

Least and greatest fixed points of a while semantics function

Fairouz Tchier
Mathematics department,
King Saud University
P.O.Box 22452
Riyadh 11495, Saudi Arabia
ftchier@hotmail.com

May 1, 2009

Abstract

The meaning of a program is given by specifying the function (from input to output) that corresponds to the program. The denotational semantic definition, thus maps syntactical things into functions. A relational semantics is a mapping of programs to relations. We consider that the input-output semantics of a program is given by a relation on its set of states. In a nondeterministic context, this relation is calculated by considering the worst behavior of the program (*demonic relational semantics*). In this paper, we concentrate on while loops. We will present some interesting results about the fixed points of the while semantics function; $f(X) = Q \vee P \circ X$ where $P^< \wedge Q^< = \emptyset$, by taking $P := t \circ B$ and $Q := t^\sim$, one gets the demonic semantics we have assigned to while loops in previous papers. We will show that the least angelic fixed point is equal to the greatest demonic fixed point of the semantics function.

Keywords: Angelic fixed points, demonic fixed points, demonic functions, while loops, relational demonic semantics.

1 Relation Algebras

Both homogeneous and heterogeneous relation algebras are employed in computer science. In this paper, we use heterogeneous relation algebras whose definition is taken from [8, 27, 28].

(1) **Definition.** A *relation algebra* \mathcal{A} is a structure $(B, \vee, \wedge, -, \circ, \smile)$ over a non-empty set B of elements, called *relations*. The unary operations $-, \smile$ are total whereas the binary operations \vee, \wedge, \circ are partial. We denote by $B_{\vee R}$ the set of those elements $Q \in B$ for which the union $R \vee Q$ is defined and we require that $R \in B_{\vee R}$ for every $R \in B$. If $Q \in B_{\vee R}$, we say that Q has the same type as R . The following conditions are satisfied.

- (a) $(B_{\vee R}, \vee, \wedge, -)$ is a Boolean algebra, with zero element 0_R and universal element 1_R . The elements of $B_{\vee R}$ are ordered by *inclusion*, denoted by \leq .
- (b) If the products $P \circ R$ and $Q \circ R$ are defined, so is $P \circ Q^\smile$. If the products $P \circ Q$ and $P \circ R$ are defined, so is $Q^\smile \circ R$. If $Q \circ R$ exists, so does $Q \circ P$ for every $P \in B_{\vee R}$.
- (c) Composition is associative: $P \circ (Q \circ R) = (P \circ Q) \circ R$.

- (d) There are elements ${}_Rid$ and id_R associated to every relation $R \in B$. ${}_Rid$ behaves as a right identity and id_R as a left identity for $B_{\vee R}$.
- (e) The Schröder rule $P \circ Q \leq R \Leftrightarrow P \smile \circ -R \leq -Q \Leftrightarrow -R \circ Q \smile \leq -P$ holds whenever one of the three expressions is defined.
- (f) $1 \circ R \circ 1 = 1$ iff $R \neq 0$ (Tarski rule).

If $R \smile \in B_{\vee R}$, then R is said to be *homogeneous*. If all $R \in \mathcal{A}$ have the same type, the operations are all total and \mathcal{A} itself is said to be *homogeneous*.

For simplicity, the universal, zero, and identity elements are all denoted by $1, 0, id$, respectively. Another operation that occurs in this article is the *reflexive transitive closure* R^* . It satisfies the well-known laws

$$R^* = \bigvee_{i \geq 0} R^i \text{ and } R^* = id \vee R \circ R^* = id \vee R^* \circ R,$$

where $R^0 = id$ and $R^{i+1} = R \circ R^i$. From Definition 1, the usual rules of the calculus of relations can be derived (see, e.g., [8, 10, 28]).

The notion of Galois connections is very important in what follows, there are many definitions of Galois connections [?]. We choose the following one [2].

- (2) **Definition.** Let (S, \leq_S) and $(S', \leq_{S'})$ be two preordered sets. A pair (f, g) of functions, where $f : S \rightarrow S'$ and $g : S' \rightarrow S$, forms a *Galois connections* iff the following formula holds for all $x \in S$ and $y \in S'$.

$$f(x) \leq_{S'} y \Leftrightarrow x \leq_S g(y).$$

The function f is called the *lower adjoint* and g the *upper adjoint*.

