The Journal of Logic and Algebraic Programming 79 (2010) 740–767

Contents lists available at ScienceDirect

The Journal of Logic and Algebraic Programming

journal homepage: www.elsevier.com/locate/jlap

Abstract representation theorems for demonic refinement algebras☆

Jean-Lou De Carufel *, Jules Desharnais **

Département d'informatique et de génie logiciel, Pavillon Adrien-Pouliot, 1065, avenue de la Médecine, Université Laval, Québec, QC, Canada G1V 0A6

ARTICLE INFO

Article history:
Available online 15 July 2010

MSC:
03G10
16Y60
68R99

Keywords:
Demonic refinement algebra
Kleene algebra with domain
Enabledness
Termination
Divergence
Representation by pairs

ABSTRACT

The main result of this article is that every demonic refinement algebra with enabledness and termination is isomorphic to an algebra of ordered pairs of elements of a Kleene algebra with domain and with a divergence operator satisfying a mild condition. Divergence is an operator producing a test interpreted as the set of states from which nontermination may occur. An example of a KAD where a divergence operator cannot be defined is given. In addition, it is shown that every demonic refinement algebra with enabledness is also a demonic refinement algebra with termination.

1. Introduction

Demonic Refinement Algebra (DRA) was introduced by von Wright in [30,31]. It is a variant of Kleene Algebra (KA) and Kleene algebra with tests (KAT) as defined by Kozen [18,19] and of Cohen's omega algebra [3]. DRA is an algebra for reasoning about total correctness of programs and has the positively conjunctive predicate transformers as its intended model. DRA was then extended with enabledness and termination operators by Solin and von Wright [27–29], giving an algebra called DRAet in [29] and in this paper. The names of these operators reflect their semantic interpretation in the realm of programs and their axiomatisation is inspired by that of the domain operator of Kleene Algebra with Domain (KAD) [11,12]. Further extensions of DRA were investigated with the goal of dealing with both angelic and demonic nondeterminism, one, called daRAet, where the algebra has dual join and meet operators and one, called daRAn, with a negation operator [26,29]. A generalisation named General Refinement Algebra was also obtained in [31] by weakening the axioms of DRA and it has been applied to the refinement of probabilistic programs in [21]. A variant of refinement algebra that includes a probabilistic choice operator is presented in [20].

We are here concerned with the structure of DRAet. The main result is that every DRAet is isomorphic to an algebra of ordered pairs of elements of a KAD with a divergence operator satisfying a mild condition. Divergence is an operator producing a test interpreted as the set of states from which nontermination may occur (see [13] for the divergence operator, and [17,23] for its dual, the convergence operator). It is shown in [17] that a similar algebra of ordered pairs of elements of an omega algebra with divergence is a DRAet; in [23], these algebras of pairs are mapped to weak omega algebras, a related structure. Our result is stronger because

☆ This is an expanded version of [6].

* Corresponding author.
** Corresponding author. Tel.: +1 418 656 2131x3760; fax: +1 418 656 2324.
E-mail addresses: jldec1@ift.ulaval.ca (J.-L. De Carufel), Jules.Desharnais@ift.ulaval.ca (J. Desharnais).

1567-8326/$ - see front matter © 2010 Elsevier Inc. All rights reserved.
doi:10.1016/j.jlap.2010.07.014

1. it does not require the algebra of pairs to have an ω operator, even though DRA has one. This is a somewhat surprising result, since divergence only produces a test, not an iterated element;
2. it states not only that the algebras of ordered pairs are DRAs, but that every DRA is isomorphic to such an algebra.

A consequence of this result is that every KAD with divergence (satisfying the mild condition) can be embedded in a DRAet.

Section 2 contains the definition of DRAet and properties that can be found in [27–31] or are easily derivable from these. We have however decided to invert the partial ordering with respect to the one used by Solin and von Wright. Their order is more convenient when axiomatising predicate transformers, but ours is more in line with the standard KA notation; in particular, this has the effect that the embedded KAD mentioned above keeps its traditional operators after the embedding. Section 3 presents new results about the structure of DRAet, such as the fact that the "bottom part" of the lattice of a DRAet D is a KAD D_K with divergence and the fact that every element x of D can be written as $x = a + t\top$, where $a, t \in D_K$ and t is a test. It is proved there that every DRA with enabledness (DRAe) is also a DRAet. In addition, there is an example of a KAD where divergence cannot be defined (no such example is to be found in the literature on KAD). Section 4 describes the algebra of ordered pairs and proves the results mentioned in the previous paragraph; it also contains an example conveying the intuition behind the formal results. Section 5 discusses prospects for further research.

2. Definition of Demonic Refinement Algebra with Enabledness and Termination

We begin with the definition of Demonic Refinement Algebra [30,31].

Definition 1. A *demonic refinement algebra* (DRA) is a structure $(D, +, \cdot, {}^*, {}^\omega, 0, 1)$ satisfying the following axioms and rules, where $\cdot$ is omitted, as is usually done (i.e., we write xy instead of $x \cdot y$), and where the order $\leq$ is defined by $x \leq y \overset{\text{def}}{\Leftrightarrow} x+y = y$. The operators * and $^\omega$ bind equally; they are followed by $\cdot$ and then $+$.

(a) $x+(y+z) = (x+y)+z$
(b) $x + y = y + x$
(c) $x + 0 = x$
(d) $x + x = x$
(e) $x(yz) = (xy)z$
(f) $1x = x = x1$
(g) $0x = 0$
(h) $x(y + z) = xy + xz$
(i) $(x + y)z = xz + yz$
(j) $x^* = xx^* + 1$
(k) $xz + y \leq z \Rightarrow x^*y \leq z$
(l) $zx + y \leq z \Rightarrow yx^* \leq z$
(m) $x^\omega = xx^\omega + 1$
(n) $z \leq xz + y \Rightarrow z \leq x^\omega y$
(o) $x^\omega = x^* + x^\omega 0$

It follows from the axioms that $\leq$ is a partial order and that x^* and x^ω are the least and greatest fixed points, respectively, of $(\lambda z \mid : xz + 1)$. All operators are isotone with respect to $\leq$.

Let

$$\top \overset{\text{def}}{=} 1^\omega. \tag{1}$$

One can show

$$x \leq \top, \tag{2}$$
$$\top x = \top, \tag{3}$$

for all $x \in D$. Hence, $\top$ is the top element and a left zero for composition. Other consequences of the axioms are the unfolding (4), sliding (5), denesting (6) and other laws that follow.

$$x^* = x^*x + 1 \qquad x^\omega = x^\omega x + 1 \tag{4}$$
$$x(yx)^* = (xy)^*x \qquad x(yx)^\omega = (xy)^\omega x \tag{5}$$
$$(x + y)^* = x^*(yx^*)^* \qquad (x + y)^\omega = x^\omega(yx^\omega)^\omega \tag{6}$$
$$(x\top)^* = x\top + 1 \qquad (x\top)^\omega = x\top + 1 \tag{7}$$
$$(x0)^* = x0 + 1 \qquad (x0)^\omega = x0 + 1 \tag{8}$$
$$x^*y = xx^*y + y \qquad yx^* = yxx^* + y \tag{9}$$

The proof of (4)–(6) is given in [29]. Properties (7) and (8) simply follow from Definition 1(j,m,g) and (3), and Properties (9) from Definition 1(h,i,f,j)K.

	$\emptyset$	$\bullet$	$\circ$	$\bullet\circ$	
f_1	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	A, $\top$
f_2	$\emptyset$	$\emptyset$	$\emptyset$	$\circ$	
f_3	$\emptyset$	$\emptyset$	$\emptyset$	$\bullet$	
f_4	$\emptyset$	$\circ$	$\emptyset$	$\circ$	
f_5	$\emptyset$	$\emptyset$	$\circ$	$\circ$	A
f_6	$\emptyset$	$\emptyset$	$\emptyset$	$\bullet\circ$	
f_7	$\emptyset$	$\bullet$	$\emptyset$	$\bullet$	A
f_8	$\emptyset$	$\emptyset$	$\bullet$	$\bullet$	
f_9	$\circ$	$\circ$	$\circ$	$\circ$	

	$\emptyset$	$\bullet$	$\circ$	$\bullet\circ$
f_{10}	$\emptyset$	$\circ$	$\emptyset$	$\bullet\circ$
f_{11}	$\emptyset$	$\emptyset$	$\circ$	$\bullet\circ$
f_{12}	$\emptyset$	$\bullet$	$\emptyset$	$\bullet\circ$
f_{13}	$\emptyset$	$\emptyset$	$\bullet$	$\bullet\circ$
f_{14}	$\bullet$	$\bullet$	$\bullet$	$\bullet$
f_{15}	$\circ$	$\circ$	$\circ$	$\bullet\circ$
f_{16}	$\emptyset$	$\bullet\circ$	$\emptyset$	$\bullet\circ$
f_{17}	$\emptyset$	$\circ$	$\bullet$	$\bullet\circ$

	$\emptyset$	$\bullet$	$\circ$	$\bullet\circ$	
f_{18}	$\emptyset$	$\bullet$	$\circ$	$\bullet\circ$	A,G, 1
f_{19}	$\emptyset$	$\emptyset$	$\bullet\circ$	$\bullet\circ$	
f_{20}	$\bullet$	$\bullet$	$\bullet$	$\bullet\circ$	
f_{21}	$\circ$	$\bullet\circ$	$\circ$	$\bullet\circ$	G
f_{22}	$\circ$	$\circ$	$\bullet\circ$	$\bullet\circ$	
f_{23}	$\bullet$	$\bullet\circ$	$\bullet$	$\bullet\circ$	
f_{24}	$\bullet$	$\bullet$	$\bullet\circ$	$\bullet\circ$	G
f_{25}	$\bullet\circ$	$\bullet\circ$	$\bullet\circ$	$\bullet\circ$	G, 0

Fig. 1. The 25 positively conjunctive predicate transformers on the set $\{\bullet, \circ\}$.

An element $t \in D$ that has a complement $\neg t$ satisfying

$$t\neg t = \neg t t = 0 \quad \text{and} \quad t + \neg t = 1 \tag{10}$$

is called a *guard*. It is easy to show that a guard has a unique complement and, since t is the complement of $\neg t$, $\neg t$ is also a guard. Let D_G be the set of guards of D. Then $(D_G, +, \cdot, \neg, 0, 1)$ is a Boolean algebra and it is a maximal one, since every t that has a complement satisfying (10) is in D_G. Properties of guards are similar to those of tests in KAT and KAD. The negation operator $\neg$ binds tighter than any binary operator; in case of conflict with unary operators, parentheses will be used to remove the ambiguity. In the proofs, transformations that use Boolean algebra are simply justified by "BA", rather than referring to a specific Boolean law. The laws that are used include (10), double negation $\neg\neg t = t$, commutativity $st = ts$, left and right zero $0t = t0 = 0$, De Morgan's laws $\neg(s + t) = \neg s\neg t$ and $\neg(st) = \neg s + \neg t$, absorption $s + \neg st = s + t$ and contrapositivity $s \leq t \Leftrightarrow \neg t \leq \neg s$.

Every guard t has a corresponding *assertion* t° defined by

$$t^\circ \stackrel{\text{def}}{=} \neg t\top + 1. \tag{11}$$

Guards and assertions are dually order-isomorphic: $s \leq t \Leftrightarrow t^\circ \leq s^\circ$ for all guards s and t. Hence, assertions form a Boolean algebra too. Choice and composition of assertions give the same result: $s^\circ + t^\circ = s^\circ t^\circ$. Thus assertions have a weaker expressive power than guards. Moreover, guards cannot be defined in terms of assertions, although the latter are defined in terms of guards [30,31]. We will see in Section 3 that it becomes possible after the introduction of the enabledness operator. It is also possible in daRA and daRAn [26,29].

Example 2. We illustrate the previous concepts with the algebra of the 25 conjunctive predicate transformers on the set $\{\bullet, \circ\}$. In the tables of Figure 1, $\emptyset$ is the empty set and $\bullet$, $\circ$ and $\bullet\circ$ abbreviate $\{\bullet\}$, $\{\circ\}$ and $\{\bullet, \circ\}$, respectively. The header of each table lists the four possible subsets of $\{\bullet, \circ\}$. The other lines define the predicate transformers. For instance, $f_4(\emptyset) = f_4(\{\circ\}) = \emptyset$ and $f_4(\{\bullet\}) = f_4(\{\bullet\circ\}) = \{\circ\}$. Choice is defined by $(f_i + f_j)(x) = f_i(x) \cap f_j(x)$ and composition by $(f_i f_j)(x) = f_i(f_j(x))$, for all $1 \leq i, j \leq 25$. The $\top$, 1 and 0 transformers are f_1, f_{18} and f_{25}, respectively. The f_i are conjunctive because $f(x \cap y) = f(x) \cap f(y)$, for all f, x, y. Some, like f_1, are not universally conjunctive, because $f_1(\{\bullet, \circ\}) \neq \{\bullet, \circ\}$ (note that $\{\bullet, \circ\}$ is the empty intersection of subsets of $\{\bullet, \circ\}$). This is why the predicate transformers are said to be positively conjunctive. The four assertions are indicated by A and the four guards by G. One can check that guards f_{21} and f_{24} are complementary, since, for all x,

$$(f_{21} + f_{24})(x) = f_{21}(x) \cap f_{24}(x) = x = f_{18}(x)$$

and

$$(f_{21} f_{24})(x) = f_{21}(f_{24}(x)) = \{\bullet, \circ\} = f_{25}(x) = (f_{24} f_{21})(x).$$

The wp-semantics of programs assigns the following meaning to predicate transformers [14]. Let P be a program whose semantics is f. For a given set of states S, the set $f(S)$ contains the states from which

1. P is guaranteed to terminate and
2. P cannot terminate in a state outside of S.

To simplify the wording, let us consider that the transformers are programs, rather than a representation of programs. Then $f_{22}(\{\bullet, \circ\}) = \{\bullet, \circ\}$ means that f_{22} always terminates. We also see that f_{22} is a so-called *miraculous* program: because $f_{22}(\emptyset) = \{\circ\}$, it terminates from state $\circ$, but it terminates in no state. Thus f_{22} may be viewed as a blocked, disabled program (it is disabled in state $\circ$). Now consider f_1; because $f_1(\{\bullet, \circ\}) = \emptyset$, f_1 never terminates.

The inversion of the ordering mentioned in the last paragraph of the introduction is reflected in this example by having $\top$ and 0 correspond to the inclusion-wise least and largest predicate transformers, respectively. More precisely, $f \leq g$ iff $f(x) \supseteq g(x)$, for all x.

In the sequel, the symbols p, q, r, s, t, possibly subscripted, denote guards or assertions (which one will be clear from the context). The sets of guards and assertions of a DRA D are denoted by D_G and D_A, respectively.

Next, we introduce the enabledness and termination operators [27–29]. The definition below is in fact that of [29], because the isolation axiom (Definition 1(o) above) and axioms (15) and (19) below are not included in [27,28]. The binding power of the enabledness and termination operators is larger than that of any binary operator; parentheses will be used to avoid ambiguities in the presence of other unary operators.

Definition 3. A *demonic refinement algebra with enabledness* (DRAe) is a structure $(D, +, \cdot, ^*, ^\omega, \ulcorner, 0, 1)$ such that $(D, +, \cdot, ^*, ^\omega, 0, 1)$ is a DRA and the *enabledness operator* $\ulcorner : D \to D_G$ (mapping elements to guards) satisfies the following axioms, where t is a guard.

$$\ulcorner x x = x \tag{12}$$
$$\ulcorner(tx) \leq t \tag{13}$$
$$\ulcorner(xy) = \ulcorner(x \ulcorner y) \tag{14}$$
$$\ulcorner x \top = x \top \tag{15}$$

A *demonic refinement algebra with enabledness and termination* (DRAet) is a structure $(D, +, \cdot, ^*, ^\omega, \ulcorner, \urcorner, 0, 1)$ such that $(D, +, \cdot, ^*, ^\omega, \ulcorner, 0, 1)$ is a DRAe and the *termination operator* $\urcorner : D \to D_A$ (mapping elements to assertions) satisfies the following axioms, where p is an assertion.

$$\urcorner x x = x \tag{16}$$
$$p \leq \urcorner(px) \tag{17}$$
$$\urcorner(xy) = \urcorner(x \urcorner y) \tag{18}$$
$$\urcorner x 0 = x 0 \tag{19}$$

Example 4. Equations (12) and (16) show that $\ulcorner x$ and $\urcorner x$ are *left preservers* of x. The identity element, 1, is also a left preserver of x, since $1x = x$. It is in fact both the largest guard and the least assertion that preserve x. The inequality (13) forces $\ulcorner x$ to be the least left-preserving guard and (17) forces $\urcorner x$ to be the largest left-preserving assertion.

