ii) $\mathrm{wp}'_{\mathsf{abort}}(x) = 0$.
(iii) $\mathrm{wp}'_{\mathsf{havoc}}(x) = 0 \dagger x$.
(iv) $\mathrm{wp}'_{\mathsf{havoc}}(1) = 1$.
(v) $\mathrm{wp}'_{S;T}(x) = \mathrm{wp}'_S(\mathrm{wp}'_T(x))$.
(vi) $\mathrm{wp}'_{S \text{ or } T}(x) = \mathrm{wp}'_S(x) \cdot \mathrm{wp}'_T(x)$.
(vii) $\mathrm{wp}'_{\mathsf{OR}_{i\in I} S_i}(x) = \prod_{i\in I} \mathrm{wp}'_{S_i}(x)$.
(viii) $\mathrm{wp}'_{\mathsf{if}\, B \,\mathsf{then}\, S \,\mathsf{else}\, T}(x) = \rho_B;\mathrm{wp}'_S(x) + \overline{\rho_B;1} \cdot \mathrm{wp}'_T(x)$.
(ix) $\mathrm{wp}'_{B\to S}(x) = \rho_B;\mathrm{wp}'_S(x)$.
(x) $\mathrm{wp}'_{\mathsf{IF}_{i\in I}(B_i \to S_i)}(x) = \prod_{i\in I}\left(\overline{\rho_{B_i};1} + \mathrm{wp}'_{S_i}(x)\right) \cdot \sum_{i\in I}(\rho_{B_i};1)$.
(xi) $\mathrm{wp}'_{\mathsf{while}\, B \,\mathsf{do}\, S}(x) = \prod\{\, y : y \geqslant (\rho_B;1 + x) \cdot \left(\overline{\rho_B;1} + \mathrm{wp}'_S(y)\right)\}$.
(xii) $\mathrm{wp}'_{\mathsf{while}\, B \,\mathsf{do}\, S}(x) = \prod\{\, y : y \geqslant \overline{\rho_B;1} \cdot x + \rho_B;\mathrm{wp}'_S(y)\}$.

Proof. According to the remarks at the beginning of this section we start with ρ, define ε, and get the correct miracle-free $\mathfrak{A}$-interpretation $\langle \mathbf{r}^\rho, \mathbf{e}^{\rho,\varepsilon}\rangle$ with its predicate transformer $\mathrm{wp}_{(\text{-})}(\text{-})$ to which **57** applies. For every $S \in \mathit{Stat}$(without μ) we have $\mathbf{r}^\rho_S \cdot \overline{\mathbf{e}^{\rho,\varepsilon}_S} = \mathbf{d}^\rho_S$ by (48) and **64**, hence $\overline{\mathbf{e}^{\rho,\varepsilon}_S} = \mathbf{d}^\rho_S;1$ by (48) and (49), so, by the remarks and computation preceding **34**, we have

$$\mathrm{wp}'_S(x) = \overline{\mathbf{d}^\rho_S;\bar{x}} \cdot \mathbf{d}^\rho_S;1 = \overline{\left(\mathbf{r}^\rho_S \cdot \overline{\mathbf{e}^{\rho,\varepsilon}_S}\right);\bar{x}} \cdot \overline{\mathbf{e}^{\rho,\varepsilon}_S} = \mathrm{wp}_S(x).$$

Therefore, all parts of **57** involving $\mathrm{wp}_{(\text{-})}(\text{-})$ also apply to $\mathrm{wp}'_{(\text{-})}(\text{-})$. □

Open Problem. Extend Definition **63** to all of Stat by adding

$$\mathbf{d}^\rho_{\mu X[S]} = \prod\{\, x : x \geqslant \mathbf{d}^\rho(X^x)_S\}, \tag{63}$$

where $\mathbf{d}^\rho(X^x)_{(\text{-})}$ is the extension obtained by reassigning ρ from ρ_X to x. Does Theorem **64** extend as well?