2 Monotypes and Related Operators

In the calculus of relations, there are two ways for viewing sets as relations; each of them has its own advantages. The first is via vectors: a relation x is

a *vector* [28] iff $x = x \circ 1$. The second way is via *monotypes* [2]: a relation a is a monotype iff $a \leq id$. The set of monotypes $\{a \mid a \in B_{\vee R}\}$, for a given R , is a complete Boolean lattice. We denote by $a \smile$ the *monotype complement* of a .

The domain and codomain of a relation R can be characterized by the vectors $R \circ 1$ and $R \smile \circ 1$, respectively [15, 28]. They can also be characterized by the corresponding monotypes. In this paper, we take the last approach. In what follows we formally define these operators and give some of their properties.

- (3) **Definition.** The *domain* and *codomain* operators of a relation R , denoted respectively by $R^<$ and $R^>$, are the monotypes defined by the equations

$$(a) \quad R^< = id \wedge R \circ 1,$$

$$(b) \quad R^> = id \wedge 1 \circ R.$$

These operators can also be characterized by Galois connections(see [2, 2]). For each relation R and each monotype a ,

$$R^< \leq a \Leftrightarrow R \leq a \circ 1,$$

$$R^> \leq a \Leftrightarrow R \leq 1 \circ a.$$

The domain and codomain operators are linked by the equation $R^> = R \smile^<$, as is easily checked.

- (4) **Definition.** Let R be a relation and a be a monotype. The *monotype right residual* and *monotype left residual* of a by R (called *factors* in [5]) are defined respectively by

$$(a) \quad a \not\! / R := ((1 \circ a) / R)^> ,$$

$$(b) \quad R \not\! \backslash a := (R \setminus (a \circ 1))^< .$$

An alternative characterization of residuals can also be given by means of a Galois connection as follows [1]:

$$b \leq a \not\! / R \Leftrightarrow (b \circ R)^> \leq a,$$

$$b \leq R \not\! \backslash a \Leftrightarrow (R \circ b)^< \leq a.$$

We have to use exhaustively the complement of the domain of a relation R , i.e the monotype a such that $a = R^< \smile$. To avoid the notation $R^< \smile$, we adopt the Notation

$$R^< := R^{<\sim}.$$

Because we assume our relation algebra to be complete, least and greatest fixed points of monotonic functions exist. We cite [12] as a general reference on fixed points.

Let f be a monotonic function. The following properties of fixed points are used below:

- (a) $\mu f = \bigwedge\{X \mid f(X) = X\} = \bigwedge\{X \mid f(X) \leq X\}$,
- (b) $\nu f = \bigvee\{X \mid f(X) = X\} = \bigvee\{X \mid X \leq f(X)\}$,
- (c) $\mu f \leq \nu f$,
- (d) $f(Y) \leq Y \Rightarrow \mu f \leq Y$,
- (e) $Y \leq f(Y) \Rightarrow Y \leq \nu f$.

In what follows, we describe notions that are useful for the description of the set of initial states of a program for which termination is guaranteed. These notions are *progressive finiteness* and the *initial part* of a relation.

A relation R is progressively finite in terms of points iff there are no infinite chains s_0, \dots, s_i such that $s_i R s_{i+1} \forall i, i \geq 0$. I.e there is no points set y which are the starting points of some path of infinite length. For every point set $y, y \leq R \circ y \Rightarrow y = 0$. The least set of points which are the starting points of paths of finite length i.e from which we can proceed only finitely many steps is called *initial part* of R denoted by $\mathcal{I}(R)$. This topic is of interest in many areas of computer science, mathematics and is related to recursion and induction principle.

(5) **Definition.**

- (a) The *initial part* of a relation R , denoted $\mathcal{I}(R)$, is given by

$$\mathcal{I}(R) = \bigwedge\{a \mid a \leq id : a \not\downarrow R = a\} = \bigwedge\{a \mid a \leq id : a \not\downarrow R \leq a\} = \mu(a : a \leq id : a \not\downarrow R),$$
 where a is a monotype.
- (b) A relation R is said to be *progressively finite* [28] iff $\mathcal{I}(R) = id$.