Consider the four guards of Example 2. Since $f_{18}f_{22} = f_{21}f_{22} = f_{22}$ and $f_{24}f_{22} = f_{25}f_{22} = f_{25}$, only f_{18} and f_{21} left preserve f_{22}. Because $f_{21} \leq f_{18}$, it is the least left-preserving guard of f_{22} and thus $\ulcorner f_{22} = f_{21}$. Both f_{21} and f_{22} are disabled in state $\circ$, and f_{21} acts as the identity on state $\bullet$, as can be seen from $f_{21}(\{\bullet\}) = \{\bullet, \circ\}$ (taking into account that f_{21} is disabled in state $\circ$). The predicate transformer terminology is that $\ulcorner x$ *skips* in those states in which program x is enabled, whence the name of the enabledness operator $\ulcorner$.

Similarly, for the four assertions, $f_5 f_4 = f_{18} f_4 = f_4$ and $f_1 f_4 = f_7 f_4 = f_1$, and thus only f_5 and f_{18} left preserve f_4. Because $f_{18} \leq f_5$, f_5 is the largest left-preserving assertion of f_4 and so $\urcorner f_4 = f_5$. Note that neither f_4 nor f_5 terminates in state $\bullet$, since $f_4(\{\bullet, \circ\}) = f_5(\{\bullet, \circ\}) = \{\circ\}$, and that f_5 is the identity on state $\circ$. It is said that $\urcorner x$ *skips* in those states in which program x terminates, whence the name of the termination operator $\urcorner$.

The intuitive meaning of enabledness and termination will become clearer in Section 4 after the introduction of the representation of a DRA by an algebra of pairs.

The termination operator is defined by four axioms in Definition 3 in order to exhibit its similarity with the enabledness operator. It turns out however that Axioms (16)–(18) can be dropped, because they follow from Axiom (19). It is also shown in [29] that $\urcorner x 0 = x 0 \Leftrightarrow \urcorner x = x 0 + 1$. Thus (16)–(19) are equivalent to $\urcorner x = x 0 + 1$ and it looks like the termination operator might be *defined* by $\urcorner x \stackrel{\text{def}}{=} x 0 + 1$, a possibility that is also mentioned in [27,28]. However, Solin and von Wright remark that this is not possible unless it is known that $x0 + 1$ is an assertion; it is shown in [26,29] that $x0 + 1$ is an assertion in daRAet. We show in Section 3 that this is the case in DRAe too.

The following equalities, where t is a guard, are laws of enabledness and guards. The proof of (20)–(22) is given in [27–29]. The other ones are easily derivable from these and the axioms, using the fact that guards form a Boolean algebra.

$$\ulcorner t = t \tag{20}$$
$$\ulcorner \top = 1 \tag{21}$$
$$\ulcorner(x + y) = \ulcorner x + \ulcorner y \tag{22}$$

$$\lceil(tx) = t\lceil x \tag{23}$$
$$\neg\lceil xx = 0 \tag{24}$$
$$\lceil x = 0 \Leftrightarrow x = 0 \tag{25}$$
$$\neg\lceil(xt)x = \neg\lceil(xt)x\neg t \tag{26}$$
$$\lceil(x\top) = \lceil x \tag{27}$$
$$\lceil(t\top) = t \tag{28}$$
$$(x\top + t)0 = x\top \tag{29}$$

Another law that will be used repeatedly is

$$\neg(s + t)(x + y) = \neg(s + t)(\neg sx + y). \tag{30}$$

It follows from BA and Definition 1(h):

$$\neg(s + t)(x + y) = \neg s\neg t(x + y) = \neg t(\neg sx + \neg sy) = \neg t(\neg s\neg sx + \neg sy) = \neg s\neg t(\neg sx + y) = \neg(s + t)(\neg sx + y).$$

Variants are of course possible, due to the commutativity of $+$.

In addition, both enabledness and termination are isotone. The first three axioms of enabledness, (12)–(14), are exactly the axioms of the domain operator in KAD.

3. Structure of Demonic Refinement Algebras with Enabledness and Termination

This section contains new results about DRAe and DRAet. It is first shown that in DRAe, guards can be defined in terms of assertions and that the termination operator can be explicitly defined rather than being implicitly defined by Axioms (16)–(19). This means that every DRAe is also a DRAet, so that the two concepts are equivalent. After introducing KAD and the divergence operator, we show that every DRAe D contains an embedded KAD D_K with divergence and that every element of D can be decomposed into its terminating and nonterminating parts, both essentially expressed by means of D_K.

Proposition 5. *Let D be a* DRAe *and $^\diamond : D_A \to D_G$ be the function defined by*

$$p^\diamond \stackrel{\text{def}}{=} \neg\lceil(p0). \tag{31}$$

Then, for any assertion p and guard t,

(a) $p^\diamond$ is a guard with complement $\lceil(p0)$,
(b) $t^{\circ\diamond} = t$,
(c) $p^{\diamond\circ} = p$. Combined with the previous item, this says that $^\circ$ and $^\diamond$ are dual bijections between guards and assertions.

Proof

(a) That $p^\diamond$ is a guard follows from the fact that $\lceil x$ is a guard for any x. Its complement is obviously $\lceil(p0)$.

(b)
$$\begin{aligned} & t^{\circ\diamond} \\ = & \quad \langle\ (31)\ \rangle \\ & \neg\lceil(t^\circ 0) \\ = & \quad \langle\ (11)\ \rangle \\ & \neg\lceil((\neg t\top + 1)0) \\ = & \quad \langle\ (29)\ \rangle \\ & \neg\lceil(\neg t\top) \\ = & \quad \langle\ (28)\ \&\ \text{BA of guards}\ \rangle \\ & t \end{aligned}$$

(c) Since p is an assertion, $p = s^\circ$ for some guard s, by (11). Then, using part b of this proposition, $p^{\diamond\circ} = s^{\circ\diamond\circ} = s^\circ = p$. □

Now let the operators $\neg\!\!\!\cdot : D_A \to D_A$ and $\sqcap : D_A \times D_A \to D_A$ be defined by

$$\neg\!\!\!\cdot p \stackrel{\text{def}}{=} (\neg(p^\diamond))^\circ \quad \text{and} \tag{32}$$

$$p \sqcap q \stackrel{\text{def}}{=} \neg\!\!\!\cdot(\neg\!\!\!\cdot p + \neg\!\!\!\cdot q), \tag{33}$$

for any assertions p and q. These two operators satisfy

$$\neg\!\!\!\cdot p = \neg\lceil(p0)\top + 1 \quad \text{and} \tag{34}$$

$$p \sqcap q = \lceil(p0)\lceil(q0)\top + 1, \tag{35}$$

as the following derivations show.

1. Proof of (34).

$$\begin{aligned}
&\neg\!\!\!\cdot p \\
=\ &\quad \langle\ (32)\ \rangle \\
&(\neg(p^\diamond))^\circ \\
=\ &\quad \langle\ (31)\ \&\ \text{BA of guards}\ \rangle \\
&(\lceil(p0))^\circ \\
=\ &\quad \langle\ (11)\ \rangle \\
&\neg\lceil(p0)\top + 1
\end{aligned}$$

2. Proof of (35).

$$\begin{aligned}
&p \sqcap q \\
=\ &\quad \langle\ (33)\ \rangle \\
&\neg\!\!\!\cdot(\neg\!\!\!\cdot p + \neg\!\!\!\cdot q) \\
=\ &\quad \langle\ (34)\ \rangle \\
&\neg\lceil((\neg\!\!\!\cdot p + \neg\!\!\!\cdot q)0)\top + 1 \\
=\ &\quad \langle\ (34)\ \rangle \\
&\neg\lceil((\neg\lceil(p0)\top + 1 + \neg\lceil(q0)\top + 1)0)\top + 1 \\
=\ &\quad \langle\ \text{Definition 1(i)}\ \&\ (29)\ \rangle \\
&\neg\lceil(\neg\lceil(p0)\top + \neg\lceil(q0)\top)\top + 1 \\
=\ &\quad \langle\ (22)\ \rangle \\
&\neg(\lceil(\neg\lceil(p0)\top) + \lceil(\neg\lceil(q0)\top))\top + 1 \\
=\ &\quad \langle\ (28)\ \rangle \\
&\neg(\neg\lceil(p0) + \neg\lceil(q0))\top + 1 \\
=\ &\quad \langle\ \text{BA of guards}\ \rangle \\
&\lceil(p0)\lceil(q0)\top + 1 \quad \square
\end{aligned}$$

The following proposition shows that $\neg\!\!\!\cdot$ and $\sqcap$ are respectively the negation and meet of assertions. It also describes the dual order-isomorphism between the BA of guards and the BA of assertions; this is of course consistent with the remark made in the previous section.

Proposition 6. *For a given* DRAe*, the structures*

$$(D_G, +, \cdot, \neg, 0, 1) \quad \textit{and} \quad (D_A, \sqcap, +, \neg\!\!\!\cdot, \top, 1)$$

are isomorphic Boolean algebras, with the isomorphism given either by $^\circ$ *or* $^\diamond$*.*

Proof. D_G is a BA [30,31]. Proposition 5 shows that $^\circ$ is a bijective function from D_G to D_A and the equations $1^\circ = 1, 0^\circ = \top$, $(\neg t)^\circ = \neg\!\!\!\cdot(t^\circ)$, $(st)^\circ = s^\circ + t^\circ$ and $(s + t)^\circ = s^\circ \sqcap t^\circ$ are easily shown as follows.

1. $1^\circ = 1$ follows from (11), the BA of guards and Definition 1(g,c): $1^\circ = \neg 1\top + 1 = 0\top + 1 = 0 + 1 = 1$.
2. $0^\circ = \top$ follows from (11), the BA of guards, Definition 1(f) and (2): $0^\circ = \neg 0\top + 1 = 1\top + 1 = \top + 1 = \top$.

3. Using (32) and Proposition 5(b) yields $\neg_{\mathsf{n}}(t^\circ) = (\neg(t^{\circ\diamond}))^\circ = (\neg t)^\circ$.
4. $(st)^\circ$
   $= \quad \langle\ (11)\ \rangle$
   $\neg(st)\top + 1$
   $= \quad \langle\ \text{BA of guards}\ \rangle$
   $(\neg s + \neg t)\top + 1$
   $= \quad \langle\ \text{Definition 1(i,d,b)}\ \rangle$
   $\neg s\top + 1 + \neg t\top + 1$
   $= \quad \langle\ (11)\ \rangle$
   $s^\circ + t^\circ$
5. $s^\circ \sqcap t^\circ$
   $= \quad \langle\ (33)\ \rangle$
   $\neg_{\mathsf{n}}(\neg_{\mathsf{n}}(s^\circ) + \neg_{\mathsf{n}}(t^\circ))$
   $= \quad \langle\ \neg_{\mathsf{n}}(t^\circ) = (\neg t)^\circ\ \text{(part 3 of this proof)}\ \rangle$
   $\neg_{\mathsf{n}}((\neg s)^\circ + (\neg t)^\circ)$
   $= \quad \langle\ (st)^\circ = s^\circ + t^\circ\ \text{(part 4 of this proof)}\ \rangle$
   $\neg_{\mathsf{n}}((\neg s \neg t)^\circ)$
   $= \quad \langle\ \neg_{\mathsf{n}}(t^\circ) = (\neg t)^\circ\ \text{(part 3 of this proof)}\ \rangle$
   $(\neg(\neg s \neg t))^\circ$
   $= \quad \langle\ \text{BA of guards}\ \rangle$
   $(s + t)^\circ \quad \square$

Since inverting the order of a Boolean algebra yields another Boolean algebra, $(D_A, +, \sqcap, \neg_{\mathsf{n}}, 1, \top)$ is also a Boolean algebra and it is ordered by the DRAe ordering $\leq$.

Lemma 7. *In a* DRAe*, $x0 + 1$ is an assertion.*

Proof. Using in turn Definition 1(g), (15), double negation (applicable since $\ulcorner(x0)$ is a guard) and (11), we get

$$x0 + 1 = x0\top + 1 = \ulcorner(x0)\top + 1 = \neg\neg\ulcorner(x0)\top + 1 = (\neg\ulcorner(x0))^\circ.$$

Thus, $x0 + 1$ is an assertion and, by Proposition 5, it uniquely corresponds to the guard $\neg\ulcorner(x0)$. $\square$

This means that it is now possible to give an explicit definition of $\urcorner$.

Definition 8. For a given DRAe D, the *termination operator* $\urcorner : D \to D_A$ is defined by $\urcorner x \stackrel{\text{def}}{=} x0 + 1$.

By the results of Solin and von Wright mentioned in Section 2, the termination operator satisfies Axioms (16)–(19).
We now recall the definition of KAD [11,12], which is essentially KAT extended with the unary $\ulcorner$ operator.

Definition 9. A *Kleene Algebra with Domain* (KAD) is a structure $(K, +, \cdot, {}^*, \ulcorner, 0, 1)$ satisfying all axioms of DRAe, except those involving $^\omega$ (i.e., Definition 1(m,n,o)) and $\top$ (i.e., (15)), with the additional axiom that 0 is a right zero of composition:

$$x0 = 0. \tag{36}$$

The range of the *domain operator* $\ulcorner$ is a Boolean subset of K denoted by $\mathsf{test}(K)$ whose elements are called *tests*. Tests satisfy the laws of guards in a DRAe (10).

The standard signature of KAT and KAD includes a sort $B \subseteq K$ of tests and a negation operator on B [11,12,19]. We have chosen not to include them here in order to have a signature close to that of DRAe. In KAT, B can be any Boolean subset of K, but in KAD, the domain operator forces B to be the maximal Boolean subset of elements below 1 [12]. Thus, the definition of tests in KAD given above imposes the same constraints as that of guards in DRA given in Section 2.

A somewhat cleaner way to define KAD is given in [10]. The signature becomes $(K, +, \cdot, {}^*, \mathsf{a}, 0, 1)$, where the unary *antidomain* operator a satisfies the axioms

$$\mathsf{a}(x)x = 0, \quad \mathsf{a}(xy) \leq \mathsf{a}(x\mathsf{a}^2(y)) \quad \text{and} \quad \mathsf{a}^2(x) + \mathsf{a}(x) = 1. \tag{37}$$

It turns out that these three axioms are enough to make the range of a a Boolean algebra. The antidomain operator acts as the negation of domain, and a domain operator can naturally be *defined* by

$$\lceil x = \mathsf{a}^2(x). \tag{38}$$

One nice thing about this axiomatisation is that no subsort of tests has to be given beforehand (it arises as the range of a) and there is no partial operator like $\neg$ in KAT or KAD as defined in Definition 9. It is shown in [10] that the two axiomatisations yield exactly the same theorems.

The good news is that the axiomatisation based on antidomain is stable and robust enough to be applicable without any change to some variants of Kleene algebra, including in particular DRA [9]. This means that DRAe can be defined from DRA by axiomatising the enabledness operator in the same way that domain is axiomatised by (37) and (38). Although we believe this new axiomatisation is better than that given in Section 2, we have decided to present the results of this paper using the latter, because it is the original one that is found in the literature and because it does not change the derivation of the results in significant ways.

When using the laws of DRAe to justify a transformation for KAD (due to Definition 9), we add a suffix K. For instance, we write "Definition 1(g)K" and "(13)K" instead of "Definition 1(g)" and "(13)".

The domain operator satisfies the following inductive law (as does the enabledness operator of DRAe) [12]:

$$\lceil(xt) + s \leq t \;\Rightarrow\; \lceil(x^*s) \leq t. \tag{39}$$

In a given KAD K, the greatest fixed point $(\nu t \mid t \in \mathsf{test}(K) : \lceil(xt))$ may or may not exist. This fixed point plays an important rôle in the sequel. We will denote it by ∇x and axiomatise it by

$$\nabla x \;\leq\; \lceil(x\nabla x), \tag{40}$$

$$t \leq \lceil(xt) \;\Rightarrow\; t \leq \nabla x. \tag{41}$$

∇x is called the *divergence of* x [13] and this test is interpreted as the set of states from which nontermination is possible. The negation of ∇x corresponds to what is known as the *halting predicate* in the modal μ-calculus [16]. The operator ∇ binds stronger than any binary operator but weaker than any unary operator. Among the properties of divergence, we note

$$\nabla x = \lceil(x\nabla x), \tag{42}$$

$$x\nabla x = \nabla x x \nabla x, \tag{43}$$

$$\neg\nabla x x = \neg\nabla x x \neg\nabla x, \tag{44}$$

$$\nabla(tx) \leq t, \tag{45}$$

$$x \leq y \Rightarrow \nabla x \leq \nabla y. \tag{46}$$

The following proposition gives an example that proves the above assertion that divergence need not exist in an arbitrary KAD (no such example is to be found in the literature on KAD).

