JEAN-LOU DE CARUFEL

Demonic Kleene Algebra

Thèse présentée
à la Faculté des études supérieures de l'Université Laval
dans le cadre du programme de doctorat en informatique
pour l'obtention du grade de Philosophiae doctor (Ph.D.)

FACULTÉ DES SCIENCES ET DE GÉNIE
UNIVERSITÉ LAVAL
QUÉBEC

2009

Résumé

Nous rappelons d'abord le concept d'algèbre de Kleene avec domaine (AKD). Puis, nous expliquons comment utiliser les opérateurs des AKD pour définir un ordre partiel appelé *raffinement démoniaque* ainsi que d'autres opérateurs démoniaques (plusieurs de ces définitions proviennent de la littérature). Nous cherchons à comprendre comment se comportent les AKD munies des opérateurs démoniaques quand on exclut les opérateurs angéliques usuels. C'est ainsi que les propriétés de ces opérateurs démoniaques nous servent de base pour axiomatiser une algèbre que nous appelons *Algèbre démoniaque avec domaine et opérateur t-conditionnel* (ADD-⍐). Les lois des ADD-⍐ qui ne concernent pas l'*opérateur de domaine* correspondent à celles présentées dans l'article *Laws of programming* par Hoare et al. publié dans la revue *Communications of the ACM* en 1987.

Ensuite, nous étudions les liens entre les ADD-⍐ et les AKD munies des opérateurs démoniaques. La question est de savoir si ces structures sont isomorphes. Nous démontrons que ce n'est pas le cas en général et nous caractérisons celles qui le sont. En effet, nous montrons qu'une AKD peut être transformée en une ADD-⍐ qui peut être transformée à son tour en l'AKD de départ. Puis, nous présentons les conditions nécessaires et suffisantes pour qu'une ADD-⍐ puisse être transformée en une AKD qui peut être transformée à nouveau en l'ADD-⍐ de départ.

Les conditions nécessaires et suffisantes mentionnées précédemment font intervenir un nouveau concept, celui de *décomposition*. Dans un contexte démoniaque, il est difficile de distinguer des transitions qui, à partir d'un même état, mènent à des états différents. Le concept de décomposition permet d'y arriver simplement. Nous présentons sa définition ainsi que plusieurs de ses propriétés.

Abstract

We first recall the concept of Kleene algebra with domain (KAD). Then we explain how to use the operators of KAD to define a demonic refinement ordering and demonic operators (many of these definitions come from the literature). We want to know how do KADs with the demonic operators but without the usual angelic ones behave. Then, taking the properties of the KAD-based demonic operators as a guideline, we axiomatise an algebra that we call *Demonic algebra with domain and t-conditional* (DAD-⨅). The laws of DAD-⨅ not concerning the *domain operator* agree with those given in the 1987 *Communications of the ACM* paper *Laws of programming* by Hoare et al.

Then, we investigate the relationship between DAD-⨅ and KAD-based demonic algebras. The question is whether every DAD-⨅ is isomorphic to a KAD-based demonic algebra. We show that it is not the case in general. However, we characterise those that are. Indeed, we demonstrate that a KAD can be transformed into a DAD-⨅ which can be transformed back into the initial KAD. We also establish necessary and sufficient conditions for which a DAD-⨅ can be transformed into a KAD which can be transformed back into the initial DAD-⨅.

Finally, we define the concept of *decomposition*. This notion is involved in the necessary and sufficient conditions previously mentioned. In a demonic context, it is difficult to distinguish between transitions that, from a given state, go to different states. The concept of decomposition enables to do it easily. We present its definition together with some of its properties.

Avant-propos

Jules, ce que j'admire le plus chez toi, c'est que tu réussisses à toujours garder la même passion et la même rigueur, que ce soit dans les moments de grande réussite ou dans les moments plus difficiles. Merci pour ta grande disponibilité et pour ton appui à chaque étape de ce travail.

Merci à ceux qui m'ont hébergé alors que j'étais sans domicile fixe : Mathieu, Sophie, Nicolas, Marie-Camille et Charlotte.

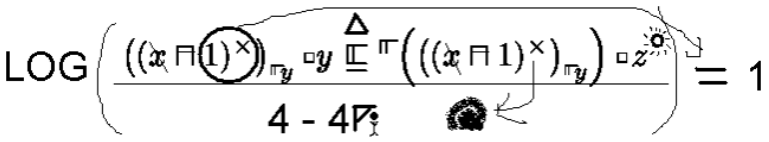
Merci à Louis qui m'a permis de garder les pieds sur terre.

André, avec toi j'apprends ce que sont la nuance et le discernement.

Je veux aussi remercier le Chef Harvey, Marie-Ève, Tristan et Nathan pour leur générosité et leur authenticité, mais surtout pour leur façon particulière de me rendre heureux.

Isabelle, merci de me faire confiance jour après jour, même lorsque c'est impossible. Tu es celle qui connaît toutes mes lubies et qui m'écoute toujours patiemment, avec amour et avec ce même sourire...

Ce travail a été supporté financièrement par le CRSNG (Conseil de recherches en sciences naturelles et en génie du Canada) et le FQRNT (Fond québécois de la recherche sur la nature et les technologies).



À Rose

M. Fourier avait l'opinion que le but principal des mathématiques était l'utilité publique et l'explication des phénomènes naturels; mais un philosophe comme lui aurait dû savoir que le but unique de la science, c'est l'honneur de l'esprit humain.

C.G.J. JACOBI

Contents

List of Tables

List of Figures

Chapter 1

Introduction

In software engineering and in computer science (as well as in many other fields of engineering), the notion of refinement is omnipresent [Som06]. Indeed, program refinement is behind many practical approaches that are used for developing software systems. In theoretical computer science, formal methods are interested in many questions including program refinement and how it can be used to improve automatic code generation. Since one of the basis of theoretical computer science is mathematics, formal methods study refinement via mathematical tools. For this task, many algebraic structures have been introduced throughout the last decades.

These structures encapsulate refinement via a partial order operator. The following list gives an idea of how a structure can mathematically represent operations on programs. Generally,

- an addition operator or supremum operator ($+$, $\sqcup$ or $\uplus$) denotes non-deterministic choice,
- a multiplication operator ($\cdot$, ";" or $\diamond$) denotes sequential composition,
- a unary exponent operator (*, $^\omega$ or $^\times$) denotes finite (or infinite) iteration
- and an inequality symbol ($\leq$, $\sqsubseteq$ or $\eqslantless$) denotes refinement. Usually

$$x \leq y \iff x + y = y$$

so that x refines y means that a non-deterministic choice between x and y is equivalent to y.

There is more than one such structure, each of them having its intended model and each of them representing a particular semantics of programs. Among other aspects, these algebraic structures handle angelic or demonic semantics. The expression "angelic semantics" may intuitively be thought of as the set of all possible behaviours, while the expression "demonic semantics" may be viewed as the set of all behaviours that can be guaranteed.

Moreover, some structures make it possible to analyse program semantics in a partial-correctness framework and others in a total-correctness framework. Partial-correctness means that the models of the structure focus only on transitions of a program that initialise and terminate successfully. Total-correctness means that the structure focuses on all possible transitions of a program, even those that do not lead to successful termination.

1.1 Three Algebraic Structures

The first structure worth mentioning is *relation algebra* (RA) [SS93, Tar41]. It is a structure that has relations as its intended model. Its axioms are satisfied by the usual operators on relations. Suppose a context where there are five possible states for a program P. Note $S_5 = \{1, 2, 3, 4, 5\}$ the set of possible states and suppose that P is represented by the relation $\{(1, 1), (1, 4), (2, 5), (3, 2)\}$. It means that the program P has four possible behaviours.

1. From state 1, it may either stay there
2. or go to state 4,
3. from state 2, it can only go to state 5
4. and from state 3, it can only go to state 2.

From other states, there is no possible action.

Intuitively[1], one can think of relations as subsets of $S \times S$ for a set of states S. The program interpretation of the usual operators on relations is as follows. Union ($\cup$) stands for non-deterministic choice, composition of relations (;) stands for sequential

[1] RA admits non representable models, but for the needs of this introduction, we only consider representable ones.

composition, reflexive transitive closure (*) stands for finite iteration and inclusion ($\subseteq$) stands for program refinement. Having in mind the previous three paragraphs, one can see that RA deals with angelic semantics in a partial-correctness framework.

Another well-known structure is *Kleene algebra* (KA) [Con71, Koz94]. Its canonical model is that of regular languages [Bro89]. Union of languages is represented by the operator $+$, concatenation of languages is represented by the operator $\cdot$, the closure of languages is represented by the operator * and inclusion of languages is represented by the partial order $\leq$. KA enables to model non-deterministic choice, program sequence, finite iteration and program refinement. It turns out that KA admits relations as a model too and it is also used for giving angelic semantics of programs in a partial-correctness framework. KA was extended to *Kleene algebra with tests* (KAT) [Koz97], which has been extended to *Kleene algebra with domain* (KAD) [DMS04, DMS06b, DMT06]. KAD has a *domain operator* that gives a grip on the inputs of the program (which is a useful tool). For the purpose of this introduction, we do not say more about it (see Chapter 2 for details), but we mention the name here for completeness. The intuition of regular languages or relations remains the best one for KA and its extensions.

In parallel to the study of relations, predicate transformers were introduced [Dij76]. Considering a fixed set of states S, one can see a predicate as a subset of S. We denote the set of subsets of S by $\wp(S)$. A predicate transformer is then a function of type $\wp(S) \longrightarrow \wp(S)$. Suppose a context where there are three possible states for a program P. Denote by $S_3 = \{1, 2, 3\}$ the set of states and suppose that P is represented by the predicate transformer

$$\begin{array}{rcl} T : \wp\,(S_3) & \longrightarrow & \wp\,(S_3) \\ \{\} & \mapsto & \{\} \\ \{1\} & \mapsto & \{1\} \\ \{2\} & \mapsto & \{\} \\ \{3\} & \mapsto & \{2\} \\ \{1,2\} & \mapsto & \{1\} \\ \{1,3\} & \mapsto & \{1,2\} \\ \{2,3\} & \mapsto & \{2\} \\ \{1,2,3\} & \mapsto & \{1,2,3\} \ . \end{array}$$

An association $A \mapsto B$ has the following interpretation: to ensure that the program P terminates in any state of A, it must start in a state of B.

- The association $\{1\} \mapsto \{1\}$ means that to terminate in state 1, the program P

must start in state 1.

- The association $\{2\} \mapsto \{\}$ means that there is no state from which the program P necessarily goes to state 2.
- The association $\{2,3\} \mapsto \{2\}$ means that to terminate in either of states 2 or 3, the program P must start in state 2.
- The association $\{1,3\} \mapsto \{1,2\}$ means that to terminate in either of states 1 or 3, the program P must start either in state 1 or 2.

Now take any two predicate transformers $T_1 : \wp(S_3) \longrightarrow \wp(S_3)$ and $T_2 : \wp(S_3) \longrightarrow \wp(S_3)$. Here is a description of some operators on predicate transformers.

- The supremum operator $\sqcup$ is such that $(T_1 \sqcup T_2)(p) = T_1(p) \cap T_2(p)$ for all $p \in \wp(S_3)$.
- The composition operator is $(T_1 \square T_2)(p) = T_1(T_2(p))$ for all $p \in \wp(S_3)$.
- For now, the easiest way to describe the iteration operator on a predicate transformer $T : \wp(S_3) \longrightarrow \wp(S_3)$ is

$$T^\times = 1 \sqcup T \sqcup (T \square T) \sqcup (T \square T \square T) \ ,$$

  where 1, defined by $1(p) = p$ for all $p \in \wp(S_3)$, is the identity for the composition operator. This iteration operator is then a finite iteration operator since it iterates T no more than *three* times. Note that this definition is only valid for S_3. The general definition (including the case where S is infinite) of $T^\times$ involves the calculation of the least fixpoint of a well-chosen function. For the time being, we skip the details.
- We write $T_1 \sqsubseteq T_2$ when $T_2(p) \subseteq T_1(p)$ for all $p \in \wp(S_3)$.

With this interpretation, predicate transformers give demonic semantics of programs in a total-correctness framework.

Recently, Von Wright defined *demonic refinement algebra* (DRA) [vW04]. This structure has the positively conjunctive predicate transformers[2] as its intended model.

[2] Let $I \neq \{\}$ be an index set. A predicate transformer T over a set of states S is *positively conjunctive* if

$$T\left(\bigcap_{i \in I} p_i\right) = \bigcap_{i \in I} T(p_i) \ ,$$

where $p_i \in \wp(S)$.

In addition to the finite iteration operator, it includes an infinite iteration operator $^\omega$ related to the calculation of the greatest fixpoint of a well-chosen function. DRA has been extended to *demonic refinement algebra with enabledness* (DRAe) [Sol07, SvW06]. The name of this operator (*enabledness operator*) reflects its semantic interpretation in the realm of programs and its axiomatisation is inspired by that of the domain operator of KAD. For the purpose of this introduction, we do not say more about it (see [DD06c, DD08b, Sol07, SvW06] for details or Section 6.2 for a brief presentation). The intuition of positively conjunctive predicate transformers remains the best one for DRA and DRAe.

1.2 The Meeting Point of Two Parallel Lines

Relations and predicate transformers seem to be the "opposite" of each other. Relations represent an angelic semantics of programs in a partial-correctness framework and they model the states where a program may go from a given state. Predicate transformers represent a demonic semantics of programs in a total-correctness framework and they model the states from which a program is guaranteed to get to a given state.

However, work has been done to bring together angelic and demonic semantics. For instance, demonic operators were defined in RA from the angelic ones [BvdW93, BZ86, DBS+95, DMN97, Kah01, Mad96, TD99]. Demonic operators were defined from the angelic ones in KAD too [DMT00, DMT06]. It is worth mentioning since, as said previously, relations are also a model of KAD. Other works relating angelic and demonic semantics have been published [BvW92, MCR07, Sol07]. At the moment, no algebraic structure has relations with demonic operators (or KAD with demonic operators) as its intended model.

It turns out that relations and predicate transformers can be connected. Take $S_2 = \{1, 2\}$. The lattice of relations over S_2 has the shape of the one of Figure 1.1. This lattice might be seen as a model of RA as well as a model of KAD. By ordering the same relations but with demonic refinement (which can be defined from the angelic operators in RA), one gets a semilattice of the shape of the one of Figure 1.2. As mentioned before, no algebraic structure has relations with demonic operators as its intended model. The lattice of positively conjunctive predicate transformers over S_2 has the shape of the one of Figure 1.3. This lattice might be seen as a model of DRAe. Looking carefully at these three semilattices, one can gather them in the lattice of Figure 1.4.

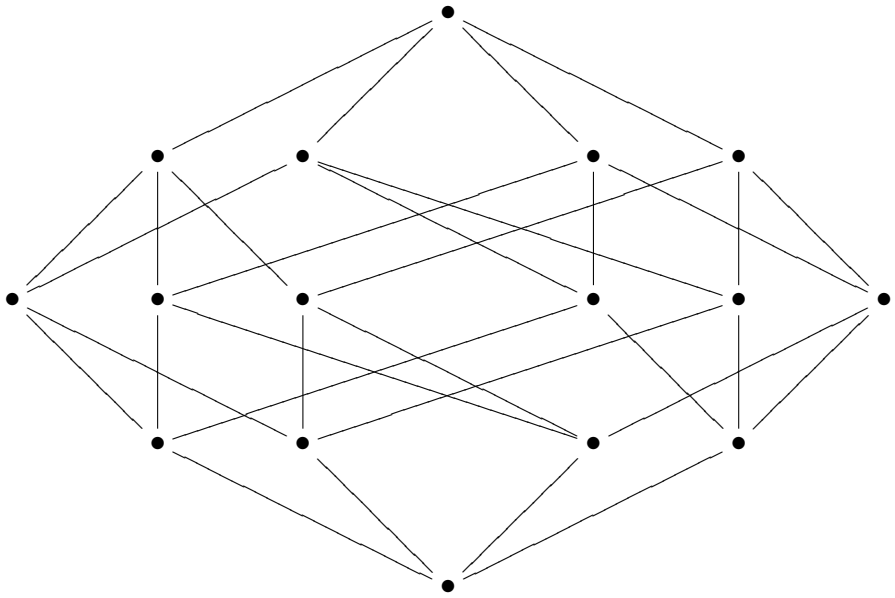


Figure 1.1: Lattice of relations over S_2 ordered by angelic refinement.

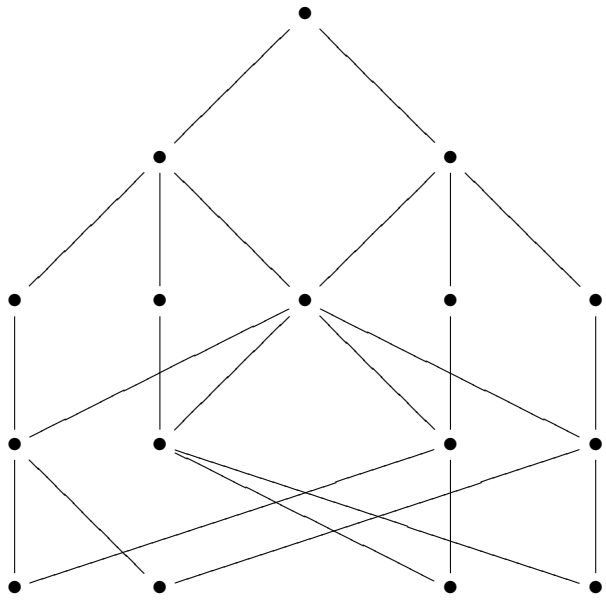


Figure 1.2: Lattice of relations over S_2 ordered by demonic refinement.