The description of $\mathcal{I}(R)$ by the formulation $a \not\downarrow R = a$ shows that $\mathcal{I}(R)$ exists, since $(a \mid a \leq id : a \not\downarrow R)$ is monotonic in the first argument and because the set of monotypes is a complete lattice, it follows from the fixed point theorem of Knaster and Tarski that this function has a least fixed point. Progressive finiteness of a relation R is the same as well-foundedness

of R^\sim . Then, $\mathcal{I}(R)$ is a monotype. In a concrete setting, $\mathcal{I}(R)$ is the set of monotypes which are not the origins of infinite paths (by R):

A relation R is *progressively finite* iff for a monotype $a, a \leq (R \circ a)^< \Rightarrow a = 0$ equivalently $\nu(a : a \leq id : (R \circ a)^<) = 0$ equivalently $\mu(a : a \leq id : a \not\downarrow R) = id$.

The next theorem involves the function $w_a(X) := Q \vee P \circ X$, which is closely related to the description of iterations. The theorem highlights the importance of progressive finiteness in the simplification of fixed point-related properties.

- (6) **Theorem.** Let $f(X) := Q \vee P \circ X$ be a function. If P is progressively finite, the function f has a unique fixed point which means that $\nu(f) = \mu(f) = P^* \circ Q$ [1]:

As the demonic calculus will serve as an algebraic apparatus for defining the denotational semantics of the nondeterministic programs, we will define in what follows these operators.

3 Demonic refinement ordering

We now define the refinement ordering (*demonic inclusion*) we will be using in the sequel. This ordering induces a complete join semilattice, called a *demonic semilattice*. The associated operations are demonic join (\sqcup), demonic meet (\sqcap) and demonic composition (\circ). We give the definitions and needed properties of these operations, and illustrate them with simple examples. For more details on relational demonic semantics and demonic operators, see [5, 8, 6, 7, 14].

- (7) **Definition.** We say that a relation Q *refines* a relation R [23], denoted by $Q \sqsubseteq R$, iff $R^< \circ Q \leq R$ and $R^< \leq Q^<$.

- (8) **Proposition.** Let Q and R be relations, then

- (a) The greatest lower (wrt \sqsubseteq) of Q and R is,

$$Q \sqcap R = Q^< \circ R^< \circ (Q \vee R),$$
 If $Q^< = R^<$ then we have \sqcup and \vee coincide i.e $Q \sqcup R = Q \vee R$.

(b) If Q and R satisfy the condition $Q^< \wedge R^< = (Q \wedge R)^<$, their least upper bound is $Q \sqcap R = Q \wedge R \vee Q^< \circ R \vee R^< \circ Q$, otherwise, the least upper bound does not exist. If $Q^< \wedge R^< = 0$ then we have \sqcap and \wedge coincide i.e $Q \sqcap R = Q \wedge R$.

For the proofs see [9, 14].

(9) **Definition.** The *demonic composition* of relations Q and R [5] is $Q \square R = (R^< \not\circ Q) \circ Q \circ R$.

In what follows we present some properties of \square .

(10) **Theorem.**

- (a) $(P \square Q) \square R = P \square (Q \square R)$,
- (b) R total $\Rightarrow Q \square R = Q \circ R$,
- (c) Q function $\Rightarrow Q \square R = Q \circ R$.

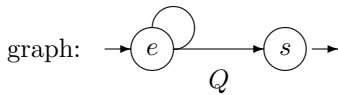
See [5, 6, 7, 14, 35].

Monotypes have very simple and convenient properties. Some of them are presented in the following proposition.

(11) **Proposition.** Let a and b be monotypes. We have

- (a) $a = a^\sim = a^2$,
- (b) $a \square b = a \wedge b = b \square a$,
- (c) $a \vee a^\sim = id$ and $a \wedge a^\sim = 0$,
- (d) $a \leq b \Leftrightarrow b^\sim \leq a^\sim$,
- (e) $a^\sim \square b^\sim = (a \vee b)^\sim$,
- (f) $(a \wedge b)^\sim = (a \square b)^\sim = a^\sim \vee b^\sim$,
- (g) $a \square b^\sim \vee b = a \vee b$,
- (h) $a \leq b \Leftrightarrow a \square 1 \leq b \square 1$.

