UNIVERSITÉ
LAVAL

FACULTÉ DES SCIENCES ET DE GÉNIE
Département d'informatique et de génie logiciel

Pavillon Adrien-Pouliot, local 3908
1065, avenue de la Médecine
Université Laval
Québec, Canada, G1V A06

ON THE STRUCTURE OF DEMONIC REFINEMENT ALGEBRAS

PAR

JEAN-LOU DE CARUFEL
ET
JULES DESHARNAIS

RAPPORT DE RECHERCHE
DIUL-RR-0802

DÉPARTEMENT D'INFORMATIQUE ET DE GÉNIE LOGICIEL
FACULTÉ DES SCIENCES ET DE GÉNIE

Pavillon Adrien-Pouliot
1065, avenue de la Médecine
Université Laval
Québec, QC, Canada
G1V 0A6

JANVIER 2008

On the Structure of Demonic Refinement Algebras*

Jean-Lou De Carufel and Jules Desharnais

Département d'informatique et de génie logiciel, Pavillon Adrien-Pouliot,
1065, avenue de la Médecine, Université Laval, Québec, QC, Canada G1V 0A6
jldec1@ift.ulaval.ca, Jules.Desharnais@ift.ulaval.ca

January 15, 2008

Abstract

The main result of this report 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.

1 Introduction

Demonic Refinement Algebra (DRA) was introduced by von Wright in [23, 24]. It is a variant of Kleene Algebra (KA) and Kleene algebra with tests (KAT) as defined by Kozen [14, 15] 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 [20, 21, 22], giving an algebra called DRAet in [20] and in this report. 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) [8, 10]. 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 [19, 20]; a generalisation named General Refinement Algebra was also obtained in [24] by weakening the axioms of DRA.

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 [9] for the divergence operator, and [17, 13] for its dual, the convergence operator). It is shown in [13] that a similar algebra of ordered pairs of elements of an omega algebra with divergence

*This is an expanded version of [7]. It contains all the proofs that could not be included in the proceedings due to space constraints.

is a DRAet; in [17], these algebras of pairs are mapped to weak omega algebras, a related structure. Our result is stronger because

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 [23, 24, 20, 21, 22] or 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. 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 [23, 24].

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* $+$.

1. $x + (y + z) = (x + y) + z$
2. $x + y = y + x$
3. $x + 0 = x$
4. $x + x = x$
5. $x(yz) = (xy)z$
6. $1x = x = x1$
7. $0x = 0$
8. $x(y + z) = xy + xz$
9. $(x + y)z = xz + yz$
10. $x^* = xx^* + 1$
11. $xz + y \leq z \Rightarrow x^*y \leq z$
12. $zx + y \leq z \Rightarrow yx^* \leq z$
13. $x^\omega = xx^\omega + 1$
14. $z \leq xz + y \Rightarrow z \leq x^\omega y$
15. $x^\omega = x^* + x^\omega 0$

It is easy to verify that $\leq$ is a partial order and that the axioms state 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.

$$x^* = x^*x + 1 \qquad x^\omega = x^\omega x + 1 \tag{4}$$

$$x(yx)^* = (xy)^*x \qquad x(yx)^\omega = (xy)^\omega x \tag{5}$$

$$(x + y)^* = x^*(yx^*)^* \qquad (x + y)^\omega = x^\omega(yx^\omega)^\omega \tag{6}$$

$$(x\top)^* = x\top + 1 \qquad (x\top)^\omega = x\top + 1 \tag{7}$$

$$(x0)^* = x0 + 1 \qquad (x0)^\omega = x0 + 1 \tag{8}$$

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

$$t\neg t = \neg tt = 0 \qquad \text{and} \qquad t + \neg t = 1 \tag{9}$$

is called 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 (9) is in D_G. Properties of guards are similar to those of tests in KAT and KAD.

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

$$t^\circ \overset{\text{def}}{=} \neg t\top + 1 \ . \tag{10}$$

Guards and assertions are order-isomorphic: $s \leq t \Leftrightarrow t^\circ \leq s^\circ$ for all guards s and t. Thus, assertions form a Boolean algebra too. Assertions have a weaker expressive power than guards and guards cannot be defined in terms of assertions, although the latter are defined in terms of guards.

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 set of guards and assertions of a DRA D are denoted by D_G and D_A, respectively. In the proofs, BA abbreviates "Boolean algebra".

Next, we introduce the enabledness and termination operators [20, 21, 22]. The definition below is in fact that of [20], because the isolation axiom (Definition 1(15) above) and axioms (14) and (18) below are not included in [21, 22].

Definition 2 *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.*

$$
\begin{align}
\ulcorner x x &= x \tag{11}\\
\ulcorner(tx) &\leq t \tag{12}\\
\ulcorner(xy) &= \ulcorner(x \ulcorner y) \tag{13}\\
\ulcorner x \top &= x \top \tag{14}
\end{align}
$$

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

$$
\begin{align}
\ulcorner\!\!\ulcorner x x &= x \tag{15}\\
p &\leq \ulcorner\!\!\ulcorner(px) \tag{16}\\
\ulcorner\!\!\ulcorner(xy) &= \ulcorner\!\!\ulcorner(x \ulcorner\!\!\ulcorner y) \tag{17}\\
\ulcorner\!\!\ulcorner x 0 &= x 0 \tag{18}
\end{align}
$$

The termination operator is defined by four axioms in Definition 2 in order to exhibit its similarity with the enabledness operator. It turns out however that Axioms (15), (16) and (17) can be dropped, because they follow from Axiom (18). It is also shown in [20] that $\ulcorner\!\!\ulcorner x0 = x0 \Leftrightarrow \ulcorner\!\!\ulcorner x = x0 + 1$. Thus (15) to (18) are equivalent to $\ulcorner\!\!\ulcorner x = x0 + 1$ and it looks like the termination operator might be *defined* by $\ulcorner\!\!\ulcorner x \stackrel{\text{def}}{=} x0 + 1$, a possibility that is also mentioned in [21, 22]. 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 [19, 20] that $x0 + 1$ is an assertion in daRAet. We show in Sect. 3 that this is the case in DRAe too.

The following are laws of enabledness.

$$
\begin{align}
\ulcorner t &= t \tag{19}\\
\ulcorner \top &= 1 \tag{20}\\
\ulcorner(x + y) &= \ulcorner x + \ulcorner y \tag{21}\\
\ulcorner(tx) &= t \ulcorner x \tag{22}\\
\neg \ulcorner x x &= 0 \tag{23}\\
\ulcorner x = 0 &\Leftrightarrow x = 0 \tag{24}\\
\neg \ulcorner(xt) x &= \neg \ulcorner(xt) x \neg t \tag{25}
\end{align}
$$

In addition, both enabledness and termination are isotone. The first three axioms of enabledness, (11), (12) and (13), are exactly the axioms of the domain operator in KAD. We do not explain at this stage the intuitive meaning of enabledness and termination. This will become clear in Sect. 4 after the introduction of the representation of DRA by algebras of pairs.

In DRA, there seems to be no way to recover by an explicit definition the guard corresponding to a given assertion. This becomes possible in daRA and daRAn [19, 20]. We show in Sect. 3 that it is also possible in DRAe.

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 in DRAe rather than being implicitly defined by Axioms (15) to (18). 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 DRAet 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 3 *Let D be a DRAe and $^\diamond : D_A \to D_G$ be the function defined by*

$$p^\diamond \stackrel{\text{def}}{=} \neg\ulcorner(p0) \ . \tag{26}$$

Then, for any assertion p and guard t

1. *$p^\diamond$ is a guard with complement $\ulcorner(p0)$,*
2. *$t^{\circ\diamond} = t$,*
3. *$p^{\diamond\circ} = p$. Combined with the previous item, this says that $^\circ$ and $^\diamond$ are dual isomorphisms.*

Proof.

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

2. $t^{\circ\diamond}$
 $=$ ⟨ (26) ⟩
 $\neg\ulcorner(t^\circ 0)$
 $=$ ⟨ (10) ⟩
 $\neg\ulcorner((\neg t\top + 1)0)$
 $=$ ⟨ Definition 1(9,6) & (3) ⟩
 $\neg\ulcorner(\neg t\top + 0)$
 $=$ ⟨ Definition 1(3) & (22) ⟩
 $\neg(\neg t\ulcorner\top)$
 $=$ ⟨ (20) & Definition 1(6) & BAof guards ⟩
 t

3. Since p is an assertion, $p = s^\circ$ for some guard s, by (10). Then, using part 2 of this proposition, $p^{\diamond\circ} = s^{\circ\diamond\circ} = s^\circ = p$. □

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

$$\neg p \stackrel{\text{def}}{=} (\neg(p^\diamond))^\circ \quad \text{and} \tag{27}$$

$$p \sqcap q \stackrel{\text{def}}{=} \neg(\neg p + \neg q) \ , \tag{28}$$

for any assertions p and q. Using (10) and (26), it is easy to see that

$$\neg p = \neg\ulcorner(p0)\top + 1 \quad \text{and} \tag{29}$$
$$p \sqcap q = \ulcorner(p0)\ulcorner(q0)\top + 1 \ , \tag{30}$$

as the following derivations show.

1. Proof of (29).

$$\neg p$$
$$= \qquad \langle\ (27)\ \rangle$$
$$(\neg(p^{\diamond}))^{\circ}$$
$$= \qquad \langle\ (26)\ \ \&\ \ \mathsf{BA}\text{ of guards}\ \rangle$$
$$(\ulcorner(p0))^{\circ}$$
$$= \qquad \langle\ (10)\ \rangle$$
$$\neg\ulcorner(p0)\top + 1$$

2. Proof of (30).

$$p \sqcap q$$
$$= \qquad \langle\ (28)\ \rangle$$
$$\neg(\neg p + \neg q)$$
$$= \qquad \langle\ (29)\ \rangle$$
$$\neg\ulcorner((\neg p + \neg q)0)\top + 1$$
$$= \qquad \langle\ (29)\ \rangle$$
$$\neg\ulcorner((\neg\ulcorner(p0)\top + 1 + \neg\ulcorner(q0)\top + 1)0)\top + 1$$
$$= \qquad \langle\ \text{Definition } 1(2,4,9,6,3)\ \rangle$$
$$\neg\ulcorner(\neg\ulcorner(p0)\top + \neg\ulcorner(q0)\top)\top + 1$$
$$= \qquad \langle\ (21)\ \rangle$$
$$\neg(\ulcorner(\neg\ulcorner(p0)\top) + \ulcorner(\neg\ulcorner(q0)\top))\top + 1$$
$$= \qquad \langle\ \text{Definition } 1(3,6)\ \ \&\ \ (22)\ \ \&\ \ (20)\ \rangle$$
$$\neg(\neg\ulcorner(p0) + \neg\ulcorner(q0))\top + 1$$
$$= \qquad \langle\ \mathsf{BA}\text{ of guards}\ \rangle$$
$$\ulcorner(p0)\ulcorner(q0)\top + 1$$

□

Proposition 4 *For a given* DRAe*, the structures*

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

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

Proof. D_G is a BA [23, 24]. That D_A is also one follows from Proposition 3. Proposition 3 shows that $^{\circ}$ is a bijective function from D_G to D_A and the equations $1^{\circ} = 1$, $0^{\circ} = \top$, $(\neg t)^{\circ} = \neg(t^{\circ})$, $(st)^{\circ} = s^{\circ} + t^{\circ}$ and $(s + t)^{\circ} = s^{\circ} \sqcap t^{\circ}$ are easily shown as follows.