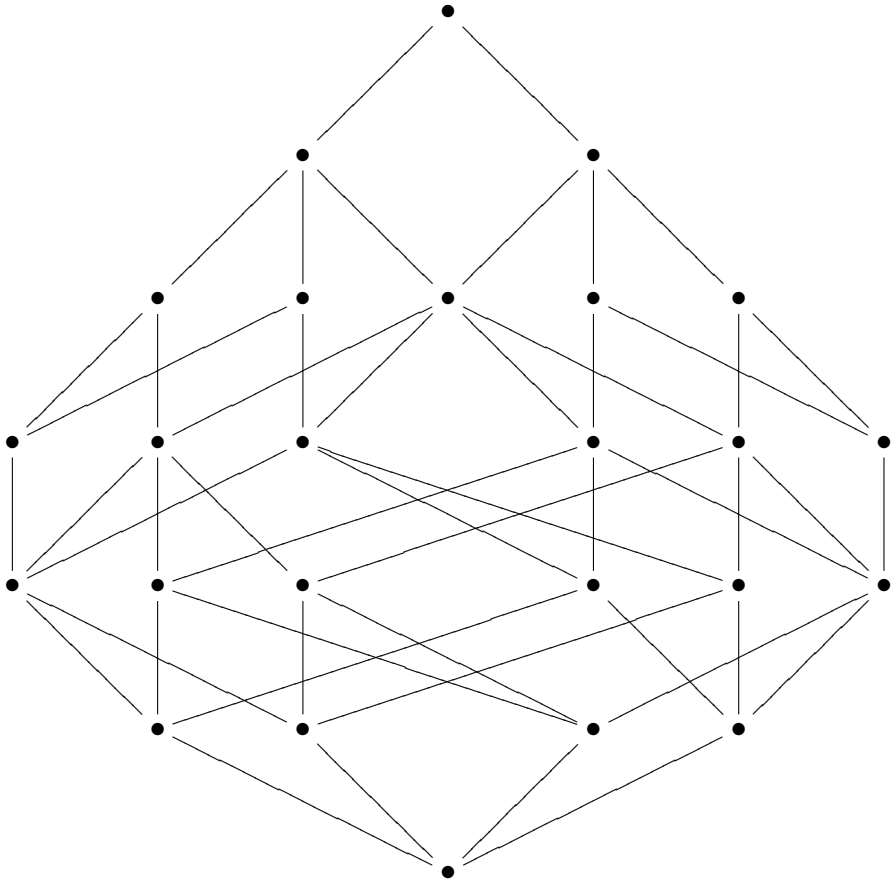


Figure 1.3: Lattice of positively conjunctive predicate transformers over S_2 ordered by $\sqsubseteq$.

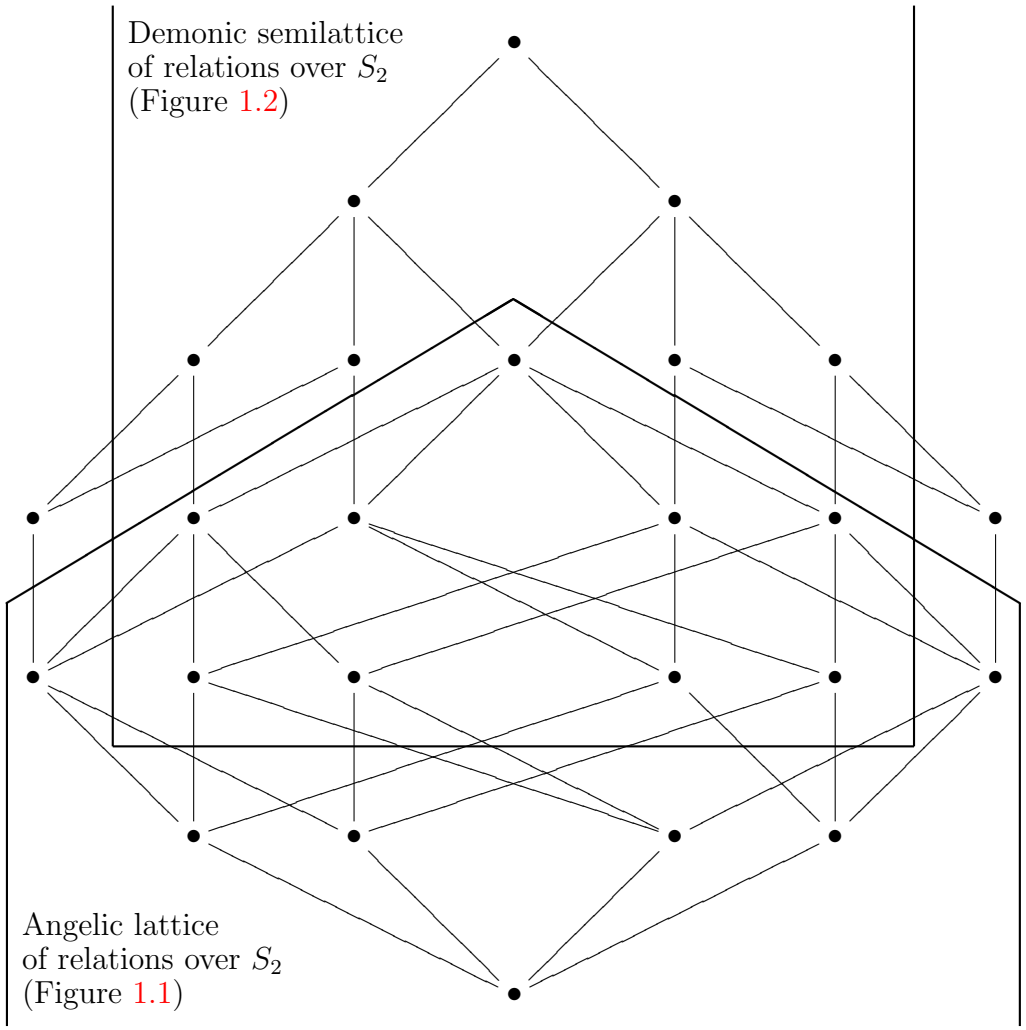


Figure 1.4: Lattice of positively conjunctive predicate transformers over S_2, a synthesis of the semilattices of Figures 1.1, 1.2 and 1.3.

Even though the lattice of Figure 1.4 is not a complete surprise, it raises questions.

- Is there a similar connection when S is any (finite or infinite) set of states?
- Is there a similar connection between KAD, RA and DRAe in general rather than just between some of their models?
- Is it possible to describe this connection in an algebraic way?

1.3 Contributions

In [DD06c, DD08b], we show that, under suitable hypotheses, every DRAe is isomorphic to an algebra of ordered pairs of elements of a KAD. This establishes an algebraic connection between the bottom part of the lattice and the whole lattice —refer to Figure 1.4. We are going to present a general survey of this result in Section 6.2.

In this thesis (as well as in [DD06a, DD06b, DD08a]),

1. To those demonic operators that were defined in the context of KAD, we add two new ones: the demonic iteration operator $^{\times_A}$ and the t-conditionnal operator $\overset{A}{\sqcap}_\bullet$.
2. We demonstrate many properties of the demonic iteration operator and the t-conditionnal operator.
3. We define an algebraic structure called *demonic algebra with domain and t-conditional* (DAD-$\sqcap_\bullet$) that has KAD with demonic operators as its intended model (so that the semilattice of Figure 1.2 might be seen as a model of DAD-$\sqcap_\bullet$).
4. We prove the independence of many axioms of DAD-$\sqcap_\bullet$ by means of appropriate counter-examples. Many of these counter-examples were generated by Mace4 [Mac], an automated theorem prover system that generates finite (counter)models from first-order axioms.
5. We demonstrate many properties of DAD-$\sqcap_\bullet$.
6. We define angelic operators from the demonic ones of DAD-$\sqcap_\bullet$.
7. We demonstrate that, under suitable hypotheses, DAD-$\sqcap_\bullet$ together with the aforementioned angelic operators form a KAD.

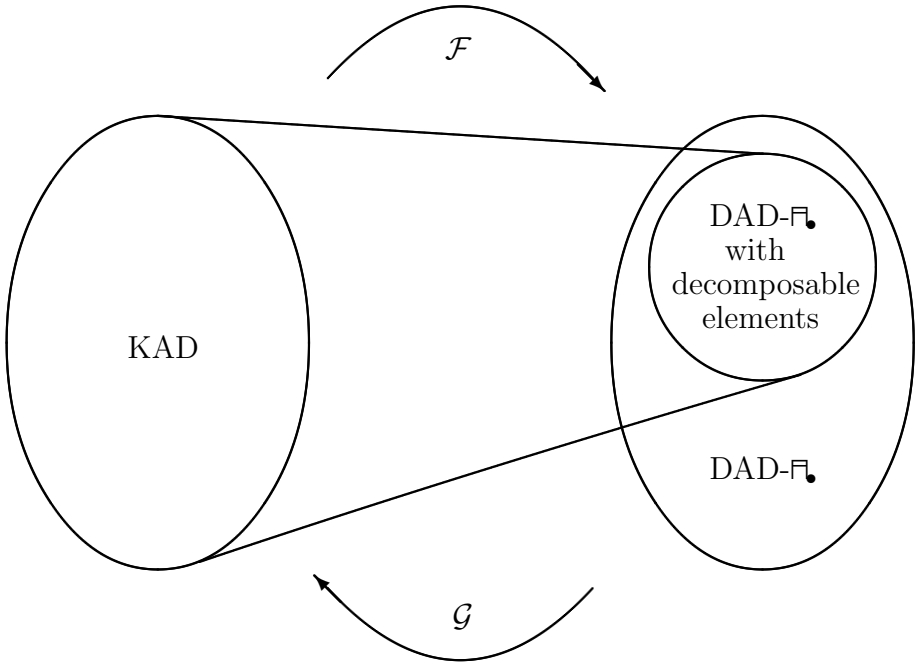


Figure 1.5: Representation of the duality between KAD and DAD-⊼.

8. We demonstrate that a KAD can be transformed into a DAD-⊼ which can be transformed back into the initial KAD. We also demonstrate that, under suitable hypotheses, a DAD-⊼ can be transformed into a KAD which can be transformed back into the initial DAD-⊼. Consequently, under the same suitable hypotheses, one can see DAD-⊼ as a dual of KAD. This duality is an algebraic connection between the bottom part and the upper part of the lattice of Figure 1.4 for any model of KAD. Showing it is the ultimate goal of this text. The suitable hypotheses mentioned above are related to the notion of *decomposable elements* and we skip the details for this introduction. Figure 1.5 gives a picture of the duality between KAD and DAD-⊼.

In [DD06c, DD08b], we also establish, under suitable hypotheses, an algebraic connection between the upper part of the lattice and the whole lattice —refer to Figure 1.4.

1.4 Plan of the Thesis

There are two kinds of tasks we have to accomplish. Firstly, the lower part of the lattice, the upper part of the lattice and the whole lattice of Figure 1.4 must have an algebraic foundation. In other words, we have to define three algebraic structures, each

one of them having one part of the lattice as its intended model. KAD is an algebraic foundation for the lower part, DAD-⍀ is an algebraic foundation for the upper part, and DRAe is an algebraic foundation for the whole lattice. Secondly, we have to define transformations from any part of the lattice to any other part of the lattice. In this thesis, we mainly concentrate on the bottom part and the upper part. The treatment of the whole lattice will only be skimmed over.

Here is how the thesis is divided. At first, in Chapter 2, we recall the definitions of *Kleene algebra* (KA) and its extensions, *Kleene algebra with tests* (KAT) and *Kleene algebra with domain* (KAD). This chapter also contains the definitions of the usual demonic operators in terms of the KAD's operators. To these operators, we add two new demonic ones and we derive new simple results about all of them. The chapter concludes with a fundamental theorem stating that the elements of a KAD together with the demonic operators form a *demonic algebra with domain and t-conditional* (defined in the following chapter). It is the first step toward the desired duality.

Secondly, in Chapter 3, we present a new structure called *demonic algebra* (DA) and its extensions, *demonic algebra with tests* (DAT), *demonic algebra with domain* (DAD) and *demonic algebra with domain and t-conditional* (DAD-⍀). We also demonstrate many results about these structures.

Thirdly, in Chapter 4, we define angelic operators from DAD-⍀'s operators. In order to do so, we need to define *decomposable elements*. These are indispensable for the definition of angelic composition. Once angelic operators are defined, we present major results about them and about decomposable elements. The chapter concludes with a fundamental theorem stating that the decomposable elements of a DAD-⍀ together with the angelic operators form a KAD. It is the second step toward the desired duality.

Then, in Chapter 5, we define —refer to Figure 1.5— functions $\mathcal{F}$ and $\mathcal{G}$ such that $\mathcal{F}(\mathcal{K})$ is a DAD-⍀ for each KAD $\mathcal{K}$ and, under suitable conditions, $\mathcal{G}(\mathcal{A})$ is a KAD for each DAD-⍀ $\mathcal{A}$. Then, we demonstrate that (under the same suitable conditions) $\mathcal{G} \circ \mathcal{F}$ is the identity on any KAD $\mathcal{K}$ and $\mathcal{F} \circ \mathcal{G}$ is the identity on any DAD-⍀ $\mathcal{A}$. It is the third and last step toward the desired duality.

In Chapter 6, we present a short discussion about two different algebras of ordered pairs. The first algebra helps understand models of DAD-⍀. The second one was defined in [DD06c, DD08b] and it is behind an algebraic connection between the bottom part of the lattice and the whole lattice of Figure 1.4.

We finally conclude in Chapter 7.

Chapter 2

Kleene Algebra with Domain and KAD-based Demonic Operators

We explained in the introduction that the ultimate goal of this thesis is to establish an algebraic connection —a duality— between the lower part and the upper part of the lattice of Figure 1.4. In order to do so, we need an algebraic description of each part.

In this chapter, we present algebraic foundations for the lower part of the lattice of Figure 1.4. Indeed, we recall basic definitions about *Kleene algebra* (KA) (Section 2.1) and its extensions, *Kleene algebra with tests* (KAT) (Section 2.2) and *Kleene algebra with domain* (KAD) (Section 2.3).

Then we present the KAD-based definition of the demonic operators (Section 2.4) together with crucial properties they satisfy (Section 2.5). It prepares the ground for Chapter 3 where we present algebraic foundations for the upper part of the lattice of Figure 1.4. It is the first step toward the desired duality (refer to Section 1.3).

2.1 Kleene Algebra

In this section, we present the concept of *Kleene algebra* (KA) and we discuss some of its axioms. Initially, different variants of KA were introduced by Conway [Con71], but since then, one of them has become well known, thanks to Kozen [Koz94]. This is the one we present in this section and use throughout this thesis.

Definition 2.1 (Kleene algebra)**.** *A* Kleene algebra *(KA) is a structure* $\mathcal{K} = (K, +, \cdot, ^*, 0, 1)$ *such that the following properties hold for all* $x, y, z \in K$*.*

$$(x + y) + z = x + (y + z) \tag{2.1}$$
$$x + y = y + x \tag{2.2}$$
$$x + x = x \tag{2.3}$$
$$0 + x = x \tag{2.4}$$
$$(x \cdot y) \cdot z = x \cdot (y \cdot z) \tag{2.5}$$
$$0 \cdot x = x \cdot 0 = 0 \tag{2.6}$$
$$1 \cdot x = x \cdot 1 = x \tag{2.7}$$
$$x \cdot (y + z) = x \cdot y + x \cdot z \tag{2.8}$$
$$(x + y) \cdot z = x \cdot z + y \cdot z \tag{2.9}$$
$$x^* = x^* \cdot x + 1 \tag{2.10}$$

Addition induces a partial order $\leq$ *such that, for all* $x, y \in K$*,*

$$x \leq y \iff x + y = y \ . \tag{2.11}$$

Finally, the following properties must be satisfied for all $x, y, z \in K$*.*

$$x \cdot z + y \leq z \implies x^* \cdot y \leq z \tag{2.12}$$
$$z \cdot x + y \leq z \implies y \cdot x^* \leq z \tag{2.13}$$

Remark 2.2. Hollenberg has shown that the following symmetric version of (2.10),

$$x^* = x \cdot x^* + 1 \ , \tag{2.14}$$

is derivable from these axioms [Hol96]. The converse is true. Indeed, if (2.10) were replaced by (2.14) in the axiomatisation of KA, then (2.10) would be derivable from these axioms. Moreover, Kozen has shown in [Koz90] that (2.12) and (2.13) are independent.

Also, one can show $x^* = \mu_{\leq}(y :: y \cdot x + 1)$ with (2.7), (2.10) and (2.13), and $x^* = \mu_{\leq}(y :: x \cdot y + 1)$ with (2.7), (2.14) and (2.12).

Finally, in the presence of the other axioms, (2.12) and (2.13) are equivalent to the following two.

$$x \cdot z \leq z \implies x^* \cdot z \leq z \tag{2.15}$$
$$z \cdot x \leq z \implies z \cdot x^* \leq z \tag{2.16}$$

The natural model of KA is regular languages. However, it is the study of relational models of KA that led us to the lattice of Figure 1.4 and inspired us for the present work. This is why, throughout this thesis, we elude regular languages.

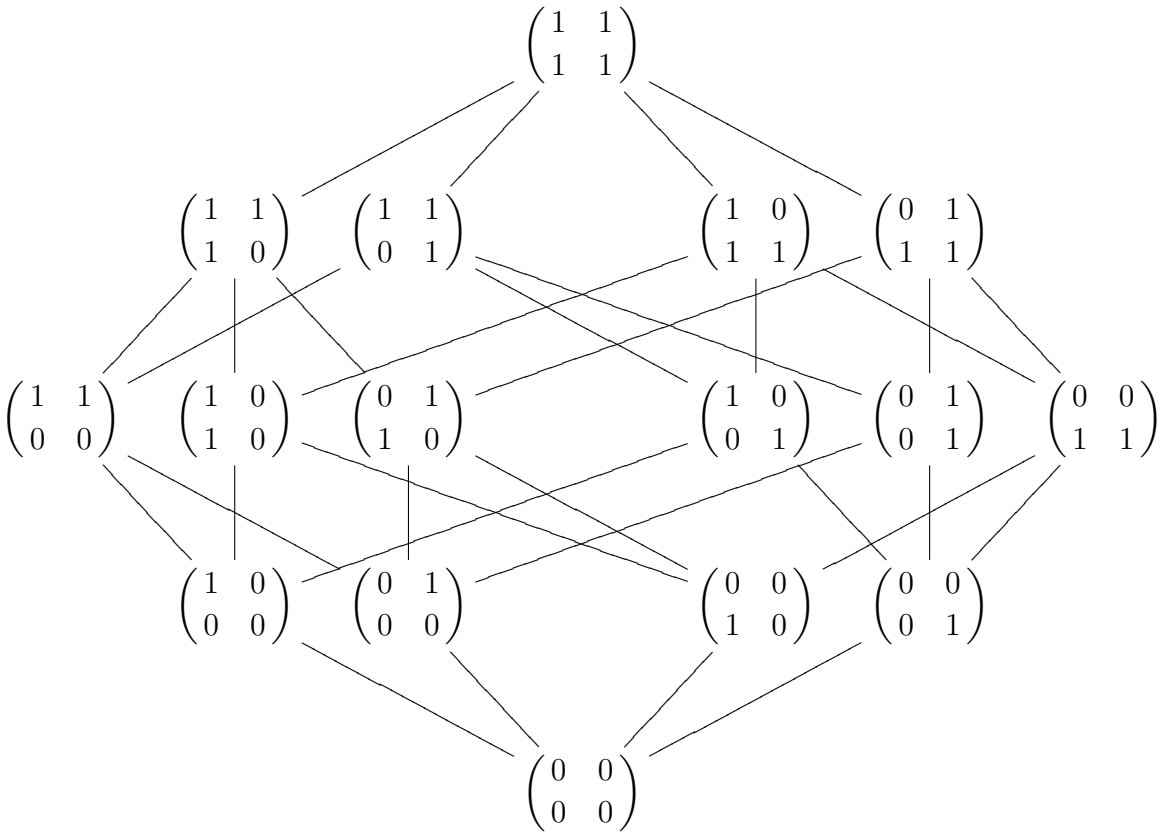


Figure 2.1: Relation algebra over the set S_2 ordered by $\subseteq$.