In previous papers [14, 13, 31, 35], we found the semantics of the while loop given by the following



(a) $\mathcal{S}(\mathcal{R}) = \mathcal{I}(P) \circ [(P \vee Q)^< \not\circ P^*] \circ P^* \circ Q$, with the restriction

(b) $P^< \wedge Q^< = 0$

Our goal is to show that the operational semantics a is equal to the denotational one which is given as the greatest fixed point of the semantic function $Q \vee P \square X$ in the demonic semilattice. In other words, we have to prove the next equation:

(a) $\mathcal{S}(\mathcal{R}) = \bigsqcup \{X \mid X \sqsubseteq Q \vee P \square X\}$;

by taking $P := t \square B$ and $Q := t^\sim$, one gets the demonic semantics we have assigned to while loops in previous papers [14, 35]. Other similar definitions of while loops can be found in [19, 25, 29].

Let us introduce the following abbreviations:

(12) **Abbreviation.** Let P , Q and X be relations subject to the restriction $P^< \wedge Q^< = 0$ (b) and x a monotype. The Abbreviations $w_d, w_a, w_<, a$ and l are defined as follows:

- $w_d(X) := Q \vee P \square X$,
- $a := (P \vee Q)^< \not\circ P^*$,
- $w_a(X) := Q \vee P \circ X$,
- $l := \mathcal{I}(P)$.
- $w_<(x) := Q^< \vee (P \square x)^< = Q \vee (P \square x)^<$

(Mnemonics: the subscripts a and d stand for angelic and demonic, respectively; the subscript $<$ refers to the fact that $w_<$ is obtained from w_d by composition with $<$; the monotype a stands for abnormal, since it represents states from which abnormal termination is not possible; finally, l stands for loop, since it represents states from which no infinite loop is possible.)

In what follows we will be concerned about the fixed point of $w_a, w_<$ and w_d .

(13) **Theorem.** Every fixed point Y of w_a (Abbreviation 12) verifies $P^* \circ Q \leq Y \leq P^* \circ Q \vee l^\sim \square 1$, and the bounds are tight (i.e. the extremal values are fixed points).

The next lemma investigates the relationship between fixed points of $w_<$ and those of w_d (cf. Abbreviation 12).

(14) **Lemma.** Let $h(X) := (P \vee Q)^{\prec} \vee (P \circ X)^{\prec}$ and $h_1(x) := (P \vee Q)^{\prec} \circ 1 \vee P \circ x$.

$$(a) Y = w_d(Y) \Rightarrow w_{<}(Y^{\prec}) = Y^{\prec},$$

$$(b) w_{<}(Y^{\prec}) = Y^{\prec} \Rightarrow h(Y^{\prec}) = Y^{\prec},$$

$$(c) h(Y^{\prec}) = Y^{\prec} \Rightarrow h_1(Y^{\prec} \circ 1) = Y^{\prec} \circ 1,$$

(15) **Lemma.** Let Y be a fixed point of w_d and b be a fixed point of $w_{<}$ (Abbreviation 12). The relation $b \circ Y$ is a fixed point of w_d .

(16) **Lemma.** If Y and Y' are two fixed points of w_d (Abbreviation 12) such that $Y^{\prec} = Y'^{\prec}$ and $Y^{\prec} \circ P$ is progressively finite, then $Y = Y'$.

The next theorem characterizes the domain of the greatest fixed point, wrt \sqsubseteq , of function w_d . This domain is the set of points for which normal termination is guaranteed (no possibility of abnormal termination or infinite loop).

(17) **Theorem.** Let W be the greatest fixed point, wrt to \sqsubseteq , of w_d (Abbreviation 12). We have $W^{\prec} = a \circ l$.