Proposition 10. *There is a* KAD K *where* $(\nu t \mid t \in \mathsf{test}(K) : \lceil(xt))$ *does not exist for some* $x \in K$ *and thus* ∇ *is not defined.*

Proof. Let E and O be the set of even and odd natural numbers, respectively. Consider the following relation on the set of natural numbers $\mathbb{N}$:

$$G \stackrel{\text{def}}{=} \{(m,n) \mid (m,n \in O \wedge m \leq n) \vee (m,n \in E \wedge m > n)\} \cup (O \times E)$$

(G is the transitive closure of the relation partially displayed in Figure 2).

Now let I be the identity relation on $\mathbb{N}$, and $\mathcal{G}$ and $\mathcal{F}$ be the sets of relations

$$\mathcal{F} \stackrel{\text{def}}{=} \{t \mid t \subseteq I \text{ and } t \text{ is finite or cofinite}\} \quad \text{and} \quad \mathcal{G} \stackrel{\text{def}}{=} \{G\} \cup \mathcal{F}.$$

Note that $I \in \mathcal{F}$, since I is cofinite. Finally, let $\mathcal{R}$ be the set of relations generated from $\mathcal{G}$ by closing it under finite unions ($\cup$), standard relational composition ($;$), standard relational transitive closure (*) and domain ($\lceil$), where $\lceil R \stackrel{\text{def}}{=} \{(m,m) \mid (\exists n \mid : (m,n) \in R)\}$ for any relation $R \in \mathcal{R}$. Then $(\mathcal{R}, \cup, ;, ^*, \lceil, \emptyset, I)$ satisfies all the laws of KAD, except possibly those that concern the structure of tests (the range of $\lceil$). This is obvious, since all operations have their standard concrete relational interpretation. For that reason, some of the following transformations invoke the laws of KAD. We will see below that the range of $\lceil$ is indeed a BA.

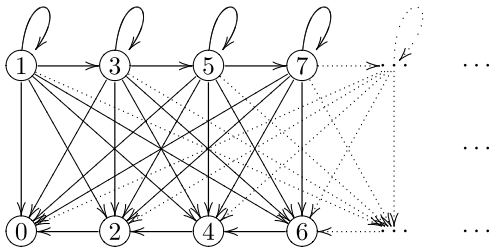

Fig. 2. The relation G of Proposition 10 is the transitive closure of this relation.

We first show that for every relation $R \in \mathcal{R}$, there are natural numbers $n \in \mathbb{N}$, $n_i \in \mathbb{N}$ and subidentities $s_i \in \mathcal{F}$, $t_{i,j} \in \mathcal{F}$ with $0 \leq i < n$ and $0 \leq j < n_i$ such that R can be written as

$$R = (\bigcup i \mid 0 \leq i < n : s_i(;j \mid 0 \leq j < n_i : Gt_{i,j})). \tag{47}$$

The proof is by induction over the structure of expressions.

1. Base case for G: $G = IGI = (\bigcup i \mid 0 \leq i < 1 : IGI) = (\bigcup i \mid 0 \leq i < 1 : I(;j \mid 0 \leq j < 1 : GI))$.
2. Base case for $t \in \mathcal{F}$: $t = tI = (\bigcup i \mid 0 \leq i < 1 : tI) = (\bigcup i \mid 0 \leq i < 1 : t(;j \mid 0 \leq j < 0 : GI))$.
3. Induction case $P \cup Q$: If P and Q have the form of R in (47), then obviously $P \cup Q$ also has this form.
4. Induction case $P;Q$: Let P and Q have the form of R in (47). More precisely,

$$P = (\bigcup i \mid 0 \leq i < m : p_i(;k \mid 0 \leq k < m_i : Gq_{i,k})),$$
$$Q = (\bigcup j \mid 0 \leq j < n : r_j(;k \mid 0 \leq k < n_j : Gs_{j,k})).$$

Then

$$\begin{aligned}
& PQ \\
&= (\bigcup i \mid 0 \leq i < m : p_i(;k \mid 0 \leq k < m_i : Gq_{i,k}))\ (\bigcup j \mid 0 \leq j < n : r_j(;k \mid 0 \leq k < n_j : Gs_{j,k})) \\
&= \quad \langle \text{ Definition 1(h,i)K } \rangle \\
&\quad (\bigcup i, j \mid 0 \leq i < m \ \wedge\ 0 \leq j < n : p_i(;k \mid 0 \leq k < m_i : Gq_{i,k})r_j(;k \mid 0 \leq k < n_j : Gs_{j,k})) \\
&= \quad \langle \text{ Define } t_{i+jm} \stackrel{\text{def}}{=} \begin{cases} p_i & \text{if } m_i > 0 \\ p_i r_j & \text{if } m_i = 0 \end{cases} \\
&\qquad \text{and } u_{i+jm,k} \stackrel{\text{def}}{=} \begin{cases} q_{i,k} & \text{if } m_i > 0 \text{ and } 0 \leq k < m_i - 1 \\ q_{i,k} r_j & \text{if } m_i > 0 \text{ and } k = m_i - 1 \\ s_{j,k-m_i} & \text{if } m_i \leq k < m_i + n_j \end{cases} \quad \rangle \\
&\quad (\bigcup i, j \mid 0 \leq i < m \ \wedge\ 0 \leq j < n : t_{i+jm}(;k \mid 0 \leq k < m_i + n_j : Gu_{i+jm,k})) \\
&= \quad \langle \text{ Let } x, y \in \mathbb{N} \text{ and let } \mathrm{rem}(x,y) \text{ and } x/y \text{ respectively denote the remainder and the result of the} \\
&\qquad \text{integer division of } x \text{ by } y. \text{ Note that } \mathrm{rem}(i + jm, m) = i \text{ and } (i + jm)/m = j \text{ when } i < m. \text{ The} \\
&\qquad \text{transformation is obtained by changing the index } l := i + jm. \\
&\qquad \text{Define } h_l \stackrel{\text{def}}{=} m_{\mathrm{rem}(l,m)} + n_{l/m},\ t_l \stackrel{\text{def}}{=} \begin{cases} p_{\mathrm{rem}(l,m)} & \text{if } m_{\mathrm{rem}(l,m)} > 0 \\ p_{\mathrm{rem}(l,m)} r_{l/m} & \text{if } m_{\mathrm{rem}(l,m)} = 0 \end{cases} \\
&\qquad \text{and } u_{l,k} \stackrel{\text{def}}{=} \begin{cases} q_{\mathrm{rem}(l,m),k} & \text{if } m_{\mathrm{rem}(l,m)} > 0 \text{ and } 0 \leq k < m_{\mathrm{rem}(l,m)} - 1 \\ q_{\mathrm{rem}(l,m),k} r_{l/m} & \text{if } m_{\mathrm{rem}(l,m)} > 0 \text{ and } k = m_{\mathrm{rem}(l,m)} - 1 \\ s_{l/m,k-m_{\mathrm{rem}(l,m)}} & \text{if } m_{\mathrm{rem}(l,m)} \leq k < m_{\mathrm{rem}(l,m)} + n_{l/m} \end{cases} \quad \rangle \\
&\quad (\bigcup l \mid 0 \leq l < mn : t_l(;k \mid 0 \leq k < h_l : Gu_{l,k})),
\end{aligned}$$

so that PQ has the appropriate form (using the comments made in the last transformation to relate it to the form of P and Q).

5. Induction case R^*: Assume (47). We first show $R^{n+1} \subseteq (\bigcup k \mid 0 \leq k \leq n : R^k)$. Since R is a finite union of n terms of the form $s_i(;j \mid 0 \leq j < n_i : Gt_{i,j})$, R^{n+1} is a finite union of n^{n+1} terms, each one being the product of $n + 1$ terms selected from the n terms of R. This means that in each term of R^{n+1}, at least one term of R is repeated. Hence, a term

of R^{n+1} has the form

$$P \stackrel{\text{def}}{=} Q_1 s_k(;l \mid 0 \le l < n_k : Gt_{k,l}) Q_2 s_k(;l \mid 0 \le l < n_k : Gt_{k,l}) Q_3,$$

where Q_1, Q_2 and Q_3 are products of terms of R. We consider two cases.

(a) Case $n_k = 0$: Then $P = Q_1 s_k Q_2 s_k Q_3 \subseteq Q_1 s_k Q_2 Q_3 = Q_1 s_k(;l \mid 0 \le l < n_k : Gt_{k,l}) Q_2 Q_3$, so that P is included in a term of R^n, since one term of R, namely $s_k(;l \mid 0 \le l < n_k : Gt_{k,l})$, has disappeared.

(b) Case $n_k > 0$:

$$\begin{aligned}
& P \\
&= Q_1 s_k(;l \mid 0 \le l < n_k : Gt_{k,l}) Q_2 s_k(;l \mid 0 \le l < n_k : Gt_{k,l}) Q_3 \\
&= Q_1 s_k(;l \mid 0 \le l < n_k - 1 : Gt_{k,l}) Gt_{k,n_k-1} Q_2 s_k(;l \mid 0 \le l < n_k - 1 : Gt_{k,l}) Gt_{k,n_k-1} Q_3 \\
&\subseteq \quad \langle \text{ Because } G \text{ is transitive and each } s_i \text{ and } t_{i,j} \text{ in (47) is included in } I,\ s_k(;l \mid 0 \le l < n_k - 1 : Gt_{k,l}) \subseteq G^* \text{ and, for the same reason, } Q_2 \subseteq G^*. \rangle \\
& Q_1 s_k(;l \mid 0 \le l < n_k - 1 : Gt_{k,l}) G G^* G^* Gt_{k,n_k-1} Q_3 \\
&\subseteq \quad \langle \ G \text{ is transitive} \ \rangle \\
& Q_1 s_k(;l \mid 0 \le l < n_k - 1 : Gt_{k,l}) Gt_{k,n_k-1} Q_3 \\
&= Q_1 s_k(;l \mid 0 \le l < n_k : Gt_{k,l}) Q_3.
\end{aligned}$$

The last term being the product of a strictly smaller number of terms than in the expression above for P, P is included in R^m for some $m \le n$.

Hence, each term of R^{n+1} is included in $(\bigcup k \mid 0 \le k \le n : R^k)$, so $R^{n+1} \subseteq (\bigcup k \mid 0 \le k \le n : R^k)$. But this implies $R^* = (\bigcup k \mid 0 \le k \le n : R^k)$. Thus R^* is a finite union of finite products of the form (47). The result then follows from the induction cases 3 and 4.

6. Induction case $\ulcorner R$: We show that $\ulcorner R$ is a finite or cofinite relation $t \in \mathcal{F}$ and thus can be written as $(\bigcup i \mid 0 \le i < 1 : t(;j \mid 0 \le j < 0 : GI))$, as for base case 2. By the induction hypothesis (47) and (22)K,

$$\ulcorner R \;=\; \ulcorner(\bigcup i \mid 0 \le i < n : s_i(;j \mid 0 \le j < n_i : Gt_{i,j})) \;=\; (\bigcup i \mid 0 \le i < n : \ulcorner(s_i(;j \mid 0 \le j < n_i : Gt_{i,j}))).$$

Since the finite union of finite and/or cofinite sets is a finite or cofinite set, it suffices to show $\ulcorner(s_i(;j \mid 0 \le j < n_i : Gt_{i,j})) \in \mathcal{F}$, for all i, j. Because by (23)K $\ulcorner(tQ) = t\ulcorner Q$ for any $t \subseteq I$,

$$\ulcorner(s_i(;j \mid 0 \le j < n_i : Gt_{i,j})) \;=\; s_i \ulcorner(;j \mid 0 \le j < n_i : Gt_{i,j}).$$

Since the finite product of finite and/or cofinite subidentities is finite or cofinite (just like the finite intersection of finite and/or cofinite sets), it suffices to prove $\ulcorner(;j \mid 0 \le j < n_i : Gt_{i,j}) \in \mathcal{F}$. We proceed by induction on n_i.

(a) Base case $n_i = 0$: $\ulcorner(;j \mid 0 \le j < 0 : Gt_{i,j}) = I$ is cofinite.

(b) Induction case $n_i > 0$: Assume $\ulcorner(;j \mid 1 \le j < n_i : Gt_{i,j}) \in \mathcal{F}$ (i.e., we assume finiteness or cofiniteness for the domain of the product of $n_i - 1$ factors $Gt_{i,j}$).

$$\begin{aligned}
& \ulcorner(;j \mid 0 \le j < n_i : Gt_{i,j}) \\
&= \ulcorner(Gt_{i,0}(;j \mid 1 \le j < n_i : Gt_{i,j})) \\
&= \quad \langle \ (14)\mathsf{K} \ \rangle \\
& \ulcorner(Gt_{i,0} \ulcorner(;j \mid 1 \le j < n_i : Gt_{i,j}))
\end{aligned}$$

Let $t \stackrel{\text{def}}{=} t_{i,0} \ulcorner(;j \mid 1 \le j < n_i : Gt_{i,j})$. By the induction hypothesis, $\ulcorner(;j \mid 1 \le j < n_i : Gt_{i,j}) \in \mathcal{F}$. By definition, $t_{i,0} \in \mathcal{F}$. Hence $t \in \mathcal{F}$ and all that remains to prove is $\ulcorner(Gt) \in \mathcal{F}$. We proceed by cases.

i. Case 1: There is an $n \in E$ such that $(n, n) \in t$. By definition of G, this implies that $\ulcorner(Gt)$ contains all (k, k) with $k \in O$ and all those with $k \in E$ such that $k > n$, that is, all (k, k) but a finite number, so $\ulcorner(Gt)$ is cofinite.

ii. Case 2: There is no $n \in E$ such that $(n, n) \in t$, so that t cannot be cofinite and thus must be finite. Since in addition each $k \in O$ has a finite number of predecessors by G, $\ulcorner(Gt)$ is finite.

The induction case for $\ulcorner$ shows that the range of $\ulcorner$ is $\mathcal{F}$, and this is a BA.[1] Thus, $(\mathcal{R}, \cup, ;, *, \ulcorner, \emptyset, I)$ is a KAD and $\mathsf{test}(\mathcal{R}) = \mathcal{F}$.

[1] The range of $\ulcorner$ includes all finite or cofinite subidentities, since $\ulcorner t = t$ for $t \in \mathcal{F}$.

Let $I_O \stackrel{\text{def}}{=} \{(n,n) \mid n \in O\}$. By definition of G, $t \subseteq \lceil(Gt)$ iff $t \subseteq I_O$ (t must not contain any pair (n,n) with $n \in E$). Consequently,

$$(\nu t \mid t \in \mathsf{test}(\mathcal{R}) : \lceil(Gt)) \;=\; (\bigcup t \mid t \in \mathsf{test}(\mathcal{R}) \wedge t \subseteq \lceil(Gt) : t) \;=\; (\bigcup t \mid t \in \mathsf{test}(\mathcal{R}) \wedge t \subseteq I_O : t) \;=\; I_O.$$

Since $I_O = \lceil(GI_O)$, I_O is indeed the greatest fixed point of $(\lambda t \mid t \in \mathsf{test}(\mathcal{R}) : \lceil(Gt))$ and O is the maximal set of points from which there is an infinite path by G. But I_O is neither finite nor cofinite, so that $I_O \notin \mathcal{R}$ and thus ∇G is not defined. □

If in Proposition 10 we had used relation

$$G' \stackrel{\text{def}}{=} \{(m,n) \mid (m,n \in O \wedge m < n) \vee (m,n \in E \wedge m > n)\} \cup (O \times E)$$

instead of G (this removes the loops on odd numbers in Figure 2), we could have shown everything that is in the proposition, except for the last paragraph. There is a single test $t \in \mathcal{F}$ that satisfies $t \subseteq \lceil(G't)$, namely $\emptyset$, so that

$$(\nu t \mid t \in \mathsf{test}(\mathcal{R}) : \lceil(G't)) = (\bigcup t \mid t \in \mathsf{test}(\mathcal{R}) \wedge t \subseteq \lceil(G't) : t) = \emptyset.$$

Hence, $\nabla G' = \emptyset$, even though there is an infinite path in G'. But it cannot even be approximated by tests larger than $\emptyset$.