Consider the relations over the set $S_2 = \{1, 2\}$. Interpreting $+$ as union ($\cup$), $\cdot$ as composition of relations (;), * as reflexive transitive closure, 0 as $\{\}$, 1 as $\{(1,1),(2,2)\}$ and $\leq$ as inclusion ($\subseteq$), one gets a model of KA. Figure 2.1 displays the Boolean matrix representation of the lattice of these relations ordered by $\subseteq$. It is a more detailed version of Figure 1.1.

2.2 Kleene Algebra with Tests

KA, as defined in the previous section, is itself an algebraic foundation of the lower part of the lattice of Figure 1.4. However, as we mentioned earlier, we want to define demonic operators in the context of KA. For this matter (see Section 2.4), we need a *domain operator* that cannot be defined without the concept of test.

Of course, at first, the purpose of tests was not to define a domain operator. His-

Program	Semantics
abort	0
skip	1
$x \llbracket y$	$x + y$
$x; y$	$x \cdot y$
if t then x else y	$t \cdot x + \neg t \cdot y$
while t do x	$(t \cdot x)^* \cdot \neg t$

Table 2.1: Angelic semantics of programs in KAT.

torically, tests have been firstly introduced to reason about programs. Indeed, a test can be seen as a precondition that must be true in order to enable a program to be executed.

Hence we present the definition of *Kleene algebra with tests* (KAT). It was first proposed by Kozen [Koz97].

Definition 2.3 (Kleene algebra with tests)**.** *A* Kleene algebra with tests *(KAT) is a structure* $\mathcal{K} = (K, \mathsf{test}(K), +, \cdot, ^*, 0, 1, \neg)$ *such that* $\mathsf{test}(K) \subseteq \{t : K \mid t \leq 1\}$*,* $(K, +, \cdot, ^*, 0, 1)$ *is a KA and* $(\mathsf{test}(K), +, \cdot, \neg, 0, 1)$ *is a Boolean algebra.*

In the sequel, we use the letters w, x, y, z for arbitrary elements of a KA and s, t, u, v for tests. In proofs and discussions, we use the hint "Boolean algebra" to indicate application of any Boolean properties of tests.

The usual semantics of programs as given by KAT is shown in Table 2.1, where $x \llbracket y$ is the non-deterministic choice between x and y. Note that in this table, we use the letters t, x and y for elementary programs as well as for their semantics. Having in mind the relational model, one can see that this semantics focuses on the set of all possible behaviours. This interpretation is pictured in the following example. Suppose there are four possible states for programs P_1 and P_2. Note $S_4 = \{1, 2, 3, 4\}$ the set of possible states and suppose that P_1 and P_2 are respectively represented by the relations $x = \{(1,1), (1,4), (2,4), (3,2)\}$ and $y = \{(2,1), (2,3), (3,4)\}$. Now take the test $t = \{(1,1), (3,3)\}$. We have

$$\begin{aligned} \text{if } t \text{ then } \mathsf{P}_1 \text{ else } \mathsf{P}_2 &= \text{if } t \text{ then } x \text{ else } y \\ &= t \cdot x + \neg t \cdot y \\ &= \{(1,1),(3,3)\} \cdot \{(1,1),(1,4),(2,4),(3,2)\} + \\ &\quad \neg\{(1,1),(3,3)\} \cdot \{(2,1),(2,3),(3,4)\} \end{aligned}$$

$$\begin{aligned} &= \{(1,1),(3,3)\} \cdot \{(1,1),(1,4),(2,4),(3,2)\} + \\ &\quad \{(2,2),(4,4)\} \cdot \{(2,1),(2,3),(3,4)\} \\ &= \{(1,1),(1,4),(3,2)\} + \{(2,1),(2,3)\} \\ &= \{(1,1),(1,4),(2,1),(2,3),(3,2)\} \end{aligned}$$

which is the set of all possible behaviours. It is now easy to see that the semantics presented in Table 2.1 are angelic ones.

2.3 Kleene Algebra with Domain

It is useful to have a grip on the inputs of the aforementioned programs. The *domain operator* encapsulates the necessary properties. Moreover, it is an essential operator in the definition of demonic operators in the context of KA (see Section 2.4).

Here is the definition of *Kleene algebra with domain* (KAD) as defined by Desharnais, Möller, Struth and Tchier [DMS04, DMS06b, DMT06].

Definition 2.4 (Kleene algebra with domain)**.** *A* Kleene algebra with domain *(KAD) is a structure* $\mathcal{K} = (K, \mathsf{test}(K), +, \cdot, ^*, 0, 1, \neg, ^\ulcorner)$ *such that* $(K, \mathsf{test}(K), +, \cdot, ^*, 0, 1, \neg)$ *is a KAT and, for all* $x \in K$ *and all* $t \in \mathsf{test}(K)$*,*

$$x \leq {}^\ulcorner x \cdot x \ , \tag{2.17}$$

$${}^\ulcorner(t \cdot x) \leq t \ , \tag{2.18}$$

$${}^\ulcorner(x \cdot {}^\ulcorner y) \leq {}^\ulcorner(x \cdot y) \ . \tag{2.19}$$

Remark 2.5. It turns out that these axioms force the test algebra $\mathsf{test}(K)$ to be the maximal Boolean algebra included in $\{t : K \mid t \leq 1\}$ (see [DMS06b]).

Note that (2.19) is satisfied for relation algebras[1]. It is called *locality*. However, there are KATs where it does not hold. Indeed, the following counter-example appears in [DM01].

Example 2.6. Take $K = \{0, 1, \mathsf{a}, \mathsf{b}\}$ and $\mathsf{test}(K) = \{0, 1\}$. The operators defined by the following tables make $(K, \mathsf{test}(K), +, \cdot, ^*, 0, 1, \neg)$ a KAT.

$+$	0	1	a	b
0	0	1	a	b
1	1	1	b	b
a	a	b	a	b
b	b	b	b	b

$\cdot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	0	a
b	0	b	a	b

	*
0	1
1	1
a	b
b	b

	$\neg$
0	1
1	0

	$^\ulcorner$
0	0
1	1
a	1
b	1

[1] For a relation R on a set S, ${}^\ulcorner R = \{(s,s) : S \times S \mid (\exists\, t : S \mid (s,t) \in R)\}$.

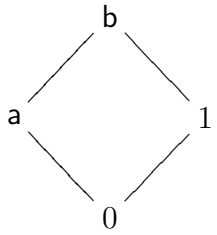


Figure 2.2: Hasse diagram of Example 2.6.

The refinement ordering corresponding to $+$ is represented in the lattice of Figure 2.2. It turns out that the present algebra is a KAT where (2.17) and (2.18) hold but not (2.19). Indeed, $\ulcorner(a \cdot \ulcorner a) = 1 \not\leq 0 = \ulcorner(a \cdot a)$.

Here is an illustration of the domain operator for the familiar model of relations.

$$\begin{aligned} \ulcorner\{(0,0),(0,1),(2,1)\} &= \{(0,0),(2,2)\} \\ \ulcorner\{(0,0),(0,1),(0,2)\} &= \{(0,0)\} \\ \ulcorner\{\} &= \{\} \end{aligned}$$

Hence the domain operator gives the states (represented by an appropriate test) from which there is a possible transition.

There are many properties about KA, KAT and KAD and we gather those that will be used later on in the following proposition. See [DMS06b, DMT06, Koz94] for proofs.

Proposition 2.7. *Let $\mathcal{K}$ be a KAD. The following laws hold for all $x, y \in K$ and all $t \in \mathsf{test}(K)$.*

1. $(x + y)^* = (x^* \cdot y)^* \cdot x^*$
2. $(x + y)^* = x^* \cdot (y \cdot x^*)^*$
3. $x = y \iff t \cdot x = t \cdot y \wedge \neg t \cdot x = \neg t \cdot y$
4. $x = y \iff x \cdot t = y \cdot t \wedge x \cdot \neg t = y \cdot \neg t$
5. $\ulcorner x = \mathsf{min}_{\leq}\{t : \mathsf{test}(K) \mid t \cdot x = x\}$
6. $\ulcorner x \cdot x = x$
7. $\ulcorner x \leq t \iff x \leq t \cdot x$
8. $\ulcorner(x \cdot \ulcorner y) = \ulcorner(x \cdot y)$

9. $\neg\ulcorner x \cdot x = 0$
10. $\ulcorner t = t$
11. $\ulcorner(t \cdot x) = t \cdot \ulcorner x$
12. $\ulcorner(x \cdot y) \leq \ulcorner x$
13. $\ulcorner(x + y) = \ulcorner x + \ulcorner y$
14. $x \leq y \implies \ulcorner x \leq \ulcorner y$
15. $\ulcorner(x \cdot t) \leq t \iff \ulcorner(x^* \cdot t) \leq t$
16. $\ulcorner(x^*) = 1$

The following operator characterises the set of states from which no computation as described by x may lead outside the domain of y. It facilitates the presentation and the comprehension of further definitions and results.

Definition 2.8 (KA-implication)**.** *Let $\mathcal{K}$ be a KAD and take $x, y \in K$. The* KA-implication $x \rightarrow y$ *is defined by*

$$x \rightarrow y = \neg\ulcorner(x \cdot \neg\ulcorner y) \ .$$

2.4 KAD-Based Demonic Operators

We are now ready to introduce demonic operators in the context of KAD. What do we need them for? When we constructed the upper part of the lattice displayed in Figure 1.4 in the introduction, we took the elements of the bottom part of the same lattice and we (partially-)ordered them by demonic refinement. Those elements are relations and it is possible to define not only demonic refinement on them, but many demonic operators (see [BvdW93, BZ86, DBS+95, DMN97, Kah01, Mad96, TD99]).

What we are trying to develop is an algebraic description of the lattice of Figure 1.4 and of its connections, but for any model of KAD. Therefore, we need to look at the definition of demonic operators, but from now, in the context of KAD. Most of them were defined in [DMT00, DMT06].

Here is the definition of demonic refinement.

Definition 2.9 (Demonic refinement)**.** *Let $\mathcal{K}$ be a KAD and take $x, y \in K$. We say that x* refines *y, noted $x \sqsubseteq_A y$, when*

$$\begin{aligned} \lceil y &\leq \lceil x \ , \\ \lceil y \cdot x &\leq y \ . \end{aligned}$$

The subscript A in $\sqsubseteq_A$ indicates that the demonic refinement is defined with the operators of the angelic world. An analogous notation will be introduced when we define angelic operators in the demonic world.

This definition can be simply illustrated with relations. Let $Q = \{(1,2),(2,4)\}$ and $R = \{(1,2),(1,3)\}$. Then $\lceil R = \{(1,1)\} \subseteq \{(1,1),(2,2)\} = \lceil Q$. Since in addition $\lceil R \cdot Q = \{(1,2)\} \subseteq R$, we have $Q \sqsubseteq_A R$.

The following proposition helps understand the definition of $\sqsubseteq_A$ (see [DMT06] for proof).

Proposition 2.10 (Demonic upper semilattice)**.**

1. *The relation $\sqsubseteq_A$ defined in KAD is a partial order and it induces an upper semilattice with* demonic join *$\sqcup_A$:*

$$x \sqsubseteq_A y \iff x \sqcup_A y = y \ .$$

2. *Demonic join satisfies the following two properties.*

$$\begin{aligned} x \sqcup_A y &= \lceil x \cdot \lceil y \cdot (x + y) \\ \lceil (x \sqcup_A y) &= \lceil x \sqcup_A \lceil y = \lceil x \cdot \lceil y \end{aligned}$$

Remark 2.11. Note that for all $s, t \in \mathsf{test}(K)$,

$$s \sqsubseteq_A t \iff t \leq s \ .$$

Figure 2.3 represents the relations over the set $S_2 = \{1,2\}$ ordered by $\sqsubseteq_A$. It is a more detailed version of Figure 1.2. It can also be seen as the demonic version of Figure 2.1.

Then we present the definition of demonic composition. The way it is defined corresponds to doing the composition of x by y, but without those states from which x may lead outside the domain of y. This last sentence reminds of the KA-implication operator (see Definition 2.8) and this is not a coincidence.

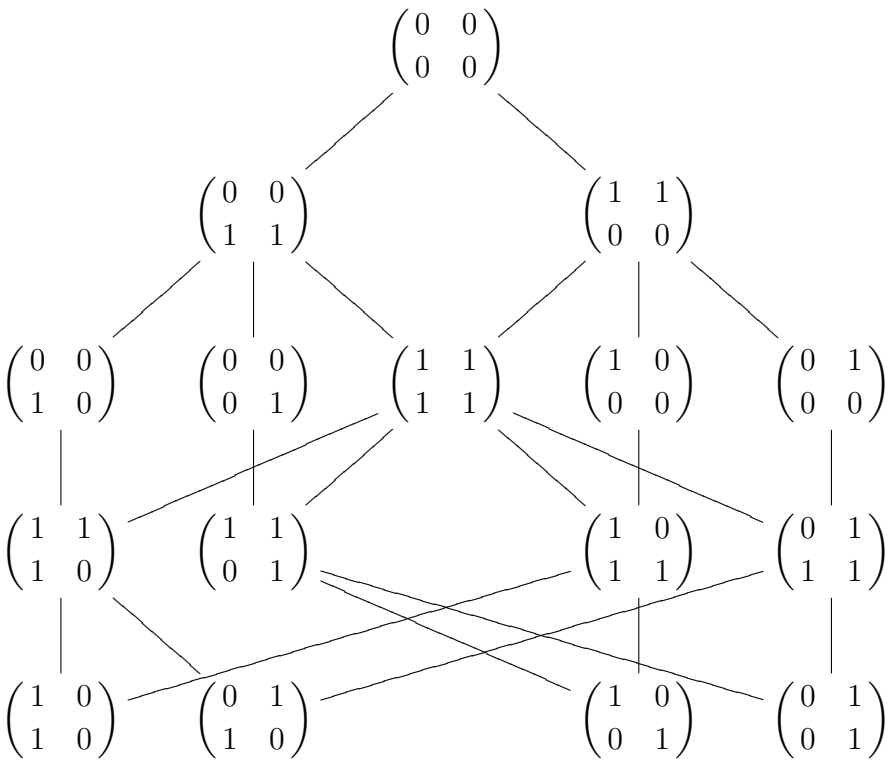


Figure 2.3: Relation algebra over the set $S_2 = \{1, 2\}$ ordered by $\sqsubseteq_A$.

Definition 2.12 (Demonic composition)**.** *Let $\mathcal{K}$ be a KAD and take $x, y \in K$. The* demonic composition *of x and y, written $x \mathbin{\square_A} y$, is defined by*

$$x \mathbin{\square_A} y = (x \rightarrow y) \cdot x \cdot y \ .$$

Again using relations, we illustrate this definition. Let $Q = \{(1,2),(1,4),(2,3),(4,1)\}$, $R = \{(1,1),(2,4)\}$ and suppose the state space is $S_4 = \{1,2,3,4\}$. Then

$$\begin{aligned}
Q \rightarrow R &= \{(1,2),(1,4),(2,3),(4,1)\} \rightarrow \{(1,1),(2,4)\} \\
&= \neg^{\Gamma}(\{(1,2),(1,4),(2,3),(4,1)\} \cdot \neg^{\Gamma}\{(1,1),(2,4)\}) \\
&= \neg^{\Gamma}(\{(1,2),(1,4),(2,3),(4,1)\} \cdot \neg\{(1,1),(2,2)\}) \\
&= \neg^{\Gamma}(\{(1,2),(1,4),(2,3),(4,1)\} \cdot \{(3,3),(4,4)\}) \\
&= \neg^{\Gamma}\{(1,4),(2,3)\} \\
&= \neg\{(1,1),(2,2)\} \\
&= \{(3,3),(4,4)\}
\end{aligned}$$

so

$$Q \mathbin{\square_A} R = (Q \rightarrow R) \cdot Q \cdot R$$

$$\begin{aligned} &= \{(3,3),(4,4)\} \cdot \{(1,2),(1,4),(2,3),(4,1)\} \cdot \{(1,1),(2,4)\} \\ &= \{(3,3),(4,4)\} \cdot \{(1,4),(4,1)\} \\ &= \{(4,1)\} \ . \end{aligned}$$

There are many properties about KA-implication and demonic composition and we gather those that will be used later on in the following proposition. See [DMT00, DMT06] for proofs.

Proposition 2.13. *Let $\mathcal{K}$ be a KAD. The following laws hold for all $x, y, z \in K$ and all $t \in \mathsf{test}(K)$.*

1. $x \,\square_A\, (y \,\square_A\, z) = (x \,\square_A\, y) \,\square_A\, z$
2. $t \,\square_A\, x = t \cdot x$
3. $\ulcorner y = 1 \implies x \,\square_A\, y = x \cdot y$
4. $\ulcorner(x \,\square_A\, y) = (x \to y) \cdot \ulcorner x$
5. $x \to y = x \to \ulcorner y$
6. $(x \to y) \cdot x = (x \to y) \cdot x \cdot \ulcorner y$
7. $(x \cdot y) \to z = x \to (y \to z)$
8. $t \leq x \to t \iff t \leq x^* \to t$
9. $x \leq y \implies y \to z \leq x \to z$
10. $y \leq z \implies x \to y \leq x \to z$
11. $x \,\square_A\, y \leq x \cdot y$
12. $x \sqsubseteq_A y \implies x \,\square_A\, z \sqsubseteq_A y \,\square_A\, z$
13. $x \sqsubseteq_A y \implies z \,\square_A\, x \sqsubseteq_A z \,\square_A\, y$

In this section, we are defining a demonic version of the usual operators of KAD. Knowing that $x^* = \mu_{\leq}(y :: y \cdot x + 1)$ (see Remark 2.2), the demonic version of the Kleene star ought to be $x^{\times_A} = \mu_{\sqsubseteq_A}(y :: y \,\square_A\, x \sqcup_A 1)$. This is the object of the following definition, lemma and proposition.

Definition 2.14 (Demonic iteration operator)**.** *Let $\mathcal{K}$ be a KAD and take $x \in K$. The* demonic iteration operator $^{\times_A}$ *is defined by* $x^{\times_A} = x^* \,\square_A\, \ulcorner x$.