The following theorem is a generalization to a non-deterministic context of the *while statement verification rule* of Mills [24]. It shows that the greatest fixed point W of w_d is uniquely characterized by conditions (a) and (b), that is, by the fact that W is a fixed point of w_d and by the fact that no infinite loop is possible when the execution is started in a state that belongs to the domain of W . Note that we also have $W^{\prec} \leq a$ (see Theorem 17), but this condition is implicitly enforced by condition (a). Half of this theorem (the \Leftarrow direction) is also proved by Sekerinski (the *main iteration theorem* [29]) in a predicative programming set-up.

(18) **Theorem.** A relation W is the greatest fixed point, wrt \sqsubseteq , of function w_d (Abbreviation 12), iff the following two conditions hold:

- (a) $W = w_d(W)$,
- (b) $W^{\prec} \leq l$.

In what follows we give some applications of our results.

4 Application

In [6, 7], Berghammer and Schmidt propose abstract relation algebra as a practical means for the specification of data types and programs. Often, in these specifications, a relation is characterized as a fixed point of some function. Can demonic operators be used in the definition of such a function? Let us now show with a simple example that the concepts presented in this paper give useful insights for answering this question.

In [6, 7], it is shown that the natural numbers can be characterized by the relations z and S (*zero* and *successor*) the laws

- (a) $\emptyset \neq z = zL \wedge zz^{\sim} \subseteq I$ (z is a point),
 $SS^{\sim} = I \wedge S^{\sim}S \subseteq I$ (S is a one to one application.),
 $Sz = \emptyset$ (z has a predecessor),
 $L = \bigcap \{x \mid z \cup S^{\sim}x = x\}$ (generation principle).

For the rest of this section, assume that we are given a relation algebra satisfying these laws. In this algebra, because of the last axiom, the inequation

$$(a) z \cup S^{\sim}X \subseteq X$$

obviously has a unique solution for X , namely, $X = L$. Because the function $g(X) := z \cup S^{\sim}X$ is \cup -continuous, this solution can be expressed as

$$(a) L = \bigcup_{n \geq 0} g^n(\emptyset) = \bigcup_{n \geq 0} S^{\sim n}z,$$

where $g^0(\emptyset) = \emptyset$, $g^{n+1}(\emptyset) = g(g^n(\emptyset))$, $S^{\sim 0} = I$ and $S^{\sim n+1} = S^{\sim}S^{\sim n}$. However, it is shown in [6, 7] that $z \sqcup S^{\sim} \circ X \subseteq X$, obtained by replacing the join and composition operators in a by their demonic counterparts, has infinitely many solutions. Indeed, from $Sz = \emptyset$ and the Schröder rule, it follows that

$$(a) z \cap S^{\sim}L = \emptyset,$$

so that, by definition of demonic join (8(a)) and demonic composition (9), $z \sqcup S^{\sim} \circ X = (z \cup S^{\sim} \circ X) \cap z \cap (S^{\sim} \circ X)L \subseteq z \cap S^{\sim}L = \emptyset$. Hence, any relation R is a solution to $z \sqcup S^{\sim} \circ X \subseteq X$. Looking at previous papers [14, 32, 33, 34, 31], one

immediately sees why it is impossible to reach L by joining anything to z (which is a point and hence is an immediate predecessor of \emptyset), since this can only lead to z or to \emptyset .

Let us now go ‘fully demonic’ and ask what is a solution to $z \sqcup S^{\smile} \sqcap X \sqsubseteq X$. By the discussion above, this is equivalent to $\emptyset \sqsubseteq X$, which has a unique solution, $X = \emptyset$. This raises the question whether it is possible to find some fully demonic inequation similar to (a), whose solution is $X = L$. Because L is in the middle of the demonic semilattice, there are in fact two possibilities: either approach L from above or from below.

For the approach from above, consider the inequation

$$X \sqsubseteq z \sqcap S^{\smile} \sqcap X.$$

Using Theorem 10(c), we have $z \sqcap S^{\smile} \sqcap X = z \sqcap S^{\smile} X$, since S^{\smile} is deterministic (axiom a(b)). From a, $z \subseteq \overline{S^{\smile} L}$; this implies $z \subseteq \overline{S^{\smile} X L}$ and $S^{\smile} X \subseteq \overline{z}$, so that, by definition of \sqcap , $z \sqcap S^{\smile} X = z \sqcap S^{\smile} X \cup z \cap \overline{S^{\smile} X L} \cup \overline{z} \cap S^{\smile} X = z \cup S^{\smile} X$.