Note that divergence may exist even if the test algebra is not complete. For instance, take $\mathcal{R}$ to be the set of finite or cofinite subsets of the identity relation on the natural numbers. With the standard relational operators as in Proposition 10, $(\mathcal{R}, \cup, ;, ^*, \lceil, \emptyset, I)$ is a KAD where the set of tests is $\mathcal{R}$ itself (it is the maximal BA of relations below the identity). $\mathcal{R}$ is not a complete BA, but it is readily checked that $\nabla x = x$ for every $x \in \mathcal{R}$.

Proposition 11. *In a* KAD *K where ∇x is defined, $\lceil(x^*s) + \nabla x$ is a fixed point of $f(t) \stackrel{\text{def}}{=} \lceil(xt) + s$ and*

$$t \leq \lceil(xt) + s \;\Rightarrow\; t \leq \lceil(x^*s) + \nabla x, \tag{48}$$

that is, $\lceil(x^*s) + \nabla x$ is the greatest fixed point of f.

The proof of this proposition is given in [13].

In the sequel, we denote by D_K the following set of elements of a DRAe D:

$$D_K \stackrel{\text{def}}{=} \{x \in D \mid x0 = 0\}. \tag{49}$$

Theorem 12. *Let D be a* DRAe*. Then $(D_K, +, \cdot, ^*, \lceil, 0, 1)$ is a* KAD *in which ∇x exists for all x. In addition, the set of tests of D_K is the set of guards D_G and*

$$\nabla x \;=\; \lceil(x^\omega 0), \tag{50}$$

$$\nabla x = 0 \wedge z \leq xz + y \Rightarrow z \leq x^* y. \tag{51}$$

Proof

1. The elements of D_K satisfy all axioms of KAD, including (36). All we need to prove in order to show that D_K is a KAD is that it is closed under the operations of KAD. First, D_K contains all guards, including 1 and 0, since $t0 \leq 10 = 0$ for any guard t. Thus, guards are the tests of D_K and form a BA with the operations $+$, $\cdot$ and $\neg$. This implies $\lceil x \in D_K$ for all x, since $\lceil x$ is a guard. Finally, for the remaining operations, we have the following, where $x0 = 0$ and $y0 = 0$ are assumed, due to (49):
   - $(x+y)0 = x0 + y0 = 0$ by Definition 1(i,c);
   - $xy0 = x0 = 0$;
   - $x^*0 \leq 0 \Leftarrow x0 + 0 \leq 0 \Leftarrow$ true by Definition 1(k,d).
2. Proof of (50). We show that $\lceil(x^\omega 0)$ satisfies the axioms of ∇x ((40) and (41)).

(a)
$$\begin{array}{ll} & \lceil(x\lceil(x^\omega 0)) \\ = & \quad \langle\ (14)\ \rangle \\ & \lceil(xx^\omega 0) \\ = & \quad \langle\ \text{Definition 1(i,f,c)}\ \rangle \\ & \lceil((xx^\omega + 1)0) \end{array}$$

$$
\begin{array}{ll}
= & \langle \text{ Definition 1(m) } \rangle \\
\quad \lceil(x^\omega 0) &
\end{array}
$$

(b)
$$
\begin{array}{ll}
& t \leq \lceil(xt) \\
\Rightarrow & \langle \text{ Isotony } \rangle \\
& t\top \leq \lceil(xt)\top \\
\Leftrightarrow & \langle \text{ (15) \& Definition 1(c) } \rangle \\
& t\top \leq xt\top + 0 \\
\Rightarrow & \langle \text{ Definition 1(n) } \rangle \\
& t\top \leq x^\omega 0 \\
\Rightarrow & \langle \ t = t1 \leq t\top \ \rangle \\
& t \leq x^\omega 0 \\
\Rightarrow & \langle \text{ Isotony of } \lceil \ \rangle \\
& \lceil t \leq \lceil(x^\omega 0) \\
\Leftrightarrow & \langle \text{ (20) } \rangle \\
& t \leq \lceil(x^\omega 0)
\end{array}
$$

Thus, ∇x exists in D; since $\lceil(x^\omega 0) \in D_K$ (because it is a guard), ∇x also exists in D_K.

3. Proof of (51).

$$
\begin{array}{ll}
& \nabla x = 0 \ \wedge \ z \leq xz + y \\
\Rightarrow & \langle \text{ Definition 1(n) } \rangle \\
& \nabla x = 0 \ \wedge \ z \leq x^\omega y \\
\Leftrightarrow & \langle \text{ Definition 1(o,i,g) } \rangle \\
& \nabla x = 0 \ \wedge \ z \leq x^* y + x^\omega 0 \\
\Rightarrow & \langle \text{ (50) \& (25) \& Definition 1(c) } \rangle \\
& z \leq x^* y \quad \square
\end{array}
$$

Theorem 13. *Let D be a* DRAe. *Then*

$$\lceil(x0)x = \lceil(x0)\top \ = \ x0, \tag{52}$$

$$x = \neg\lceil(x0)x + \lceil(x0)\top, \tag{53}$$

$$x = \neg\lceil(x0)x + x0. \tag{54}$$

Every $x \in D$ can be written as $x = a + t\top$, where t is a guard in D (hence in D_K), $a \in D_K$ and $ta = 0$.

Proof

1. Proof of (52). The refinement $\lceil(x0)x \leq \lceil(x0)\top$ follows from $x \leq \top$. The other refinement and the equality follow from (15), Definition 1(g), (12) and $0 \leq 1$: $\lceil(x0)\top = x0\top = x0 = \lceil(x0)x0 \leq \lceil(x0)x$.
2. Proof of (53). This follows from the BA of guards, Definition 1(i) and (52):

$$x = (\neg\lceil(x0) + \lceil(x0))x = \neg\lceil(x0)x + \lceil(x0)x = \neg\lceil(x0)x + \lceil(x0)\top.$$

3. Proof of (54). This follows from (53) and (52).

Because $\neg\lceil(x0)x0 = 0$ by (24), $\neg\lceil(x0)x \in D_K$ by (49). Thus, by (53), $x = a + t\top$, with $a \stackrel{\text{def}}{=} \neg\lceil(x0)x \in D_K$ and $t \stackrel{\text{def}}{=} \lceil(x0) \in D_K$ satisfying $ta = 0$ by BA and Definition 1(g). $\square$

In (54), $\neg\lceil(x0)x$ is the *finite* or *terminating* part of x and $x0$ (which is equal to $\lceil(x0)\top$ by (53)) is its *infinite* or *nonterminating* part [22]. The possibility offered by (53) to write any element of D as $a + t\top$ with $a, t \in D_K$ and $ta = 0$ means that both the terminating part a and the nonterminating part $t\top$ are essentially described by the elements a and t of the KAD D_K. Under this form, we already foresee the algebra of ordered pairs (a, t) of Section 4.

Another part of the DRAe structure worth mentioning is the set

$$D_D \stackrel{\text{def}}{=} \{x \in D \mid x\top = \top\}. \tag{55}$$

This set contains all the assertions, since for any guard t, $t^\circ\top = (\neg t\top + 1)\top = \top$, by (11). Its elements are the *total* or *nonmiraculous* elements and they satisfy $\ulcorner x = 1$. As already remarked in [17], the substructure D_D of D is a *Demonic Algebra with Domain* (DAD) in the sense of [4,5,7,8]. The set D_D is the image of D_K by the transformation

$$\phi(x) \stackrel{\text{def}}{=} x + \neg\ulcorner x\top. \tag{56}$$

Now let $\psi(x) = \neg\ulcorner(x0)x$, where $x \in D_D$. It is easy to prove that ψ is the inverse of ϕ. The following properties can then be derived. In these, $x, y, t \in D_K$ and t is a guard. The notation for the demonic operators is that of [4,5,7,8] (in the definition of demonic negation, the "$\neg$" at the left of $\stackrel{\text{def}}{=}$ is demonic negation, while the one at the right is DRA negation). The demonic operators of DAD are concerned only with the terminating part of the elements of D_D. For each operator, the $\stackrel{\text{def}}{=}$ transformation is obtained by calculating the image in D_D of x and y, using ϕ. An operation of D is then applied and, finally, the terminating part of the result is kept, using ψ. The final expression given for each operator is exactly the expression defining KAD-based demonic operators in [4,5,7,8].

1. Demonic join: $x \sqcup y \stackrel{\text{def}}{=} \psi(\phi(x) + \phi(y)) = \ulcorner x\ulcorner y(x + y)$.
2. Demonic composition: $x \boxdot y \stackrel{\text{def}}{=} \psi(\phi(x)\phi(y)) = \neg\ulcorner(x\neg\ulcorner y)xy$.
3. Demonic star: $x^\times \stackrel{\text{def}}{=} \psi((\phi(x))^*) = x^* \boxdot \ulcorner x$.
4. Demonic negation: $\neg t \stackrel{\text{def}}{=} \psi(\neg(\phi(t))) = \neg t$.
5. Demonic domain: $\urcorner x \stackrel{\text{def}}{=} \psi(\urcorner(\phi(x))) = \ulcorner x$.

The proof of these assertions follows.

1. Proof of $\psi(\phi(x) + \phi(y)) = \ulcorner x\ulcorner y(x + y)$.

$$\begin{aligned}
&\psi(\phi(x) + \phi(y)) \\
&= \psi(x + \neg\ulcorner x\top + y + \neg\ulcorner y\top) \\
&= \neg\ulcorner((x + \neg\ulcorner x\top + y + \neg\ulcorner y\top)0)(x + \neg\ulcorner x\top + y + \neg\ulcorner y\top) \\
&= \quad \langle \text{ Definition 1(i,c) \& (3) \& } x, y \in D_K \text{ \& (49) } \rangle \\
&\quad \neg\ulcorner(\neg\ulcorner x\top + \neg\ulcorner y\top)(x + \neg\ulcorner x\top + y + \neg\ulcorner y\top) \\
&= \quad \langle \text{ (22) \& (28) } \rangle \\
&\quad \neg(\neg\ulcorner x + \neg\ulcorner y)(x + \neg\ulcorner x\top + y + \neg\ulcorner y\top) \\
&= \quad \langle \text{ BA } \rangle \\
&\quad \ulcorner x\ulcorner y(x + \neg\ulcorner x\top + y + \neg\ulcorner y\top) \\
&= \quad \langle \text{ Definition 1(h,g) \& BA (in particular } \ulcorner x\ulcorner y\neg\ulcorner x = \ulcorner y\ulcorner x\neg\ulcorner x = \ulcorner y0 = 0) \rangle \\
&\quad \ulcorner x\ulcorner y(x + y)
\end{aligned}$$

2. Proof of $\psi(\phi(x)\phi(y)) = \neg\ulcorner(x\neg\ulcorner y)xy$.

$$\begin{aligned}
&\psi(\phi(x)\phi(y)) \\
&= \psi((x + \neg\ulcorner x\top)(y + \neg\ulcorner y\top)) \\
&= \quad \langle \text{ Definition 1(h,i) \& (3) } \rangle \\
&\quad \psi(xy + x\neg\ulcorner y\top + \neg\ulcorner x\top) \\
&= \neg\ulcorner((xy + x\neg\ulcorner y\top + \neg\ulcorner x\top)0)(xy + x\neg\ulcorner y\top + \neg\ulcorner x\top) \\
&= \quad \langle \text{ Definition 1(i,c) \& (3) \& } x, y \in D_K \text{ \& (49) } \rangle \\
&\quad \neg\ulcorner(x\neg\ulcorner y\top + \neg\ulcorner x\top)(xy + x\neg\ulcorner y\top + \neg\ulcorner x\top) \\
&= \quad \langle \text{ (22) \& (27) \& (28) } \rangle \\
&\quad \neg(\ulcorner(x\neg\ulcorner y) + \neg\ulcorner x)(xy + x\neg\ulcorner y\top + \neg\ulcorner x\top) \\
&= \quad \langle \text{ BA } \rangle
\end{aligned}$$

$$
\begin{aligned}
& \neg\lceil(x\neg\lceil y)\rceil x(xy + x\neg\lceil y\top + \neg\lceil x\top) \\
= & \qquad \langle \text{ Definition 1(h,g,c) \& (12) \& BA \& (24) } \rangle \\
& \neg\lceil(x\neg\lceil y)xy
\end{aligned}
$$

3. Proof of $\psi((\phi(x))^*) = x^* \,\square\, \lceil x$.

$$
\begin{aligned}
& \psi((\phi(x))^*) \\
= & \ \psi((x + \neg\lceil x\top)^*) \\
= & \qquad \langle \text{ (6) } \rangle \\
& \psi(x^*(\neg\lceil x\top x^*)^*) \\
= & \qquad \langle \text{ (3) \& (7) } \rangle \\
& \psi(x^*(\neg\lceil x\top + 1)) \\
= & \ \neg\lceil(x^*(\neg\lceil x\top + 1)0)x^*(\neg\lceil x\top + 1) \\
= & \qquad \langle \text{ (29) } \rangle \\
& \neg\lceil(x^*\neg\lceil x\top)x^*(\neg\lceil x\top + 1) \\
= & \qquad \langle \text{ (27) } \rangle \\
& \neg\lceil(x^*\neg\lceil x)x^*(\neg\lceil x\top + 1) \\
= & \qquad \langle \text{ (26) \& BA } \rangle \\
& \neg\lceil(x^*\neg\lceil x)x^*\lceil x(\neg\lceil x\top + 1) \\
= & \qquad \langle \text{ Definition 1(h,g,c) \& BA } \rangle \\
& \neg\lceil(x^*\neg\lceil x)x^*\lceil x \\
= & \qquad \langle \text{ Part 2 of this proof \& (20) } \rangle \\
& x^* \,\square\, \lceil x
\end{aligned}
$$

4. Proof of $\psi(\neg(\phi(t))) = \neg t$.

$$
\begin{aligned}
& \psi(\neg(\phi(t))) \\
= & \qquad \langle \text{ (20) } \rangle \\
& \psi(\neg(t + \neg t\top)) \\
= & \qquad \langle \text{ (34) \& } t + \neg t\top \text{ is an assertion since } t^\circ = \neg t\top + 1 = \neg t\top + \neg t1 + t = \neg t\top + t \text{ by (11), BA,} \\
& \qquad \quad \text{Definition 1(f) and isotony. Hence } \neg \text{ can be applied to it } \rangle \\
& \psi(\neg\lceil((t + \neg t\top)0)\top + 1) \\
= & \qquad \langle \text{ (29) } \rangle \\
& \psi(\neg\lceil(\neg t\top)\top + 1) \\
= & \qquad \langle \text{ (28) \& BA } \rangle \\
& \psi(t\top + 1) \\
= & \ \neg\lceil((t\top + 1)0)(t\top + 1) \\
= & \qquad \langle \text{ (29) } \rangle \\
& \neg\lceil(t\top)(t\top + 1) \\
= & \qquad \langle \text{ Definition 1(h,f,c) \& (24) } \rangle \\
& \neg\lceil(t\top) \\
= & \qquad \langle \text{ (28) } \rangle \\
& \neg t
\end{aligned}
$$

5. Proof of $\psi(\lceil\!\!\lceil(\phi(x))) = \lceil x$.

$$
\begin{aligned}
& \psi(\lceil\!\!\lceil(\phi(x))) \\
= & \ \psi(\lceil\!\!\lceil(x + \neg\lceil x\top))
\end{aligned}
$$

$$
\begin{array}{ll}
= & \langle \text{ Definition 8 } \rangle \\
\quad \psi((x + \neg\ulcorner x\top)0 + 1) & \\
= & \langle \text{ Definition 1(i,c) \& (3) \& } x \in D_K \text{ \& (49) } \rangle \\
\quad \psi(\neg\ulcorner x\top + 1) & \\
= \neg\ulcorner((\neg\ulcorner x\top + 1)0)(\neg\ulcorner x\top + 1) & \\
= & \langle \text{ (29) } \rangle \\
\quad \neg\ulcorner(\neg\ulcorner x\top)(\neg\ulcorner x\top + 1) & \\
= & \langle \text{ Definition 1(h,f,c) \& (24) } \rangle \\
\quad \neg\ulcorner(\neg\ulcorner x\top) & \\
= & \langle \text{ (28) \& BA } \rangle \\
\quad \ulcorner x \quad \square &
\end{array}
$$

Demonic join induces a refinement ordering $\sqsubseteq$: for $x, y \in D_K$, $x \sqsubseteq y \Leftrightarrow x \sqcup y = y$. Using the definition of $\sqcup$ and the fact that ψ and ϕ are each other's inverse, we see that $\sqsubseteq$ on D_K corresponds to $\leq$ on D_D:

$$x \sqsubseteq y \Leftrightarrow x \sqcup y = y \Leftrightarrow \psi(\phi(x)+\phi(y)) = y \Leftrightarrow \phi(\psi(\phi(x)+\phi(y))) = \phi(y) \Leftrightarrow \phi(x)+\phi(y) = \phi(y) \Leftrightarrow \phi(x) \leq \phi(y).$$

This means that the KAD D_K with the refinement $\sqsubseteq$ and the demonic operators is a (KAD-based) DAD that is isomorphic to the DAD D_D.