Lemma 2.15. *Let $\mathcal{K}$ be a KAD and take $x \in K$. Then*

$$\ulcorner(x^{\times_A}) = x^* \rightarrow \ulcorner x \ .$$

Proof :

$$\begin{array}{ll} & \ulcorner(x^{\times_A}) \\ = & \qquad \langle \text{ by Definition 2.14 } \rangle \\ & \ulcorner(x^* \sqsubset_A \ulcorner x) \\ = & \qquad \langle \text{ by Proposition 2.13-4 } \rangle \\ & (x^* \rightarrow \ulcorner x) \cdot \ulcorner(x^*) \\ = & \qquad \langle \text{ by Proposition 2.7-16 and Boolean algebra } \rangle \\ & x^* \rightarrow \ulcorner x \end{array}$$

□

Proposition 2.16. *Let $\mathcal{K}$ be a KAD and take $x, y, z \in K$.*

1. $x^{\times_A} = x^{\times_A} \sqsubset_A x \sqcup_A 1$
2. $x \sqsubset_A z \sqsubseteq_A z \implies x^{\times_A} \sqsubset_A z \sqsubseteq_A z$
3. $z \sqsubset_A x \sqsubseteq_A z \implies z \sqsubset_A x^{\times_A} \sqsubseteq_A z$
4. $x \sqsubset_A z \sqcup_A y \sqsubseteq_A z \implies x^{\times_A} \sqsubset_A y \sqsubseteq_A z$
5. $z \sqsubset_A x \sqcup_A y \sqsubseteq_A z \implies y \sqsubset_A x^{\times_A} \sqsubseteq_A z$

Proof :

1. $$\begin{array}{ll} & x^{\times_A} \sqsubset_A x \sqcup_A 1 \\ = & \qquad \langle \text{ by Definition 2.14 and Proposition 2.13-1 } \rangle \\ & x^* \sqsubset_A (\ulcorner x \sqsubset_A x) \sqcup_A 1 \\ = & \qquad \langle \text{ by Propositions 2.13-2 and 2.7-6 } \rangle \\ & x^* \sqsubset_A x \sqcup_A 1 \end{array}$$

$$
\begin{array}{ll}
= & \langle \text{ by Propositions 2.10 and 2.7-10, and (2.7) } \rangle \\
& \ulcorner(x^* \mathbin{\square_A} x) \cdot (x^* \mathbin{\square_A} x + 1) \\
= & \langle \text{ by Proposition 2.13-4 and Definition 2.12 } \rangle \\
& (x^* \to x) \cdot \ulcorner(x^*) \cdot ((x^* \to x) \cdot x^* \cdot x + 1) \\
= & \langle \text{ by Proposition 2.7-16 and (2.7) } \rangle \\
& (x^* \to x) \cdot ((x^* \to x) \cdot x^* \cdot x + 1) \\
= & \langle \text{ by (2.8) and Boolean algebra } \rangle \\
& (x^* \to x) \cdot (x^* \cdot x + 1) \\
= & \langle \text{ by (2.10) } \rangle \\
& (x^* \to x) \cdot x^* \\
= & \langle \text{ by Propositions 2.13-6 and 2.7-6 } \rangle \\
& (x^* \to x) \cdot x^* \cdot \ulcorner x \\
= & \langle \text{ by Definitions 2.12 and 2.14 } \rangle \\
& x^{\times_A}
\end{array}
$$

2.

$$
\begin{array}{ll}
& x^{\times_A} \mathbin{\square_A} z \mathbin{\sqsubseteq_A} z \\
\iff & \langle \text{ by Definition 2.14 and Proposition 2.13-1 } \rangle \\
& x^* \mathbin{\square} (\ulcorner x \mathbin{\square_A} z) \mathbin{\sqsubseteq_A} z \\
\iff & \langle \text{ by Proposition 2.13-2 } \rangle \\
& x^* \mathbin{\square_A} (\ulcorner x \cdot z) \mathbin{\sqsubseteq_A} z \\
\iff & \langle \text{ by Definition 2.9 } \rangle \\
& \ulcorner z \le \ulcorner(x^* \mathbin{\square_A} (\ulcorner x \cdot z)) \ \wedge \ \ulcorner z \cdot (x^* \mathbin{\square_A} (\ulcorner x \cdot z)) \le z \\
\iff & \langle \text{ by Proposition 2.13-4 and Definition 2.12 } \rangle \\
& \ulcorner z \le (x^* \to (\ulcorner x \cdot z)) \cdot \ulcorner(x^*) \ \wedge \ \ulcorner z \cdot (x^* \to (\ulcorner x \cdot z)) \cdot x^* \cdot \ulcorner x \cdot z \le z \\
\iff & \langle \text{ by Proposition 2.7-16 and (2.7) } \rangle \\
& \ulcorner z \le x^* \to (\ulcorner x \cdot z) \ \wedge \ \ulcorner z \cdot (x^* \to (\ulcorner x \cdot z)) \cdot x^* \cdot \ulcorner x \cdot z \le z \\
\iff & \langle \text{ by Boolean algebra } \rangle \\
& \ulcorner z \le x^* \to (\ulcorner x \cdot z) \ \wedge \ \ulcorner z \cdot x^* \cdot \ulcorner x \cdot z \le z \\
\impliedby & \langle \text{ by Proposition 2.7-6, Boolean algebra and since } \ulcorner z \le \ulcorner x, \\
& \quad z = \ulcorner z \cdot z = \ulcorner x \cdot \ulcorner z \cdot z = \ulcorner x \cdot z \ \rangle \\
& \ulcorner z \le \ulcorner x \ \wedge \ \ulcorner z \le x^* \to z \ \wedge \ \ulcorner z \cdot x^* \cdot z \le z \\
\iff & \langle \text{ by Proposition 2.13-5, (2.8) and Boolean algebra } \rangle
\end{array}
$$

$$\begin{array}{ll}
& \ulcorner z \le \ulcorner x \ \wedge\ \ulcorner z \le x^* \cdot \ulcorner z \ \wedge\ \ulcorner z \cdot (\ulcorner z \cdot x + \neg \ulcorner z \cdot x)^* \cdot z \le z \\
\iff & \quad \langle \text{ by Propositions 2.13-8 and 2.7-1 } \rangle \\
& \ulcorner z \le \ulcorner x \ \wedge\ \ulcorner z \le x \cdot \ulcorner z \ \wedge\ \ulcorner z \cdot ((\ulcorner z \cdot x)^* \cdot \neg \ulcorner z \cdot x)^* \cdot (\ulcorner z \cdot x)^* \cdot z \le z \\
\iff & \quad \langle \text{ by Boolean algebra, Propositions 2.13-4 and 2.13-6,} \\
& \quad \text{and since } \ulcorner z \le x \cdot \ulcorner z, \\
& \quad \ulcorner z \cdot x = \ulcorner z \cdot (x \cdot \ulcorner z) \cdot x = \ulcorner z \cdot (x \cdot \ulcorner z) \cdot x \cdot \ulcorner z = \ulcorner z \cdot x \cdot \ulcorner z \ \rangle \\
& \ulcorner z \le \ulcorner x \ \wedge\ \ulcorner z \le x \cdot \ulcorner z \ \wedge\ \ulcorner z \cdot ((\ulcorner z \cdot x \cdot \ulcorner z)^* \cdot \neg \ulcorner z \cdot x)^* \cdot (\ulcorner z \cdot x)^* \cdot z \le z \\
\iff & \quad \langle \text{ by (2.10) } \rangle \\
& \ulcorner z \le \ulcorner x \ \wedge\ \ulcorner z \le x \cdot \ulcorner z \ \wedge \\
& \ulcorner z \cdot \Big(((\ulcorner z \cdot x \cdot \ulcorner z)^* \cdot \ulcorner z \cdot x \cdot \ulcorner z + 1) \cdot \neg \ulcorner z \cdot x\Big)^* \cdot (\ulcorner z \cdot x)^* \cdot z \le z \\
\iff & \quad \langle \text{ by (2.9), (2.4) and Boolean algebra } \rangle \\
& \ulcorner z \le \ulcorner x \ \wedge\ \ulcorner z \le x \cdot \ulcorner z \ \wedge\ \ulcorner z \cdot (\neg \ulcorner z \cdot x)^* \cdot (\ulcorner z \cdot x)^* \cdot z \le z \\
\iff & \quad \langle \text{ by Proposition 2.13-5 and (2.14) } \rangle \\
& \ulcorner z \le \ulcorner x \ \wedge\ \ulcorner z \le x \cdot z \ \wedge\ \ulcorner z \cdot (\neg \ulcorner z \cdot x \cdot (\neg \ulcorner z \cdot x)^* + 1) \cdot (\ulcorner z \cdot x)^* \cdot z \le z \\
\iff & \quad \langle \text{ by (2.8), (2.4), (2.7) and Boolean algebra } \rangle \\
& \ulcorner z \le \ulcorner x \ \wedge\ \ulcorner z \le x \cdot z \ \wedge\ \ulcorner z \cdot (\ulcorner z \cdot x)^* \cdot z \le z \\
\impliedby & \quad \langle \text{ by Proposition 2.7-6,} \\
& \quad (\ulcorner z \cdot x)^* \cdot z \le z \implies \ulcorner z \cdot (\ulcorner z \cdot x)^* \cdot z \le z \ \rangle \\
& \ulcorner z \le \ulcorner x \ \wedge\ \ulcorner z \le x \cdot z \ \wedge\ (\ulcorner z \cdot x)^* \cdot z \le z \\
\impliedby & \quad \langle \text{ by (2.15) } \rangle \\
& \ulcorner z \le \ulcorner x \ \wedge\ \ulcorner z \le x \cdot z \ \wedge\ \ulcorner z \cdot x \cdot z \le z \\
\iff & \quad \langle \text{ by Boolean algebra } \rangle \\
& \ulcorner z \le (x \cdot z) \cdot \ulcorner x \ \wedge\ \ulcorner z \cdot (x \cdot z) \cdot x \cdot z \le z \\
\iff & \quad \langle \text{ by Proposition 2.13-4 and Definition 2.12 } \rangle \\
& \ulcorner z \le \ulcorner (x \mathbin{\square_A} z) \ \wedge\ \ulcorner z \cdot (x \mathbin{\square_A} z) \le z \\
\iff & \quad \langle \text{ by Definition 2.9 } \rangle \\
& x \mathbin{\square_A} z \mathbin{\sqsubseteq_A} z
\end{array}$$

3.
$$\begin{array}{ll}
& z \mathbin{\square_A} x \mathbin{\sqsubseteq_A} z \\
\iff & \quad \langle \text{ by Definition 2.9 } \rangle \\
& \ulcorner z \le \ulcorner (z \mathbin{\square_A} x) \ \wedge\ \ulcorner z \cdot (z \mathbin{\square_A} x) \le z \\
\iff & \quad \langle \text{ by Proposition 2.13-4 and Definition 2.12 } \rangle \\
& \ulcorner z \le (z \cdot x) \cdot \ulcorner z \ \wedge\ \ulcorner z \cdot (z \cdot x) \cdot z \cdot x \le z
\end{array}$$

$$
\begin{array}{ll}
\iff & \langle \text{ by Boolean algebra and Proposition 2.7-6 } \rangle \\
\quad \lceil z \leq (z \rightarrow x) \cdot \lceil z \ \wedge \ z \cdot x \leq z & \\
\implies & \langle \text{ by Proposition 2.13-5 and (2.16) } \rangle \\
\quad \lceil z \leq (z \rightarrow \lceil x) \cdot \lceil z \ \wedge \ z \cdot x^* \leq z &
\end{array}
$$

This derivation thus gives

$$\lceil z \ \leq \ (z \rightarrow \lceil x) \cdot \lceil z \ , \tag{2.20}$$

$$z \cdot x^* \ \leq \ z \ . \tag{2.21}$$

$$
\begin{array}{ll}
& \lceil z \\
\leq & \langle \text{ by (2.20) } \rangle \\
& (z \rightarrow \lceil x) \cdot \lceil z \\
\leq & \langle \text{ by (2.21) and Proposition 2.13-9 } \rangle \\
& ((z \cdot x^*) \rightarrow \lceil x) \cdot \lceil z \\
= & \langle \text{ by Proposition 2.13-7 } \rangle \\
& (z \rightarrow (x^* \rightarrow \lceil x)) \cdot \lceil z \\
= & \langle \text{ by Proposition 2.7-16 and (2.7) } \rangle \\
& (z \rightarrow ((x^* \rightarrow \lceil x) \cdot \lceil (x^*))) \cdot \lceil z \\
= & \langle \text{ by Propositions 2.13-4 and 2.13-5 } \rangle \\
& (z \rightarrow (x^* \ \square_A \lceil x)) \cdot \lceil z \\
= & \langle \text{ by Proposition 2.13-4 } \rangle \\
& \lceil (z \ \square_A \ (x^* \ \square_A \lceil x)) \\
= & \langle \text{ by Definition 2.14 } \rangle \\
& \lceil (z \ \square_A \ x^{\times_A})
\end{array}
$$

The following inequality is also needed.

$$
\begin{array}{ll}
& \lceil z \cdot (z \ \square_A \ x^{\times_A}) \\
= & \langle \text{ by Definition 2.14 } \rangle \\
& \lceil z \cdot (z \ \square_A \ (x^* \ \square_A \lceil x)) \\
\leq & \langle \text{ Proposition 2.12-11 } \rangle \\
& \lceil z \cdot z \cdot (x^* \ \square_A \lceil x) \\
\leq & \langle \text{ Proposition 2.12-11 } \rangle
\end{array}
$$

$$
\begin{array}{ll}
& \ulcorner z \cdot z \cdot x^* \cdot \ulcorner x \\
\leq & \qquad \langle \text{ by (2.21) and because } \ulcorner z \leq 1 \text{ and } \ulcorner x \leq 1 \ \rangle \\
& z
\end{array}
$$

The result then follows from Definition 2.9.

4. Suppose $x \mathbin{\triangleright_A} z \uplus_A y \sqsubseteq_A z$. Then $y \sqsubseteq_A z$ and $x \mathbin{\triangleright_A} z \sqsubseteq_A z$ by Proposition 2.10. Then Part 2 of the present proposition gives $x^{\times_A} \mathbin{\triangleright_A} z \sqsubseteq_A z$. This is used in the following derivation.

$$
\begin{array}{ll}
& x^{\times_A} \mathbin{\triangleright_A} y \\
\sqsubseteq_A & \qquad \langle \text{ by the hypothesis and Proposition 2.13-13,} \\
& \quad y \sqsubseteq_A x \mathbin{\triangleright_A} z \uplus_A y \sqsubseteq_A z \ \rangle \\
& x^{\times_A} \mathbin{\triangleright_A} z \\
\sqsubseteq_A & \qquad \langle \text{ derived above from the hypothesis } \rangle \\
& z
\end{array}
$$

5. The proof is similar to the previous one. □

Based on the partial order $\sqsubseteq_A$, one can focus on tests and calculate the demonic meet of tests.

Definition 2.17 (Demonic meet of tests)**.** *Let $\mathcal{K}$ be a KAD. For each $s, t \in \mathsf{test}(K)$, define*

$$s \sqcap_A t = s + t \ .$$

Remark 2.11 together with Proposition 2.10 confirm that the operator $\sqcap_A$ really is the demonic meet of tests with respect to $\sqsubseteq_A$. We now define, for any test t, the t-conditional operator $\sqcap_{At}$ that generalises the demonic meet of tests to any elements of a KAD. Since the demonic meet of x and y does not exist in general[2], $x \sqcap_{At} y$ is not the demonic meet of x and y, but rather the demonic meet of $t \mathbin{\triangleright_A} x$ and $\neg t \mathbin{\triangleright_A} y$.

Definition 2.18 (t-conditional operator)**.** *Let $\mathcal{K}$ be a KAD. For each $x, y \in K$ and $t \in \mathsf{test}(K)$, the* t-conditional operator *is defined by $x \sqcap_{At} y = t \cdot x + \neg t \cdot y$. The family of t-conditional operators corresponds to a single ternary operator $\sqcap_{A\bullet}$ taking as arguments a test t and two arbitrary elements x and y.*

[2]Indeed, look at $\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$ in Figure 2.3.

The following proposition says that the t-conditionnal operator does generalise the demonic meet of tests and that it calculates the demonic meet of $t \rhd_A x$ and $\neg t \rhd y$ for any test t.

Proposition 2.19. *Let $\mathcal{K}$ be a KAD. The following properties hold for all $x, y \in K$ and all $s, t \in \mathsf{test}(K)$.*

1. $1 \barwedge_{A_s} t = s \barwedge_A t$
2. *The demonic meet of $t \rhd_A x$ and $\neg t \rhd_A y$ with respect to $\sqsubseteq_A$ exists and it is equal to $x \barwedge_{A_t} y$.*

Proof :

1. $$\begin{aligned} & 1 \barwedge_{A_s} t \\ = & \quad \langle \text{ by Definition 2.18 } \rangle \\ & s \cdot 1 + \neg s \cdot t \\ = & \quad \langle \text{ by Boolean algebra } \rangle \\ & s + t \\ = & \quad \langle \text{ by Definition 2.17 } \rangle \\ & s \barwedge_A t \end{aligned}$$

2. We have to show that $x \barwedge_{A_t} y \sqsubseteq_A t \rhd_A x$, $x \barwedge_{A_t} y \sqsubseteq_A \neg t \rhd_A y$ and that $x \barwedge_{A_t} y$ is the greatest element with these two properties.

$$\begin{aligned} & z \sqsubseteq_A t \rhd_A x \ \wedge \ z \sqsubseteq_A \neg t \rhd_A y \\ \iff & \quad \langle \text{ by Proposition 2.10 } \rangle \\ & z \sqcup_A t \rhd_A x = t \rhd_A x \ \wedge \ z \sqcup_A \neg t \rhd_A y = \neg t \rhd_A y \\ \iff & \quad \langle \text{ by Proposition 2.13-2 } \rangle \\ & z \sqcup_A t \cdot x = t \cdot x \ \wedge \ z \sqcup_A \neg t \cdot y = \neg t \cdot y \\ \iff & \quad \langle \text{ by Proposition 2.10 } \rangle \\ & \lceil z \cdot \lceil (t \cdot x) \cdot (z + t \cdot x) = t \cdot x \ \wedge \ \lceil z \cdot \lceil (\neg t \cdot y) \cdot (z + \neg t \cdot y) = \neg t \cdot y \\ \iff & \quad \langle \text{ by (2.8), Boolean algebra and Proposition 2.7-6 } \rangle \\ & \lceil (t \cdot x) \cdot z + \lceil z \cdot t \cdot x = t \cdot x \ \wedge \ \lceil (\neg t \cdot y) \cdot z + \lceil z \cdot \neg t \cdot y = \neg t \cdot y \\ \iff & \quad \langle \text{ by (2.8), Propositions 2.7-11 and 2.7-10, Boolean algebra, (2.6) and (2.4) } \rangle \end{aligned}$$

$$
\begin{array}{ll}
& \lceil(t \cdot x) \cdot z + \lceil(\neg t \cdot y) \cdot z + \lceil z \cdot t \cdot x + \lceil z \cdot \neg t \cdot y = t \cdot x + \neg t \cdot y \\
\iff & \quad \langle \text{ by (2.8) and (2.9) } \rangle \\
& (\lceil(t \cdot x) + \lceil(\neg t \cdot y)) \cdot z + \lceil z \cdot (t \cdot x + \neg t \cdot y) = t \cdot x + \neg t \cdot y \\
\iff & \quad \langle \text{ by Proposition 2.7-13 } \rangle \\
& \lceil(t \cdot x + \neg t \cdot y) \cdot z + \lceil z \cdot (t \cdot x + \neg t \cdot y) = t \cdot x + \neg t \cdot y \\
\iff & \quad \langle \text{ by Definition 2.18 } \rangle \\
& \lceil(x \mathbin{⊓_{At}} y) \cdot z + \lceil z \cdot (x \mathbin{⊓_{At}} y) = x \mathbin{⊓_{At}} y \\
\iff & \quad \langle \text{ by Proposition 2.7-6, Boolean algebra and (2.8) } \rangle \\
& \lceil z \cdot \lceil(x \mathbin{⊓_{At}} y) \cdot (z + (x \mathbin{⊓_{At}} y)) = x \mathbin{⊓_{At}} y \\
\iff & \quad \langle \text{ by Proposition 2.10 } \rangle \\
& z \mathbin{⊑_A} x \mathbin{⊓_{At}} y
\end{array}
$$

We derived

$$z \mathbin{⊑_A} t \mathbin{▫_A} x \ \wedge\ z \mathbin{⊑_A} \neg t \mathbin{▫_A} y \iff z \mathbin{⊑_A} x \mathbin{⊓_{At}} y \ . \tag{2.22}$$

Taking $z = x \mathbin{⊓_{At}} y$ in (2.22), we see that $x \mathbin{⊓_{At}} y$ is a lower bound of $t \mathbin{▫_A} x$ and $\neg t \mathbin{▫_A} y$. Then (2.22) says that $x \mathbin{⊓_{At}} y$ is the greatest lower bound of $t \mathbin{▫_A} x$ and $\neg t \mathbin{▫_A} y$. □

The demonic join operator $⊔_A$ is used to give the semantics of demonic non-deterministic choices and $▫_A$ is used for sequences. Among the interesting properties of $▫_A$, we cite $t \mathbin{▫_A} x = t \cdot x$ (Proposition 2.13-2), which says that composing a test t with an arbitrary element x is the same in the angelic and demonic worlds, and $x \mathbin{▫_A} y = x \cdot y$ if $\lceil y = 1$ (Proposition 2.13-3), which says that if the second element of a composition is total, then again the angelic and demonic compositions coincide. The ternary operator $⊓_{A\bullet}$ is similar to the *conditional choice operator* $\_ \triangleleft \_ \triangleright \_$ of Hoare et al. [HHJ+87, HJ98]. It corresponds to a guarded choice with disjoint alternatives. The demonic iteration operator $^{\times_A}$ rejects the finite computations that go through a state from which it is possible to reach a state where no computation is defined (e.g., due to blocking or abnormal termination).