1. $1^\circ = 1$ follows from (10), the BA of guards and Definition 1(7,3): $1^\circ = \neg 1 \top + 1 = 0 \top + 1 = 0 + 1 = 1$.

2. $0^\circ = \top$ follows from (10), the BA of guards, Definition 1(6) and (2): $0^\circ = \neg 0 \top + 1 = 1 \top + 1 = \top + 1 = \top$.

3. Using (27) and Proposition 3(2) yields $\neg(t^\circ) = (\neg(t^{\circ\diamond}))^\circ = (\neg t)^\circ$.

4. $$\begin{array}{ll} & (st)^\circ \\ = & \langle\ (10)\ \rangle \\ & \neg(st)\top + 1 \\ = & \langle\ \mathsf{BA}\text{ of guards}\ \rangle \\ & (\neg s + \neg t)\top + 1 \\ = & \langle\ \text{Definition } 1(9,4,2)\ \rangle \\ & \neg s\top + 1 + \neg t\top + 1 \\ = & \langle\ (10)\ \rangle \\ & s^\circ + t^\circ \end{array}$$

5. $$\begin{array}{ll} & s^\circ \sqcap t^\circ \\ = & \langle\ (28)\ \rangle \\ & \neg(\neg(s^\circ) + \neg(t^\circ)) \\ = & \langle\ \neg(t^\circ) = (\neg t)^\circ \text{ (proved above)}\ \rangle \\ & \neg((\neg s)^\circ + (\neg t)^\circ) \\ = & \langle\ (st)^\circ = s^\circ + t^\circ \text{ (proved above)}\ \rangle \\ & \neg((\neg s \neg t)^\circ) \\ = & \langle\ \neg(t^\circ) = (\neg t)^\circ \text{ (proved above)}\ \rangle \\ & (\neg(\neg s \neg t))^\circ \\ = & \langle\ \mathsf{BA}\text{ of guards}\ \rangle \\ & (s + t)^\circ \end{array}$$ □

This is of course consistent with the remark about the order-isomorphism of assertions and guards made in the previous section. Since inverting the order of a Boolean algebra yields another Boolean algebra, $(D_A, +, \sqcap, \neg, 1, \top)$ is also a Boolean algebra and it is ordered by the DRAe ordering $\leq$.

Lemma 5 *In a* DRAe, $x0 + 1$ *is an assertion.*

Proof. Using in turn Definition 1(7), (14), double negation (applicable since $\ulcorner(x0)$ is a guard) and (10), 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 3, it uniquely corresponds to the guard $\neg\ulcorner(x0)$. □

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

Definition 6 *For a given* DRAe D*, the* termination operator $\ulcorner\!\!\ulcorner : D \to D_A$ *is defined by* $\ulcorner\!\!\ulcorner x \stackrel{\text{def}}{=} x0 + 1$.

By the results of Solin and von Wright mentioned in Sect. 2, the termination operator satisfies Axioms (15) to (18).

We now recall the definition of KAD [8, 10].

Definition 7 *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(13,14,15)) and* $\top$ *(i.e., (14)), with the additional axiom that* 0 *is a right zero of composition:*

$$x0 = 0 \ . \tag{31}$$

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 *(9).*

The standard signature of KAT and KAD includes a sort $B \subseteq K$ of tests and a negation operator on B [15, 8, 10]. 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 [10]. Thus, the definition of tests in KAD given above imposes the same constraints as that of guards in DRA given in Sect. 2.

When using the laws of DRAe to justify a transformation for KAD (due to Definition 7), we add a suffix K. For instance, we write Definition 1(7)K and (12)K.

The domain operator satisfies the following inductive law (as does the enabledness operator of DRAe) [10]:

$$\ulcorner(xt) + s \le t \ \Rightarrow\ \ulcorner(x^*s) \le t \ . \tag{32}$$

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

$$\triangledown x \quad \le \quad \ulcorner(x \triangledown x) \ , \tag{33}$$

$$t \le \ulcorner(xt) \quad \Rightarrow \quad t \le \triangledown x \ . \tag{34}$$

$\triangledown x$ is called the *divergence of* x [9] and this test is interpreted as the set of states from which nontermination is possible. The negation of $\triangledown x$ corresponds to what is known as the *halting predicate* in the modal μ-calculus [12]. The operator $\triangledown$ binds stronger than any binary operator but weaker than any unary operator. Among the properties of divergence, we note

$$\triangledown x \quad = \quad \ulcorner(x \triangledown x) \ , \tag{35}$$

$$x \triangledown x \quad = \quad \triangledown x x \triangledown x \ , \tag{36}$$

$$\neg \triangledown x x \quad = \quad \neg \triangledown x x \neg \triangledown x \ , \tag{37}$$

$$\triangledown(tx) \quad \le \quad t \ , \tag{38}$$

$$x \le y \quad \Rightarrow \quad \triangledown x \le \triangledown y \ . \tag{39}$$

Proposition 8 *In a* KAD K *where* ∇x *exists for every* $x \in K$, $\ulcorner(x^*s) + \nabla x$ *is a fixed point of* $f(t) \stackrel{\text{def}}{=} \ulcorner(xt) + s$ *and*

$$t \le \ulcorner(xt) + s \;\Rightarrow\; t \le \ulcorner(x^*s) + \nabla x \;, \tag{40}$$

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

The proof of this proposition is given in [9].

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

$$D_K \stackrel{\text{def}}{=} \{x \in D \mid x0 = 0\} \;. \tag{41}$$

Theorem 9 *Let* D *be a* DRAe. *Then* $(D_K, +, \cdot, {}^*, \ulcorner, 0, 1)$ *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*

$$\nabla x \;=\; \ulcorner(x^\omega 0) \;, \tag{42}$$

$$\nabla x = 0 \;\wedge\; z \le xz + y \;\Rightarrow\; z \le x^* y \;. \tag{43}$$

Proof.

1. The elements of D_K satisfy all axioms of KAD, including (31). 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 1 and 0, since $10 = 0$ and $00 = 0$. Next, if t is a guard, then $t \in D_K$, since $t0 \le 10 = 0$. Thus, guards are the tests of D_K and form a BA with the operations $+, \cdot$ and $\neg$. This implies $\ulcorner x \in D_K$ for all x, since $\ulcorner x$ is a guard. Finally, for the remaining operations, we have the following, where $x0 = 0$ and $y0 = 0$ are assumed, due to (41):
   - $(x + y)0 = x0 + y0 = 0$ by Definition 1(9,4);
   - $xy0 = x0 = 0$;
   - $x^*0 \le 0 \Leftarrow x0 + 0 \le 0 \Leftarrow$ true by Definition 1(11,4).

2. Proof of (42). We show that $\ulcorner(x^\omega 0)$ satisfies the axioms of ∇x ((33) and (34)).

   (a) $\ulcorner(x\ulcorner(x^\omega 0))$

   $=$ ⟨ (13) ⟩

   $\ulcorner(xx^\omega 0)$

   $=$ ⟨ Definition 1(9,6,3) ⟩

   $\ulcorner((xx^\omega + 1)0)$

   $=$ ⟨ Definition 1(13) ⟩

   $\ulcorner(x^\omega 0)$

   (b) $t \le \ulcorner(xt)$

   $\Rightarrow$ ⟨ Isotony ⟩

   $t\top \le \ulcorner(xt)\top$

   $\Leftrightarrow$ ⟨ (14) & Definition 1(3) ⟩

$$
\begin{array}{ll}
& t\top \le xt\top + 0 \\
\Rightarrow & \quad \langle \text{ Definition 1(14) } \rangle \\
& t\top \le x^\omega 0 \\
\Rightarrow & \quad \langle\ t = t1 \le t\top\ \rangle \\
& t \le x^\omega 0 \\
\Rightarrow & \quad \langle \text{ Isotony of } \ulcorner\ \rangle \\
& \ulcorner t \le \ulcorner(x^\omega 0) \\
\Leftrightarrow & \quad \langle\ (19)\ \rangle \\
& t \le \ulcorner(x^\omega 0)
\end{array}
$$

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

3. Proof of (43).

$$
\begin{array}{ll}
& \nabla x = 0 \ \wedge\ z \le xz + y \\
\Rightarrow & \quad \langle \text{ Definition 1(14) } \rangle \\
& \nabla x = 0 \ \wedge\ z \le x^\omega y \\
\Leftrightarrow & \quad \langle \text{ Definition 1(15,9,7) } \rangle \\
& \nabla x = 0 \ \wedge\ z \le x^* y + x^\omega 0 \\
\Rightarrow & \quad \langle\ (42)\ \ \&\ \ (24)\ \ \&\ \text{ Definition 1(3) } \rangle \\
& z \le x^* y
\end{array}
$$

□

Theorem 10 *Let D be a* DRAe *and t be a guard in D (hence in D_K). Then*

$$\ulcorner(x0)x \;=\; \ulcorner(x0)\top = x0 \ , \tag{44}$$

$$x \;=\; \neg\ulcorner(x0)x + \ulcorner(x0)\top \ , \tag{45}$$

$$x \;=\; \neg\ulcorner(x0)x + x0 \ . \tag{46}$$

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

Proof. We start with (44). The refinement $\ulcorner(x0)x \le \ulcorner(x0)\top$ follows from $x \le \top$. The other refinement and the equality follow from (14), Definition 1(7), (11) and $0 \le 1$: $\ulcorner(x0)\top = x0\top = x0 = \ulcorner(x0)x0 \le \ulcorner(x0)x$. This is used in the proof of (45), together with the BA of guards and Definition 1(9): $x = (\neg\ulcorner(x0) + \ulcorner(x0))x = \neg\ulcorner(x0)x + \ulcorner(x0)x = \neg\ulcorner(x0)x + \ulcorner(x0)\top$. Equation (46) follows from (45), (14) and Definition 1(7). And $\neg\ulcorner(x0)x \in D_K$, since $\neg\ulcorner(x0)x0 = 0$ by (23), so that, by (45), $x = a + t\top$, with $a \overset{\text{def}}{=} \neg\ulcorner(x0)x \in D_K$ and $t \overset{\text{def}}{=} \ulcorner(x0) \in D_K$ satisfying $ta = 0$ by BA and Definition 1(7). □

In (46), $x0$ is the *infinite* or *nonterminating* part of x and $\neg\ulcorner(x0)x$ is its *finite* or *terminating* part [16]. The possibility 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 Sect. 4.