This problem amounts to asking whether one can show $\mathbf{r}^\rho_{\mu X[S]} \cdot \overline{\mathbf{e}^{\rho,\varepsilon}_{\mu X[S]}} = \mathbf{d}^\rho_{\mu X[S]}$ for every S. It seems reasonable to conjecture that this can be done, but one of the difficulties encountered is that $\mathbf{d}^\rho(X^{(\text{-})})_S$ may not be monotonic. Here is a case in which this happens that may also serve as a test case for proving this conjecture. Suppose X does not occur free R or T. Let $S = \mu X[\mathsf{if}\, B \,\mathsf{then}\, R;X;X \,\mathsf{else}\, T]$. As inductive hypotheses assume $\mathbf{r}^\rho_R \cdot \overline{\mathbf{e}^{\rho,\varepsilon}_R} = \mathbf{d}^\rho_R$ and $\mathbf{r}^\rho_T \cdot \overline{\mathbf{e}^{\rho,\varepsilon}_T} = \mathbf{d}^\rho_T$. The problem is to prove $w \cdot n = d$, where

$$w = \mathbf{r}^\rho_{\mu X[\mathsf{if}\, B \,\mathsf{then}\, R;X;X \,\mathsf{else}\, T]}, \quad n = \overline{\mathbf{e}^{\rho,\varepsilon}_{\mu X[\mathsf{if}\, B \,\mathsf{then}\, R;X;X \,\mathsf{else}\, T]}}, \quad d = \mathbf{d}^\rho_{\mu X[\mathsf{if}\, B \,\mathsf{then}\, R;X;X \,\mathsf{else}\, T]}.$$

By **39**, **63**, (63), and the inductive hypotheses,

$$
\begin{aligned}
w &= \prod \left\{ x : x \geqslant \rho_B ; \mathbf{r}_R^\rho ; x ; x + \overline{\rho_B ; 1} \cdot \mathbf{r}_T^\rho \right\}, \\
n &= \prod \left\{ x : x \geqslant \rho_B ; 1 \cdot \overline{\mathbf{e}_R^{\rho,\varepsilon}} \cdot \overline{\mathbf{r}_R^\rho ; \overline{x}} \cdot \overline{\mathbf{r}_R^\rho ; w ; \overline{x}} + \overline{\rho_B ; 1} \cdot \overline{\mathbf{e}_T^{\rho,\varepsilon}} \right\}, \\
d &= \prod \left\{ x : x \geqslant \rho_B ; 1 \cdot \mathbf{d}_R^\rho ; x ; x \cdot \overline{\mathbf{d}_R^\rho ; \overline{x ; 1}} \cdot \overline{\mathbf{d}_R^\rho ; x ; \overline{x ; 1}} + \overline{\rho_B ; 1} \cdot \mathbf{d}_T^\rho \right\} \\
&= \prod \left\{ x : x \geqslant \rho_B ; 1 \cdot \overline{\mathbf{e}_R^{\rho,\varepsilon}} \cdot \mathbf{r}_R^\rho ; x ; x \cdot \overline{\mathbf{r}_R^\rho ; \overline{x ; 1}} \cdot \overline{\mathbf{r}_R^\rho ; x ; \overline{x ; 1}} + \overline{\rho_B ; 1} \cdot \mathbf{r}_T^\rho \cdot \overline{\mathbf{e}_T^{\rho,\varepsilon}} \right\},
\end{aligned}
$$

so the problem in this case is to show that the intersection of the least fixed points of the monotonic functions $\rho_B ; \mathbf{r}_R^\rho ; (\text{-}) ; (\text{-}) + \overline{\rho_B ; 1} \cdot \mathbf{r}_T^\rho$ and $\rho_B ; 1 \cdot \overline{\mathbf{e}_R^{\rho,\varepsilon}} \cdot \overline{\mathbf{r}_R^\rho ; \overline{(\text{-})}} \cdot \overline{\mathbf{r}_R^\rho ; w ; \overline{(\text{-})}} + \overline{\rho_B ; 1} \cdot \overline{\mathbf{e}_T^{\rho,\varepsilon}}$ is the meet of all elements contracted by the nonmonotonic function $\rho_B ; 1 \cdot \overline{\mathbf{e}_R^{\rho,\varepsilon}} \cdot \mathbf{r}_R^\rho ; (\text{-}) ; (\text{-}) \cdot \overline{\mathbf{r}_R^\rho ; \overline{(\text{-}) ; 1}} \cdot \overline{\mathbf{r}_R^\rho ; (\text{-}) ; \overline{(\text{-}) ; 1}} + \overline{\rho_B ; 1} \cdot \mathbf{r}_T^\rho \cdot \overline{\mathbf{e}_T^{\rho,\varepsilon}}$.