However, unlike what is shown for KAD in Theorem 16 below, not every DAD can be embedded in a DRA, because not every DAD is the image of a KAD. It is shown in [5,8] that some DADs contain so-called *nondecomposable* elements, but in D_D, all elements are decomposable.

4. A Demonic Refinement Algebra of Pairs

This section contains the main theorem of the paper (Theorem 16), about the isomorphism between any DRAe and an algebra of ordered pairs. We first define this algebra of pairs, show that it is a DRAe and then prove Theorem 16. At the end of the section, Example 17 provides a semantically intuitive understanding of the results of the paper.

Definition 14. Let K be a KAD such that

$$\nabla \text{ is defined} \quad \text{and} \quad \nabla x = 0 \ \wedge\ z \leq xz + y \ \Rightarrow\ z \leq x^* y. \tag{57}$$

Define the set of ordered pairs P by

$$P \stackrel{\text{def}}{=} \{(x, t) \mid x \in K \ \wedge\ t \in \mathsf{test}(K) \ \wedge\ tx = 0\}.$$

We define the following operations on P.

1. $(x, s) \oplus (y, t) \stackrel{\text{def}}{=} (\neg(s + t)(x + y), s + t)$
2. $(x, s) \odot (y, t) \stackrel{\text{def}}{=} (\neg\ulcorner(xt)xy, s + \ulcorner(xt))$
3. $(x, t)^{\circledast} \stackrel{\text{def}}{=} (\neg\ulcorner(x^*t)x^*, \ulcorner(x^*t))$
4. $(x, t)^{\tilde{\omega}} \stackrel{\text{def}}{=} (\neg\ulcorner(x^*t)\neg\nabla xx^*, \ulcorner(x^*t) + \nabla x)$
5. $\ulcorner(x, t) \stackrel{\text{def}}{=} (\ulcorner x + t, 0)$

It is easy to verify that the result of each operation is a pair of P. The condition on pairs can be expressed in many equivalent ways

$$tx = 0 \ \Leftrightarrow\ t \leq \neg\ulcorner x \ \Leftrightarrow\ \ulcorner x \leq \neg t \ \Leftrightarrow\ \neg tx = x \ \Leftrightarrow\ \neg t\ulcorner x = \ulcorner x, \tag{58}$$

by (25)K, (23)K, (12)K and Boolean algebra. The programming interpretation of a pair (x, t) is that t denotes the set of states from which nontermination is possible, while x denotes the terminating computations.

If K were a complete lattice (in particular, if K were finite), only the existence of ∇x would be needed to get all of (57) [1]. We do not know if this is the case for an arbitrary KAD, but the appendix presents some results that may help find the answer. Note that D_K satisfies (57), by Theorem 12.

Theorem 15. *The algebra* $(P, \oplus, \odot, {}^{\circledast}, {}^{\tilde{\omega}}, {}^{\ulcorner}, (0,0), (1,0))$ *is a* DRAe. *Moreover,*

(a) $(x,s) \sqsubseteq (y,t) \;\Leftrightarrow\; s \leq t \wedge \neg tx \leq y$, *where* $(x,s) \sqsubseteq (y,t) \overset{\text{def}}{\Leftrightarrow} (x,s) \oplus (y,t) = (y,t)$,
(b) the top element is $(0,1)$,
(c) guards have the form $(t,0)$, *and* $\neg(t,0) = (\neg t, 0)$,
(d) the assertion corresponding to the guard $(t,0)$ *is* $(t, \neg t)$,
(e) $\neg(t,\neg t) = (\neg t, t)$,
(f) ${}^{\urcorner}(x,t) = (\neg t, t)$.

Proof. In the derivations below, steps that use Definition 14 are not justified. Also, the constraint on pairs is usually not invoked (e.g., $tx = 0$ for the pair (x,t)).

Verification of the axioms of DRA *(Definition 1).* For the verification of the * and $^\omega$ axioms, we assume $(x,s) \sqsubseteq (y,t) \;\Leftrightarrow\; s \leq t \wedge \neg tx \leq y$, which is item a of the theorem; this is shown after verifying the axioms of DRA and those of ${}^{\ulcorner}$.

(a)
$$\begin{aligned}
&(x,r) \oplus ((y,s) \oplus (z,t)) \\
&= (x,r) \oplus (\neg(s+t)(y+z), s+t) \\
&= (\neg(r+s+t)(x+\neg(s+t)(y+z)), r+s+t) \\
&= \quad \langle\ (30)\mathsf{K}\ \rangle \\
&\quad (\neg(r+s+t)(x+y+z), r+s+t) \\
&= \quad \langle\ \text{Symmetric transformations}\ \rangle \\
&\quad ((x,r) \oplus (y,s)) \oplus (z,t)
\end{aligned}$$

(b) $(x,s) \oplus (y,t) = (y,t) \oplus (x,s)$ is obvious from the definition of $\oplus$.
(c) $(x,t) \oplus (0,0) = (\neg(t+0)(x+0), t+0) = (\neg tx, t) = (x,t)$ by Definition 1(c)K and (58).
(d) $(x,t) \oplus (x,t) = (x,t)$ is obvious from the definition of $\oplus$ and (58).

(e)
$$\begin{aligned}
&(x,r) \odot ((y,s) \odot (z,t)) \\
&= (x,r) \odot (\neg{}^{\ulcorner}(yt)yz, s + {}^{\ulcorner}(yt)) \\
&= (\neg{}^{\ulcorner}(x(s+{}^{\ulcorner}(yt)))x\neg{}^{\ulcorner}(yt)yz, r + {}^{\ulcorner}(x(s+{}^{\ulcorner}(yt)))) \\
&= \quad \langle\ \text{Definition 1(h)K \& (22)K \& BA}\ \rangle \\
&\quad (\neg{}^{\ulcorner}(xs)\neg{}^{\ulcorner}(x{}^{\ulcorner}(yt))x\neg{}^{\ulcorner}(yt)yz, r + {}^{\ulcorner}(xs) + {}^{\ulcorner}(x{}^{\ulcorner}(yt))) \\
&= \quad \langle\ (26)\mathsf{K}\ \&\ (14)\mathsf{K}\ \rangle \\
&\quad (\neg{}^{\ulcorner}(xs)\neg{}^{\ulcorner}(xyt)xyz, r + {}^{\ulcorner}(xs) + {}^{\ulcorner}(xyt)) \\
&= \quad \langle\ (23)\mathsf{K}\ \&\ \mathsf{BA}\ \rangle \\
&\quad (\neg{}^{\ulcorner}(\neg{}^{\ulcorner}(xs)xyt)\neg{}^{\ulcorner}(xs)xyz, r + {}^{\ulcorner}(xs) + {}^{\ulcorner}(\neg{}^{\ulcorner}(xs)xyt)) \\
&= (\neg{}^{\ulcorner}(xs)xy, r + {}^{\ulcorner}(xs)) \odot (z,t) \\
&= ((x,r) \odot (y,s)) \odot (z,t)
\end{aligned}$$

(f)
$$\begin{aligned}
&(x,t) \odot (1,0) \\
&= (\neg{}^{\ulcorner}(x0)x1, t + {}^{\ulcorner}(x0)) \\
&= \quad \langle\ (36)\ \&\ (20)\mathsf{K}\ \&\ \mathsf{BA}\ \&\ \text{Definition 1(f)K}\ \rangle \\
&\quad (x,t) \\
&= \quad \langle\ \mathsf{BA}\ \&\ (20)\mathsf{K}\ \&\ (58)\ \rangle \\
&\quad (\neg{}^{\ulcorner}(1t)1x, 0 + {}^{\ulcorner}(1t)) \\
&= (1,0) \odot (x,t)
\end{aligned}$$

(g)
$$\begin{aligned}
&(0,0) \odot (x,t) \\
&= (\neg{}^{\ulcorner}(0t)0x, 0 + {}^{\ulcorner}(0t)) \\
&= \quad \langle\ \text{Definition 1(g)K \& (20)K \& BA}\ \rangle \\
&\quad (0,0)
\end{aligned}$$

(h) $(x,r)\odot((y,s)\oplus(z,t))$
$=(x,r)\odot(\neg(s+t)(y+z),s+t)$
$=(\neg\ulcorner(x(s+t))x\neg(s+t)(y+z),r+\ulcorner(x(s+t)))$
$=$ ⟨ (26)K & (58) ⟩
$(\neg\ulcorner(x(s+t))\neg rx(y+z),r+\ulcorner(x(s+t)))$
$=$ ⟨ Definition 1(h)K & (22)K ⟩
$(\neg(\ulcorner(xs)+\ulcorner(xt))\neg r(xy+xz),r+\ulcorner(xs)+\ulcorner(xt))$
$=$ ⟨ (30)K & BA ⟩
$(\neg r\neg(\ulcorner(xs)+\ulcorner(xt))(\neg\ulcorner(xs)xy+\neg\ulcorner(xt)xz),r+\ulcorner(xs)+\ulcorner(xt))$
$=$ ⟨ BA ⟩
$(\neg(r+\ulcorner(xs)+r+\ulcorner(xt))(\neg\ulcorner(xs)xy+\neg\ulcorner(xt)xz),r+\ulcorner(xs)+r+\ulcorner(xt))$
$=(\neg\ulcorner(xs)xy,r+\ulcorner(xs))\oplus(\neg\ulcorner(xt)xz,r+\ulcorner(xt))$
$=(x,r)\odot(y,s)\oplus(x,r)\odot(z,t)$

(i) $((x,r)\oplus(y,s))\odot(z,t)$
$=(\neg(r+s)(x+y),r+s)\odot(z,t)$
$=(\neg\ulcorner(\neg(r+s)(x+y)t)\neg(r+s)(x+y)z,r+s+\ulcorner(\neg(r+s)(x+y)t))$
$=$ ⟨ (23)K & Definition 1(i)K & (22)K ⟩
$(\neg(\neg(r+s)(\ulcorner(xt)+\ulcorner(yt)))\neg(r+s)(x+y)z,r+s+\neg(r+s)(\ulcorner(xt)+\ulcorner(yt)))$
$=$ ⟨ BA ⟩
$(\neg(r+s)\neg(\ulcorner(xt)+\ulcorner(yt))(x+y)z,r+s+\ulcorner(xt)+\ulcorner(yt))$
$=$ ⟨ Definition 1(i)K & (30)K & BA ⟩
$(\neg(r+\ulcorner(xt)+s+\ulcorner(yt))(\neg\ulcorner(xt)xz+\neg\ulcorner(yt)yz),r+\ulcorner(xt)+s+\ulcorner(yt))$
$=(\neg\ulcorner(xt)xz,r+\ulcorner(xt))\oplus(\neg\ulcorner(yt)yz,s+\ulcorner(yt))$
$=(x,r)\odot(z,t)\oplus(y,s)\odot(z,t)$

(j) $(x,t)\odot(x,t)^{\circledast}\oplus(1,0)$
$=(x,t)\odot(\neg\ulcorner(x^*t)x^*,\ulcorner(x^*t))\oplus(1,0)$
$=(\neg\ulcorner(x\ulcorner(x^*t))x\neg\ulcorner(x^*t)x^*,t+\ulcorner(x\ulcorner(x^*t)))\oplus(1,0)$
$=$ ⟨ (26)K ⟩
$(\neg\ulcorner(x\ulcorner(x^*t))xx^*,t+\ulcorner(x\ulcorner(x^*t)))\oplus(1,0)$
$=$ ⟨ (58) & (14)K ⟩
$(\neg\ulcorner(xx^*t)\neg txx^*,t+\ulcorner(xx^*t))\oplus(1,0)$
$=$ ⟨ BA & (20)K & (22)K & (9)K ⟩
$(\neg\ulcorner(x^*t)xx^*,\ulcorner(x^*t))\oplus(1,0)$
$=(\neg(\ulcorner(x^*t)+0)(\neg\ulcorner(x^*t)xx^*+1),\ulcorner(x^*t)+0)$
$=$ ⟨ (30)K & BA & Definition 1(j)K ⟩
$(\neg\ulcorner(x^*t)x^*,\ulcorner(x^*t))$
$=(x,t)^{\circledast}$

(k) $(x,r)^{\circledast}\odot(y,s)\sqsubseteq(z,t)$
$\Leftrightarrow(\neg\ulcorner(x^*r)x^*,\ulcorner(x^*r))\odot(y,s)\sqsubseteq(z,t)$
$\Leftrightarrow(\neg\ulcorner(\neg\ulcorner(x^*r)x^*s)\neg\ulcorner(x^*r)x^*y,\ulcorner(x^*r)+\ulcorner(\neg\ulcorner(x^*r)x^*s))\sqsubseteq(z,t)$
$\Leftrightarrow$ ⟨ (23)K & BA ⟩
$(\neg\ulcorner(x^*r)\neg\ulcorner(x^*s)x^*y,\ulcorner(x^*r)+\ulcorner(x^*s))\sqsubseteq(z,t)$

$\Leftrightarrow$ ⟨ Part a of this theorem, proved below ⟩
$\lceil(x^*r) + \lceil(x^*s) \leq t \ \wedge\ \neg t\neg\lceil(x^*r)\neg\lceil(x^*s)x^*y \leq z$
$\Leftrightarrow$ ⟨ $\lceil(x^*r) + \lceil(x^*s) \leq t \ \Rightarrow\ \neg t \leq \neg\lceil(x^*r)\neg\lceil(x^*s)$ & BA & (22)K & Definition 1(h)K ⟩
$\lceil(x^*(r+s)) \leq t \ \wedge\ \neg tx^*y \leq z$
$\Leftarrow$ ⟨ (39) ⟩
$\lceil(xt) + r + s \leq t \ \wedge\ \neg tx^*y \leq z$
$\Leftarrow$ ⟨ $\neg tx^* \leq (\neg tx)^*\neg t$
$\Leftarrow$ ⟨ Definition 1(l)K ⟩
$(\neg tx)^*\neg tx + \neg t \leq (\neg tx)^*\neg t$
$\Leftrightarrow$ ⟨ $\lceil(xt) \leq t \ \Rightarrow\ \neg t \leq \neg\lceil(xt)$ & BA ⟩
$(\neg tx)^*\neg t\neg\lceil(xt)x + \neg t \leq (\neg tx)^*\neg t$
$\Leftrightarrow$ ⟨ (26)K ⟩
$(\neg tx)^*\neg t\neg\lceil(xt)x\neg t + \neg t \leq (\neg tx)^*\neg t$
$\Leftarrow$ ⟨ $\neg\lceil(xt) \leq 1$ & Definition 1(i,f)K ⟩
$((\neg tx)^*\neg tx + 1)\neg t \leq (\neg tx)^*\neg t$
$\Leftrightarrow$ ⟨ (4)K ⟩
true
⟩
$\lceil(xt) + r + s \leq t \ \wedge\ (\neg tx)^*\neg ty \leq z$
$\Leftarrow$ ⟨ Definition 1(k)K ⟩
$\lceil(xt) + r + s \leq t \ \wedge\ \neg txz + \neg ty \leq z$
$\Leftrightarrow$ ⟨ Definition 1(h)K ⟩
$\lceil(xt) + r + s \leq t \ \wedge\ \neg t(xz + y) \leq z$
$\Leftrightarrow$ ⟨ $\lceil(xt) + r + s \leq t \ \Rightarrow\ \neg t \leq \neg(\lceil(xt) + r + s)$ & BA ⟩
$\lceil(xt) + r + s \leq t \ \wedge\ \neg t\neg(\lceil(xt) + r + s)(xz + y) \leq z$
$\Leftrightarrow$ ⟨ Part a of this theorem, proved below ⟩
$(\neg(\lceil(xt) + r + s)(xz + y), \lceil(xt) + r + s) \sqsubseteq (z, t)$
$\Leftrightarrow$ ⟨ (30)K & BA ⟩
$(\neg(r + \lceil(xt) + s)(\neg\lceil(xt)xz + y), r + \lceil(xt) + s) \sqsubseteq (z, t)$
$\Leftrightarrow (\neg\lceil(xt)xz, r + \lceil(xt)) \oplus (y, s) \sqsubseteq (z, t)$
$\Leftrightarrow (x, r) \odot (z, t) \oplus (y, s) \sqsubseteq (z, t)$