This means that 4 reduces to

$$(a) \quad X \sqsubseteq z \cup S^{\smile} X.$$

By definition of refinement (7), this implies that $z \cup S^{\smile} X L \subseteq X L$; this is a variant of (a), thus having $X L = L$ as only solution. This means that any solution to 4 must be a total relation. But L is total and in fact is the largest (by \sqsubseteq) total relation. It is also a solution to 4 (since by axiom a(d), $z \cup S^{\smile} L = L$) so that $L = \bigsqcup \{X | X \sqsubseteq z \sqcap S^{\smile} \sqcap X\}$; that is, L is the greatest fixed point in $(\mathcal{B}_L, \sqsubseteq)$ of $f(X) := z \sqcap S^{\smile} \sqcap X$. Now consider $\bigsqcap_{n \geq 0} S^{\smile n} \sqcap z$, where $S^{\smile n}$ is a n -fold demonic composition defined by $S^{\smile 0} = I$ and $S^{\smile n+1} = S^{\smile} \sqcap S^{\smile n}$. By axiom a(b), S^{\smile} is deterministic, so that, by 10(c) and associativity of demonic composition, $\text{con} S^{\smile n} \sqcap z = S^{\smile n} z$. Hence,

It is easy to show that for any $n \geq 0$, $S^{\smile n} z$ is a point (it is the n -th successor of zero) and that $m \neq n \Rightarrow S^{\smile m} z \neq S^{\smile n} z$. Hence, in $(\mathcal{B}_L, \sqsubseteq)$, $\{S^{\smile n} z | n \geq 0\}$ (i.e. $\{S^{\smile n} \sqcap z | n \geq 0\}$) is the set of immediate predecessors of \emptyset ; looking at [31] shows

how the universal relation L arises as the greatest lower bound $\bigsqcap_{n \geq 0} S^{\smile n} \sqcap z$ of this set of points. Note that, whereas there is a unique solution to a, there are infinitely many solutions to 4 (equivalently, to a), for example $\bigsqcap_{n \geq k} S^{\smile n}$ ($= \bigcup_{n \geq k} S^{\smile n}$), for any k .

For the upward approach, consider

$$z^{\smile} \sqcup X \sqcap S \sqsubseteq X.$$

Here also there are infinitely many solutions to this inequation; in particular, any vector v , including \emptyset and L , is a solution to 4. Because $(\mathcal{B}_L, \sqsubseteq)$ is only a join semilattice, it is not at all obvious that the least fixed point of $h(X) := z^{\smile} \sqcup X \sqcap S$ exists. It does, however, since the following derivation shows that $\bigsqcap_{n \geq 0} z^{\smile} \sqcap S^{\smile n}$ ($= \bigsqcap_{n \geq 0} h^n(z^{\smile})$), where $h^0(z^{\smile}) = z^{\smile}$ is a fixed point of h and hence is obviously the least solution of 4: Because z^{\smile} and S are mappings, property 10(c) implies that $z^{\smile} \sqcap S^{\smile n} = z^{\smile} S^{\smile n}$, for any $n \geq 0$. But $z^{\smile} S^{\smile n}$ is also a mapping (it is the inverse of the point $S^{\smile n} z$) and hence is total, from which, by Proposition 8(a) and equation a, $\bigsqcap_{n \geq 0} z^{\smile} \sqcap S^{\smile n} = \bigsqcap_{n \geq 0} z^{\smile} S^{\smile n} = \bigcup_{n \geq 0} z^{\smile} S^{\smile n} = (\bigcup_{n \geq 0} S^{\smile n} z)^{\smile} = L^{\smile} = L$. This means that L is the least upper bound of the set of mappings $\{z^{\smile} \sqcap S^{\smile n} | n \geq 0\}$. Again, a look at [31] gives some intuition to understand this result, after recalling that mappings are minimal elements in $(\mathcal{B}_L, \sqsubseteq)$ (though not all mappings have the form $z^{\smile} \sqcap S^{\smile n}$).