Acknowledgement

For (alphabetically) advice, comments, criticism, encouragement, invitations, patience, and suggestions at various stages in the development of this paper and its predecessor [34], I would like to thank (alphabetically) Chris Brink, Willem-Paul de Roever, Maurice Nivat, and Giuseppe Scollo.

References

[1] R. Backhouse and J. van der Woude, *Demonic operators and monotype factors*, Tech. Report, Eindhoven, 1993.

[2] H. Bekić, *Definable operations in general algebras, and the theory of automata and flowcharts*, Tech. Report, IBM Laboratory, Vienna, 1969.

[3] R. Berghammer and H. Zierer, Relational algebraic semantics of deterministic and nondeterministic programs, *Theoret. Comput. Sci.* **43** (1986) 123–147.

[4] G. Boole, *The Mathematical Analysis of Logic; Being an Essay Towards a Calculus of Deductive Reasoning* (B. Blackwell, Oxford, 1948, first published in London and Cambridge, 1847).

[5] M. Broy, R. Gnatz and M. Wirsing, Semantics of nondeterministic and noncontinuous constructs, in: F. L. Bauer and M. Broy, eds., Program Construction Lecture Notes in Computer Science, Vol. 69 (Springer, Berlin, 1979) International Summer School, Marktoberdorf (1978), 553–592.

[6] L.H. Chin and A. Tarski, *Distributive and modular laws in the arithmetic of relation algebras*, University of California Publications in Mathematics, New Series Vol. **1** (1951) 341–384.

[7] P. Cousot, *Methods and Logics for Proving Programs*, in: J. van Leeuwen, ed., *Handbook of Theoretical Computer Science, Vol. B, Formal Models and Semantics* (Elsevier, Amsterdam, 1990) 841–993.

[8] J.W. de Bakker, Semantics and termination of nondeterministic recursive programs, in: S. Michaelson and R. Milner, eds., *Proc. 3rd Internat. Coll. on Automata, Languages, and Programming* (Edinburgh Univ. Press, Edinburg 1976) 436–477.

[9] J.W. de Bakker, *Mathematical Theory of Program Correctness*, (Prentice-Hall, Englewood Cliffs, NJ, 1980).

[10] J.W. de Bakker and W.-P. de Roever, A calculus for recursive program schemes, in: M. Nivat ed., *Proc. 1st Internat. Coll. on Automata, Languages, and Programming, Proc. Symp. (IRIA)*, 3–7 July 1972, Rocquencourt, (North-Holland, Amsterdam 1973), 167–196.

[11] W.-P. de Roever, Recursion and parameter mechanisms: an axiomatic approach, in: (J. Loeckx, ed.) *Proc. 2nd Internat. Coll. on Automata, Languages, and Programming*, Lecture Notes in Computer Science, Vol. 14 (Springer, Berlin 1973) 34–65.

[12] W.P. de Roever, *Recursive Program Schemes: Semantics and Proof Theory* Mathematical Centre Tracts, Vol. 70, Centre for Mathematics and Computer Science (1976), ix+112.

[13] E.W. Dijkstra, Guarded commands, nondeterminacy, and formal derivation of programs, *Comm. ACM* (1975) 453–457.

[14] E.W. Dijkstra, *A Discipline of Programming*, (Prentice-Hall, Englewoods Cliffs, NJ, 1976).

[15] E.W. Dijkstra and C.S. Scholten, *Predicate Calculus and Program Semantics*, Texts and Monographs in Computer Science (Springer, New York, 1990).

[16] L. Henkin, J. Donald Monk, and A. Tarski, *Cylindric Algebras, Part I*, (North-Holland, Amsterdam, 1971).