2.5 A Framework for Demonic Algebra with Domain and t-Conditional Within KAD

We now present four theorems about the demonic operators introduced in the previous section. Theorem 2.20 contains laws relating $\sqcup_A$, $\sqsubset_A$ and ${}^{\times_A}$. Theorem 2.21 concerns the Boolean lattice of demonic tests. Theorem 2.22 is about the relationship between $\sqcup_A$, $\sqsubset_A$, ${}^{\times_A}$ and $\ulcorner$. And Theorem 2.21 concerns the t-conditional operator $\sqcap_{At}$.

These theorems are the best witnesses of what might be an algebraic structure that has the upper part of the lattice of Figure 1.4 as its intended model. Consequently, their laws will be taken as axioms of *demonic algebra with domain and* $\sqcap_{A\bullet}$ (DAD-$\sqcap_{A\bullet}$) in Chapter 3.

As usual, unary operators have the highest precedence, and demonic composition $\sqsubset_A$ binds stronger than $\sqcup_A$ and $\sqcap_{A\bullet}$, which have the same precedence.

Theorem 2.20. *Let $\mathcal{K}$ be a KAD. The following properties hold for all $x, y, z \in K$, so $(K, \sqcup_A, \sqsubset_A, {}^{\times_A}, 0, 1)$ is a demonic algebra (see Definition 3.1).*

1. $x \sqcup_A (y \sqcup_A z) = (x \sqcup_A y) \sqcup_A z$
2. $x \sqcup_A y = y \sqcup_A x$
3. $x \sqcup_A x = x$
4. $0 \sqcup_A x = 0$
5. $x \sqsubset_A (y \sqsubset_A z) = (x \sqsubset_A y) \sqsubset_A z$
6. $0 \sqsubset_A x = x \sqsubset_A 0 = 0$
7. $1 \sqsubset_A x = x \sqsubset_A 1 = x$
8. $x \sqsubset_A (y \sqcup_A z) = x \sqsubset_A y \sqcup_A x \sqsubset_A z$
9. $(x \sqcup_A y) \sqsubset_A z = x \sqsubset_A z \sqcup_A y \sqsubset_A z$
10. $x^{\times_A} = x^{\times_A} \sqsubset_A x \sqcup_A 1$
11. $x \sqsubseteq_A y \iff x \sqcup_A y = y$
12. $z \sqsubset_A x \sqcup_A y \sqsubseteq_A z \implies y \sqsubset_A x^{\times_A} \sqsubseteq_A z$
13. $x \sqsubset_A z \sqcup_A y \sqsubseteq_A z \implies x^{\times_A} \sqsubset_A y \sqsubseteq_A z$

PROOF : See [DMT06] for the proof of 1 to 9 and 11. Refer to Proposition 2.16 for the proof of 10, 12 and 13. □

Theorem 2.21. *Let $\mathcal{K}$ be a KAD. Then $(\mathsf{test}(K), \sqcup_A, \sqcap_A, \neg, 1, 0)$ is a Boolean algebra, so $(K, \mathsf{test}(K), \sqcup_A, \diamond_A, {}^{\times_A}, 0, 1, \neg, \sqcap_A)$ is a demonic algebra with tests (see Definition 3.4).*

PROOF : The fact that $(\mathsf{test}(K), \sqcup_A, \sqcap_A, \neg, 1, 0)$ is a Boolean algebra is a direct consequence of Proposition 2.10 and Definition 2.17. Therefore, $(K, \mathsf{test}(K), \sqcup_A, \diamond_A, {}^{\times_A}, 0, 1, \neg, \sqcap_A)$ is a demonic algebra with tests by Theorem 2.20. □

Theorem 2.21 together with Remark 2.11 show that the Boolean lattice of tests in the demonic world is the same as in the angelic world, but reversed. Therefore, in any relational model, the demonic tests are the subidentities.

Theorem 2.22. *Let $\mathcal{K}$ be a KAD. The following properties hold for all $x, y \in K$ and all $t \in \mathsf{test}(K)$, so $(K, \mathsf{test}(K), \sqcup_A, \diamond_A, {}^{\times_A}, 0, 1, \neg, \sqcap_A, \ulcorner)$ is a demonic algebra with domain (see Definition 3.8).*

1. $\ulcorner(x \diamond_A t) \diamond_A x = x \diamond_A t$
2. $\ulcorner(x \diamond_A y) = \ulcorner(x \diamond_A \ulcorner y)$
3. $\ulcorner(x \sqcup_A y) = \ulcorner x \sqcup_A \ulcorner y$
4. $\ulcorner(x \diamond_A t) \sqsubseteq_A t \implies \ulcorner(x^{\times_A} \diamond_A t) \sqsubseteq_A t$

PROOF :

1.
$$\begin{aligned} & \ulcorner(x \diamond_A t) \diamond_A x \\ = & \quad \langle \text{ by Propositions 2.13-2, 2.13-4 and 2.7-6 } \rangle \\ & (x \rightarrow t) \cdot x \\ = & \quad \langle \text{ by Propositions 2.13-6 and 2.7-10 } \rangle \\ & (x \rightarrow t) \cdot x \cdot t \\ = & \quad \langle \text{ by Definition 2.12 } \rangle \\ & x \diamond_A t \end{aligned}$$

2.
$$\begin{aligned} & \ulcorner(x \diamond_A y) \\ = & \quad \langle \text{ by Proposition 2.13-4 } \rangle \end{aligned}$$

$$
\begin{array}{ll}
& (x \rightarrow y) \cdot \ulcorner x \\
= & \quad \langle \text{ by Proposition 2.13-5 } \rangle \\
& (x \rightarrow \ulcorner y) \cdot \ulcorner x \\
= & \quad \langle \text{ by Proposition 2.13-4 } \rangle \\
& \ulcorner(x \,\square_A\, \ulcorner y)
\end{array}
$$

3.
$$
\begin{array}{ll}
& \ulcorner(x \sqcup_A y) \\
= & \quad \langle \text{ by Proposition 2.10 } \rangle \\
& \ulcorner x \cdot \ulcorner y \\
= & \quad \langle \text{ by Boolean algebra } \rangle \\
& \ulcorner x \cdot \ulcorner y \cdot (\ulcorner x + \ulcorner y) \\
= & \quad \langle \text{ by Propositions 2.10 and 2.7-10 } \rangle \\
& \ulcorner x \sqcup_A \ulcorner y
\end{array}
$$

4.
$$
\begin{array}{ll}
& \ulcorner(x \,\square_A\, t) \sqsubseteq_A t \\
\Longleftrightarrow & \quad \langle \text{ by Remark 2.11 and Proposition 2.13-4 } \rangle \\
& t \leq (x \rightarrow t) \cdot \ulcorner x \\
\Longleftrightarrow & \quad \langle \text{ by Boolean algebra } \rangle \\
& t \leq x \rightarrow t \;\wedge\; t \leq \ulcorner x \\
\Longrightarrow & \quad \langle \text{ by Proposition 2.13-8 } \rangle \\
& t \leq x^* \rightarrow t \;\wedge\; t \leq \ulcorner x \\
\Longrightarrow & \quad \langle \text{ by Proposition 2.13-10 } \rangle \\
& t \leq x^* \rightarrow t \;\wedge\; t \leq x^* \rightarrow \ulcorner x
\end{array}
$$

These two inequalities will be used.

$$t \leq x^* \rightarrow t \tag{2.23}$$
$$t \leq x^* \rightarrow \ulcorner x \tag{2.24}$$

$$
\begin{array}{ll}
& \ulcorner(x^{\times_A} \,\square_A\, t) \sqsubseteq_A t \\
\Longleftrightarrow & \quad \langle \text{ by Remark 2.11 and Proposition 2.13-4 } \rangle \\
& t \leq (x^{\times_A} \rightarrow t) \cdot \ulcorner(x^{\times_A}) \\
\Longleftrightarrow & \quad \langle \text{ by Boolean algebra } \rangle \\
& t \leq x^{\times_A} \rightarrow t \;\wedge\; t \leq \ulcorner(x^{\times_A}) \\
\Longleftrightarrow & \quad \langle \text{ by Definition 2.14 } \rangle
\end{array}
$$

$$
\begin{array}{ll}
& t \leq (x^* \mathbin{\rhd_A} \lceil x) \to t \ \wedge \ t \leq \lceil (x^* \mathbin{\rhd_A} \lceil x) \\
\iff & \quad \langle \text{ by Definition 2.12, Propositions 2.13-4 and 2.7-16, and (2.7) } \rangle \\
& t \leq ((x^* \to \lceil x) \cdot x^* \cdot \lceil x) \to t \ \wedge \ t \leq x^* \to \lceil x \\
\iff & \quad \langle \text{ by (2.24) } \rangle \\
& t \leq ((x^* \to \lceil x) \cdot x^* \cdot \lceil x) \to t \\
\impliedby & \quad \langle \text{ by Proposition 2.13-9 } \rangle \\
& t \leq x^* \to t \\
\iff & \quad \langle \text{ by (2.23) } \rangle \\
& \mathsf{true}
\end{array}
$$

Therefore, $(K, \mathsf{test}(K), \sqcup_A, \rhd_A, {}^{\times_A}, 0, 1, \neg, \sqcap_A, \lceil\ )$ is a demonic algebra with domain by Theorem 2.21. □

Theorem 2.23. *Let $\mathcal{K}$ be a KAD. Then*

$$x \sqcap_{A_t} y = z \iff t \mathbin{\rhd_A} x = t \mathbin{\rhd_A} z \wedge \neg t \mathbin{\rhd_A} y = \neg t \mathbin{\rhd_A} z$$

for all $x, y, z \in K$ and all $t \in \mathsf{test}(K)$, so $(K, \mathsf{test}(K), \sqcup_A, \rhd_A, {}^{\times_A}, 0, 1, \neg, \sqcap_A, \lceil, \sqcap_{A\bullet})$ is a demonic algebra with domain and t-conditional (see Definition 3.18).

Proof :

$$
\begin{array}{ll}
& x \sqcap_{A_t} y = z \\
\iff & \quad \langle \text{ by Definition 2.18 } \rangle \\
& t \cdot x + \neg t \cdot y = z \\
\iff & \quad \langle \text{ by Proposition 2.7-3 } \rangle \\
& t \cdot (t \cdot x + \neg t \cdot y) = t \cdot z \ \wedge \ \neg t \cdot (t \cdot x + \neg t \cdot y) = \neg t \cdot z \\
\iff & \quad \langle \text{ by (2.8), Boolean algebra, (2.6) and (2.4) } \rangle \\
& t \cdot x = t \cdot z \ \wedge \ \neg t \cdot y = \neg t \cdot z \\
\iff & \quad \langle \text{ by Proposition 2.13-2 } \rangle \\
& t \mathbin{\rhd_A} x = t \mathbin{\rhd_A} z \ \wedge \ \neg t \mathbin{\rhd_A} y = \neg t \mathbin{\rhd_A} z
\end{array}
$$

Therefore, $(K, \mathsf{test}(K), \sqcup_A, \rhd_A, {}^{\times_A}, 0, 1, \neg, \sqcap_A, \lceil, \sqcap_{A\bullet})$ is a demonic algebra with domain and t-conditional by Theorem 2.22. □

Chapter 3

Axiomatisation of Demonic Algebra with Domain and t-Conditional

In the previous chapter, we demonstrated that the demonic operators introduced in Section 2.4 satisfy Theorems 2.20, 2.21, 2.22 and 2.23. Since we want to know how do KADs with the demonic operators but without the usual angelic ones behave, these laws will become axioms for a new algebraic structure called *demonic algebra with domain and t-conditional* (DAD-⍰). Therefore, it is easy to see that any model of KAD can be transformed into a DAD-⍰ by taking the elements of the KAD and the demonic operators defined in Section 2.4, and then forgetting the angelic operators.

We expect DAD-⍰ to be an algebraic foundation for the upper part of the lattice of Figure 1.4. Also, we want to define algebraic transformations between the lower part and the upper part of this lattice. This last goal guided our choice of laws for the theorems of Section 2.5 and hence, our choice of axioms for Definitions 3.1, 3.4, 3.8 and 3.18.

In the presentation of the next definitions, we follow the same path as for the definition of KAD. That is, we first define *demonic algebra* (DA) (Section 3.1), then *demonic algebra with tests* (DAT) (Section 3.2) and *demonic algebra with domain* (DAD) (Section 3.3). Finally, and it is a difference between DA and KA, we need an extra operator, so we define *demonic algebra with domain and t-conditional* (DAD-⍰) (Section 3.4). The reasons why we need this operator will be discussed in Section 3.4.

3.1 Demonic Algebra

In this section, we present *demonic algebra* (DA), we discuss some of its axioms and we look at a first proposition about this structure.

Like KA, DA has a sum, a composition and an iteration operator. Moreover, its sum induces a partial order.

Definition 3.1 (Demonic algebra)**.** *A* demonic algebra *(DA) is a structure* $\mathcal{A} = (A, \sqcup, \boxdot, ^\times, \top, 1)$ *such that the following properties are satisfied for all* $x, y, z \in A$*.*

$$x \sqcup (y \sqcup z) = (x \sqcup y) \sqcup z \tag{3.1}$$
$$x \sqcup y = y \sqcup x \tag{3.2}$$
$$x \sqcup x = x \tag{3.3}$$
$$\top \sqcup x = \top \tag{3.4}$$
$$x \boxdot (y \boxdot z) = (x \boxdot y) \boxdot z \tag{3.5}$$
$$\top \boxdot x = x \boxdot \top = \top \tag{3.6}$$
$$1 \boxdot x = x \boxdot 1 = x \tag{3.7}$$
$$x \boxdot (y \sqcup z) = x \boxdot y \sqcup x \boxdot z \tag{3.8}$$
$$(x \sqcup y) \boxdot z = x \boxdot z \sqcup y \boxdot z \tag{3.9}$$
$$x^\times = x^\times \boxdot x \sqcup 1 \tag{3.10}$$

There is a partial order $\sqsubseteq$ *induced by* $\sqcup$ *such that for all* $x, y \in A$*,*

$$x \sqsubseteq y \iff x \sqcup y = y \ . \tag{3.11}$$

The next two properties are also satisfied for all $x, y, z \in A$*.*

$$x \boxdot z \sqcup y \sqsubseteq z \implies x^\times \boxdot y \sqsubseteq z \tag{3.12}$$
$$z \boxdot x \sqcup y \sqsubseteq z \implies y \boxdot x^\times \sqsubseteq z \tag{3.13}$$

When comparing Definitions 2.1 and 3.1, one observes the obvious correspondences $+ \leftrightarrow \sqcup, \cdot \leftrightarrow \boxdot, ^* \leftrightarrow ^\times, 0 \leftrightarrow \top, 1 \leftrightarrow 1$. The only difference in the axiomatisation between KA and DA is that 0 is the left and right identity of addition in KA ($+$), while $\top$ is a left and right zero of addition in DA ($\sqcup$). However, this minor difference has a rather important impact. While KAs and DAs are upper semilattices with $+$ as the join operator for KAs and $\sqcup$ for DAs, the element 0 is the bottom of the semilattice for KAs and $\top$ is the top of the semilattice for DAs. Indeed, by (3.4) and (3.11),

$$x \sqsubseteq \top \tag{3.14}$$

for all $x \in A$.

The following obvious refinements will be used in what follows.

$$x \sqsubseteq x \sqcup y \;\wedge\; y \sqsubseteq x \sqcup y \tag{3.15}$$

They hold by (3.11), (3.2) and (3.3).

All operators are monotonic with respect to the refinement ordering $\sqsubseteq$. That is, for all $x, y, z \in A$,

$$x \sqsubseteq y \implies z \sqcup x \sqsubseteq z \sqcup y \wedge z \mathbin{\triangledown} x \sqsubseteq z \mathbin{\triangledown} y \wedge x \mathbin{\triangledown} z \sqsubseteq y \mathbin{\triangledown} z \wedge x^\times \sqsubseteq y^\times \;.$$

Monotonicity of $\sqcup$ and $\triangledown$ can easily be derived from (3.11), (3.8) and (3.9). That of $^\times$ is shown from (3.10) and (3.13) as follows:

$$x \sqsubseteq y \implies y^\times \mathbin{\triangledown} x \sqcup 1 \sqsubseteq y^\times \mathbin{\triangledown} y \sqcup 1 \iff y^\times \mathbin{\triangledown} x \sqcup 1 \sqsubseteq y^\times \implies x^\times \sqsubseteq y^\times \;.$$

Most of the time, this property will be used without explicit mention.