Another part of the DRAe structure worth mentioning is the set

$$D_D \stackrel{\text{def}}{=} \{x \in D \mid x\top = \top\} \ . \tag{47}$$

This set contains all the assertions, since for any guard t, $t^\circ\top = (\neg t\top + 1)\top = \top$ (see (10)). Its elements are the *total* or *nonmiraculous* elements and they satisfy $\ulcorner x = 1$. As already remarked in [13], the substructure D_D of D is a *Demonic Algebra with Domain* (DAD) in the sense of [4, 5, 6]. The set D_D is the image of D_K by the transformation

$$\phi(x) \stackrel{\text{def}}{=} x + \neg\ulcorner x\top. \tag{48}$$

The ordering $\sqsubseteq$ of DAD satisfies $x \sqsubseteq y \Leftrightarrow \phi(x) \leq \phi(y)$. 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, 6] (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, 6].

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

The proof of these assertions follows.

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

$$\begin{array}{cl}
& \psi(\phi(x) + \phi(y)) \\
= & \psi(x + \neg\ulcorner x\top + y + \neg\ulcorner y\top) \\
= & \neg\ulcorner((x + \neg\ulcorner x\top + y + \neg\ulcorner y\top)0)(x + \neg\ulcorner x\top + y + \neg\ulcorner y\top) \\
= & \qquad\qquad \langle \text{ Definition 1(9) } \ \& \ (3) \ \& \ x, y \in D_K \ \& \ (41) \ \rangle \\
& \neg\ulcorner(\neg\ulcorner x\top + \neg\ulcorner y\top)(x + \neg\ulcorner x\top + y + \neg\ulcorner y\top) \\
= & \qquad\qquad \langle \ (21) \ \& \ (13) \ \& \ (20) \ \& \ \text{Definition 1(6)} \ \& \ (19) \ \rangle \\
& \neg(\neg\ulcorner x + \neg\ulcorner y)(x + \neg\ulcorner x\top + y + \neg\ulcorner y\top) \\
= & \qquad\qquad \langle \text{ BA } \rangle \\
& \ulcorner x\ulcorner y(x + \neg\ulcorner x\top + y + \neg\ulcorner y\top) \\
= & \qquad\qquad \langle \text{ Definition 1(8,7) } \ \& \ \text{BA } \rangle \\
& \ulcorner x\ulcorner y(x + y)
\end{array}$$

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

$$
\begin{aligned}
& \psi(\phi(x)\phi(y)) \\
= \;& \psi((x + \neg\ulcorner x\top)(y + \neg\ulcorner y\top)) \\
= \;& \qquad\qquad \langle\ \text{Definition } 1(8,9) \ \ \&\ \ (3)\ \rangle \\
& \psi(xy + x\neg\ulcorner y\top + \neg\ulcorner x\top) \\
= \;& \neg\ulcorner((xy + x\neg\ulcorner y\top + \neg\ulcorner x\top)0)(xy + x\neg\ulcorner y\top + \neg\ulcorner x\top) \\
= \;& \qquad\qquad \langle\ \text{Definition } 1(9) \ \ \&\ \ (3) \ \ \&\ \ x, y \in D_K \ \ \&\ \ (41)\ \rangle \\
& \neg\ulcorner(x\neg\ulcorner y\top + \neg\ulcorner x\top)(xy + x\neg\ulcorner y\top + \neg\ulcorner x\top) \\
= \;& \qquad\qquad \langle\ (21) \ \ \&\ \ (13) \ \ \&\ \ (20) \ \ \&\ \ \text{Definition } 1(6) \ \ \&\ \ (19)\ \rangle \\
& \neg(\ulcorner(x\neg\ulcorner y) + \neg\ulcorner x)(xy + x\neg\ulcorner y\top + \neg\ulcorner x\top) \\
= \;& \qquad\qquad \langle\ \mathsf{BA}\ \rangle \\
& \neg\ulcorner(x\neg\ulcorner y)\ulcorner x(xy + x\neg\ulcorner y\top + \neg\ulcorner x\top) \\
= \;& \qquad\qquad \langle\ \text{Definition } 1(8,7) \ \ \&\ \ (11) \ \ \&\ \ \mathsf{BA}\ \&\ \ (23)\ \rangle \\
& \neg\ulcorner(x\neg\ulcorner y)xy
\end{aligned}
$$

3. Proof of $\psi((\phi(x))^*) = x^* \Box \ulcorner x$.

$$
\begin{aligned}
& \psi((\phi(x))^*) \\
= \;& \psi((x + \neg\ulcorner x\top)^*) \\
= \;& \qquad\qquad \langle\ (6)\ \rangle \\
& \psi(x^*(\neg\ulcorner x\top x^*)^*) \\
= \;& \qquad\qquad \langle\ (3) \ \ \&\ \ (7)\ \rangle \\
& \psi(x^*(\neg\ulcorner x\top + 1)) \\
= \;& \neg\ulcorner(x^*(\neg\ulcorner x\top + 1)0)x^*(\neg\ulcorner x\top + 1) \\
= \;& \qquad\qquad \langle\ \text{Definition } 1(9,6) \ \ \&\ \ (3)\ \rangle \\
& \neg\ulcorner(x^*\neg\ulcorner x\top)x^*(\neg\ulcorner x\top + 1) \\
= \;& \qquad\qquad \langle\ (13) \ \ \&\ \ (20) \ \ \&\ \ \text{Definition } 1(6)\ \rangle \\
& \neg\ulcorner(x^*\neg\ulcorner x)x^*(\neg\ulcorner x\top + 1) \\
= \;& \qquad\qquad \langle\ (25)\ \rangle \\
& \neg\ulcorner(x^*\neg\ulcorner x)x^*\ulcorner x(\neg\ulcorner x\top + 1) \\
= \;& \qquad\qquad \langle\ \text{Definition } 1(8,7) \ \ \&\ \ \mathsf{BA}\ \rangle \\
& \neg\ulcorner(x^*\neg\ulcorner x)x^*\ulcorner x \\
= \;& \qquad\qquad \langle\ \text{Part } 2 \text{ just proved}\ \rangle \\
& x^* \Box \ulcorner x
\end{aligned}
$$

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

$\psi(\neg(\phi(t)))$

$=$ $\langle$ (19) $\rangle$

$\psi(\neg(t + \neg t\top))$

$=$ $\langle$ (29) $\rangle$

$\psi(\neg\ulcorner((t + \neg t\top)0)\top + 1)$

$=$ $\langle$ Definition 1(9) & (3) & $t \in D_K$ & (41) $\rangle$

$\psi(\neg\ulcorner(\neg t\top)\top + 1)$

$=$ $\langle$ (13) & (20) & Definition 1(6) $\rangle$

$\psi(\neg\ulcorner(\neg t)\top + 1)$

$=$ $\langle$ (19) & BA $\rangle$

$\psi(t\top + 1)$

$=$ $\langle$ (19) & BA $\rangle$

$\neg\ulcorner((t\top + 1)0)(t\top + 1)$

$=$ $\langle$ Definition 1(9,6) & (3) $\rangle$

$\neg\ulcorner(t\top)(t\top + 1)$

$=$ $\langle$ Definition 1(8,6) & (23) $\rangle$

$\neg\ulcorner(t\top)$

$=$ $\langle$ (13) & (20) & Definition 1(6) & (19) $\rangle$

$\neg t$

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

$\psi(\ulcorner\!\ulcorner(\phi(x)))$

$= \psi(\ulcorner\!\ulcorner(x + \neg\ulcorner x\top))$

$=$ $\langle$ Definition 6 $\rangle$

$\psi((x + \neg\ulcorner x\top)0 + 1)$

$=$ $\langle$ Definition 1(9) & (3) & $x \in D_K$ & (41) $\rangle$

$\psi(\neg\ulcorner x\top + 1)$

$= \neg\ulcorner((\neg\ulcorner x\top + 1)0)(\neg\ulcorner x\top + 1)$

$=$ $\langle$ Definition 1(9,6) & (3) $\rangle$

$\neg\ulcorner(\neg\ulcorner x\top)(\neg\ulcorner x\top + 1)$

$=$ $\langle$ Definition 1(8,6) & (23) $\rangle$

$\neg\ulcorner(\neg\ulcorner x\top)$

$=$ $\langle$ (13) & (20) & Definition 1(6) & (19) $\rangle$

$\neg\ulcorner(\neg\ulcorner x)$

$=$ $\langle$ (19) & BA $\rangle$

$\ulcorner x$ $\square$

However, unlike what is shown for KAD in Theorem 13 below, not every DAD can be embedded in a DRA, because not every DAD is the image of a KAD. It is shown in [6] 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 report (Theorem 13), 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 13. At the end of the section, Example 14 provides a semantically intuitive understanding of the results of the paper.

Definition 11 *Let K be a* KAD *such that*

$$\nabla x \text{ exists for all } x \in K \qquad \text{and} \qquad \nabla x = 0 \wedge z \leq xz + y \;\Rightarrow\; z \leq x^* y \ . \tag{49}$$

Define the set of ordered pairs P by

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

We define the following operations on P.

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

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

$$tx = 0 \Leftrightarrow t \leq \neg\ulcorner x \Leftrightarrow \ulcorner x \leq \neg t \Leftrightarrow \neg tx = x \Leftrightarrow \neg t\ulcorner x = \ulcorner x, \tag{50}$$

by (24)K, (22)K, (11)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 (49) [1]. We do not know if this is the case for an arbitrary KAD. Note that D_K satisfies (49), by Theorem 9.