(l) $(y, s) \odot (x, r)^{\circledast} \sqsubseteq (z, t)$
$\Leftrightarrow (y, s) \odot (\neg\lceil(x^*r)x^*, \lceil(x^*r)) \sqsubseteq (z, t)$
$\Leftrightarrow (\neg\lceil(y\lceil(x^*r))y\neg\lceil(x^*r)x^*, s + \lceil(y\lceil(x^*r))) \sqsubseteq (z, t)$
$\Leftrightarrow$ ⟨ (26)K & (14)K ⟩
$(\neg\lceil(yx^*r)yx^*, s + \lceil(yx^*r)) \sqsubseteq (z, t)$
$\Leftrightarrow$ ⟨ Part a of this theorem, proved below ⟩
$s + \lceil(yx^*r) \leq t \ \wedge\ \neg t\neg\lceil(yx^*r)yx^* \leq z$
$\Leftrightarrow$ ⟨ $\lceil(yx^*r) \leq t \ \Rightarrow\ \neg t \leq \neg\lceil(yx^*r)$ & BA ⟩
$s + \lceil(yx^*r) \leq t \ \wedge\ \neg tyx^* \leq z$
$\Leftarrow$ ⟨ By isotony, (23)K and BA, $\neg tyx^* \leq z \ \Rightarrow\ \neg tyx^*r \leq zr \ \Rightarrow\ \lceil(\neg tyx^*r) \leq \lceil(zr) \Leftrightarrow \neg t\lceil(yx^*r) \leq \lceil(zr) \Leftrightarrow \lceil(yx^*r) \leq \lceil(zr) + t \Rightarrow \lceil(yx^*r) \leq t$ (the last step uses $\lceil(zr) \leq t$ from the next line) ⟩
$\lceil(zr) + s \leq t \ \wedge\ \neg tyx^* \leq z$
$\Leftarrow$ ⟨ Definition 1(l)K ⟩

$$
\begin{array}{ll}
& \lceil(zr) + s \leq t \ \wedge \ zx + \neg ty \leq z \\
\Leftrightarrow & \quad \langle \text{ Definition 1(h)K \& (58) } \rangle \\
& \lceil(zr) + s \leq t \ \wedge \ \neg t(zx + y) \leq z \\
\Leftrightarrow & \quad \langle \text{ BA \& } t + \lceil(zr) + s \leq t \ \Rightarrow \ \neg t \leq \neg(t + \lceil(zr) + s) \rangle \\
& t + \lceil(zr) + s \leq t \ \wedge \ \neg t\neg(t + \lceil(zr) + s)(zx + y) \leq z \\
\Leftrightarrow & \quad \langle \text{ Part a of this theorem, proved below } \rangle \\
& (\neg(t + \lceil(zr) + s)(zx + y), t + \lceil(zr) + s) \sqsubseteq (z, t) \\
\Leftrightarrow & \quad \langle \text{ (30)K } \rangle \\
& (\neg(t + \lceil(zr) + s)(\neg\lceil(zr)zx + y), t + \lceil(zr) + s) \sqsubseteq (z, t) \\
\Leftrightarrow & (\neg\lceil(zr)zx, t + \lceil(zr)) \oplus (y, s) \sqsubseteq (z, t) \\
= & (z, t) \odot (x, r) \oplus (y, s) \sqsubseteq (z, t)
\end{array}
$$

(m)
$$
\begin{array}{ll}
& (x, t) \odot (x, t)^{\widetilde{\omega}} \oplus (1, 0) \\
= & (x, t) \odot (\neg\lceil(x^*t)\neg\nabla xx^*, \lceil(x^*t) + \nabla x) \oplus (1, 0) \\
= & (\neg\lceil(x(\lceil(x^*t) + \nabla x))x\neg\lceil(x^*t)\neg\nabla xx^*, t + \lceil(x(\lceil(x^*t) + \nabla x))) \oplus (1, 0) \\
= & \quad \langle \text{ Definition 1(h)K \& (22)K } \rangle \\
& (\neg(\lceil(x\lceil(x^*t)) + \lceil(x\nabla x))x\neg\lceil(x^*t)\neg\nabla xx^*, t + \lceil(x\lceil(x^*t)) + \lceil(x\nabla x)) \oplus (1, 0) \\
= & \quad \langle \text{ BA \& (26)K \& (14)K \& (20)K \& (22)K } \rangle \\
& (\neg\lceil(xx^*t)\neg\lceil(x\nabla x)xx^*, \lceil(t + xx^*t) + \lceil(x\nabla x)) \oplus (1, 0) \\
= & \quad \langle \text{ (9)K \& (42) } \rangle \\
& (\neg\lceil(xx^*t)\neg\nabla xxx^*, \lceil(x^*t) + \nabla x) \oplus (1, 0) \\
= & (\neg(\lceil(x^*t) + \nabla x + 0)(\neg\lceil(xx^*t)\neg\nabla xxx^* + 1), \lceil(x^*t) + \nabla x + 0) \\
= & \quad \langle \text{ Definition 1(c)K \& BA } \rangle \\
& (\neg\lceil(x^*t)\neg\nabla x(\neg\lceil(xx^*t)\neg\nabla xxx^* + 1), \lceil(x^*t) + \nabla x) \\
= & \quad \langle \text{ Definition 1(h)K \& } xx^*t \leq x^*t \text{ by Definition 1(j)K, hence } \neg\lceil(x^*t)\neg\lceil(xx^*t) = \neg\lceil(x^*t) \text{ \& BA } \rangle \\
& (\neg\lceil(x^*t)\neg\nabla x(xx^* + 1), \lceil(x^*t) + \nabla x) \\
= & \quad \langle \text{ Definition 1(j)K } \rangle \\
& (\neg\lceil(x^*t)\neg\nabla xx^*, \lceil(x^*t) + \nabla x) \\
= & (x, t)^{\widetilde{\omega}}
\end{array}
$$

(n) In this proof, the abbreviation $p \stackrel{\text{def}}{=} \lceil(x^*(r + s)) + \nabla x$ is used. Note that p is a guard.

$$
\begin{array}{ll}
& (z, t) \sqsubseteq (x, r)^{\widetilde{\omega}} \odot (y, s) \\
\Leftrightarrow & (z, t) \sqsubseteq (\neg\lceil(x^*r)\neg\nabla xx^*, \lceil(x^*r) + \nabla x) \odot (y, s) \\
\Leftrightarrow & (z, t) \sqsubseteq (\neg\lceil(\neg\lceil(x^*r)\neg\nabla xx^*s)\neg\lceil(x^*r)\neg\nabla xx^*y, \lceil(x^*r) + \nabla x + \lceil(\neg\lceil(x^*r)\neg\nabla xx^*s)) \\
\Leftrightarrow & \quad \langle \text{ (23)K \& BA } \rangle \\
& (z, t) \sqsubseteq (\neg\lceil(x^*r)\neg\lceil(x^*s)\neg\nabla xx^*y, \lceil(x^*r) + \lceil(x^*s) + \nabla x) \\
\Leftrightarrow & \quad \langle \text{ BA \& (22)K \& Definition 1(h)K } \rangle \\
& (z, t) \sqsubseteq (\neg px^*y, p) \\
\Leftrightarrow & \quad \langle \text{ Part a of this theorem, proved below } \rangle \\
& t \leq p \ \wedge \ \neg pz \leq \neg px^*y \\
\Leftarrow & \quad \langle \text{ Multiplying both sides of the right inequality below by } \neg p \text{ \& BA } \rangle \\
& t \leq p \ \wedge \ \neg pz \leq x^*y \\
\Leftarrow & \quad \langle \text{ Definition 1(f)K \& } \neg p \leq 1 \text{ \& Isotony } \rangle \\
& t \leq p \ \wedge \ \neg pz \leq (\neg px)^*y \\
\Leftarrow & \quad \langle \text{ (57) \& } \nabla(\neg px) = 0, \text{ since } \nabla(\neg px) \leq \neg p\nabla x \leq \neg\nabla x\nabla x = 0 \text{ by (45), (46), the definition of } p \text{ and BA } \rangle \\
& t \leq p \ \wedge \ \neg pz \leq \neg px\neg pz + y
\end{array}
$$

$\Leftrightarrow$ ⟨ We show $\neg px = \neg px\neg p$.

$\neg px$
$=$ ⟨ BA & Definition of p ⟩
$\neg\lceil x^*(r+s)\rceil\neg\triangledown xx$
$=$ ⟨ (9)K & (42) ⟩
$\neg\lceil xx^*(r+s)+r+s\rceil\neg\lceil x\triangledown x\rceil x$
$=$ ⟨ BA & (22)K & (20)K ⟩
$\neg(r+s+\lceil xx^*(r+s)+x\triangledown x\rceil)x$
$=$ ⟨ Definition 1(h)K & (14)K & (22)K & (20)K & Definition of p & BA ⟩
$\neg(r+s)\neg\lceil xp\rceil x$
$=$ ⟨ (26)K ⟩
$\neg(r+s)\neg\lceil xp\rceil x\neg p$
$=$ ⟨ Reversing the previous steps on $\neg(r+s)\neg\lceil xp\rceil$ ⟩
$\neg px\neg p$
⟩

$t \le p \ \wedge\ \neg pz \le \neg pxz + y$
$\Leftarrow$ ⟨ Definition 1(h,f)K & $\neg p \le 1$ & Isotony ⟩
$t \le p \ \wedge\ \neg pz \le \neg p(xz+y)$
$\Leftarrow$ ⟨ Multiplying each side of the right inequality below by $\neg p$ and using that $\neg p \le \neg(\lceil xt\rceil + r + s)$ because

$\lceil xt\rceil + r + s$
$\le$ ⟨ Using the left inequality $t \le p$ ⟩
$\lceil xp\rceil + r + s$
$=$ ⟨ Definition of p & Definition 1(h)K & (22)K & (14)K ⟩
$\lceil xx^*(r+s)+x\triangledown x\rceil + r + s$
$=$ ⟨ (20)K & (22)K ⟩
$\lceil xx^*(r+s)+r+s\rceil + \lceil x\triangledown x\rceil$
$=$ ⟨ (9)K & (42) & Definition of p ⟩
p
⟩

$t \le p \ \wedge\ \neg(\lceil xt\rceil + r + s)z \le \neg(\lceil xt\rceil + r + s)(xz+y)$
$\Leftarrow$ ⟨ Definition of p & (48) ⟩
$t \le \lceil xt\rceil + r + s \ \wedge\ \neg(\lceil xt\rceil + r + s)z \le \neg(\lceil xt\rceil + r + s)(xz+y)$
$\Leftrightarrow$ ⟨ Part a of this theorem, proved below ⟩
$(z,t) \sqsubseteq (\neg(\lceil xt\rceil + r + s)(xz+y), \lceil xt\rceil + r + s)$
$\Leftrightarrow$ ⟨ (30) ⟩
$(z,t) \sqsubseteq (\neg(r + \lceil xt\rceil + s)(\neg\lceil xt\rceil xz + y), r + \lceil xt\rceil + s)$
$\Leftrightarrow (z,t) \sqsubseteq (\neg\lceil xt\rceil xz, r + \lceil xt\rceil) \oplus (y,s)$
$\Leftrightarrow (z,t) \sqsubseteq (x,r) \odot (z,t) \oplus (y,s)$

(o) $(x,t)^{\circledast} \oplus (x,t)^{\widetilde{\omega}} \odot (0,0)$
$= (x,t)^{\circledast} \oplus (\neg\lceil x^*t\rceil\neg\triangledown xx^*, \lceil x^*t\rceil + \triangledown x) \odot (0,0)$
$= (\neg\lceil x^*t\rceil x^*, \lceil x^*t\rceil) \oplus (\neg\lceil\neg\lceil x^*t\rceil\neg\triangledown xx^*0\rceil\neg\lceil x^*t\rceil\neg\triangledown xx^*0, \lceil x^*t\rceil + \triangledown x + \lceil\neg\lceil x^*t\rceil\neg\triangledown xx^*0\rceil)$
$=$ ⟨ (36) & (20)K & BA ⟩
$(\neg\lceil x^*t\rceil x^*, \lceil x^*t\rceil) \oplus (0, \lceil x^*t\rceil + \triangledown x)$
$= (\neg(\lceil x^*t\rceil + \lceil x^*t\rceil + \triangledown x)(\neg\lceil x^*t\rceil x^* + 0), \lceil x^*t\rceil + \lceil x^*t\rceil + \triangledown x)$

$$
\begin{aligned}
&= && \langle \text{ Definition 1(c)K \& BA } \rangle \\
&\quad (\neg\lceil(x^*t)\neg\nabla x x^*, \lceil(x^*t) + \nabla x) \\
&= (x, t)^{\tilde{\omega}}
\end{aligned}
$$

Verification of the axioms of enabledness ((12)–(15))

(12)
$$
\begin{aligned}
&\lceil(x, t) \odot (x, t) \\
&= (\lceil x + t, 0) \odot (x, t) \\
&= (\neg\lceil((\lceil x + t)t)(\lceil x + t)x, 0 + \lceil((\lceil x + t)t)) \\
&= && \langle \text{ BA \& (20)K } \rangle \\
&\quad (\neg t\lceil x x, t) \\
&= && \langle \text{ (12)K \& (58) } \rangle \\
&\quad (x, t)
\end{aligned}
$$

(13) Assume that guards have the form $(t, 0)$, as stated in part c of the theorem; this is shown below.

$$
\begin{aligned}
&\lceil((t, 0) \odot (x, s)) \\
&= \lceil(\neg\lceil(ts)tx, 0 + \lceil(ts)) \\
&= && \langle \text{ (20)K \& BA } \rangle \\
&\quad \lceil(t\neg sx, ts) \\
&= (\lceil(t\neg sx) + ts, 0) \\
&= && \langle \text{ (58) \& (23)K \& BA } \rangle \\
&\quad (t(\lceil x + s), 0) \\
&\sqsubseteq && \langle \text{ Part a of this theorem, proved below \& BA } \rangle \\
&\quad (t, 0)
\end{aligned}
$$

(14)
$$
\begin{aligned}
&\lceil((x, s) \odot (y, t)) \\
&= \lceil(\neg\lceil(xt)xy, s + \lceil(xt)) \\
&= (\lceil(\neg\lceil(xt)xy) + s + \lceil(xt), 0) \\
&= && \langle \text{ (23)K \& BA } \rangle \\
&\quad (\lceil(xy) + \lceil(xt) + s, 0) \\
&= && \langle \text{ (14)K \& (22)K \& Definition 1(h)K } \rangle \\
&\quad (\lceil(x(\lceil y + t)) + s, 0) \\
&= \lceil(x(\lceil y + t), s) \\
&= && \langle \text{ (36) \& (20)K \& BA \& Definition 1(f)K } \rangle \\
&\quad \lceil(\neg\lceil(x0)x(\lceil y + t), s + \lceil(x0)) \\
&= \lceil((x, s) \odot (\lceil y + t, 0)) \\
&= \lceil((x, s) \odot \lceil(y, t))
\end{aligned}
$$

(15) Assume that the top element is $(0, 1)$, as stated in part b of the theorem; this is shown below.

$$
\begin{aligned}
&\lceil(x, t) \odot (0, 1) \\
&= (\lceil x + t, 0) \odot (0, 1) \\
&= (\neg\lceil((\lceil x + t)1)(\lceil x + t)0, 0 + \lceil((\lceil x + t)1)) \\
&= && \langle \text{ (36) \& BA \& (20)K } \rangle \\
&\quad (0, \lceil x + t) \\
&= && \langle \text{ (36) \& Definition 1(f) } \rangle \\
&\quad (\neg\lceil(x1)x0, t + \lceil(x1)) \\
&= (x, t) \odot (0, 1)
\end{aligned}
$$

Verification of statements a to f of the theorem

(a) $(x, s) \sqsubseteq (y, t)$
$\Leftrightarrow$ ⟨ Definition of $\sqsubseteq$ ⟩
$(x, s) \oplus (y, t) = (y, t)$
$\Leftrightarrow (\neg(s + t)(x + y), s + t) = (y, t)$
$\Leftrightarrow$ ⟨ BA & Definition 1(h)K ⟩
$(\neg t \neg s x + \neg s \neg t y, s + t) = (y, t)$
$\Leftrightarrow$ ⟨ $\neg sx = x$ by (58) & $\neg ty = y$ by (58) & Equality of pairs & Definition of $\leq$ ⟩
$s \leq t \ \wedge \ \neg tx + \neg sy = y$
$\Leftrightarrow$ ⟨ $ty = 0$ & $s \leq t \Rightarrow sy \leq ty \Rightarrow sy = 0$ & Definition 1(c,i)K ⟩
$s \leq t \ \wedge \ \neg tx + (s + \neg s)y = y$
$\Leftrightarrow$ ⟨ BA & Definition 1(f)K & Definition of $\leq$ ⟩
$s \leq t \ \wedge \ \neg tx \leq y$

(b) $(x, t) \sqsubseteq (0, 1)$
$\Leftrightarrow$ ⟨ Part a of this theorem ⟩
$t \leq 1 \ \wedge \ \neg 1 x \leq 0$
$\Leftrightarrow$ ⟨ BA & Definition 1(g)K ⟩
true

(c) A pair (x, s) is a guard iff there exists a complement (y, t) satisfying (10), that is, $(x, s) \odot (y, t) = (y, t) \odot (x, s) = (0, 0)$ and $(x, s) \oplus (y, t) = (1, 0)$. Now,
$(x, s) \odot (y, t) = (0, 0)$
$\Leftrightarrow (\neg^{\lceil}(xt)xy, s + {}^{\lceil}(xt)) = (0, 0)$
$\Leftrightarrow$ ⟨ Equality of pairs ⟩
$\neg^{\lceil}(xt)xy = 0 \ \wedge \ s + {}^{\lceil}(xt) = 0$
$\Rightarrow$ ⟨ BA & Definition 1(f)K ⟩
$xy = 0 \ \wedge \ s = 0.$

Similarly, $(y, t) \odot (x, s) = (0, 0) \Rightarrow yx = 0 \wedge t = 0$. Using $s = t = 0$ in the constraint $(x, s) \oplus (y, t) = (1, 0)$, we get $(x, 0) \oplus (y, 0) = (1, 0) \Leftrightarrow x + y = 1$. Hence, x and y are guards and $y = \neg x$.