Thus, building L from below using the set of mappings $\{z^{\smile} \sqcap S^{\smile n} | n \geq 0\}$ is symmetric to building it from above using the set of points $\{S^{\smile n} \sqcap z | n \geq 0\}$.

5 Conclusion

We presented a theorem that can be also used to find the fixed points of functions of the form $f(X) := Q \vee P \sqcap X$ (no restriction on the domains of P and Q). This theorem can be applied also to the program verification and construction (as in the precedent example). Half of this theorem (the \Leftarrow direction) is also proved by Sekerinski (the *main iteration theorem* [29]) in a predicative programming set-up. Our theorem is more general because there is no restriction on the domains of the relations P and Q .

The approach to demonic input-output relation presented here is not the only possible one. In [19, 20, 21], the infinite looping has been treated by adding to the state space a fictitious state \perp to denote nontermination. In [8, 18, 22, 26], the demonic input-output relation is given as a pair (relation, set). The relation describes the input-output behavior of the program, whereas the set component represents the domain of guaranteed termination.

We note that the preponderant formalism employed until now for the description of demonic input-output relation is the wp-calculus. For more details see [3, 4, 17].

References

- [1] Backhouse, R. C., and Doombos, H.: Mathematical Induction Made Computational. Computing science note 94/16, Department of Mathematics and Computer Science, Eindhoven University of Technology, The Netherlands, 1994.
- [2] Backhouse, R. C., Hoogendijk, P., Voermans, E. and van der Woude, J.: A Relational Theory of Datatypes. Research report, Department of Mathematics and Computer Science, Eindhoven University of Technology, The Netherlands, 1992.
- [3] R. J. R. Back. : On the correctness of refinement in program development. Thesis, Department of Computer Science, University of Helsinki, 1978.
- [4] R. J. R. Back and J. von Wright.: Combining angels, demons and miracles in program specifications. *Theoretical Computer Science*, 100, 1992, 365–383.
- [5] Backhouse, R. C. and van der Woude, J.: Demonic Operators and Monotype Factors. *Mathematical Structures in Comput. Sci.*, **3(4)**, 417–433, Dec. (1993). Also: Computing Science Note 92/11, Department of Mathematics and Computer Science, Eindhoven University of Technology, The Netherlands, 1992.
- [6] Berghammer, R.: Relational Specification of Data Types and Programs. Technical report 9109, Fakultät für Informatik, Universität der Bundeswehr München, Germany, Sept. 1991.
- [7] Berghammer, R. and Schmidt, G.: Relational Specifications. In C. Rauszer, editor, *Algebraic Logic*, **28** of *Banach Center Publications*. Polish Academy of Sciences, 1993.
- [8] Berghammer, R. and Zierer, H.: Relational Algebraic Semantics of Deterministic and Nondeterministic Programs. *Theoretical Comput. Sci.*, **43**, 123–147 (1986).
- [9] Boudriga, N., Elloumi, F. and Mili, A.: On the Lattice of Specifications: Applications to a Specification Methodology. *Formal Aspects of Computing*, **4**, 544–571 (1992).
- [10] Chin, L. H. and Tarski, A.: Distributive and Modular Laws in the Arithmetic of Relation Algebras. *University of California Publications*, **1**, 341–384 (1951).
- [11] Conway, J. H.: *Regular Algebra and Finite Machines*. Chapman and Hall, London, 1971.
- [12] Davey, B. A. and Priestley, H. A.: *Introduction to Lattices and Order*. Cambridge Mathematical Textbooks. Cambridge University Press, Cambridge, 1990.
- [13] J. Desharnais, B. Möller, and F. Tchier. Kleene under a demonic star. *8th International Conference on Algebraic Methodology And Software Technology (AMAST 2000)*, May 2000, Iowa City, Iowa, USA, *Lecture Notes in Computer Science*, Vol. 1816, pages 355–370, Springer-Verlag, 2000.
- [14] Desharnais, J., Belkhit, N., Ben Mohamed Sghaier, S., Tchier, F., Jaoua, A., Mili, A. and Zaguia, N.: Embedding a Demonic Semilattice in a Relation Algebra. *Theoretical Computer Science*, 149(2):333–360, 1995.