Theorem 12 *The algebra $(P, \oplus, \odot, ^{\circledast}, ^{\tilde{\omega}}, ^{\ulcorner}, (0, 0), (1, 0))$ is a* DRAe*. Moreover,*

1. $(x, s) \sqsubseteq (y, t) \Leftrightarrow s \leq t \wedge \neg tx \leq y$*, where* $(x, s) \sqsubseteq (y, t) \overset{\text{def}}{\Leftrightarrow} (x, s) \oplus (y, t) = (y, t)$*,*
2. *the top element is* $(0, 1)$*,*
3. *guards have the form* $(t, 0)$*, and* $\neg(t, 0) = (\neg t, 0)$*,*

4. *the assertion corresponding to the guard* $(t, 0)$ *is* $(t, \neg t)$,

5. $\neg(t, \neg t) = (\neg t, t)$,

6. $\ulcorner\!\!\ulcorner(x, t) = (\neg t, t)$.

Proof. In the derivations below, steps that use Definition 11 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 $(x, s) \sqsubseteq (y, t) \Leftrightarrow s \le t \wedge \neg tx \le y$, which is item 1 of the theorem; this is shown after verifying the axioms of DRA and those of $\ulcorner$.

1.
$$\begin{aligned}
& (x, r) \oplus ((y, s) \oplus (z, t)) \\
= \; & (x, r) \oplus (\neg(s + t)(y + z), s + t) \\
= \; & (\neg(r + s + t)(x + \neg(s + t)(y + z)), r + s + t) \\
= \; & \qquad \langle \text{ Definition 1(8)K \& BA } \rangle \\
& (\neg(r + s + t)(x + y + z), r + s + t) \\
= \; & \qquad \langle \text{ Symmetric transformations } \rangle \\
& ((x, r) \oplus (y, s)) \oplus (z, t)
\end{aligned}$$

2. $(x, s) \oplus (y, t) = (y, t) \oplus (x, s)$ is obvious from the definition of $\oplus$.

3. $(x, t) \oplus (0, 0) = (\neg(t + 0)(x + 0), t + 0) = (\neg tx, t) = (x, t)$ by (50).

4. $(x, t) \oplus (x, t) = (x, t)$ is obvious from the definition of $\oplus$ and (50).

5.
$$\begin{aligned}
& (x, r) \odot ((y, s) \odot (z, t)) \\
= \; & (x, r) \odot (\neg\ulcorner(yt)yz, s + \ulcorner(yt)) \\
= \; & (\neg\ulcorner(x(s + \ulcorner(yt)))x\neg\ulcorner(yt)yz, r + \ulcorner(x(s + \ulcorner(yt)))) \\
= \; & \qquad \langle \text{ Definition 1(8)K \& (21)K \& BA } \rangle \\
& (\neg\ulcorner(xs)\neg\ulcorner(x\ulcorner(yt))x\neg\ulcorner(yt)yz, r + \ulcorner(xs) + \ulcorner(x\ulcorner(yt))) \\
= \; & \qquad \langle \text{ (25)K \& (13)K } \rangle \\
& (\neg\ulcorner(xs)\neg\ulcorner(xyt)xyz, r + \ulcorner(xs) + \ulcorner(xyt)) \\
= \; & \qquad \langle \text{ (22)K \& BA } \rangle \\
& (\neg\ulcorner(\neg\ulcorner(xs)xyt)\neg\ulcorner(xs)xyz, r + \ulcorner(xs) + \ulcorner(\neg\ulcorner(xs)xyt)) \\
= \; & (\neg\ulcorner(xs)xy, r + \ulcorner(xs)) \odot (z, t) \\
= \; & ((x, r) \odot (y, s)) \odot (z, t)
\end{aligned}$$

6.
$$\begin{aligned}
& (x, t) \odot (1, 0) \\
= \; & (\neg\ulcorner(x0)x1, t + \ulcorner(x0)) \\
= \; & \qquad \langle \text{ (31) \& (19)K \& BA \& Definition 1(6,3)K } \rangle \\
& (x, t)
\end{aligned}$$

$$
\begin{aligned}
&= \quad \langle \text{ Definition } 1(6,2,3)\mathsf{K} \ \ \& \ \ (19)\mathsf{K} \ \ \& \ \ (50) \rangle \\
&\quad (\neg\ulcorner(1t)1x, 0 + \ulcorner(1t)) \\
&= (1,0) \odot (x,t)
\end{aligned}
$$

7. $(0,0) \odot (x,t)$

$$
\begin{aligned}
&= (\neg\ulcorner(0t)0x, 0 + \ulcorner(0t)) \\
&= \quad \langle \ (31) \ \ \& \ \text{Definition } 1(7,3)\mathsf{K} \ \ \& \ \ (19)\mathsf{K} \rangle \\
&\quad (0,0)
\end{aligned}
$$

8. $(x,r) \odot ((y,s) \oplus (z,t))$

$$
\begin{aligned}
&= (x,r) \odot (\neg(s+t)(y+z), s+t) \\
&= (\neg\ulcorner(x(s+t))x\neg(s+t)(y+z), r + \ulcorner(x(s+t))) \\
&= \quad \langle \ (25)\mathsf{K} \ \ \& \ \ (50) \rangle \\
&\quad (\neg\ulcorner(x(s+t))\neg r x(y+z), r + \ulcorner(x(s+t))) \\
&= \quad \langle \text{ Definition } 1(8)\mathsf{K} \ \ \& \ \ (21)\mathsf{K} \rangle \\
&\quad (\neg(\ulcorner(xs) + \ulcorner(xt))\neg r(xy + xz), r + \ulcorner(xs) + \ulcorner(xt)) \\
&= \quad \langle \text{ Definition } 1(8)\mathsf{K} \ \ \& \ \ \mathsf{BA} \rangle \\
&\quad (\neg r\neg(\ulcorner(xs) + \ulcorner(xt))(\neg\ulcorner(xs)xy + \neg\ulcorner(xt)xz), r + \ulcorner(xs) + \ulcorner(xt)) \\
&= \quad \langle \ \mathsf{BA} \rangle \\
&\quad (\neg(r + \ulcorner(xs) + r + \ulcorner(xt))(\neg\ulcorner(xs)xy + \neg\ulcorner(xt)xz), r + \ulcorner(xs) + r + \ulcorner(xt)) \\
&= (\neg\ulcorner(xs)xy, r + \ulcorner(xs)) \oplus (\neg\ulcorner(xt)xz, r + \ulcorner(xt)) \\
&= (x,r) \odot (y,s) \oplus (x,r) \odot (z,t)
\end{aligned}
$$

9. $((x,r) \oplus (y,s)) \odot (z,t)$

$$
\begin{aligned}
&= (\neg(r+s)(x+y), r+s) \odot (z,t) \\
&= (\neg\ulcorner(\neg(r+s)(x+y)t)\neg(r+s)(x+y)z, r + s + \ulcorner(\neg(r+s)(x+y)t)) \\
&= \quad \langle \ (22)\mathsf{K} \ \ \& \ \text{Definition } 1(9)\mathsf{K} \ \ \& \ \ (21)\mathsf{K} \rangle \\
&\quad (\neg(\neg(r+s)(\ulcorner(xt) + \ulcorner(yt)))\neg(r+s)(x+y)z, r + s + \neg(r+s)(\ulcorner(xt) + \ulcorner(yt))) \\
&= \quad \langle \ \mathsf{BA} \rangle \\
&\quad (\neg(r+s)\neg(\ulcorner(xt) + \ulcorner(yt))(x+y)z, r + s + \ulcorner(xt) + \ulcorner(yt)) \\
&= \quad \langle \text{ Definition } 1(8,9)\mathsf{K} \ \ \& \ \ \mathsf{BA} \rangle \\
&\quad (\neg(r + \ulcorner(xt) + s + \ulcorner(yt))(\neg\ulcorner(xt)xz + \neg\ulcorner(yt)yz), r + \ulcorner(xt) + s + \ulcorner(yt)) \\
&= (\neg\ulcorner(xt)xz, r + \ulcorner(xt)) \oplus (\neg\ulcorner(yt)yz, s + \ulcorner(yt)) \\
&= (x,r) \odot (z,t) \oplus (y,s) \odot (z,t)
\end{aligned}
$$

10. $(x,t) \odot (x,t)^{\circledast} \oplus (1,0)$

$$
\begin{aligned}
&= (x,t) \odot (\neg\ulcorner(x^*t)x^*, \ulcorner(x^*t)) \oplus (1,0) \\
&= (\neg\ulcorner(x\ulcorner(x^*t))x\neg\ulcorner(x^*t)x^*, t + \ulcorner(x\ulcorner(x^*t))) \oplus (1,0)
\end{aligned}
$$

$= \quad \langle\ (25)\mathsf{K}\ \rangle$

$(\neg\ulcorner(x\ulcorner(x^*t))xx^*, t + \ulcorner(x\ulcorner(x^*t))) \oplus (1,0)$

$= \quad \langle\ (50)\ \ \&\ \ (13)\mathsf{K}\ \rangle$

$(\neg\ulcorner(xx^*t)\neg txx^*, t + \ulcorner(xx^*t)) \oplus (1,0)$

$= \quad \langle\ \mathsf{BA}\ \&\ (19)\mathsf{K}\ \ \&\ \ (21)\mathsf{K}\ \ \&\ \ \text{Definition } 1(9,10)\mathsf{K}\ \rangle$

$(\neg\ulcorner(x^*t)xx^*, \ulcorner(x^*t)) \oplus (1,0)$

$= (\neg(\ulcorner(x^*t) + 0)(\neg\ulcorner(x^*t)xx^* + 1), \ulcorner(x^*t) + 0)$

$= \quad \langle\ \mathsf{BA}\ \&\ \text{Definition } 1(8,10)\mathsf{K}\ \rangle$

$(\neg\ulcorner(x^*t)x^*, \ulcorner(x^*t))$

$= (x,t)^{\circledast}$

11. $(x,r)^{\circledast} \odot (y,s) \sqsubseteq (z,t)$

$\Leftrightarrow (\neg\ulcorner(x^*r)x^*, \ulcorner(x^*r)) \odot (y,s) \sqsubseteq (z,t)$

$\Leftrightarrow (\neg\ulcorner(\neg\ulcorner(x^*r)x^*s)\neg\ulcorner(x^*r)x^*y, \ulcorner(x^*r) + \ulcorner(\neg\ulcorner(x^*r)x^*s)) \sqsubseteq (z,t)$

$\Leftrightarrow \quad \langle\ (22)\mathsf{K}\ \ \&\ \ \mathsf{BA}\ \rangle$

$(\neg\ulcorner(x^*r)\neg\ulcorner(x^*s)x^*y, \ulcorner(x^*r) + \ulcorner(x^*s)) \sqsubseteq (z,t)$

$\Leftrightarrow \quad \langle$ Part 1 of this theorem, proved below $\rangle$

$\ulcorner(x^*r) + \ulcorner(x^*s) \le t\ \wedge\ \neg t\neg\ulcorner(x^*r)\neg\ulcorner(x^*s)x^*y \le z$