(d) By (11), parts b and c of this theorem, BA and (20)K, $(t, 0)^{\circ} = \neg(t, 0) \odot (0, 1) \oplus (1, 0) = (\neg t, 0) \odot (0, 1) \oplus (1, 0) = (0, \neg t) \oplus (1, 0) = (t, \neg t)$.

(e) By (34), parts b and c of this theorem, BA and (20)K, $\neg_{\shortmid}(t, \neg t) = \neg^{\lceil}((t, \neg t) \odot (0, 0)) \odot (0, 1) \oplus (1, 0) = \neg^{\lceil}(0, \neg t) \odot (0, 1) \oplus (1, 0) = \neg(\neg t, 0) \odot (0, 1) \oplus (1, 0) = (t, 0) \odot (0, 1) \oplus (1, 0) = (0, t) \oplus (1, 0) = (\neg t, t)$.

(f) By Definition 8, (36), (20)K and BA, ${}^{\shortmid}(x, t) = (x, t) \odot (0, 0) \oplus (1, 0) = (0, t) \oplus (1, 0) = (\neg t, t)$. □

And now the main theorem.

Theorem 16

(a) Every DRAe *is isomorphic to an algebra of ordered pairs as in Definition 14. The isomorphism is given by* $\phi(x) \stackrel{\text{def}}{=} (\neg^{\lceil}(x0)x, {}^{\lceil}(x0))$, *with inverse* $\psi((x, t)) \stackrel{\text{def}}{=} x + t\top$.

(b) Every KAD *K satisfying (57) can be embedded in a* DRAe *D in such a way that* D_K *is the image of K by the embedding.*

Proof

(a) Let D be a DRAe. The sub-Kleene algebra $(D_K, +, \cdot, {}^*, {}^{\lceil}, 0, 1)$ of D satisfies (57), by Theorem 12. Use D_K to construct an algebra of pairs $(P, \oplus, \odot, {}^{\circledast}, {}^{\tilde{\omega}}, {}^{\lceil}, (0, 0), (1, 0))$ as per Definition 14. We first show that ψ is the inverse of ϕ, so that they both are bijective functions.

i. $\psi(\phi(x))$
$= \psi((\neg\ulcorner(x0)x, \ulcorner(x0)))$
$= \neg\ulcorner(x0)x + \ulcorner(x0)\top$
$= \quad \langle\ (53)\ \rangle$
x

ii. $\phi(\psi((x,t)))$
$= \phi(x + t\top)$
$= (\neg\ulcorner((x + t\top)0)(x + t\top), \ulcorner((x + t\top)0))$
$= \quad \langle$ Definition 1(i) & (3) $\rangle$
$(\neg\ulcorner(x0 + t\top)(x + t\top), \ulcorner(x0 + t\top))$
$= \quad \langle$ Since $x \in D_K, x0 = 0$ by (49) & Definition 1(c) $\rangle$
$(\neg\ulcorner(t\top)(x + t\top), \ulcorner(t\top))$
$= \quad \langle\ (28)\ \rangle$
$(\neg t(x + t\top), t)$
$= \quad \langle$ Definition 1(h,g,c) & BA & $\neg tx = x$ by (58) $\rangle$
(x, t)

What remains to show is that ϕ preserves the operations. Since ψ is the inverse of ϕ, it is equivalent to show that ψ preserves the operations and this is what we do (it is somewhat simpler).

i. $\psi((x,s) \oplus (y,t))$
$= \psi((\neg(s + t)(x + y), s + t))$
$= \neg(s + t)(x + y) + (s + t)\top$
$= \quad \langle$ BA & Definition 1(h,i) $\rangle$
$\neg t\neg sx + \neg s\neg ty + s\top + t\top$
$= \quad \langle\ \neg sx = x$ and $\neg ty = y$ by (58) & $tx \leq t\top$ by (2) & $sy \leq s\top$ by (2) $\rangle$
$\neg tx + tx + \neg sy + sy + s\top + t\top$
$= \quad \langle$ Definition 1(i,f) & BA $\rangle$
$x + s\top + y + t\top$
$= \psi((x,s)) + \psi((y,t))$

ii. $\psi((x,s) \odot (y,t))$
$= \psi((\neg\ulcorner(xt)xy, s + \ulcorner(xt)))$
$= \neg\ulcorner(xt)xy + (s + \ulcorner(xt))\top$
$= \quad \langle$ Definition 1(i) & $\ulcorner(xt)xy \leq \ulcorner(xt)\top$ by (2) $\rangle$
$\neg\ulcorner(xt)xy + \ulcorner(xt)xy + s\top + \ulcorner(xt)\top$
$= \quad \langle$ Definition 1(i,f) & BA & (15) $\rangle$
$xy + s\top + xt\top$
$= \quad \langle$ Definition 1(i,h) & (3) $\rangle$
$(x + s\top)(y + t\top)$
$= \psi((x,s)) \cdot \psi((y,t))$

iii. $\psi((x,t)^{\circledast})$
$= \psi((\neg\ulcorner(x^*t)x^*, \ulcorner(x^*t)))$
$= \neg\ulcorner(x^*t)x^* + \ulcorner(x^*t)\top$
$= \quad \langle\ \ulcorner(x^*t)x^* \leq \ulcorner(x^*t)\top$ by (2) $\rangle$
$\neg\ulcorner(x^*t)x^* + \ulcorner(x^*t)x^* + \ulcorner(x^*t)\top$

$$
\begin{aligned}
&= && \langle \text{ Definition 1(i,f) \& BA \& (15) } \rangle \\
&\quad x^* + x^* t \top \\
&= && \langle \text{ Definition 1(h,f) \& (7) } \rangle \\
&\quad x^*(t\top)^* \\
&= && \langle \text{ (3) } \rangle \\
&\quad x^*(t\top x^*)^* \\
&= && \langle \text{ (6) } \rangle \\
&\quad (x + t\top)^* \\
&= (\psi((x,t)))^*
\end{aligned}
$$

iv.
$$
\begin{aligned}
&\psi((x,t)^{\widetilde{\omega}}) \\
&= \psi((\neg\lceil(x^*t)\neg\nabla x x^*, \lceil(x^*t) + \nabla x)) \\
&= \neg\lceil(x^*t)\neg\nabla x x^* + (\lceil(x^*t) + \nabla x)\top \\
&= && \langle \text{ BA \& } (\lceil(x^*t) + \nabla x)x^* \leq (\lceil(x^*t) + \nabla x)\top \text{ by (2) } \rangle \\
&\quad \neg(\lceil(x^*t) + \nabla x)x^* + (\lceil(x^*t) + \nabla x)x^* + (\lceil(x^*t) + \nabla x)\top \\
&= && \langle \text{ Definition 1(i,f) \& BA \& (50) } \rangle \\
&\quad x^* + \lceil(x^*t)\top + \lceil(x^\omega 0)\top \\
&= && \langle \text{ (15) \& } x^\omega 0 = x^\omega 0 t\top \text{ by Definition 1(g) } \rangle \\
&\quad x^* + x^* t\top + x^\omega 0 + x^\omega 0 t\top \\
&= && \langle \text{ Definition 1(i,o) } \rangle \\
&\quad x^\omega + x^\omega t\top \\
&= && \langle \text{ Definition 1(f,h) \& (7) } \rangle \\
&\quad x^\omega(t\top)^\omega \\
&= && \langle \text{ (6) \& } t\top x^\omega = t\top \text{ by (3) } \rangle \\
&\quad (x + t\top)^\omega \\
&= (\psi((x,t)))^\omega
\end{aligned}
$$

v.
$$
\begin{aligned}
&\psi(\lceil(x,t)) \\
&= \psi((\lceil x + t, 0)) \\
&= \lceil x + t + 0\top \\
&= && \langle \text{ Definition 1(g,c) } \rangle \\
&\quad \lceil x + t \\
&= && \langle \text{ (22) \& (28) } \rangle \\
&\quad \lceil(x + t\top) \\
&= \lceil(\psi((x,t)))
\end{aligned}
$$

vi. By definition of ψ and Definition 1(g,c), $\psi((0,0)) = 0 + 0\top = 0$.

vii. By definition of ψ and Definition 1(g,c), $\psi((1,0)) = 1 + 0\top = 1$.

viii. By Theorem 15(c) and Definition 1(g,c), $\psi(\neg(t,0)) = \psi((\neg t, 0)) = \neg t + 0\top = \neg t = \neg(t + 0\top) = \neg\psi(t,0)$.

(b) By Theorem 15, the construction in Definition 14 can be used to produce a DRAe P of pairs from K. Since $(x,t)\odot(0,0) = (t,0)$, as is easily verified, the pairs of the form $(x,0)$ are precisely those that satisfy $(x,0)\odot(0,0) = (0,0)$ and thus constitute a KAD by Theorem 12. In addition, $(x,0)\oplus(y,0) = (x+y,0)$, $(x,0)\odot(y,0) = (xy,0)$, $(x,0)^{\circledast} = (x^*,0)$, $\lceil(x,0) = (\lceil x,0)$ and $\neg(t,0) = (\neg t,0)$, as is readily checked. Thus the embedding of K in P is simply $x \mapsto (x,0)$. □

Example 17. Figure 3 may help visualising some of the results. It displays the DRAe of ordered pairs built from the algebra of all 16 relations over the set $\{\bullet, \circ\}$. The following abbreviations are used: $\mathsf{a} = \{(\bullet,\circ)\}$, $\mathsf{b} = \{(\circ,\bullet)\}$, $\mathsf{s} = \{(\bullet,\bullet)\}$, $\mathsf{t} = \{(\circ,\circ)\}$, $0 = \{\}$, $\top\!\!\top = \mathsf{a} + \mathsf{b} + \mathsf{s} + \mathsf{t}$, $1 = \mathsf{s} + \mathsf{t}$, $\overline{1} = \mathsf{a} + \mathsf{b}$. The guards are $(0,0)$, $(\mathsf{s},0)$, $(\mathsf{t},0)$, $(1,0)$ and the assertions are $(1,0)$, (t,s), (s,t), $(0,1)$. The conjunctive predicate transformer f corresponding to a pair (x,t) is given by $f(s) \stackrel{\text{def}}{=} \neg t\neg\lceil(x\neg s)$. In words, a transition by x is guaranteed to reach a state in s if the initial state cannot lead to nontermination ($\neg t$) and it is not possible for x to reach a state that is not in s ($\neg\lceil(x\neg s)$). The predicate transformers for all pairs follow. The entry for line $(\mathsf{t} + \overline{1}, 0)$ and column t, for instance, is s because $f(\mathsf{t}) = \neg 0\neg\lceil((\mathsf{t} + \overline{1})\neg\mathsf{t}) = \mathsf{s}$, as is readily checked. Modulo the representation of sets by subidentity relations, these predicate transformers are the same as those of

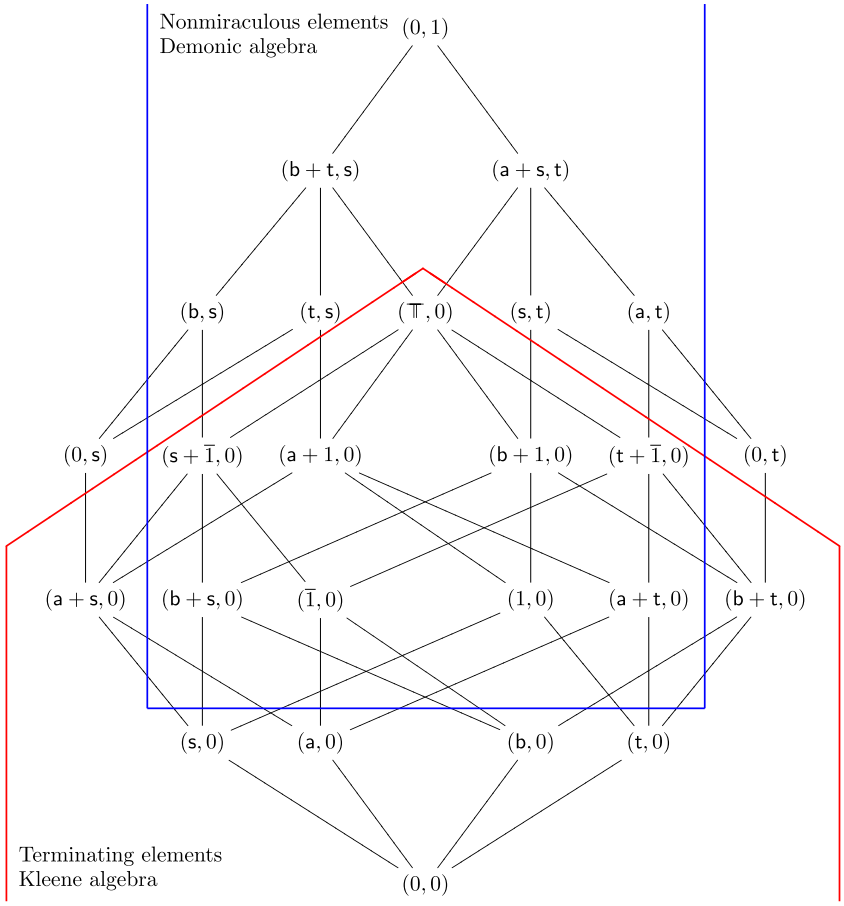

Fig. 3. A demonic refinement algebra of ordered pairs.

Figure 1 and they are listed in the same order. For instance, the complementary guards f_{21} and f_{24} of Example 2 correspond to the guards (s, 0) and (t, 0) in the following table.

	0 s t 1
(0, 1)	0 0 0 0
(b + t, s)	0 0 0 t
(a + s, t)	0 0 0 s
(b, s)	0 t 0 t
(t, s)	0 0 t t
(⊤, 0)	0 0 0 1
(s, t)	0 s 0 s
(a, t)	0 0 s s
(0, s)	t t t t

	0 s t 1
(s + 1̄, 0)	0 t 0 1
(a + 1, 0)	0 0 t 1
(b + 1, 0)	0 s 0 1
(t + 1̄, 0)	0 0 s 1
(0, t)	s s s s
(a + s, 0)	t t t 1
(b + s, 0)	0 1 0 1
(1̄, 0)	0 t s 1

	0 s t 1
(1, 0)	0 s t 1
(a + t, 0)	0 0 1 1
(b + t, 0)	s s s 1
(s, 0)	t 1 t 1
(a, 0)	t t 1 1
(b, 0)	s 1 s 1
(t, 0)	s s 1 1
(0, 0)	1 1 1 1

Going back to Figure 3, we see that the *terminating elements*, that is, those of the form $(x, 0)$, form a Kleene algebra, in this case a relation algebra isomorphic to the full algebra of relations over $\{\bullet, \circ\}$. For these terminating elements, $\ulcorner(x, 0) = (\ulcorner x, 0)$ (by Definition 14), so that enabledness on pairs directly corresponds to the domain operator on the first component relation.

Another subset of the pairs is identified as the *nonmiraculous elements*, or *demonic algebra*, in the figure. This subset forms a demonic algebra [4,5,7,8]. Its pairs are total, that is, $\ulcorner(x, t) = (\ulcorner x + t, 0) = (1, 0)$ (the identity element on pairs). From any starting state, (x, t) is *enabled*, in the sense that it either leads to a result or to nontermination.