- [15] Desharnais, J., Jaoua, A., Mili, F., Boudriga, N. and Mili, A.: A Relational Division Operator: The Conjugate Kernel. *Theoretical Comput. Sci.*, **114**, 247–272 (1993).
- [16] Dilworth, R. P.: Non-commutative Residuated Lattices. *Trans. Amer. Math. Sci.*, **46**, 426–444 (1939).
- [17] E. W. Dijkstra. : *A Discipline of Programming*. Prentice-Hall, Englewood Cliffs, N.J., 1976.
- [18] H. Doornbos. : A relational model of programs without the restriction to Egli-Milner monotone constructs. *IFIP Transactions*, A-56:363–382. North-Holland, 1994.
- [19] C. A. R. Hoare and J. He. : The weakest prespecification. *Fundamenta Informaticae IX*, 1986, Part I: 51–84, 1986.
- [20] C. A. R. Hoare and J. He. : The weakest prespecification. *Fundamenta Informaticae IX*, 1986, Part II: 217–252, 1986.
- [21] C. A. R. Hoare and al. : Laws of programming. *Communications of the ACM*, 30:672–686, 1986.
- [22] R. D. Maddux. : Relation-algebraic semantics. *Theoretical Computer Science*, 160:1–85, 1996.
- [23] Mili, A., Desharnais, J. and Mili, F.: Relational Heuristics for the Design of Deterministic Programs. *Acta Inf.*, **24(3)**, 239–276 (1987).
- [24] Mills, H. D., Basili, V. R., Gannon, J. D. and Hamlet, R. G.: *Principles of Computer Programming. A Mathematical Approach*. Allyn and Bacon, Inc., 1987.
- [25] Nguyen, T. T.: A Relational Model of Demonic Nondeterministic Programs. *Int. J. Foundations Comput. Sci.*, **2(2)**, 101–131 (1991).
- [26] D. L. Parnas. A Generalized Control Structure and its Formal Definition. *Communications of the ACM*, 26:572–581, 1983
- [27] Schmidt, G.: Programs as Partial Graphs I: Flow Equivalence and Correctness. *Theoretical Comput. Sci.*, **15**, 1–25 (1981).
- [28] Schmidt, G. and Ströhlein, T.: *Relations and Graphs*. EATCS Monographs in Computer Science. Springer-Verlag, Berlin, 1993.
- [29] Sekerinski, E.: A Calculus for Predicative Programming. In R. S. Bird, C. C. Morgan, and J. C. P. Woodcock, editors, *Second International Conference on the Mathematics of Program Construction*, volume 669 of *Lecture Notes in Comput. Sci.* Springer-Verlag, 1993.
- [30] Tarski, A.: On the calculus of relations. *J. Symb. Log.* **6**, 3, 1941, 73–89.
- [31] F. Tchier.: Sémantiques relationnelles démoniaques et vérification de boucles non déterministes. Theses of doctorat, Département de Mathématiques et de statistique, Université Laval, Canada, 1996.
- [32] F. Tchier.: Demonic semantics by monotypes. *International Arab conference on Information Technology (Acit2002)*, University of Qatar, Qatar, 16-19 December 2002.
- [33] F. Tchier.: Demonic relational semantics of compound diagrams. In: Jules Desharnais, Marc Frappier and Wendy MacCaull, editors. *Relational Methods in computer Science: The Québec seminar*, pages 117-140, Methods Publishers 2002.
- [34] F. Tchier.: While loop d demonic relational semantics monotype/residual style. *2003 International Conference on Software Engineering Research and Practice (SERP03)*, Las Vegas, Nevada, USA, 23-26, June 2003.
- [35] F. Tchier.: Demonic Semantics: using monotypes and residuals. *IJMMS* 2004:3 (2004) 135-160. (International Journal of Mathematics and Mathematical Sciences)
- [36] M. Walicki and S. Medal.: Algebraic approaches to nondeterminism: An overview. *ACM computing Surveys*, **29(1)**, 1997, 30-81.
- [37] L.Xu, M. Takeichi and H. Iwasaki.: Relational semantics for locally nondeterministic

programs. *New Generation Computing* 15, 1997,
339-362.