$\Leftrightarrow \quad \langle\ \ulcorner(x^*r) + \ulcorner(x^*s) \le t \Rightarrow \neg t \le \neg\ulcorner(x^*r)\neg\ulcorner(x^*s)\ \ \&\ \ (21)\mathsf{K}\ \ \&$
Definition $1(8)\mathsf{K}$ $\rangle$

$\ulcorner(x^*(r+s)) \le t\ \wedge\ \neg tx^*y \le z$

$\Leftarrow \quad \langle\ (32)\ \rangle$

$\ulcorner(xt) + r + s \le t\ \wedge\ \neg tx^*y \le z$

$\Leftarrow \quad \langle$

$\neg tx^* \le (\neg tx)^*\neg t$

$\Leftarrow \quad \langle$ Definition $1(12)\mathsf{K}$ $\rangle$

$(\neg tx)^*\neg tx + \neg t \le (\neg tx)^*\neg t$

$\Leftrightarrow \quad \langle\ \ulcorner(xt) \le t \Rightarrow \neg t \le \neg\ulcorner(xt)\ \rangle$

$(\neg tx)^*\neg t\neg\ulcorner(xt)x + \neg t \le (\neg tx)^*\neg t$

$\Leftrightarrow \quad \langle\ (25)\mathsf{K}\ \rangle$

$(\neg tx)^*\neg t\neg\ulcorner(xt)x\neg t + \neg t \le (\neg tx)^*\neg t$

$\Leftarrow \quad \langle\ \neg\ulcorner(xt) \le 1\ \ \&\ \ \text{Definition } 1(9,6)\mathsf{K}\ \rangle$

$((\neg tx)^*\neg tx + 1)\neg t \le (\neg tx)^*\neg t$

$\Leftrightarrow \quad \langle\ (4)\mathsf{K}\ \rangle$

true

$\rangle$

$\ulcorner(xt) + r + s \le t\ \wedge\ (\neg tx)^*\neg ty \le z$

$\Leftarrow$ $\langle$ Definition 1(11)K $\rangle$

$\ulcorner(xt) + r + s \leq t \;\wedge\; \neg txz + \neg ty \leq z$

$\Leftrightarrow$ $\langle$ Definition 1(8)K $\rangle$

$\ulcorner(xt) + r + s \leq t \;\wedge\; \neg t(xz + y) \leq z$

$\Leftrightarrow$ $\langle\ \ulcorner(xt) + r + s \leq t \Rightarrow \neg t \leq \neg(\ulcorner(xt) + r + s)\ \rangle$

$\ulcorner(xt) + r + s \leq t \;\wedge\; \neg t\neg(\ulcorner(xt) + r + s)(xz + y) \leq z$

$\Leftrightarrow$ $\langle$ Part 1 of this theorem, proved below $\rangle$

$(\neg(\ulcorner(xt) + r + s)(xz + y), \ulcorner(xt) + r + s) \sqsubseteq (z, t)$

$\Leftrightarrow$ $\langle$ Definition 1(8)K & BA $\rangle$

$(\neg(r + \ulcorner(xt) + s)(\neg\ulcorner(xt)xz + y), r + \ulcorner(xt) + s) \sqsubseteq (z, t)$

$\Leftrightarrow (\neg\ulcorner(xt)xz, r + \ulcorner(xt)) \oplus (y, s) \sqsubseteq (z, t)$

$\Leftrightarrow (x, r) \odot (z, t) \oplus (y, s) \sqsubseteq (z, t)$

12. $(y, s) \odot (x, r)^{\circledast} \sqsubseteq (z, t)$

$\Leftrightarrow (y, s) \odot (\neg\ulcorner(x^*r)x^*, \ulcorner(x^*r)) \sqsubseteq (z, t)$

$\Leftrightarrow (\neg\ulcorner(y\ulcorner(x^*r))y\neg\ulcorner(x^*r)x^*, s + \ulcorner(y\ulcorner(x^*r))) \sqsubseteq (z, t)$

$\Leftrightarrow$ $\langle$ (25)K & (13)K $\rangle$

$(\neg\ulcorner(yx^*r)yx^*, s + \ulcorner(yx^*r)) \sqsubseteq (z, t)$

$\Leftrightarrow$ $\langle$ Part 1 of this theorem, proved below $\rangle$

$s + \ulcorner(yx^*r) \leq t \;\wedge\; \neg t\neg\ulcorner(yx^*r)yx^* \leq z$

$\Leftrightarrow$ $\langle\ \ulcorner(yx^*r) \leq t \Rightarrow \neg t \leq \neg\ulcorner(yx^*r)\ \rangle$

$s + \ulcorner(yx^*r) \leq t \;\wedge\; \neg tyx^* \leq z$

$\Leftarrow$ $\langle$ By isotony, (22)K and BA, $\neg tyx^* \leq z \Rightarrow \neg tyx^*r \leq zr \Rightarrow \ulcorner(\neg tyx^*r) \leq \ulcorner(zr) \Leftrightarrow \neg t\ulcorner(yx^*r) \leq \ulcorner(zr) \Leftrightarrow \ulcorner(yx^*r) \leq \ulcorner(zr) + t$. Hence, $\ulcorner(zr) \leq t \wedge \neg tyx^* \leq z \Rightarrow \ulcorner(yx^*r) \leq t$ $\rangle$

$\ulcorner(zr) + s \leq t \;\wedge\; \neg tyx^* \leq z$

$\Leftarrow$ $\langle$ Definition 1(12)K $\rangle$

$\ulcorner(zr) + s \leq t \;\wedge\; zx + \neg ty \leq z$

$\Leftrightarrow$ $\langle$ Definition 1(8)K & $\neg tz = z$ by (50) $\rangle$

$\ulcorner(zr) + s \leq t \;\wedge\; \neg t(zx + y) \leq z$

$\Leftrightarrow$ $\langle$ BA & $t + \ulcorner(zr) + s \leq t \Rightarrow \neg t \leq \neg(t + \ulcorner(zr) + s)$ $\rangle$

$t + \ulcorner(zr) + s \leq t \;\wedge\; \neg t\neg(t + \ulcorner(zr) + s)(zx + y) \leq z$

$\Leftrightarrow$ $\langle$ Part 1 of this theorem, proved below $\rangle$

$(\neg(t + \ulcorner(zr) + s)(zx + y), t + \ulcorner(zr) + s) \sqsubseteq (z, t)$

$\Leftrightarrow$ $\langle$ Definition 1(8)K & BA $\rangle$

$(\neg(t + \ulcorner(zr) + s)(\neg\ulcorner(zr)zx + y), t + \ulcorner(zr) + s) \sqsubseteq (z, t)$

$\Leftrightarrow (\neg\ulcorner(zr)zx, t + \ulcorner(zr)) \oplus (y, s) \sqsubseteq (z, t)$

$= (z,t) \odot (x,r) \oplus (y,s) \sqsubseteq (z,t)$

13. $(x,t) \odot (x,t)^{\widetilde{\omega}} \oplus (1,0)$
$= (x,t) \odot (\neg\ulcorner(x^*t)\neg\nabla x x^*, \ulcorner(x^*t) + \nabla x) \oplus (1,0)$
$= (\neg\ulcorner(x(\ulcorner(x^*t) + \nabla x))x\neg\ulcorner(x^*t)\neg\nabla x x^*, t + \ulcorner(x(\ulcorner(x^*t) + \nabla x))) \oplus (1,0)$
$=$ ⟨ Definition 1(8)K & (21)K ⟩
$(\neg(\ulcorner(x\ulcorner(x^*t)) + \ulcorner(x\nabla x))x\neg\ulcorner(x^*t)\neg\nabla x x^*, t + \ulcorner(x\ulcorner(x^*t)) + \ulcorner(x\nabla x)) \oplus (1,0)$
$=$ ⟨ BA & (25)K & (13)K & (19)K & (21)K ⟩
$(\neg\ulcorner(xx^*t)\neg\ulcorner(x\nabla x)xx^*, \ulcorner(t + xx^*t) + \ulcorner(x\nabla x)) \oplus (1,0)$
$=$ ⟨ Definition 1(6,9,10)K & (35) ⟩
$(\neg\ulcorner(xx^*t)\neg\nabla x x x^*, \ulcorner(x^*t) + \nabla x) \oplus (1,0)$
$= (\neg(\ulcorner(x^*t) + \nabla x + 0)(\neg\ulcorner(xx^*t)\neg\nabla x x x^* + 1), \ulcorner(x^*t) + \nabla x + 0)$
$=$ ⟨ Definition 1(3)K & De Morgan ⟩
$(\neg\ulcorner(x^*t)\neg\nabla x(\neg\ulcorner(xx^*t)\neg\nabla x x x^* + 1), \ulcorner(x^*t) + \nabla x)$
$=$ ⟨ Definition 1(8)K & $xx^*t \le x^*t$ by Definition 1(10)K & BA ⟩
$(\neg\ulcorner(x^*t)\neg\nabla x(xx^* + 1), \ulcorner(x^*t) + \nabla x)$
$=$ ⟨ Definition 1(10)K ⟩
$(\neg\ulcorner(x^*t)\neg\nabla x x^*, \ulcorner(x^*t) + \nabla x)$
$= (x,t)^{\widetilde{\omega}}$

14. In this proof, the abbreviation $p \overset{\text{def}}{=} \ulcorner(x^*(r+s)) + \nabla x$ is used.

$(z,t) \sqsubseteq (x,r)^{\widetilde{\omega}} \odot (y,s)$
$\Leftrightarrow (z,t) \sqsubseteq (\neg\ulcorner(x^*r)\neg\nabla x x^*, \ulcorner(x^*r) + \nabla x) \odot (y,s)$
$\Leftrightarrow (z,t) \sqsubseteq (\neg\ulcorner(\neg\ulcorner(x^*r)\neg\nabla x x^* s)\neg\ulcorner(x^*r)\neg\nabla x x^* y, \ulcorner(x^*r) + \nabla x + \ulcorner(\neg\ulcorner(x^*r)\neg\nabla x x^* s))$
$\Leftrightarrow$ ⟨ (22)K & BA ⟩
$(z,t) \sqsubseteq (\neg\ulcorner(x^*r)\neg\ulcorner(x^*s)\neg\nabla x x^* y, \ulcorner(x^*r) + \ulcorner(x^*s) + \nabla x)$
$\Leftrightarrow$ ⟨ De Morgan & (21)K & Definition 1(8)K ⟩
$(z,t) \sqsubseteq (\neg p x^* y, p)$
$\Leftrightarrow$ ⟨ Part 1 of this theorem, proved below ⟩
$t \le p \;\wedge\; \neg p z \le \neg p x^* y$
$\Leftarrow$ ⟨ Multiplying both sides of the right inequality below by $\neg p$ & BA ⟩
$t \le p \;\wedge\; \neg p z \le x^* y$
$\Leftarrow$ ⟨ $\neg p \le 1$ & Isotony ⟩
$t \le p \;\wedge\; \neg p z \le (\neg p x)^* y$
$\Leftarrow$ ⟨ (49) & $\nabla(\neg p x) = 0$, since $\nabla(\neg p x) \le \neg p \nabla x \le \neg\nabla x \nabla x$ by (38), (39) and the definition of p ⟩
$t \le p \;\wedge\; \neg p z \le \neg p x \neg p z + y$

$\Leftrightarrow$ ⟨ We show $\neg px = \neg px\neg p$. Only $\leq$ need be shown, the other direction being direct by isotony.