The termination operator applied to (x, t) gives $\lceil\!\lceil(x, t) = (\neg t, t)$ (Theorem 15(f)). This is interpreted as saying that termination is guaranteed for initial states in $\neg t$. In the demonic algebra of [4,5,7,8], the demonic domain of x, $\lceil\!\lceil x$, is equal to $\neg t$, so that the termination operator and demonic domain correspond on the subset of nonmiraculous elements.

Some elements are nonterminating, some are miraculous, and some are both, such as $(0, \mathtt{t})$. This element does not terminate for initial states in t (here, $\{\circ\}$) and terminates for states in $\neg$t while producing no result (this is the miracle), due to the first component being 0.

The set of terminating elements (the Kleene algebra) is the set D_K defined in (49). The set of nonmiraculous elements (the demonic algebra) is the set D_D defined in (55). For pairs, the function ϕ mapping D_K to D_D (see (56)) is $\phi((x, t)) = (x, \neg\lceil x)$, by Definition 14 and Theorem 15. For instance, $\phi((0, 0)) = (0, 1)$ and $\phi((\mathtt{a}, 0)) = (\mathtt{a}, \mathtt{t})$. The terminating and nonmiraculous elements have the form $(x, 0)$, with $\lceil x = 1$. They are mapped to themselves. For instance, $\phi((\top\!\!\top, 0)) = (\top\!\!\top, 0)$.

Instead of viewing pairs as the representation of programs, we can view them as specifications. The weakest specification is $(0, 1)$ at the top of the lattice. It does not even require termination for a single initial state. Lower down, there is the *havoc* element $(\top\!\!\top, 0)$. As a specification, it requires termination, but arbitrary final states are assigned to initial states. Still lower, there is the identity element $(1, 0)$. It requires termination and assigns a single final state to each initial state. The least element of the lattice, $(0, 0)$, also requires termination, but it is a specification so strong that it assigns no final state to any initial state; we could say it is a contradictory specification.

5. Conclusion

The main theorem of this paper, Theorem 16, provides an alternative, equivalent way to view a DRAe as an algebra of ordered pairs of elements of a KAD (whence the word *abstract* in the title of the paper). This view, or the related decomposition of any element x of a DRAe as $x = a + t\top$ (Theorem 13), offers an intuitive grasp of the underlying programming concepts that is easier to understand than the predicate transformer model of DRAe for the relationally minded (this may explain why pair-based representations have been used numerous times, such as in [2,15,17,23,24], to cite just a few).

It is asserted in [13] that the divergence operator often provides a more convenient description of nontermination than the ω operator of omega algebra. Theorem 16 brings some weight to this assertion, because DRAe, although it has an ω operator (different from that of omega algebra, though), is equivalent to an algebra of ordered pairs of elements of a KAD with divergence and without an ω operator.

A side effect of Theorem 16 is that the complexity of the theory of DRAe is at most that of KAD with a divergence operator satisfying the implication in (57) (this complexity is unknown at the moment).

As future work, we plan to look at the variants of DRAe mentioned in the introduction to see if similar results can be obtained. We would also like to determine whether the second condition in (57) holds in every KAD where $\triangledown$ is defined.

Acknowledgements

We thank Georg Struth and the anonymous referees of this special issue of *The Journal of Logic and Algebraic Programming* as well as those of the *10th International Conference on Relational Methods in Computer Science (RelMiCS10) and 5th International Conference on Applications of Kleene Algebra (AKA5)* for their helpful comments. This research was partially supported by NSERC (Natural Sciences and Engineering Research Council of Canada) and FQRNT (Fonds québécois de la recherche sur la nature et les technologies).

Appendix A. On the Mild Condition in (57)

We have not been able to determine whether the "mild condition" in (57) holds in every KAD where $\triangledown$ is defined. What follows are related results that may help find the answer.

Lemma 18. *Let K be a* KAD *where* $\triangledown$ *is defined. Then*

$$\triangledown x = 0 \;\wedge\; z \leq xz + y \;\Rightarrow\; \lceil z \leq \lceil(x^* y).$$

Proof

$$\begin{array}{ll} & \triangledown x = 0 \;\wedge\; z \leq xz + y \\ \Rightarrow & \qquad \langle\ (22)\mathsf{K}\ \&\ (14)\mathsf{K}\ \rangle \\ & \triangledown x = 0 \;\wedge\; \lceil z \leq \lceil(x\lceil z) + \lceil y \end{array}$$

$$
\begin{array}{ll}
\Rightarrow & \langle\ (48)\ \rangle \\
\quad \nabla x = 0 \ \wedge\ \lceil z \leq \lceil (x^* \lceil y) + \nabla x \\
\Rightarrow & \langle\ (14)\mathsf{K}\ \rangle \\
\quad \lceil z \leq \lceil (x^* y) & \square
\end{array}
$$

Lemma 19. *Let K be a* KAD *where ∇ is defined and suppose $\nabla x = 0$. If there exists a z' such that $z' \leq xz' + y$ and $z' \not\leq x^* y$, then there exists a z such that*

$$x^* y \leq z, \quad z \not\leq x^* y, \quad z \leq xz + y \quad \textit{and} \quad \lceil z = \lceil (x^* y).$$

Proof. Take $z \stackrel{\text{def}}{=} z' + x^* y$. The first two properties and $\lceil (x^* y) \leq \lceil z$ are direct from the definition of z. The third property also follows from the definition of z, the hypothesis $z' \leq xz' + y$ and (9)K. Finally, $\lceil z \leq \lceil (x^* y)$ follows from Lemma 18. $\square$

Lemma 20. *Let K be a* KAD *where ∇ is defined. Suppose $\nabla x = 0$ and $z \leq xz + y$. Then, for all $n \in \mathbb{N}$,*

$$\neg \lceil (x^n x^* y) z \leq x^* y. \tag{A.1}$$

Proof. The proof is by induction. For $n = 0$, (A.1) follows from $x^0 = 1$, Definition 1(f,g)K, (12)K, Lemma 18 and BA:

$$\neg \lceil (x^0 x^* y) z = \neg \lceil (x^* y) \lceil z z = 0 \leq x^* y.$$

For the induction step, assume (A.1).

$$
\begin{array}{ll}
 & \neg \lceil (x^{n+1} x^* y) z \\
\leq & \langle\ z \leq xz + y\ \&\ \text{Definition 1(h)K}\ \rangle \\
 & \neg \lceil (x^{n+1} x^* y) xz + \neg \lceil (x^{n+1} x^* y) y \\
\leq & \langle\ x^{n+1} = x x^n\ \&\ (14)\mathsf{K}\ \&\ \neg \lceil x \leq 1 \text{ for all } x\ \&\ \text{Definition 1(f)K}\ \rangle \\
 & \neg \lceil (x \lceil (x^n x^* y)) xz + y \\
= & \langle\ (26)\ \rangle \\
 & \neg \lceil (x \lceil (x^n x^* y)) x \neg \lceil (x^n x^* y) z + y \\
\leq & \langle\ \neg \lceil x \leq 1 \text{ for all } x\ \&\ \text{Definition 1(f)K}\ \&\ \text{Induction hypothesis}\ \rangle \\
 & x x^* y + y \\
= & \langle\ (9)\mathsf{K}\ \rangle \\
 & x^* y \quad \square
\end{array}
$$

If $z \not\leq x^* y$, there must exist a test $t \neq 0$ such that $tz \not\leq x^* y$. By (A.1), we can take $t \leq \lceil (x^n x^* y)$ and this must hold for all $n \in \mathbb{N}$. Assuming that infinite products of tests exist,

$$t \leq (\prod n \mid 0 \leq n : \lceil (x^n x^* y)). \tag{A.2}$$

Now,

$$(\prod n \mid 0 \leq n : \lceil (x^n)) = 0 \tag{A.3}$$

expresses that x is *progressively bounded*, i.e., thinking relationally, that the length of all paths by x starting from any point is bounded, while $\nabla x = 0$ expresses that x is *progressively finite*, i.e., that there are no infinite paths by x from any point (see [25]). For relations, progressive boundedness implies progressive finiteness. This can be shown in KAD as follows: from (40) and (14)K, it is easy to show by induction that $\nabla x \leq \lceil (x^n \nabla x) \leq \lceil (x^n)$ for all $n \in \mathbb{N}$, so that $\nabla x \leq (\prod n \mid n \in \mathbb{N} : \lceil x^n) \leq 0$ if x is progressively bounded.

Let $\mathsf{PB}(x)$ denote that x is progressively bounded, i.e., (A.3) holds. Because $\lceil (x^n x^* y) \leq \lceil (x^n)$, we get from the previous discussion

$$\mathsf{PB}(x) \ \Rightarrow\ (\prod n \mid 0 \leq n : \lceil (x^n x^* y)) = 0$$

and thus

$$\mathsf{PB}(x) \ \Rightarrow\ \nabla x = 0 \ \wedge\ (z \leq xz + y \ \Rightarrow\ z \leq x^* y).$$

Consider the following relation on $\mathbb{N}$ [25]:

$$R \stackrel{\text{def}}{=} \{(n+1, n) \mid n \in \mathbb{N}\} \cup \{(\bullet, n) \mid n \in \mathbb{N}\}.$$

This relation is progressively finite but not progressively bounded, because the length of paths from $\bullet$ is not bounded. Now take $Q \stackrel{\text{def}}{=} \{(0,0)\}$. Then $(\prod n \mid 0 \leq n : \ulcorner(R^n R^* Q)) = \{(\bullet, \bullet)\}$. However, it does not seem possible to violate (57) using R, so that finding a $t \neq 0$ that satisfies (A.2) is not a guarantee to find a counterexample to (57).

In conclusion, if there is a counterexample to (57) in a KAD where $\triangledown$ is defined, the following three conditions must be met:

1. the KAD must not be a complete lattice;
2. either $(\prod n \mid 0 \leq n : \ulcorner(x^n))$ does not exist or it exists and it is different from 0;
3. $z = x^* y + w$, with $w \not\leq x^* y$ and $\ulcorner w \leq \ulcorner(x^* y)$.

References

[1] R. Backhouse, Galois connections and fixed point calculus, in: R. Backhouse, R. Crole, J. Gibbons (Eds.), Algebraic and Coalgebraic Methods in the Mathematics of Program Construction, Lecture Notes in Computer Science, vol. 2297, Springer, 2002, pp. 89–150.
[2] R. Berghammer, H. Zierer, Relational algebraic semantics of deterministic and nondeterministic programs, Theor. Comput. Sci. 43 (2–3) (1986) 123–147.
[3] E. Cohen, Separation and reduction, in: R. Backhouse, J.N. Oliveira (Eds.), Mathematics of Program Construction, Lecture Notes in Computer Science, vol. 1837, Springer, 2000, pp. 45–59.
[4] J.-L. De Carufel, J. Desharnais, Demonic algebra with domain, in: R.A. Schmidt (Ed.), Relations and Kleene Algebra in Computer Science, Lecture Notes in Computer Science, vol. 4136, Springer, 2006, pp. 120–134.
[5] J.-L. De Carufel, J. Desharnais, Latest news about demonic algebra with domain, in: R. Berghammer, B. Möller (Eds.), Relations and Kleene Algebra in Computer Science, Lecture Notes in Computer Science, vol. 4988, Springer, 2008, pp. 53–67.
[6] J.-L. De Carufel, J. Desharnais, On the structure of demonic refinement algebras with enabledness and termination, in: R. Berghammer, B. Möller (Eds.), Relations and Kleene Algebra in Computer Science, Lecture Notes in Computer Scince, vol. 4988, Springer, 2008, pp. 68–82.
[7] J.-L. De Carufel, J. Desharnais, Demonic algebra with domain, Research report DIUL-RR-0601, Département d'informatique et de génie logiciel, Université Laval, Canada, June 2006. Available at: <http://www.ift.ulaval.ca/∼Desharnais/Recherche/RR/DIUL-RR-0601.pdf>.
[8] J.-L. De Carufel, Demonic Kleene Algebra, Ph.D. Thesis, Université Laval, 2009. Available at: <http://www2.ift.ulaval.ca/∼Desharnais/Recherche/Theses/index.html>.
[9] J. Desharnais, G. Struth, Domain axioms for a family of near-semirings, in: J. Meseguer, G. Roşu (Eds.), Algebraic Methodology and Software Technology, Lecture Notes in Computer Science, vol. 5140, Springer, 2008, pp. 330–345.
[10] J. Desharnais, G. Struth, Modal semirings revisited, in: P. Audebaud, C. Paulin-Mohring (Eds.), Mathematics of Program Construction, Lecture Notes in Computer Science, vol. 5133, Springer, 2008, pp. 360–387.
[11] J. Desharnais, B. Möller, G. Struth, Modal Kleene algebra and applications – a survey – JoRMiCS, J. Relat. Methods Comput. Sci. 1 (2004) 93–131.
[12] J. Desharnais, B. Möller, G. Struth, Kleene algebra with domain, ACM Trans. Comput. Logic (TOCL) 7 (4) (2006) 798–833.
[13] J. Desharnais, B. Möller, G. Struth, Algebraic Notions of Termination, Research Report 2006-23, Institut für Informatik, Universität Augsburg, Germany, October 2006.
[14] E.W. Dijkstra, A Discipline of Programming, Prentice Hall, 1976.
[15] H. Doornbos, A relational model of programs without the restriction to Egli-Milner-monotone constructs, in: PROCOMET '94: Proceedings of the IFIP TC2/WG2.1/WG2.2/WG2.3 Working Conference on Programming Concepts, Methods and Calculi, North-Holland, 1994, pp. 363–382.
[16] D. Harel, D. Kozen, J. Tiuryn, Dynamic Logic, MIT Press, 2000.
[17] P. Höfner, B. Möller, K. Solin, Omega algebra, demonic refinement algebra and commands, in: R.A. Schmidt (Ed.), Relations and Kleene Algebra in Computer Science, Lecture Notes in Computer Science, vol. 4136, Springer, 2006, pp. 222–234.
[18] D. Kozen, A completeness theorem for Kleene algebras and the algebra of regular events, Inform. and Comput. 110 (2) (1994) 366–390.
[19] D. Kozen, Kleene algebra with tests, ACM Trans. Program. Lang. Systems 19 (3) (1997) 427–443.
[20] L.A. Meinicke, I.J. Hayes, Probabilistic choice in refinement algebra, in: P. Audebaud, C. Paulin-Mohring (Eds.), Mathematics of Program Construction, Lecture Notes in Computer Science, vol. 5133, Springer, 2008, pp. 243–267.
[21] L.A. Meinicke, K. Solin, Reactive probabilistic programs and refinement algebra, in: R. Berghammer, B. Möller (Eds.), Relations and Kleene Algebra in Computer Science, Lecture Notes in Computer Science, vol. 4988, Springer, 2008, pp. 304–319.
[22] B. Möller, Kleene getting lazy, Sci. Comput. Programming 65 (2007) 195–214.
[23] B. Möller, G. Struth, `wp` is `wlp`, in: W. MacCaull, M. Winter, I. Düntsch (Eds.), Relational Methods in Computer Science, Lecture Notes in Computer Science, vol. 3929, Springer, 2005, pp. 200–211.
[24] D.L. Parnas, A generalized control structure and its formal definition, Commun. ACM 26 (8) (1983) 572–581.
[25] G. Schmidt, T. Ströhlein, Relations and Graphs, Springer, 1988.
[26] K. Solin, On two dually nondeterministic refinement algebras, in: R.A. Schmidt (Ed.), Relations and Kleene Algebra in Computer Science, Lecture Notes in Computer Science, vol. 4136, Springer, 2006, pp. 373–387.
[27] K. Solin, J. von Wright, Refinement algebra with operators for enabledness and termination, in: T. Uustalu (Ed.), Mathematics of Program Construction, Lecture Note in Computer Science, vol. 4014, Springer, 2006, pp. 397–415.
[28] K. Solin, J. von Wright, Refinement algebra extended with operators for enabledness and termination, Tech. Rep. 658, Turku Center for Computer Science, University of Turku, Finland, TUCS Technical Report, January 2005.
[29] K. Solin, Abstract Algebra of Program Refinement, Ph.D. Thesis, Turku Center for Computer Science, University of Turku, Finland, 2007.
[30] J. von Wright, From Kleene algebra to refinement algebra, in: E.A. Boiten, B. Möller (Eds.), Mathematics of Program Construction, Lecture Notes in Computer Science, vol. 2386, Springer, 2002, pp. 233–262.
[31] J. von Wright, Towards a refinement algebra, Sci. Comput. Programming 51 (2004) 23–45.