[17] P. Hitchcock and D.M.R. Park, Induction rules and termination proofs, in: M. Nivat, ed., *Proc. 1st Internat. Coll. on Automata, Languages, and Programming, Proc. Symp. (IRIA)*, 3-7 July 1972, Rocquencourt, (North-Holland, Amsterdam 1973) 225–251.

[18] C.A.R. Hoare, I.J. Hayes, He Jifeng, C. C. Morgan, A. W. Roscoe, J. W. Sanders, I. H. Sorenson, J. M. Spivey and B. A. Sufrin, *Laws of programming*, Comm. A C M. (1987) 672–686, 770.

[19] C.A.R. Hoare and He Jifeng, The weakest prespecification, Part I, *Fund. Inform.* **9** (1986) 51–84.

[20] C.A.R. Hoare and He Jifeng, The weakest prespecification, Part II, *Fund. Inform.* **9** (1986) 217–252.

[21] E.V. Huntington, New sets of independent postulates for the algebra of logic, with special reference to Whitehead and Russell's Principia Mathematica, *Trans. Amer. Math. Soc.* **35** (1933) 274–304.

[22] E.V. Huntington, Boolean algebra. A correction, *Trans. Amer. Math. Soc.* **35** (1933) 557–558.

[23] B. Jónsson, Varieties of relation algebras, *Algebra Universalis* **15** (1982) 273–298.

[24] B. Jónsson, The theory of binary relations, in: H. Andréka, J. D. Monk, , and I. Németi, eds. *Algebraic Logic (Proc. Conf., Budapest, 1988)*, Colloq. Math. Soc. J. Bolyai, Vol. 54, (North-Holland, Amsterdam 1991), 245–292.

[25] B. Jónsson and A. Tarski, Representation problems for relation algebras, *Bull. Amer. Math. Soc.* **54** (1948) 80 and 1192, Abstract 89.

[26] B. Jónsson and A. Tarski, Boolean algebras with operators, Part I, *Amer. J. Math.* **73** (1951) 891–939.

[27] B. Jónsson and A. Tarski, Boolean algebras with operators, Part II, *Amer. J. Math.* **74** (1952) 127–162.

[28] B. Knaster, Un Thérème sur les fonctions d'ensembles, Rocznik Polskiego Towarzystwa Matematycznego (Annales de la Société Polonaise de Mathématique) **6** (1927, published 1928) 133–134.

[29] J. Leszczylowski, A theorem on resolving equations in the space of languages, *Bull. Acad. Polon. Sci., Ser. Sci. Math. Astr. Phys.* **19** (1971) 967–970.

[30] R.D. Maddux, Some nonrepresentable relation algebras, *Notices Amer. Math. Soc.* **23** (1976) A–431, A–557.

[31] R.D. Maddux, Finite integral relation algebras, in: *Universal Algebra and Lattice Theory* (Springer, Berlin, 1985) *Proc. Southeastern Conf. in Universal Algebra and Lattice Theory*, Charleston, S.C., July 11-14, 1984, Lecture Notes in Math., Vol. 1149, 175–197.

[32] R.D. Maddux, Introductory course on relation algebras, finite-dimensional cylindric algebras, and their interconnections, in: H. Andréka, J. D. Monk and I. Németi, eds., *Algebraic Logic (Proc. Conf., Budapest 1988)* Colloq. Math. Soc. J. Bolyai, Vol. 54, (North-Holland, Amsterdam 1991), 361–392.

[33] R.D. Maddux, The origin of relation algebras in the development and axiomatization of the calculus of relations, *Studia Logica* **50** (1991) 421–455.

[34] R.D. Maddux, A working relational model: The derivation of the Dijkstra-Scholten predicate transformer semantics from Tarski's axioms for the Peirce-Schröder calculus of relations, *South African Comput. J.* **9** (1993) 92–130.

[35] A. De Morgan, On the symbols of logic, the theory of the syllogism, and in particular of the copula, and the application of the theory of probabilities to some questions in the theory of evidence, *Trans. Cambridge Philos. Soc.* **9** (1856) 79–127, reprinted in [37].