Remark 3.2. Like for the corresponding unfolding law (2.14) in KA, the following symmetric version of (3.10),

$$x^\times = x \mathbin{\triangledown} x^\times \sqcup 1 \;, \tag{3.16}$$

is derivable from these axioms. Indeed,

$$\begin{array}{ll}
& x^\times \sqsubseteq x \mathbin{\triangledown} x^\times \sqcup 1 \\
\Longleftarrow & \quad \langle \text{ by (3.12) and (3.7) } \rangle \\
& x \mathbin{\triangledown} (x \mathbin{\triangledown} x^\times \sqcup 1) \sqcup 1 \sqsubseteq x \mathbin{\triangledown} x^\times \sqcup 1 \\
\Longleftarrow & \quad \langle \text{ by monotonicity of } \triangledown \text{ and } \sqcup \rangle \\
& x \mathbin{\triangledown} x^\times \sqcup 1 \sqsubseteq x^\times \qquad \text{—this is the other inequality we have to show} \\
\Longleftrightarrow & \quad \langle \text{ by (3.10) } \rangle \\
& x \mathbin{\triangledown} x^\times \sqcup 1 \sqsubseteq x^\times \mathbin{\triangledown} x \sqcup 1 \\
\Longleftarrow & \quad \langle \text{ by monotonicity of } \sqcup \rangle \\
& x \mathbin{\triangledown} x^\times \sqsubseteq x^\times \mathbin{\triangledown} x \\
\Longleftarrow & \quad \langle \text{ by (3.13) } \rangle \\
& x^\times \mathbin{\triangledown} x \mathbin{\triangledown} x \sqcup x \sqsubseteq x^\times \mathbin{\triangledown} x \\
\Longleftrightarrow & \quad \langle \text{ by (3.10), (3.9) and (3.7) } \rangle \\
& \mathsf{true} \;.
\end{array}$$

Also, one can show $x^\times = \mu_{\sqsubseteq}(y :: y \circ x \sqcup 1)$ with (3.7), (3.10) and (3.13), and $x^\times = \mu_{\sqsubseteq}(y :: x \circ y \sqcup 1)$ with (3.7), (3.16) and (3.12).

Finally, in the presence of the other axioms, (3.12) and (3.13) are equivalent to the following two.

$$x \circ z \sqsubseteq z \implies x^\times \circ z \sqsubseteq z \tag{3.17}$$

$$z \circ x \sqsubseteq z \implies z \circ x^\times \sqsubseteq z \tag{3.18}$$

The following proposition presents properties of the iteration operator $^\times$. They might be thought of as the demonic version of properties of the Kleene star *.

Proposition 3.3. *Let $\mathcal{A}$ be a DA. The following laws hold for all $x, y \in A$.*

1. $1 \sqsubseteq x^\times$, $x^\times \circ x \sqsubseteq x^\times$ *and* $x \circ x^\times \sqsubseteq x^\times$
2. $x \sqsubseteq x^\times$
3. $x \circ y \sqsubseteq y \circ x \implies x^\times \circ y \sqsubseteq y \circ x^\times$
4. $y \circ x \sqsubseteq x \circ y \implies y \circ x^\times \sqsubseteq x^\times \circ y$
5. $x^\times \circ x^\times = x^\times$
6. $(x^\times)^\times = x^\times$
7. $x \circ (y \circ x)^\times = (x \circ y)^\times \circ x$
8. $(x \sqcup y)^\times = x^\times \circ (y \circ x^\times)^\times = (x^\times \circ y)^\times \circ x^\times$

Proof :

1. This is direct from (3.10), (3.16) and (3.15).
2. This follows from (3.7) and Proposition 3.3-1. Indeed $x = 1 \circ x \sqsubseteq x^\times \circ x \sqsubseteq x^\times$.
3. Assume $x \circ y \sqsubseteq y \circ x$.

$$\begin{array}{ll} & x^\times \circ y \sqsubseteq y \circ x^\times \\ \Longleftarrow & \quad \langle \text{ by (3.12) } \rangle \\ & x \circ y \circ x^\times \sqcup y \sqsubseteq y \circ x^\times \end{array}$$

$\Longleftarrow$ ⟨ by the hypothesis ⟩

$y \circ x \circ x^{\times} \sqcup y \sqsubseteq y \circ x^{\times}$

$\Longleftrightarrow$ ⟨ by (3.7), (3.8) and (3.16) ⟩

true

4. Assume $y \circ x \sqsubseteq x \circ y$.

$y \circ x^{\times} \sqsubseteq x^{\times} \circ y$

$\Longleftarrow$ ⟨ by (3.13) ⟩

$x^{\times} \circ y \circ x \sqcup y \sqsubseteq x^{\times} \circ y$

$\Longleftarrow$ ⟨ by the hypothesis ⟩

$x^{\times} \circ x \circ y \sqcup y \sqsubseteq x^{\times} \circ y$

$\Longleftrightarrow$ ⟨ by (3.7), (3.9) and (3.10) ⟩

true

5. $x^{\times} \circ x^{\times}$

$\sqsubseteq$ ⟨ by Proposition 3.3-1 and (3.17) ⟩

$x^{\times}$

$\sqsubseteq$ ⟨ by Proposition 3.3-1 ⟩

$x^{\times} \circ x^{\times}$

6. We first derive $(x^{\times})^{\times} \sqsubseteq x^{\times}$.

$(x^{\times})^{\times} \sqsubseteq x^{\times}$

$\Longleftarrow$ ⟨ by (3.12) and (3.7) ⟩

$x^{\times} \circ x^{\times} \sqcup 1 \sqsubseteq x^{\times}$

$\Longleftrightarrow$ ⟨ by Propositions 3.3-1 and 3.3-5 ⟩

true

By Proposition 3.3-2, $x^{\times} \sqsubseteq (x^{\times})^{\times}$.

7. We first derive $x \circ (y \circ x)^{\times} \sqsubseteq (x \circ y)^{\times} \circ x$.

$x \circ (y \circ x)^{\times} \sqsubseteq (x \circ y)^{\times} \circ x$

$\Longleftarrow$ ⟨ by (3.13) ⟩

$$
\begin{array}{ll}
& (x \mathbin{\triangleright} y)^{\times} \mathbin{\triangleright} x \mathbin{\triangleright} y \mathbin{\triangleright} x \sqcup x \sqsubseteq (x \mathbin{\triangleright} y)^{\times} \mathbin{\triangleright} x \\
\iff & \quad \langle \text{ by Proposition 3.3-1, (3.9) and (3.7) } \rangle \\
& \mathsf{true}.
\end{array}
$$

The derivation of $(x \mathbin{\triangleright} y)^{\times} \mathbin{\triangleright} x \sqsubseteq x \mathbin{\triangleright} (y \mathbin{\triangleright} x)^{\times}$ is similar, using (3.12).

8. We first derive $(x \sqcup y)^{\times} \sqsubseteq x^{\times} \mathbin{\triangleright} (y \mathbin{\triangleright} x^{\times})^{\times}$.

$$
\begin{array}{ll}
& (x \sqcup y)^{\times} \sqsubseteq x^{\times} \mathbin{\triangleright} (y \mathbin{\triangleright} x^{\times})^{\times} \\
\impliedby & \quad \langle \text{ by (3.12) and (3.7) } \rangle \\
& (x \sqcup y) \mathbin{\triangleright} x^{\times} \mathbin{\triangleright} (y \mathbin{\triangleright} x^{\times})^{\times} \sqcup 1 \sqsubseteq x^{\times} \mathbin{\triangleright} (y \mathbin{\triangleright} x^{\times})^{\times} \\
\iff & \quad \langle \text{ by Proposition 3.3-1, (3.7) and (3.9) } \rangle \\
& x \mathbin{\triangleright} x^{\times} \mathbin{\triangleright} (y \mathbin{\triangleright} x^{\times})^{\times} \sqcup y \mathbin{\triangleright} x^{\times} \mathbin{\triangleright} (y \mathbin{\triangleright} x^{\times})^{\times} \sqsubseteq x^{\times} \mathbin{\triangleright} (y \mathbin{\triangleright} x^{\times})^{\times} \\
\impliedby & \quad \langle \text{ by Proposition 3.3-1 and (3.16) } \rangle \\
& (y \mathbin{\triangleright} x^{\times})^{\times} \sqsubseteq x^{\times} \mathbin{\triangleright} (y \mathbin{\triangleright} x^{\times})^{\times} \\
\iff & \quad \langle \text{ by Proposition 3.3-1 and (3.7) } \rangle \\
& \mathsf{true}.
\end{array}
$$

And here is the derivation of $x^{\times} \mathbin{\triangleright} (y \mathbin{\triangleright} x^{\times})^{\times} \sqsubseteq (x \sqcup y)^{\times}$.

$$
\begin{array}{ll}
& \mathsf{true} \\
\iff & \quad \langle \text{ by (3.15) and Proposition 3.3-2 } \rangle \\
& y \sqsubseteq (x \sqcup y)^{\times} \ \wedge \ x^{\times} \sqsubseteq (x \sqcup y)^{\times} \\
\implies & \quad \langle \text{ by Propositions 3.3-5 and 3.3-6 } \rangle \\
& (y \mathbin{\triangleright} x^{\times})^{\times} \sqsubseteq (x \sqcup y)^{\times} \ \wedge \ x^{\times} \sqsubseteq (x \sqcup y)^{\times} \\
\implies & \quad \langle \text{ by Proposition 3.3-5 } \rangle \\
& x^{\times} \mathbin{\triangleright} (y \mathbin{\triangleright} x^{\times})^{\times} \sqsubseteq (x \sqcup y)^{\times}
\end{array}
$$

The proof of $(x \sqcup y)^{\times} = (x^{\times} \mathbin{\triangleright} y)^{\times} \mathbin{\triangleright} x^{\times}$ is similar. □

3.2 Demonic Algebra with Tests

Now comes the first extension of DA, *demonic algebra with tests* (DAT). This extension has a concept of Boolean algebra of tests like the one in KAT and it also adds the ⊓

operator. Introducing $\sqcap$ provides a way to express the meet of tests, as will be shown below. In KAT, $+$ and $\cdot$ are respectively the join and meet operators of the Boolean lattice of tests. But in Section 3.3, it will turn out that for any tests s and t, $s \sqcup t = s \triangledown t$, so that $\sqcup$ and $\triangledown$ both act as the join operator on tests (this is also the case for the KAD-based definition of these operators given in Section 2.4, as can be checked).

In this section, we also discuss the implications of the definition of DAT and we present a simple lemma related to demonic tests.

Here is how we deal with tests in a demonic world.

Definition 3.4 (Demonic algebra with tests)**.** *A* demonic algebra with tests *(DAT) is a structure* $\mathcal{A} = (A, \mathsf{test}(A), \sqcup, \triangledown, ^\times, \top, 1, \neg, \sqcap)$ *such that* $\{1, \top\} \subseteq \mathsf{test}(A) \subseteq A$, $(A, \sqcup, \triangledown, ^\times, \top, 1)$ *is a DA and* $(\mathsf{test}(A), \sqcup, \sqcap, \neg, 1, \top)$ *is a Boolean algebra. The elements in* $\mathsf{test}(A)$ *are called (demonic) tests. The operator* $\sqcap$ *stands for the infimum of elements in* $\mathsf{test}(A)$ *with respect to* $\sqsubseteq$*.*

Note that 1 and $\top$ are respectively the bottom and the top of the Boolean lattice of tests. We insist that the operators $\sqcap$ and $\neg$ are defined exclusively on $\mathsf{test}(A)$. In the sequel, we use the letters w, x, y, z for arbitrary elements of DA and s, t, u, v for demonic tests.

A basic property of *demonic algebra with domain* (DAD) (see Section 3.3) is that $s \triangledown t = s \sqcup t$ (see Proposition 3.14-3). Therefore, in DAD, $s \triangledown \neg s = s \sqcup \neg s = \top$ and $\neg 1 = \top$. This is why we are going to say that two tests s and t are *disjoint* when $s \triangledown t = s \sqcup t = \top$. The following example presents a situation where this does not stand in DAT. It was constructed using Mace4 [Mac].

Example 3.5. For this example, $A = \mathsf{test}(A) = \{\top, \mathsf{s}, \mathsf{t}, 1\}$. The demonic operators are defined by the following tables.

$\sqcup$	$\top$	s	t	1
$\top$	$\top$	$\top$	$\top$	$\top$
s	$\top$	s	$\top$	s
t	$\top$	$\top$	t	t
1	$\top$	s	t	1

$\triangledown$	$\top$	s	t	1
$\top$	$\top$	$\top$	$\top$	$\top$
s	$\top$	$\top$	$\top$	s
t	$\top$	$\top$	$\top$	t
1	$\top$	s	t	1

	$^\times$
$\top$	$\top$
s	$\top$
t	$\top$
1	1

	$\neg$
$\top$	1
s	t
t	s
1	$\top$

$\sqcap$	$\top$	s	t	1
$\top$	$\top$	s	t	1
s	s	s	1	1
t	t	1	t	1
1	1	1	1	1

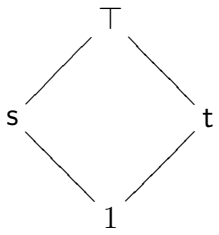


Figure 3.1: Hasse diagram of Example 3.5.

The demonic refinement ordering corresponding to $\sqcup$ is represented in the semilattice of Figure 3.1. It turns out that the present algebra is a DAT where $s \mathbin{▫} t = s \sqcup t$ does not hold. Indeed, $\mathsf{s} \sqcup \mathsf{s} = \mathsf{s} \neq \top = \mathsf{s} \mathbin{▫} \mathsf{s}$. Note that $s \mathbin{▫} (t \sqcap u) = s \mathbin{▫} t \sqcap s \mathbin{▫} u$ does not hold either. Indeed, $\mathsf{s} \mathbin{▫} (\mathsf{s} \sqcap \mathsf{t}) = \mathsf{s} \neq \top = \mathsf{s} \mathbin{▫} \mathsf{s} \sqcap \mathsf{s} \mathbin{▫} \mathsf{t}$.

Definition 3.4 does not even tell whether $\mathsf{test}(A)$ is closed under $▫$. It is not the case, as can be seen in the following example (also constructed by Mace4 [Mac]).

Example 3.6. For this example, $A = \{\top, \mathsf{s}, \mathsf{t}, 1, \mathsf{a}\}$ and $\mathsf{test}(A) = \{\top, \mathsf{s}, \mathsf{t}, 1\}$. The demonic operators are defined by the following tables.

$\sqcup$	$\top$	s	t	1	a
$\top$	$\top$	$\top$	$\top$	$\top$	$\top$
s	$\top$	s	$\top$	s	a
t	$\top$	$\top$	t	t	$\top$
1	$\top$	s	t	1	a
a	$\top$	a	$\top$	a	a

$▫$	$\top$	s	t	1	a
$\top$	$\top$	$\top$	$\top$	$\top$	$\top$
s	$\top$	a	$\top$	s	$\top$
t	$\top$	$\top$	$\top$	t	$\top$
1	$\top$	s	t	1	a
a	$\top$	$\top$	$\top$	a	$\top$

	$^\times$
$\top$	$\top$
s	$\top$
t	$\top$
1	1
a	$\top$

	$\neg$
$\top$	1
s	t
t	s
1	$\top$

$\sqcap$	$\top$	s	t	1
$\top$	$\top$	s	t	1
s	s	s	1	1
t	t	1	t	1
1	1	1	1	1

The demonic refinement ordering corresponding to $\sqcup$ is represented in the semilattice of Figure 3.2. In that DAT, $\mathsf{test}(A)$ is not closed under $▫$. Indeed, $\mathsf{s} \mathbin{▫} \mathsf{s} = \mathsf{a} \notin \mathsf{test}(A)$.

The axioms provided by demonic algebra with domain (see Section 3.3) will bring light to these questions. But before leaving this section, let us introduce the following lemma.

Lemma 3.7. *Let $\mathcal{A}$ be a DAT. The following refinements hold for all $x \in A$ and all $s, t \in \mathsf{test}(A)$.*

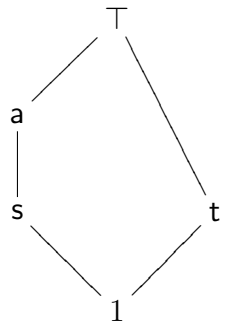


Figure 3.2: Hasse diagram of Example 3.6.

1. $x \sqsubseteq t \triangleright x \ \wedge \ x \sqsubseteq x \triangleright t$
2. $s \sqcup t \sqsubseteq s \triangleright t$
3. $t \triangleright \neg t = \neg t \triangleright t = \top$
4. $1 \sqsubseteq s \triangleright t$
5. $t \triangleright x \sqsubseteq x \implies \top \sqsubseteq \neg t \triangleright x$
6. $t \sqsubseteq x^{\times} \triangleright t$ *and* $t \sqsubseteq t \triangleright x^{\times}$

Proof :

1. true
   $\iff$ ⟨ by Boolean algebra ⟩
   $1 \sqsubseteq t$
   $\implies$ ⟨ by (3.7) ⟩
   $x \sqsubseteq t \triangleright x$

   The proof of the second refinement is similar.
2. By Lemma 3.7-1, $s \sqsubseteq s \triangleright t$ and $t \sqsubseteq s \triangleright t$. So $s \sqcup t \sqsubseteq s \triangleright t$ by (3.3).
3. $\top$
   $=$ ⟨ by Boolean algebra ⟩
   $t \sqcup \neg t$
   $\sqsubseteq$ ⟨ by Lemma 3.7-2 ⟩
   $t \triangleright \neg t$

   So $t \triangleright \neg t = \top$ by (3.14). The proof of the second equality is similar.

4. By Boolean algebra, $1 \sqsubseteq s$ and $1 \sqsubseteq t$. So $1 \sqsubseteq s \circ t$ by (3.7).

5. $$\begin{array}{ll} & t \circ x \sqsubseteq x \\ \Longrightarrow & \langle\ \rangle \\ & \neg t \circ t \circ x \sqsubseteq \neg t \circ x \\ \Longleftrightarrow & \langle \text{ by Lemma 3.7-3 } \rangle \\ & \top \circ x \sqsubseteq \neg t \circ x \\ \Longleftrightarrow & \langle \text{ by (3.6) } \rangle \\ & \top \sqsubseteq \neg t \circ x \end{array}$$

6. By Proposition 3.3-1, $t = 1 \circ t \sqsubseteq x^\times \circ t$ and $t = t \circ 1 \sqsubseteq t \circ x^\times$. □

3.3 Demonic Algebra with Domain

Still following KAD's footsteps, the next extension consists in adding a *domain operator* to DAT to obtain the *demonic algebra with domain* (DAD). In this section, we also demonstrate that axioms of DAD are independent, we present an important proposition about the domain operator (Proposition 3.14) and we demonstrate a technical lemma that is going to simplify many derivations in subsequent chapters.

In the demonic world, we denote the domain operator by the symbol $\Box$.