$\neg px$

$=$ ⟨ De Morgan ⟩

$\neg\ulcorner(x^*(r+s))\neg\nabla xx$

$=$ ⟨ Definition 1(10,9)K & (35) ⟩

$\neg\ulcorner(xx^*(r+s)+r+s)\neg\ulcorner(x\nabla x)x$

$=$ ⟨ (21)K & (13)K & BA & (19)K ⟩

$\neg(r+s)\neg\ulcorner(xp)x$

$=$ ⟨ (25)K ⟩

$\neg(r+s)\neg\ulcorner(xp)x\neg p$

$=$ ⟨ Reversing the previous steps on $\neg(r+s)\neg\ulcorner(xp)$ ⟩

$\neg px\neg p$

⟩

$t \leq p \ \wedge\ \neg pz \leq \neg pxz + y$

$\Leftarrow$ ⟨ Definition 1(8)K & $\neg p \leq 1$ ⟩

$t \leq p \ \wedge\ \neg pz \leq \neg p(xz + y)$

$\Leftarrow$ ⟨ Multiplying each side of the right inequality by $\neg p$ and using that $\neg p \leq \neg(\ulcorner(xt) + r + s)$ because

$\ulcorner(xt) + r + s$

$\leq$ ⟨ Using the left inequality $t \leq p$ ⟩

$\ulcorner(xp) + r + s$

$=$ ⟨ Definition 1(8)K & (21)K & (13)K ⟩

$\ulcorner(xx^*(r+s) + x\nabla x) + r + s$

$=$ ⟨ (19)K & (21)K ⟩

$\ulcorner(xx^*(r+s) + r + s) + \ulcorner(x\nabla x)$

$=$ ⟨ Definition 1(6,9,10)K & (35) ⟩

p

⟩

$t \leq p \ \wedge\ \neg(\ulcorner(xt) + r + s)z \leq \neg(\ulcorner(xt) + r + s)(xz + y)$

$\Leftarrow$ ⟨ Proposition 8 ⟩

$t \leq \ulcorner(xt) + r + s \ \wedge\ \neg(\ulcorner(xt) + r + s)z \leq \neg(\ulcorner(xt) + r + s)(xz + y)$

$\Leftrightarrow$ ⟨ Part 1 of this theorem, proved below ⟩

$(z, t) \sqsubseteq (\neg(\ulcorner(xt) + r + s)(xz + y), \ulcorner(xt) + r + s)$

$\Leftrightarrow$ ⟨ Definition 1(9)K & BA ⟩

$(z, t) \sqsubseteq (\neg(r + \ulcorner(xt) + s)(\neg\ulcorner(xt)xz + y), r + \ulcorner(xt) + s)$

$\Leftrightarrow (z, t) \sqsubseteq (\neg\ulcorner(xt)xz, r + \ulcorner(xt)) \oplus (y, s)$

$\Leftrightarrow (z,t) \sqsubseteq (x,r) \odot (z,t) \oplus (y,s)$

15. $(x,t)^{\circledast} \oplus (x,t)^{\widetilde{\omega}} \odot (0,0)$

$= (x,t)^{\circledast} \oplus (\neg\ulcorner(x^*t)\neg\nabla x x^*, \ulcorner(x^*t) + \nabla x) \odot (0,0)$

$= (\neg\ulcorner(x^*t)x^*, \ulcorner(x^*t)) \oplus$

$(\neg\ulcorner(\neg\ulcorner(x^*t)\neg\nabla x x^*0)\neg\ulcorner(x^*t)\neg\nabla x x^*0, \ulcorner(x^*t) + \nabla x + \ulcorner(\neg\ulcorner(x^*t)\neg\nabla x x^*0))$

$=$ ⟨ (31) & (19)K & Definition 1(3)K ⟩

$(\neg\ulcorner(x^*t)x^*, \ulcorner(x^*t)) \oplus (0, \ulcorner(x^*t) + \nabla x)$

$= (\neg(\ulcorner(x^*t) + \ulcorner(x^*t) + \nabla x)(\neg\ulcorner(x^*t)x^* + 0), \ulcorner(x^*t) + \ulcorner(x^*t) + \nabla x)$

$=$ ⟨ Definition 1(3)K & BA ⟩

$(\neg\ulcorner(x^*t)\neg\nabla x x^*, \ulcorner(x^*t) + \nabla x)$

$= (x,t)^{\widetilde{\omega}}$

Verification of the axioms of enabledness ((11), (12), (13), (14)).

(11) $\ulcorner(x,t) \odot (x,t)$

$= (\ulcorner x + t, 0) \odot (x,t)$

$= (\neg\ulcorner((\ulcorner x + t)t)(\ulcorner x + t)x, 0 + \ulcorner((\ulcorner x + t)t))$

$=$ ⟨ BA & (19)K ⟩

$(\neg t\ulcorner x x, t)$

$=$ ⟨ (11)K & $\neg t x = x$ by (50) ⟩

(x,t)

(12) Assume that guards have the form $(t,0)$, as stated in part 3 of the theorem; this is shown below.

$\ulcorner((t,0) \odot (x,s))$

$= \ulcorner(\neg\ulcorner(ts)tx, 0 + \ulcorner(ts))$

$=$ ⟨ BA & (19)K ⟩

$\ulcorner(t\neg s x, ts)$

$= (\ulcorner(t\neg s x) + ts, 0)$

$=$ ⟨ (22)K & BA ⟩

$(t(\ulcorner x + s), 0)$

$\sqsubseteq$ ⟨ Part 1 of this theorem, proved below & BA ⟩

$(t,0)$

(13) $\ulcorner((x,s) \odot (y,t))$

$= \ulcorner(\neg\ulcorner(xt)xy, s + \ulcorner(xt))$

$= (\ulcorner(\neg\ulcorner(xt)xy) + s + \ulcorner(xt), 0)$

$=$ ⟨ (22)K & BA ⟩

$(\ulcorner(xy) + \ulcorner(xt) + s, 0)$

$=$ ⟨ (13)K & (21)K & Definition 1(9)K ⟩

$(\ulcorner(x(\ulcorner y + t)) + s, 0)$

$= \ulcorner(x(\ulcorner y + t), s)$

$=$ ⟨ (31) & (19)K & BA & Definition 1(6)K ⟩

$\ulcorner(\neg\ulcorner(x0)x(\ulcorner y + t), s + \ulcorner(x0))$

$= \ulcorner((x, s) \odot (\ulcorner y + t, 0))$

$= \ulcorner((x, s) \odot \ulcorner(y, t))$

(14) Assume that the top element is $(0, 1)$, as stated in part 2 of the theorem; this is shown below.

$\ulcorner(x, t) \odot (0, 1)$

$= (\ulcorner x + t, 0) \odot (0, 1)$

$= (\neg\ulcorner((\ulcorner x + t)1)(\ulcorner x + t)0, 0 + \ulcorner((\ulcorner x + t)1))$

$=$ ⟨ (31) & Definition 1(2,3,6) & (19)K ⟩

$(0, \ulcorner x + t)$

$=$ ⟨ (31) & Definition 1(2,6) ⟩

$(\neg\ulcorner(x1)x0, t + \ulcorner(x1))$

$= (x, t) \odot (0, 1)$

Verification of statements 1 to 6 of the theorem.

1. $(x, s) \sqsubseteq (y, t)$

$\Leftrightarrow$ ⟨ Definition of $\sqsubseteq$ ⟩

$(x, s) \oplus (y, t) = (y, t)$

$\Leftrightarrow (\neg(s + t)(x + y), s + t) = (y, t)$

$\Leftrightarrow$ ⟨ BA & Definition 1(8)K ⟩

$(\neg t\neg sx + \neg s\neg ty, s + t) = (y, t)$

$\Leftrightarrow$ ⟨ $\neg sx = x$ by (50) & $\neg ty = y$ by (50) & 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(3,9)K ⟩

$s \leq t \;\wedge\; \neg tx + (s + \neg s)y = y$

$\Leftrightarrow$ ⟨ BA & Definition 1(6)K & Definition of $\leq$ ⟩

$s \leq t \wedge \neg tx \leq y$

2. $(x, t) \sqsubseteq (0, 1)$

$\Leftrightarrow$ ⟨ Part 1 of this theorem ⟩

$t \leq 1 \wedge \neg 1x \leq 0$

$\Leftrightarrow$ $\langle$ BA & Definition 1(7)K $\rangle$

true

3. By (9), a pair (x, s) is a guard iff there exists a complement (y, t) satisfying (9), that is, $(x, s) \odot (y, t) = (y, t) \odot (x, s) = (0, 0)$ and $(x, s) \oplus (y, t) = (1, 0)$. Now,

$$
\begin{aligned}
& (x, s) \odot (y, t) = (0, 0) \\
\Leftrightarrow\ & (\neg\ulcorner(xt)xy, s + \ulcorner(xt)) = (0, 0) \\
\Leftrightarrow\ & \neg\ulcorner(xt)xy = 0 \ \wedge\ s + \ulcorner(xt) = 0 \\
\Rightarrow\ & \quad \langle \text{ BA \& By (24), } \ulcorner(xt) = 0 \Leftrightarrow xt = 0 \ \text{ \& (19)K } \rangle \\
& xy = 0 \ \wedge\ s = 0 \ .
\end{aligned}
$$

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

4. By (10), parts 2 and 3 of this theorem, and (19)K, $(t, 0)^{\circ} = \neg(t, 0) \odot (0, 1) \oplus (1, 0) = (\neg t, 0) \odot (0, 1) \oplus (1, 0) = (0, \neg t) \oplus (1, 0) = (t, \neg t)$.