[36] A. De Morgan, On the syllogism, no. IV, and on the logic of relations, *Trans. Cambridge Philos. Soc.* **10** (1864) 331–358, reprinted in [37].

[37] A. De Morgan, *On the Syllogism, and Other Logical Writings*, (Yale Univ. Press, New Haven, 1966), edited, with an Introduction by P. Heath.

[38] T. T. Nguyen, A relational model of demonic nondeterministic programs, *Internat. J. Foundations Comput. Sci.* **2**, (1991) 101–131.

[39] T. T. Nguyen, The connection between predicate logic and demonic relation calculus, Tech. Report CRIN 92-R-187, Centre de Recherche en Informatique de Nancy, 18 November. 1992.
[40] D. Park, Fixpoint induction and proofs of program properties, in: B. Meltzer and D. Richie, eds., *Machine Intelligence*, Vol. 5, (Edinburgh Univ. Press, Edinburgh 1969) 59–77.
[41] D. Park, On the semantics of fair parallelism, *Abstract Software Specification*, Lecture Notes in Computer Science, Vol. 86, (Springer, Berlin 1980) 504–526.
[42] C.S. Peirce, Description of a notation for the logic of relatives, resulting from an amplification of the conceptions of Boole's calculus of logic, Mem. Amer. Academy Sci. **9** (1870) 317–378, (reprinted by Welch, Bigelow and Co., Cambridge, MA 1870 1–62); also reprinted in [45, 46].
[43] C.S. Peirce, On the algebra of logic, *Amer. J. Math.* **3** (1880) 15–57, reprinted in [45].
[44] C.S. Peirce, Note B: the logic of relatives, in: C. S. Peirce, ed., *Studies in Logic by Members of the Johns Hopkins University* (Little, Brown, and Co., Boston, 1883) book reprinted, with an Introduction by M. H. Fisch and a Preface by A. Eschbach, by John Benjamins Publishing Co., Amsterdam and Philadelphia, (1983), lviii, vi+203; paper reprinted in [45, pp. 187–203].
[45] C.S. Peirce, in: C. Hartshorne and Paul Weiss, eds., *Collected Papers, Vol. III*, (Harvard Univ. Press, Cambridge, 1933).
[46] C.S. Peirce, in: E.C. Moore, M.H. Fisch, C.J.W. Kloesel, D.D. Roberts and L.A. Ziegler, eds., *Writings of Charles S. Peirce, A Chronological Edition*, (Indiana Univ. Press, Bloomington, 1984).
[47] G. Schmidt, Programs as partial graphs I: flow equivalence and correctness, *Theoret. Comput. Sci.* **15** (1981) 1–25.
[48] G. Schmidt, Programs as partial graphs II: recursion, *Theoret. Comput. Sci.* **15** (1981), 159–179.
[49] G. Schmidt and T. Ströhlein, in: W. Brauer, G. Rozenberg and A. Salomaa, eds., *Relations and Graphs*, (Springer, Berlin, 1993).
[50] F.W.K. Ernst Schröder, *Vorlesungen über die Algebra der Logik (exacte Logik), Vol. 3, Algebra und Logik der Relative, Part I*, (Chelsea, Bronx, New York), 2nd ed., 1966, first published in Leipzig, 1895.
[51] D.S. Scott and J.W. de Bakker, *A theory of programs*, unpublished seminar notes, 1969.
[52] A. Tarski, On the calculus of relations, *J. Symbolic Logic* **6** (1941) 73–89.
[53] A. Tarski, A lattice-theoretical fixpoint theorem and its applications, *Pacific J. Math.* **5** (1955) 285–309.
[54] A. Tarski and S.R. Givant, *A Formalization of Set Theory without Variables*, Colloquium Publications, Vol. 41. (American Mathematical Society, 1987).
[55] J. van der Woude, Calculations with relations, an example, in: W. Feijen, A. J. M. van Gasteren, D. Gries, and J. Misra, eds., *Beauty is our Business* (Springer, Berlin, 1990), 435–441.