Definition 3.8 (Demonic algebra with domain)**.** *A* demonic algebra with domain *(DAD) is a structure* $\mathcal{A} = (A, \mathsf{test}(A), \sqcup, \circ, ^\times, \top, 1, \neg, \boxminus, \Box)$*, where* $(A, \mathsf{test}(A), \sqcup, \circ, ^\times, \top, 1, \neg, \boxminus)$ *is a DAT, and the domain operator* $\Box : A \to \mathsf{test}(A)$ *satisfies the following properties for all* $x, y \in A$ *and all* $t \in \mathsf{test}(A)$*.*

$$\Box(x \circ t) \circ x = x \circ t \tag{3.19}$$
$$\Box(x \circ y) = \Box(x \circ \Box y) \tag{3.20}$$
$$\Box(x \sqcup y) = \Box x \sqcup \Box y \tag{3.21}$$
$$\Box(x \circ t) \sqsubseteq t \implies \Box(x^\times \circ t) \sqsubseteq t \tag{3.22}$$

Remark 3.9. As noted above, the axiomatisation of DA (respectively DAT) is very similar to that of KA (respectively KAT), so one might expect the resemblance to continue between DAD and KAD. In particular, looking at the angelic version of Definition 3.8, namely Definition 2.4, one might expect to find axioms like $\Box x \circ x \sqsubseteq x$ and $t \sqsubseteq \Box(t \circ x)$. These two properties can be derived from the chosen axioms (see Propositions 3.14-7 and 3.14-10) but (3.19) cannot be derived from them, even when assuming (3.20),

(3.21) and (3.22) (see Example 3.10). Nevertheless (3.19) holds in KAD-based demonic algebras (see Theorem 2.22-1). Since our goal is to come as close as possible to these, we include (3.19) as an axiom.

Examples 3.10, 3.11, 3.12 and 3.13 illustrate the independence of Axioms (3.19), (3.20), (3.21) and (3.22). Except for Example 3.13, which is an infinite one, they were all constructed by Mace4 [Mac].

Example 3.10. For this example, $A = \{\top, \mathsf{s}, \mathsf{t}, 1, \mathsf{a}, \mathsf{b}\}$ and $\mathsf{test}(A) = \{\top, \mathsf{s}, \mathsf{t}, 1\}$. The demonic operators are defined by the following tables.

$\sqcup$	$\top$	s	t	1	a	b
$\top$	$\top$	$\top$	$\top$	$\top$	$\top$	$\top$
s	$\top$	s	$\top$	s	a	b
t	$\top$	$\top$	t	t	$\top$	$\top$
1	$\top$	s	t	1	a	b
a	$\top$	a	$\top$	a	a	b
b	$\top$	b	$\top$	b	b	b

$\circ$	$\top$	s	t	1	a	b
$\top$	$\top$	$\top$	$\top$	$\top$	$\top$	$\top$
s	$\top$	s	$\top$	s	a	b
t	$\top$	$\top$	t	t	$\top$	$\top$
1	$\top$	s	t	1	a	b
a	$\top$	b	$\top$	a	b	b
b	$\top$	b	$\top$	b	b	b

	$^\times$
$\top$	$\top$
s	s
t	t
1	1
a	b
b	b

	$\neg$
$\top$	1
s	t
t	s
1	$\top$

$\sqcap$	$\top$	s	t	1
$\top$	$\top$	s	t	1
s	s	s	1	1
t	t	1	t	1
1	1	1	1	1

	$\lceil$
$\top$	$\top$
s	s
t	t
1	1
a	s
b	s

The demonic refinement ordering corresponding to $\sqcup$ is represented in the semilattice of Figure 3.3. This algebra is a DAT for which $\lceil x \circ x \sqsubseteq x$, $t \sqsubseteq \lceil (t \circ x)$, (3.20), (3.21) and (3.22) all hold, but (3.19) does not. Indeed $\lceil(\mathsf{a} \circ \mathsf{s}) \circ \mathsf{a} = \mathsf{a} \neq \mathsf{b} = \mathsf{a} \circ \mathsf{s}$.

Then why choose (3.19) rather than $\lceil x \circ x \sqsubseteq x$ and $t \sqsubseteq \lceil (t \circ x)$? The justification is twofold. Firstly, as already mentioned in Remark 3.9, models that come from KAD satisfy property (3.19). Secondly, there are strong indications that this law is essential to reach the main goal of this thesis (refer to item 8 of Section 1.3).

Law (3.20) is locality in a demonic world.

In KAD, it is not necessary to have an axiom like (3.21), because additivity of $\lceil$ (Proposition 2.7-13) can be demonstrated from the laws of KAD. However, it is necessary in the context of DA, since the following example satisfies all prescribed laws except that one.

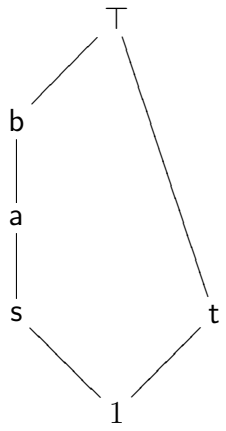


Figure 3.3: Hasse diagram of Example 3.10.

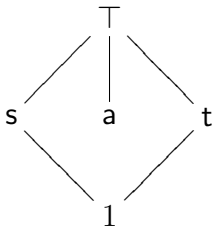


Figure 3.4: Hasse diagram of Example 3.11.

Example 3.11. For this example, $A = \{\top, \mathsf{s}, \mathsf{t}, 1, \mathsf{a}\}$ and $\mathsf{test}(A) = \{\top, \mathsf{s}, \mathsf{t}, 1\}$. The demonic operators are defined by the following tables.

⊔	⊤	s	t	1	a
⊤	⊤	⊤	⊤	⊤	⊤
s	⊤	s	⊤	s	⊤
t	⊤	⊤	t	t	⊤
1	⊤	s	t	1	⊤
a	⊤	⊤	⊤	⊤	a

▫	⊤	s	t	1	a
⊤	⊤	⊤	⊤	⊤	⊤
s	⊤	s	⊤	s	a
t	⊤	⊤	t	t	⊤
1	⊤	s	t	1	a
a	⊤	⊤	⊤	a	⊤

	×
⊤	⊤
s	s
t	t
1	1
a	⊤

	¬
⊤	1
s	t
t	s
1	⊤

⊓	⊤	s	t	1
⊤	⊤	s	t	1
s	s	s	1	1
t	t	1	t	1
1	1	1	1	1

	⊓
⊤	⊤
s	s
t	t
1	1
a	s

The demonic refinement ordering corresponding to ⊔ is represented in the semilattice of Figure 3.4. This algebra is a DAT and, in addition, (3.19), (3.20) and (3.22) are satisfied, but (3.21) is not. Indeed $⌈(1 ⊔ \mathsf{a}) = ⊤ ≠ \mathsf{s} = ⌈1 ⊔ ⌈\mathsf{a}$.

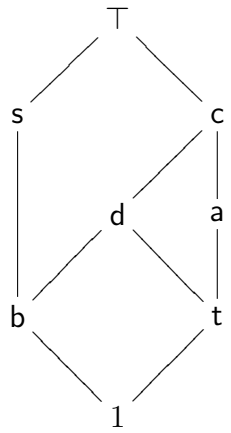


Figure 3.5: Hasse diagram of Example 3.12.

Example 3.12. For this example, $A = \{\top, \mathsf{s}, \mathsf{t}, 1, \mathsf{a}, \mathsf{b}, \mathsf{c}, \mathsf{d}\}$ and $\mathsf{test}(A) = \{\top, \mathsf{s}, \mathsf{t}, 1\}$. The demonic operators are defined by the following tables.

⊔	⊤	s	t	1	a	b	c	d
⊤	⊤	⊤	⊤	⊤	⊤	⊤	⊤	⊤
s	⊤	s	⊤	s	⊤	s	⊤	⊤
t	⊤	⊤	t	t	a	d	c	d
1	⊤	s	t	1	a	b	c	d
a	⊤	⊤	a	a	a	c	c	c
b	⊤	s	d	b	c	b	c	d
c	⊤	⊤	c	c	c	c	c	c
d	⊤	⊤	d	d	c	d	c	d

▫	⊤	s	t	1	a	b	c	d
⊤	⊤	⊤	⊤	⊤	⊤	⊤	⊤	⊤
s	⊤	s	⊤	s	⊤	s	⊤	⊤
t	⊤	⊤	t	t	a	d	c	d
1	⊤	s	t	1	a	b	c	d
a	⊤	⊤	a	a	a	⊤	⊤	⊤
b	⊤	s	⊤	b	⊤	b	⊤	⊤
c	⊤	⊤	⊤	c	⊤	⊤	⊤	⊤
d	⊤	⊤	⊤	d	⊤	d	⊤	⊤

	×
⊤	⊤
s	s
t	t
1	1
a	a
b	b
c	⊤
d	⊤

	¬
⊤	1
s	t
t	s
1	⊤

⊓	⊤	s	t	1
⊤	⊤	s	t	1
s	s	s	1	1
t	t	1	t	1
1	1	1	1	1

	⌜
⊤	⊤
s	s
t	t
1	1
a	t
b	1
c	t
d	t

The demonic refinement ordering corresponding to ⊔ is represented in the semilattice of Figure 3.5. In this DAT, (3.19), (3.21) and (3.22) are satisfied, but (3.20) is not. Indeed $⌜(\mathsf{a} ▫ \mathsf{b}) = \top \neq \mathsf{t} = ⌜(\mathsf{a} ▫ ⌜\mathsf{b})$.

Finally, we add Axiom (3.22) since it is true in KAD-based demonic algebras (see Theorem 2.22-4) and it helps manipulating $^\times$ with $⌜$. Moreover, like Axiom (3.19),

there are strong indications that this law is essential to reach the main goal of this thesis.

Examples 3.10, 3.11 and 3.12 show that Axioms (3.19), (3.20) and (3.21) are independent from each other and also from (3.22). The following example completes the proof of independence of (3.19), (3.20), (3.21) and (3.22).

Example 3.13. For this example, $A = \{E : \wp(\mathbf{N}) \mid E \text{ is finite}\}$ and $\mathsf{test}(A) = \{\{\}, \{0\}\}$. The demonic operators are as follows.

$$\begin{array}{rcl} \sqcup : A \times A & \longrightarrow & A \\ (E, F) & \mapsto & \begin{cases} E \cup F & \text{if } E \neq \{\} \text{ and } F \neq \{\} \\ \{\} & \text{if } E = \{\} \text{ or } F = \{\} \end{cases} \end{array}$$

$$\begin{array}{rcl} \mathbin{\square} : A \times A & \longrightarrow & A \\ (E, F) & \mapsto & \{x : \mathbf{N} \mid (\exists\, e : E, f : F \mid x = e + f)\} \end{array}$$

$$\begin{array}{rcl} {}^{\times} : A & \longrightarrow & A \\ E & \mapsto & \begin{cases} \{0\} & \text{if } E = \{0\} \\ \{\} & \text{if } E \neq \{0\} \end{cases} \end{array}$$

$$\begin{array}{rcl} {}^{\sqcap} : A & \longrightarrow & \mathsf{test}(A) \\ E & \mapsto & \begin{cases} \{0\} & \text{if } E \neq \{\} \\ \{\} & \text{if } E = \{\} \end{cases} \end{array}$$

Hence $\{\}$ is the top of the upper semilattice $(A, \sqsubseteq)$ and $\{0\}$ is neutral for demonic composition. Since the only tests are $\{0\}$ and $\{\}$, the operators $\neg$ and $\sqcap$ are trivially defined. In this DAT, (3.19), (3.20) and (3.21) are satisfied, but (3.22) is not. Indeed,

$$\sqcap(\{1\} \mathbin{\square} \{0\}) \sqsubseteq \{0\} \iff \mathsf{true} \not\Longrightarrow \mathsf{false} \iff \sqcap(\{1\}^{\times} \mathbin{\square} \{0\}) \sqsubseteq \{0\} \ .$$

By Proposition 3.14-7 below, $\sqcap x$ is a *left preserver* of x. By Proposition 3.14-14, it is the greatest left preserver. Similarly, by Proposition 3.14-17, $\neg\sqcap x$ is a *left annihilator* of x. By Proposition 3.14-16, it is the least left annihilator (since Proposition 3.14-16 can be rewritten as $\neg\sqcap x \sqsubseteq t \iff \top \sqsubseteq t \mathbin{\square} x$). Hence, on the left of the equivalence of Proposition 3.14-13, t acts as a left preserver of x and on the right, $\neg t$ acts as a left annihilator.

The axioms of DAD impose important restrictions on demonic tests. It turns out that these restrictions are actually useful properties and they are presented in the following proposition together with properties of $\sqcap$.

Proposition 3.14. *Let $\mathcal{A}$ be a DAD. The following laws hold for all $x, y \in A$ and all $s, t, u \in \mathsf{test}(A)$.*

1. $\lceil t = t$
2. $t \circ t = t$
3. $s \sqcup t = s \circ t$ *and hence* $\mathsf{test}(A)$ *is closed under* $\circ$
4. $s \circ (t \sqcap u) = s \circ t \sqcap s \circ u$ *and* $(s \sqcap t) \circ u = s \circ u \sqcap t \circ u$
5. $s \circ t = t \circ s$
6. $x \sqsubseteq t \circ y \iff t \circ x \sqsubseteq t \circ y$
7. $\lceil x \circ x = x$
8. $x \sqsubseteq y \implies \lceil x \sqsubseteq \lceil y$
9. $\lceil (t \circ x) = t \circ \lceil x$
10. $t \sqsubseteq \lceil (t \circ x)$
11. $x \sqcup y = \lceil x \circ \lceil y \circ (x \sqcup y)$
12. $\lceil (x \circ s) \circ \lceil (x \circ t) = \lceil (x \circ s \circ t)$
13. $t \circ x \sqsubseteq x \iff \top \sqsubseteq \neg t \circ x$
14. $t \sqsubseteq \lceil x \iff t \circ x \sqsubseteq x$
15. $\lceil x = \mathsf{max}_{\sqsubseteq}\{t : \mathsf{test}(A) \mid t \circ x = x\}$
16. $t \sqsubseteq \lceil x \iff \top \sqsubseteq \neg t \circ x$
17. $\neg \lceil x \circ x = \top$
18. $\lceil x \sqsubseteq \lceil (x \circ y)$
19. $\lceil x = \top \iff x = \top$
20. $t \circ (x \sqcup y) = t \circ x \sqcup y \;=\; x \sqcup t \circ y$
21. $\lceil x \circ \lceil y = \top \implies \lceil x \circ y = \lceil y \circ x$
22. $\lceil x = 1 \implies \lceil (x^{\times}) = 1$

Proof :

1. This is direct from (3.19) with $x := 1$ and (3.7).

2. This is direct from (3.19) with $x, t := t, 1$, (3.7) and Proposition 3.14-1.

3. $$\begin{array}{ll} & s \triangleleft t \\ \sqsubseteq & \quad \langle \text{ by (3.15) } \rangle \\ & (s \sqcup t) \triangleleft (s \sqcup t) \\ = & \quad \langle \text{ by Proposition 3.14-2 } \rangle \\ & s \sqcup t \\ \sqsubseteq & \quad \langle \text{ by Lemma 3.7-2 } \rangle \\ & s \triangleleft t \end{array}$$

4. This follows from Proposition 3.14-3 and Boolean algebra.

5. This follows from Proposition 3.14-3 and Boolean algebra.

6. $$\begin{array}{ll} & x \sqsubseteq t \triangleleft y \\ \Longrightarrow & \quad \langle \ \rangle \\ & t \triangleleft x \sqsubseteq t \triangleleft t \triangleleft y \\ \Longleftrightarrow & \quad \langle \text{ by Proposition 3.14-2 } \rangle \\ & t \triangleleft x \sqsubseteq t \triangleleft y \\ \Longrightarrow & \quad \langle \text{ by Lemma 3.7-1 and transitivity of } \sqsubseteq \rangle \\ & x \sqsubseteq t \triangleleft y \end{array}$$

7. This is direct from (3.19) with $t := 1$ and (3.7).

8. $$\begin{array}{ll} & x \sqsubseteq y \\ \Longleftrightarrow & \quad \langle \text{ by (3.11) } \rangle \\ & x \sqcup y = y \\ \Longrightarrow & \quad \langle \text{ by Leibniz and (3.21) } \rangle \\ & \top x \sqcup \top y = \top y \\ \Longleftrightarrow & \quad \langle \text{ by (3.11) } \rangle \\ & \top x \sqsubseteq \top y \end{array}$$

9. $$\begin{array}{ll} & t \triangleleft \top x \\ = & \quad \langle \text{ by Propositions 3.14-3 and 3.14-1 } \rangle \\ & \top (t \triangleleft \top x) \end{array}$$

$$
\begin{array}{ll}
= & \langle \text{ by (3.20) } \rangle \\
& \Gamma(t \triangleright x)
\end{array}
$$

10. By Lemma 3.7-1 and Proposition 3.14-9, $t \sqsubseteq t \triangleright \Gamma x = \Gamma(t \triangleright x)$.

11.
$$
\begin{array}{ll}
& x \sqcup y \\
= & \langle \text{ by Proposition 3.14-7 } \rangle \\
& \Gamma(x \sqcup y) \triangleright (x \sqcup y) \\
= & \langle \text{ by (3.21) } \rangle \\
& (\Gamma x \sqcup \Gamma y) \triangleright (x \sqcup y) \\
= & \langle \text{ by Proposition 3.14-3 } \rangle \\
& \Gamma x \triangleright \Gamma y \triangleright (x \sqcup y)
\end{array}
$$

12.
$$
\begin{array}{ll}
& \Gamma(x \triangleright s) \triangleright \Gamma(x \triangleright t) \\
= & \langle \text{ by Proposition 3.14-3 } \rangle \\
& \Gamma(x \triangleright s) \sqcup \Gamma(x \triangleright t) \\
= & \langle \text{ by (3.21) } \rangle \\
& \Gamma((x \triangleright s) \sqcup (x \triangleright t)) \\
= & \langle \text{ by (3.8) } \rangle \\
& \Gamma(x \triangleright (s \sqcup t)) \\
= & \langle \text{ by Proposition 3.14-3 } \rangle \\
& \Gamma(x \triangleright s \triangleright t)
\end{array}
$$

13.
$$
\begin{array}{ll}
& t \triangleright x \sqsubseteq x \\
\Longrightarrow & \langle \text{ by Lemma 3.7-5 } \rangle \\
& \top \sqsubseteq \neg t \triangleright x \\
\Longrightarrow & \langle \text{ by Proposition 3.14-8 } \rangle \\
& \Gamma\top \sqsubseteq \Gamma(\neg t \triangleright x) \\
\Longleftrightarrow & \langle \text{ by Propositions 3.14-1 and 3.14-9 } \rangle \\
& \top \sqsubseteq \neg t \triangleright \Gamma x \\
\Longrightarrow & \langle \text{ by Boolean algebra } \rangle \\
& t \triangleright \Gamma x \sqsubseteq t \triangleright \Gamma x \sqcap \neg t \triangleright \Gamma x \\
\Longleftrightarrow & \langle \text{ by Proposition 3.14-4, Boolean algebra and (3.7) } \rangle \\
& t \triangleright \Gamma x \sqsubseteq \Gamma x
\end{array}
$$

$\Longrightarrow$ ⟨ by Proposition 3.14-7 ⟩

$t \mathbin{▫} x \sqsubseteq x$

14. [$\Longrightarrow$] By assumption, monotonicity of $▫$ and Proposition 3.14-7, $t \mathbin{▫} x \sqsubseteq {\sqcap}x \mathbin{▫} x = x$.
[$\Longleftarrow$]

$t \mathbin{▫} x \sqsubseteq x$

$\Longrightarrow$ ⟨ by Proposition 3.14-8 ⟩

${\sqcap}(t \mathbin{▫} x) \sqsubseteq {\sqcap}x$

$\Longrightarrow$ ⟨ by Proposition 3.14-10 ⟩

$t \sqsubseteq {\sqcap}x$

15. This is direct from Proposition 3.14-14.

16. This is direct from Propositions 3.14-14 and 3.14-13.

17. This law follows directly from Proposition 3.14-16 and (3.14).

18. Since ${\sqcap}x \mathbin{▫} (x \mathbin{▫} y) = ({\sqcap}x \mathbin{▫} x) \mathbin{▫} y = x \mathbin{▫} y$, the result follows from Proposition 3.14-14.