5. By (29), $\neg(t, \neg t) = \neg\ulcorner((t, \neg t) \odot (0, 0)) \odot (0, 1) \oplus (1, 0) = \neg\ulcorner(0, \neg t) \odot (0, 1) \oplus (1, 0) = \neg(\neg t, 0) \odot (0, 1) \oplus (1, 0) = (t, 0) \odot (0, 1) \oplus (1, 0) = (0, t) \oplus (1, 0) = (\neg t, t)$.

6. By Definition 6, $\ulcorner\!\ulcorner(x, t) = (x, t) \odot (0, 0) \oplus (1, 0) = (0, t) \oplus (1, 0) = (\neg t, t)$. □

And now the main theorem.

Theorem 13 1. *Every* DRAe *is isomorphic to an algebra of ordered pairs as in Definition 11. The isomorphism is given by* $\phi(x) \stackrel{\text{def}}{=} (\neg\ulcorner(x0)x, \ulcorner(x0))$, *with inverse* $\psi((x, t)) \stackrel{\text{def}}{=} x + t\top$.

2. *Every* KAD K *satisfying (49) can be embedded in a* DRAe D *in such a way that* D_K *is the image of* K *by the embedding.*

PROOF.

1. Let D be a DRAe. The sub-Kleene algebra $(D_K, +, \cdot, {}^*, \ulcorner, 0, 1)$ of D satisfies (49), by Theorem 9. Use D_K to construct an algebra of pairs $(P, \oplus, \odot, {}^{\circledast}, {}^{\widetilde{\omega}}, \ulcorner, (0, 0), (1, 0))$ as per Definition 11. We first show that ψ is the inverse of ϕ, so that they both are bijective functions.

(a)
$$
\begin{aligned}
& \psi(\phi(x)) \\
=\ & \psi((\neg\ulcorner(x0)x, \ulcorner(x0))) \\
=\ & \neg\ulcorner(x0)x + \ulcorner(x0)\top \\
=\ & \quad \langle \text{ (14) \& Definition 1(7) } \rangle \\
& \neg\ulcorner(x0)x + x0 \\
=\ & \quad \langle \text{ (46) } \rangle \\
& x
\end{aligned}
$$

(b) $\phi(\psi((x,t)))$

$= \phi(x + t\top)$

$= (\neg\ulcorner((x + t\top)0)(x + t\top), \ulcorner((x + t\top)0))$

$=$ $\langle$ Definition 1(9) & (3) $\rangle$

$(\neg\ulcorner(x0 + t\top)(x + t\top), \ulcorner(x0 + t\top))$

$=$ $\langle$ Since $x \in D_K$, $x0 = 0$ by (41) & Definition 1(3) $\rangle$

$(\neg\ulcorner(t\top)(x + t\top), \ulcorner(t\top))$

$=$ $\langle$ (13) & (20) & Definition 1(6) & (19) $\rangle$

$(\neg t(x + t\top), t)$

$=$ $\langle$ Definition 1(8,7,3) & BA & $\neg tx = x$ by (50) $\rangle$

(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).

(a) $\psi((x,s) \oplus (y,t))$

$= \psi((\neg(s + t)(x + y), s + t))$

$= \neg(s + t)(x + y) + (s + t)\top$

$=$ $\langle$ BA & Definition 1(8,9) $\rangle$

$\neg t\neg sx + \neg s\neg ty + s\top + t\top$

$=$ $\langle$ $sx = 0$ & $ty = 0$ & (50) & $tx \leq t\top$ & $sy \leq s\top$ $\rangle$

$\neg tx + tx + \neg sy + sy + s\top + t\top$

$=$ $\langle$ Definition 1(9,2,6) & BA $\rangle$

$x + s\top + y + t\top$

$= \psi((x,s)) + \psi((y,t))$

(b) $\psi((x,s) \odot (y,t))$

$= \psi((\neg\ulcorner(xt)xy, s + \ulcorner(xt)))$

$= \neg\ulcorner(xt)xy + (s + \ulcorner(xt))\top$

$=$ $\langle$ Definition 1(9) & $\ulcorner(xt)xy \leq \ulcorner(xt)\top$ $\rangle$

$\neg\ulcorner(xt)xy + \ulcorner(xt)xy + s\top + \ulcorner(xt)\top$

$=$ $\langle$ Definition 1(9,6) & BA & (14) $\rangle$

$xy + s\top + xt\top$

$=$ $\langle$ Definition 1(9,8) & (3) $\rangle$

$(x + s\top)(y + t\top)$

$= \psi((x,s)) \cdot \psi((y,t))$

(c) $\psi((x,t)^{\circledast})$

$= \psi((\neg\ulcorner(x^*t)x^*, \ulcorner(x^*t)))$

$= \neg\ulcorner(x^*t)x^* + \ulcorner(x^*t)\top$

$=$ $\langle\ \ulcorner(x^*t)x^* \leq \ulcorner(x^*t)\top\ \rangle$

$\neg\ulcorner(x^*t)x^* + \ulcorner(x^*t)x^* + \ulcorner(x^*t)\top$

$=$ $\langle$ Definition 1(9,6) & BA & (14) $\rangle$

$x^* + x^*t\top$

$=$ $\langle$ Definition 1(8,2,6) & (7) $\rangle$

$x^*(t\top)^*$

$=$ $\langle$ (3) $\rangle$

$x^*(t\top x^*)^*$

$=$ $\langle$ (6) $\rangle$

$(x + t\top)^*$

$= (\psi((x,t)))^*$

(d) $\psi((x,t)^{\widetilde{\omega}})$

$= \psi((\neg\ulcorner(x^*t)\neg\triangledown x x^*, \ulcorner(x^*t) + \triangledown x))$

$= \neg\ulcorner(x^*t)\neg\triangledown x x^* + (\ulcorner(x^*t) + \triangledown x)\top$

$=$ $\langle$ De Morgan & $(\ulcorner(x^*t) + \triangledown x)x^* \leq (\ulcorner(x^*t) + \triangledown x)\top$ $\rangle$

$\neg(\ulcorner(x^*t) + \triangledown x)x^* + (\ulcorner(x^*t) + \triangledown x)x^* + (\ulcorner(x^*t) + \triangledown x)\top$

$=$ $\langle$ Definition 1(9,6) & BA & (42) $\rangle$

$x^* + \ulcorner(x^*t)\top + \ulcorner(x^\omega 0)\top$

$=$ $\langle$ (14) & Definition 1(7) & $x^\omega 0 = x^\omega 0t\top$ $\rangle$

$x^* + x^*t\top + x^\omega 0 + x^\omega 0t\top$

$=$ $\langle$ Definition 1(2,9,15) $\rangle$

$x^\omega + x^\omega t\top$

$=$ $\langle$ Definition 1(6,8,2) & (7) $\rangle$

$x^\omega(t\top)^\omega$

$=$ $\langle$ (6) & (3) $\rangle$

$(x + t\top)^\omega$

$= (\psi((x,t)))^\omega$

(e) $\psi(\ulcorner(x,t))$

$= \psi((\ulcorner x + t, 0))$

$= \ulcorner x + t + 0\top$

$=$ $\langle$ Definition 1(7,3) $\rangle$

$\ulcorner x + t$

$=$ $\langle$ (21) & (13) & (20) & Definition 1(6) $\rangle$

$\ulcorner(x + t\top)$

$= \ulcorner(\psi((x,t)))$

(f) By definition of ψ and Definition 1(7,3), $\psi((0,0)) = 0 + 0\top = 0$.

(g) By definition of ψ and Definition 1(7,3), $\psi((1,0)) = 1 + 0\top = 1$. □

2. By Theorem 12, the construction in Definition 11 can be used to produce a DRAe P of pairs. 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 9. In addition, $(x,0) \oplus (y,0) = (x + y, 0)$, $(x,0) \odot (y,0) = (xy, 0)$, $(x,0)^{\circledast} = (x^*, 0)$, $\ulcorner(x,0) = (\ulcorner x, 0)$ and $\triangledown(x,0) = (\triangledown x, 0)$, as is readily checked. Thus the embedding of K in P is simply $x \mapsto (x,0)$.

Example 14 Figure 1 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: $\mathsf{a} = \{(\bullet,\circ)\}, \mathsf{b} = \{(\circ,\bullet)\}, \mathsf{s} = \{(\bullet,\bullet)\}, \mathsf{t} = \{(\circ,\circ)\}, 0 = \{\}, \mathbb{T} = \mathsf{a}+\mathsf{b}+\mathsf{s}+\mathsf{t}, 1 = \mathsf{s}+\mathsf{t}, \overline{1} = \mathsf{a}+\mathsf{b}$. The guards are $(0,0), (\mathsf{s},0), (\mathsf{t},0), (1,0)$ and the assertions are $(1,0), (\mathsf{t},\mathsf{s}), (\mathsf{s},\mathsf{t}), (0,1)$. The conjunctive predicate transformer f corresponding to a pair (x,t) is given by $f(s) \stackrel{\text{def}}{=} \neg t \neg \ulcorner(x \neg s)$. 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 ($\neg\ulcorner(x\neg s)$). The predicate transformers for all pairs follow. The entry for line $(\mathsf{t}+\overline{1},0)$ and column t, for instance, is s because $f(\mathsf{t}) = \neg 0 \neg \ulcorner((\mathsf{t}+\overline{1})\neg\mathsf{t}) = \mathsf{s}$, as is readily checked.

	0	s	t	1
$(0,1)$	0	0	0	0
$(\mathsf{b}+\mathsf{t},\mathsf{s})$	0	0	0	t
$(\mathsf{a}+\mathsf{s},\mathsf{t})$	0	0	0	s
(b,s)	0	t	0	t
(t,s)	0	0	t	t
$(\mathbb{T},0)$	0	0	0	1
(s,t)	0	s	0	s
(a,t)	0	0	s	s
$(0,\mathsf{s})$	t	t	t	t

	0	s	t	1
$(\mathsf{s}+\overline{1},0)$	0	t	0	1
$(\mathsf{a}+1,0)$	0	0	t	1
$(\mathsf{b}+1,0)$	0	s	0	1
$(\mathsf{t}+\overline{1},0)$	0	0	s	1
$(0,\mathsf{t})$	s	s	s	s
$(\mathsf{a}+\mathsf{s},0)$	t	t	t	1
$(\mathsf{b}+\mathsf{s},0)$	0	1	0	1
$(\overline{1},0)$	0	t	s	1

	0	s	t	1
$(1,0)$	0	s	t	1
$(\mathsf{a}+\mathsf{t},0)$	0	0	1	1
$(\mathsf{b}+\mathsf{t},0)$	s	s	s	1
$(\mathsf{s},0)$	t	1	t	1
$(\mathsf{a},0)$	t	t	1	1
$(\mathsf{b},0)$	s	1	s	1
$(\mathsf{t},0)$	s	s	1	1
$(0,0)$	1	1	1	1

Going back to Figure 1, 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 11), 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, 6]. 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 $\ulcorner\!\ulcorner(x,t) = (\neg t, t)$ (Theorem 12(6)). This is interpreted as saying that termination is guaranteed for initial states in $\neg t$. In the demonic algebra of [4, 5, 6], the demonic domain of x, $\ulcorner\!\ulcorner x$, 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 $(0,\mathsf{t})$. This element does not terminate for initial states in t (here, $\{\circ\}$) and terminates for states in $\neg\mathsf{t}$ while producing no result (due to the first component being 0).

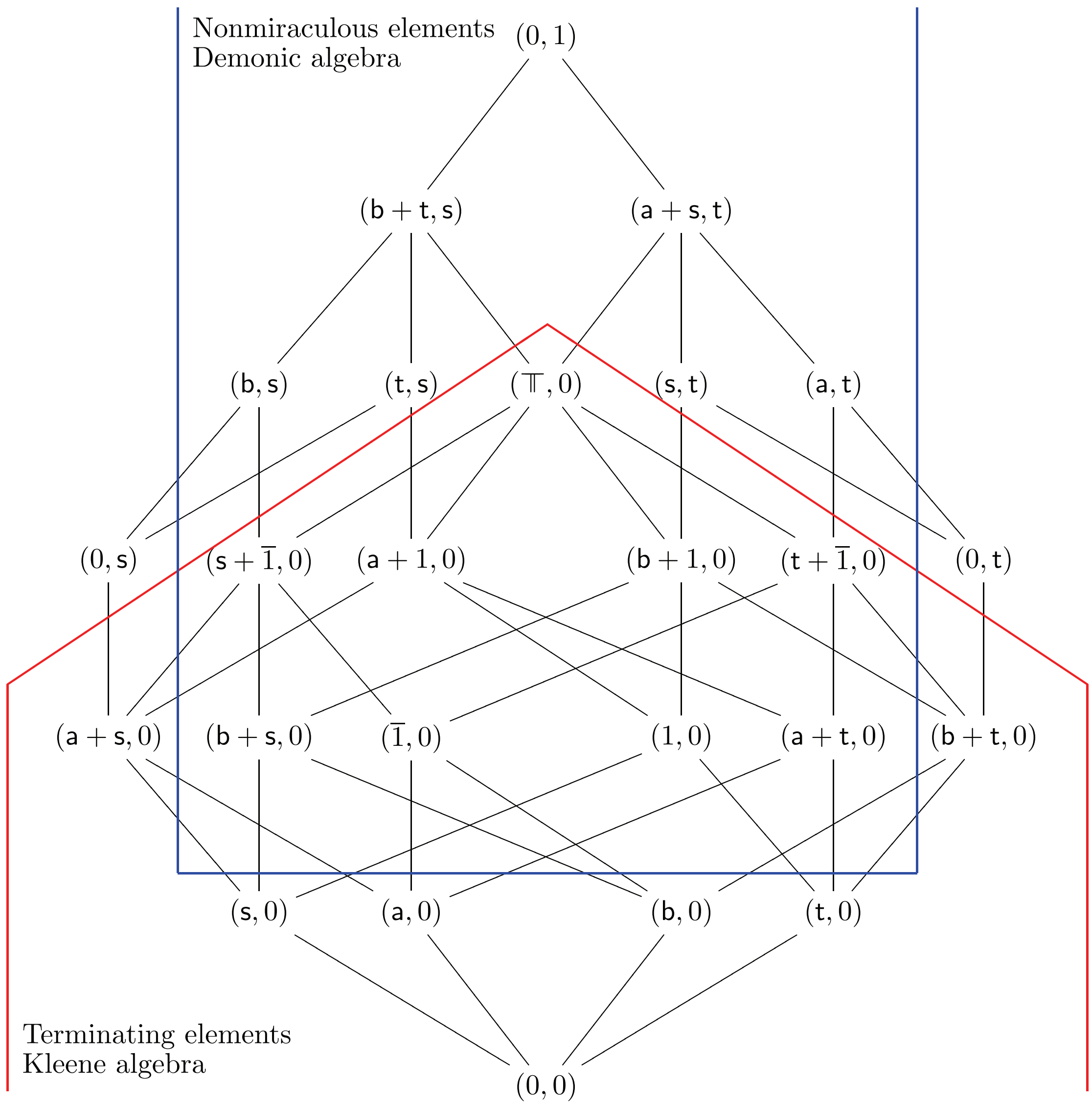

Figure 1: A demonic refinement algebra of ordered pairs.

The set of terminating elements (the Kleene algebra) is the set D_K defined in (41). The set of nonmiraculous elements (the demonic algebra) is the set D_D defined in (47). For pairs, the function ϕ mapping D_K to D_D (see (48)) is $\phi((x,t)) = (x, \neg\ulcorner x)$, by Definition 11 and Theorem 12. For instance, $\phi((0,0)) = (0,1)$ and $\phi((\mathsf{a},0)) = (\mathsf{a},\mathsf{t})$. The terminating and nonmiraculous elements have the form $(x,0)$, with $\ulcorner x = 1$. They are mapped to themselves. For instance, $\phi((\mathbb{T},0)) = (\mathbb{T},0)$.

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 $(\mathbb{T},0)$. 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 report, Theorem 13, provides an alternative, equivalent way to view a DRAe as an algebra of ordered pairs. This view, or the related decomposition of any element x of a DRAe as $x = a + t\top$ (Theorem 10), 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, 11, 13, 17, 18], to cite just a few).

It is asserted in [9] that the divergence operator often provides a more convenient description of nontermination than the ω operator of omega algebra. Theorem 13 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 13 is that the complexity of the theory of DRAe is at most that of KAD with a divergence operator satisfying the implication in 49 (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.

Acknowledgements

We thank Georg Struth and the anonymous referees 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 (Fond québécois de la recherche sur la nature et les technologies).

References

[1] R. Backhouse. Galois connections and fixed point calculus. In R. Backhouse, R. Crole, and J. Gibbons, editors, *Algebraic and Coalgebraic Methods in the Mathematics of Program Construction*, volume 2297 of *Lecture Notes in Computer Science*, pages 89–150. Springer, 2002.

[2] R. Berghammer and H. Zierer. Relational algebraic semantics of deterministic and nondeterministic programs. *Theoretical Computer Science*, 43(2–3):123–147, 1986.

[3] E. Cohen. Separation and reduction. In R. Backhouse and J. N. Oliveira, editors, *Mathematics of Program Construction*, volume 1837 of *Lecture Notes in Computer Science*, pages 45–59. Springer, 2000.

[4] J.-L. De Carufel and 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.

[5] J.-L. De Carufel and J. Desharnais. Demonic algebra with domain. In R. A. Schmidt, editor, *Relations and Kleene Algebra in Computer Science*, volume 4136 of *Lecture Notes in Computer Science*, pages 120–134. Springer, 2006.

[6] J.-L. De Carufel and J. Desharnais. Latest news about demonic algebra with domain. In R. Berghammer and B. Möller, editors, *10th International Conference on Relational Methods in Computer Science (RelMiCS10) and 5th International Conference on Applications of Kleene Algebra (AKA5)*, volume 4988 of *Lecture Notes in Computer Science*. Springer, 2008.

[7] J.-L. De Carufel and J. Desharnais. On the structure of demonic refinement algebras with enabledness and termination. In R. Berghammer and B. Möller, editors, *10th International Conference on Relational Methods in Computer Science (RelMiCS10) and 5th International Conference on Applications of Kleene Algebra (AKA5)*, volume 4988 of *Lecture Notes in Computer Science*. Springer, 2008.

[8] J. Desharnais, B. Möller, and G. Struth. Modal Kleene algebra and applications —A survey—. *JoRMiCS — Journal on Relational Methods in Computer Science*, 1:93–131, 2004.

[9] J. Desharnais, B. Möller, and G. Struth. Algebraic notions of termination. Research report 2006-23, Institut für Informatik, Universität Augsburg, Germany, Oct. 2006.

[10] J. Desharnais, B. Möller, and G. Struth. Kleene algebra with domain. *ACM Transactions on Computational Logic (TOCL)*, 7(4):798–833, Oct. 2006.

[11] 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*, pages 363–382. North-Holland, 1994.

[12] D. Harel, D. Kozen, and J. Tiuryn. *Dynamic Logic*. MIT Press, 2000.

[13] P. Höfner, B. Möller, and K. Solin. Omega algebra, demonic refinement algebra and commands. In R. A. Schmidt, editor, *Relations and Kleene Algebra in Computer Science*, volume 4136 of *Lecture Notes in Computer Science*, pages 222–234. Springer, 2006.

[14] D. Kozen. A completeness theorem for Kleene algebras and the algebra of regular events. *Information and Computation*, 110(2):366–390, May 1994.

[15] D. Kozen. Kleene algebra with tests. *ACM Transactions on Programming Languages and Systems*, 19(3):427–443, 1997.

[16] B. Möller. Kleene getting lazy. *Science of Computer Programming*, 65:195–214, 2007.

[17] B. Möller and G. Struth. wp is wlp. In W. MacCaull, M. Winter, and I. Düntsch, editors, *Relational Methods in Computer Science*, volume 3929 of *Lecture Notes in Computer Science*, pages 200–211. Springer, 2005.

[18] D. L. Parnas. A generalized control structure and its formal definition. *Communications of the ACM*, 26(8):572–581, 1983.

[19] K. Solin. On two dually nondeterministic refinement algebras. In R. A. Schmidt, editor, *Relations and Kleene Algebra in Computer Science*, volume 4136 of *Lecture Notes in Computer Science*, pages 373–387. Springer, 2006.

[20] K. Solin. *Abstract Algebra of Program Refinement*. PhD thesis, Turku Center for Computer Science, University of Turku, Finland, 2007.

[21] K. Solin and J. von Wright. Refinement algebra extended with operators for enabledness and termination. Technical Report 658, Turku Center for Computer Science, University of Turku, Finland, Jan. 2005. TUCS Technical Report.

[22] K. Solin and J. von Wright. Refinement algebra with operators for enabledness and termination. In T. Uustalu, editor, *Mathematics of Program Construction*, volume 4014 of *Lecture Note in Computer Science*, pages 397–415. Springer, 2006.

[23] J. von Wright. From Kleene algebra to refinement algebra. Technical Report 450, Turku Center for Computer Science, Mar. 2002.

[24] J. von Wright. Towards a refinement algebra. *Science of Computer Programming*, 51:23–45, 2004.