19. ${\sqcap}x = \top$

$\Longleftrightarrow$ ⟨ by (3.14) ⟩

$\top \sqsubseteq {\sqcap}x$

$\Longleftrightarrow$ ⟨ by Proposition 3.14-14 ⟩

$\top \mathbin{▫} x \sqsubseteq x$

$\Longleftrightarrow$ ⟨ by (3.6) ⟩

$\top \sqsubseteq x$

$\Longleftrightarrow$ ⟨ by (3.14) ⟩

$x = \top$

20. $t \mathbin{▫} x \sqcup y$

$=$ ⟨ by Proposition 3.14-11 ⟩

${\sqcap}(t \mathbin{▫} x) \mathbin{▫} {\sqcap}y \mathbin{▫} (t \mathbin{▫} x \sqcup y)$

$=$ ⟨ by Proposition 3.14-9 ⟩

$t \mathbin{▫} {\sqcap}x \mathbin{▫} {\sqcap}y \mathbin{▫} (t \mathbin{▫} x \sqcup y)$

$=$ ⟨ by Propositions 3.14-5 and 3.14-2, and (3.8) ⟩

$$
\begin{array}{ll}
& t \mathbin{\triangleright} \ulcorner x \mathbin{\triangleright} t \mathbin{\triangleright} \ulcorner y \mathbin{\triangleright} (t \mathbin{\triangleright} x \sqcup t \mathbin{\triangleright} y) \\
= & \quad \langle \text{ by Proposition 3.14-9 } \rangle \\
& \ulcorner (t \mathbin{\triangleright} x) \mathbin{\triangleright} \ulcorner (t \mathbin{\triangleright} y) \mathbin{\triangleright} (t \mathbin{\triangleright} x \sqcup t \mathbin{\triangleright} y) \\
= & \quad \langle \text{ by Proposition 3.14-11 and (3.8) } \rangle \\
& t \mathbin{\triangleright} (x \sqcup y)
\end{array}
$$

The derivation for the second equality is similar.

21.
$$
\begin{array}{ll}
& \ulcorner x \mathbin{\triangleright} \ulcorner y = \top \\
\iff & \quad \langle \text{ by Propositions 3.14-19 and 3.14-9, and Boolean algebra } \rangle \\
& \ulcorner x \mathbin{\triangleright} y = \top \ \wedge \ \ulcorner y \mathbin{\triangleright} x = \top \\
\implies & \quad \langle \ \rangle \\
& \ulcorner x \mathbin{\triangleright} y = \ulcorner y \mathbin{\triangleright} x
\end{array}
$$

22.
$$
\begin{array}{ll}
& \ulcorner x = 1 \\
\iff & \quad \langle \text{ by (3.7) and Boolean algebra } \rangle \\
& \ulcorner (x \mathbin{\triangleright} 1) \sqsubseteq 1 \\
\implies & \quad \langle \text{ by (3.22) } \rangle \\
& \ulcorner (x^{\times} \mathbin{\triangleright} 1) \sqsubseteq 1 \\
\iff & \quad \langle \text{ by (3.7) and Boolean algebra } \rangle \\
& \ulcorner (x^{\times}) = 1
\end{array}
$$

□

All the above laws except 12 are identical to laws of $\ulcorner$, after compensating for the reverse ordering of the Boolean lattice (on tests, $\sqsubseteq$ corresponds to $\geq$).

Although Proposition 3.14-1 is a quite basic property, its proof uses (3.19). Furthermore, Proposition 3.14-1 and (3.19) are used in the proof of Propositions 3.14-2, 3.14-3, 3.14-4, 3.14-5, 3.14-6 and 3.14-7. Since (3.19) is not as natural as the others, it would be interesting to find an argument that only involves (3.20) and (3.21). It turns out that it is not possible. Indeed, see Example 3.15 (also constructed by Mace4 [Mac]).

Example 3.15. For this example, $A = \mathsf{test}(A) = \{\top, \mathsf{s}, \mathsf{t}, 1\}$. The demonic operators

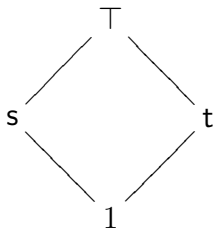


Figure 3.6: Hasse diagram of Example 3.15.

are defined by the following tables.

$\sqcup$	$\top$	s	t	1
$\top$	$\top$	$\top$	$\top$	$\top$
s	$\top$	s	$\top$	s
t	$\top$	$\top$	t	t
1	$\top$	s	t	1

$\circ$	$\top$	s	t	1
$\top$	$\top$	$\top$	$\top$	$\top$
s	$\top$	$\top$	$\top$	s
t	$\top$	$\top$	$\top$	t
1	$\top$	s	t	1

	$^\times$
$\top$	$\top$
s	$\top$
t	$\top$
1	1

	$\neg$
$\top$	1
s	t
t	s
1	$\top$

$\sqcap$	$\top$	s	t	1
$\top$	$\top$	s	t	1
s	s	s	1	1
t	t	1	t	1
1	1	1	1	1

	$\lceil$
$\top$	$\top$
s	$\top$
t	$\top$
1	$\top$

The demonic refinement ordering corresponding to $\sqcup$ is represented in the semilattice of Figure 3.6. This algebra is a DAT and, in addition, (3.20), (3.21) and (3.22) are satisfied, but (3.19) and $\lceil t = t$ are not. Indeed $\lceil(\mathsf{s}\circ 1)\circ\mathsf{s} = \top \neq \mathsf{s} = \mathsf{s}\circ 1$ and $\lceil 1 = \top \neq 1$. Note that Propositions 3.14-2, 3.14-3, 3.14-4, 3.14-6 and 3.14-7 are not satisfied neither.

For those who are wondering, the major difference between Example 3.10 and Example 3.15 is that $\lceil x\circ x \sqsubseteq x$ is satisfied in the former and not in the latter.

The following derivation closes the discussion about the choice of axioms for DAD. Suppose $\lceil x\circ x \sqsubseteq x$ and $t \sqsubseteq \lceil(t\circ x)$ for all $x \in A$ and all $t \in \mathsf{test}(A)$. Then, by Lemma 3.7-1, one has $\lceil t\circ t \sqsubseteq t \sqsubseteq \lceil t\circ t$, so that $\lceil t\circ t = t$. Therefore,

$$
\begin{array}{ll}
 & t \\
\sqsubseteq & \quad \langle \text{ by the hypothesis with } x, t := 1, t \ \rangle \\
 & \lceil t \\
\sqsubseteq & \quad \langle \text{ by Lemma 3.7-1} \ \rangle
\end{array}
$$

$$\begin{array}{ll} & {}^{\sqcap}t{\circ}t \\ = & \qquad \langle \text{ derived above from the hypothesis } \rangle \\ & t \ , \end{array}$$

so ${}^{\sqcap}t = t$.

In conclusion,

$$\begin{array}{rcl} {}^{\sqcap}x{\circ}x \sqsubseteq x \wedge t \sqsubseteq {}^{\sqcap}(t{\circ}x) \wedge (3.20) \wedge (3.21) & \not\Longrightarrow & (3.19) \ , \\ (3.19) \wedge (3.20) \wedge (3.21) & \Longrightarrow & {}^{\sqcap}x{\circ}x \sqsubseteq x \wedge t \sqsubseteq {}^{\sqcap}(t{\circ}x) \ , \\ (3.20) \wedge (3.21) & \not\Longrightarrow & {}^{\sqcap}t = t \ , \\ {}^{\sqcap}x{\circ}x \sqsubseteq x \wedge t \sqsubseteq {}^{\sqcap}(t{\circ}x) \wedge (3.20) \wedge (3.21) & \Longrightarrow & {}^{\sqcap}t = t \ . \end{array}$$

Remark 3.16. Since in any DAD $\mathcal{A}$, $s{\circ}t = s{\sqcup}t$ for all $s, t \in \mathsf{test}(A)$ (see Proposition 3.14-3), the Boolean algebra of demonic tests $\mathsf{test}(A)$ may be viewed as $(\mathsf{test}(A), \sqcup, \sqcap, \neg, 1, \top)$ or as $(\mathsf{test}(A), \circ, \sqcap, \neg, 1, \top)$. Therefore, each time we use a law from Boolean algebra, whether it is written with $\sqcup$ or with $\circ$, we will invoke "Boolean algebra".

We finish this section with a lemma that will mostly be used in Sections 4.4 and 4.5. It is presented here because it is a natural continuation of Proposition 3.14.

Lemma 3.17. *In any DAD $\mathcal{A}$, the domain operator satisfies the following properties for all $x \in A$ and all $s, t \in \mathsf{test}(A)$.*

1. ${}^{\sqcap}x{\circ}{}^{\sqcap}(x{\circ}t) = {}^{\sqcap}(x{\circ}t)$
2. $\neg{}^{\sqcap}x{\circ}{}^{\sqcap}(x{\circ}t) = \top$
3. $\neg{}^{\sqcap}x{\circ}\neg{}^{\sqcap}(x{\circ}t) = \neg{}^{\sqcap}x$
4. ${}^{\sqcap}(x{\circ}t){\circ}{}^{\sqcap}(x{\circ}\neg t) = \top$
5. ${}^{\sqcap}(x{\circ}t){\circ}\neg{}^{\sqcap}(x{\circ}\neg t) = {}^{\sqcap}(x{\circ}t)$ *and hence* $\neg{}^{\sqcap}(x{\circ}\neg t) \sqsubseteq {}^{\sqcap}(x{\circ}t)$
6. ${}^{\sqcap}(x{\circ}(s \sqcap t)) \sqsubseteq {}^{\sqcap}(x{\circ}s)$ *and* ${}^{\sqcap}(x{\circ}(s \sqcap t)) \sqsubseteq {}^{\sqcap}(x{\circ}t)$

Proof :

1. It follows from Propositions 3.14-9 and 3.14-7.

2. It follows from Propositions 3.14-9, 3.14-17, and 3.14-1, and (3.6).

3. $$\begin{array}{ll} & \mathsf{true} \\ \iff & \langle \text{ by Proposition 3.14-18 } \rangle \\ & \ulcorner x \urcorner \sqsubseteq \ulcorner x \circ t \urcorner \\ \iff & \langle \text{ by Boolean algebra and Proposition 3.14-3 } \rangle \\ & \neg \ulcorner x \urcorner \circ \neg \ulcorner x \circ t \urcorner = \neg \ulcorner x \urcorner \end{array}$$

4. It follows from Propositions 3.14-12, and 3.14-1, and (3.6).

5. $$\begin{array}{ll} & \mathsf{true} \\ \iff & \langle \text{ by Lemma 3.17-4 } \rangle \\ & \ulcorner x \circ t \urcorner \circ \ulcorner x \circ \neg t \urcorner = \top \\ \iff & \langle \text{ by Proposition 3.14-3 and Boolean algebra } \rangle \\ & \neg \ulcorner x \circ \neg t \urcorner \sqsubseteq \ulcorner x \circ t \urcorner \\ \iff & \langle \text{ by Boolean algebra and Proposition 3.14-3 } \rangle \\ & \ulcorner x \circ t \urcorner \circ \neg \ulcorner x \circ \neg t \urcorner = \ulcorner x \circ t \urcorner \end{array}$$

6. It follows from Boolean algebra and Proposition 3.14-8. □

3.4 Demonic Algebra with Domain and *t*-Conditional

At this point, we have defined DA, which is an algebraic foundation for the upper part of the lattice of Figure 1.4 and we have extended it to DAT and then to DAD in such a way that we followed the same path as for the definition of KAD. In this section, we define another operator, the *t*-conditional operator $\rightarrow\!\!\!\!\bullet$. We also demonstrate that the definition of the $\rightarrow\!\!\!\!\bullet$ operator is independent from the definition of DAD.

There are two important reasons why we need this extra operator. Now that we have an algebraic foundation for both the lower and the upper part of the lattice of Figure 1.4, we are looking for connections between those parts of the lattice. The upward link from KAD to DAD is well defined thanks to Theorems 2.20, 2.21 and 2.22. The strategy to define a downward link from DAD to KAD could be inspired by the one for the upward link: define angelic operators from DAD and demonstrate that the elements of DAD together with these angelic operators constitute a KAD. But it is

not that easy. It seems impossible to achieve without the $⍈$ operator (the reading of Chapter 4 might convince you).

The other reason why we add an operator to DAD is related to the $⍗$ operator defined on $\mathsf{test}(A)$. Of course, it is essential since it ensures that we have a Boolean algebra of demonic tests, but it is unfortunate that it is exclusively defined on $\mathsf{test}(A)$. Therefore, $⍈$ is an operator defined on A that is introduced as a generalisation of $⍗$. In KAD, the addition of an analogous operator is not necessary since $\cdot$ already corresponds to the meet of tests.

At first sight, this extra operator could complicate things with the upward link established by Theorems 2.20, 2.21 and 2.22. Does the link from KAD to DAD extend to a link from KAD to DAD-$⍈$? Thanks to Theorem 2.23, the answer is yes. And then the downward link we are looking for is from DAD-$⍈$ to KAD.

The axiom for the operator $⍈$ (see (3.23)) was chosen having two things in mind. Firstly, it has to respect $⍗$ when evaluated on demonic tests. Secondly, we want it to behave like a choice operator.

Definition 3.18 (Demonic algebra with domain and t-conditional)**.** *A* demonic algebra with domain and t-conditional *(DAD-$⍈$) is a structure* $\mathcal{A} = (A, \mathsf{test}(A), ⨅, ▫, ^\times, \top, 1, \neg, ⍗, ⍐, ⍈)$*, where* $(A, \mathsf{test}(A), ⨅, ▫, ^\times, \top, 1, \neg, ⍗, ⍐)$ *is a DAD and the* t-conditional operator $⍈$ *is a ternary operator of type* $\mathsf{test}(A) \times A \times A \to A$ *that can be thought of as a family of binary operators. For each* $t \in \mathsf{test}(A)$*,* $⍈_t$ *is an operator of type* $A \times A \to A$*, and of type* $\mathsf{test}(A) \times \mathsf{test}(A) \to \mathsf{test}(A)$ *if its two arguments belong to* $\mathsf{test}(A)$*. It satisfies the following property for all* $x, y, z \in A$ *and all* $t \in \mathsf{test}(A)$*.*

$$x \,⍈_t\, y = z \iff t▫x = t▫z \wedge \neg t▫y = \neg t▫z \tag{3.23}$$

The following example shows that (3.23) is independent from laws of DAD. It was constructed by Mace4 [Mac].

Example 3.19. For this example, $A = \{\top, \mathsf{s}, \mathsf{t}, 1, \mathsf{a}\}$ and $\mathsf{test}(A) = \{\top, \mathsf{s}, \mathsf{t}, 1\}$.

⨅	⊤	s	t	1	a
⊤	⊤	⊤	⊤	⊤	⊤
s	⊤	s	⊤	s	s
t	⊤	⊤	t	t	t
1	⊤	s	t	1	1
a	⊤	s	t	1	a

▫	⊤	s	t	1	a
⊤	⊤	⊤	⊤	⊤	⊤
s	⊤	s	⊤	s	s
t	⊤	⊤	t	t	t
1	⊤	s	t	1	a
a	⊤	s	t	a	a

	$^\times$
⊤	⊤
s	s
t	t
1	1
a	1

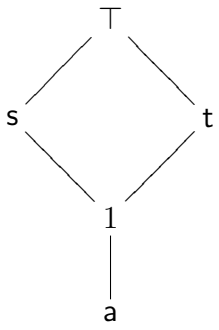


Figure 3.7: Hasse diagram of Example 3.19.

	$\neg$
$\top$	1
s	t
t	s
1	$\top$

$\sqcap$	$\top$	s	t	1
$\top$	$\top$	s	t	1
s	s	s	1	1
t	t	1	t	1
1	1	1	1	1

	$\sqcap$
$\top$	$\top$
s	s
t	t
1	1
a	1

The demonic refinement ordering corresponding to $\sqcup$ is represented in the semilattice of Figure 3.7. This algebra is a DAD, but (3.23) is not satisfied. Indeed,

$$\mathsf{true} \iff \mathsf{s}\circ 1 = \mathsf{s}\circ 1 \wedge \neg\,\mathsf{s}\circ 1 = \neg\,\mathsf{s}\circ 1 \iff 1 \mathbin{⫐_{\mathsf{s}}} 1 = 1$$

and

$$\mathsf{true} \iff \mathsf{s}\circ 1 = \mathsf{s}\circ \mathsf{a} \wedge \neg\,\mathsf{s}\circ 1 = \neg\,\mathsf{s}\circ \mathsf{a} \iff 1 \mathbin{⫐_{\mathsf{s}}} 1 = \mathsf{a}$$

would give $1 = \mathsf{a}$.

We now prove some properties of $⫐_t$.

Proposition 3.20. *Let $\mathcal{A}$ be a DAD-$⫐_\bullet$. The following properties are true for all $x, x_1, x_2, y, y_1, y_2, z \in A$ and all $s, t, u \in \mathsf{test}(A)$.*

1. $t\circ(x \mathbin{⫐_t} y) = t\circ x \;\wedge\; \neg t\circ(x \mathbin{⫐_t} y) = \neg t\circ y$
2. $x \mathbin{⫐_t} y = y \mathbin{⫐_{\neg t}} x$
3. $(t\circ x) \mathbin{⫐_t} y = x \mathbin{⫐_t} y$
4. $x \mathbin{⫐_t} (\neg t\circ y) = x \mathbin{⫐_t} y$
5. $x \mathbin{⫐_t} \top = t\circ x$
6. $\top \mathbin{⫐_t} x = \neg t\circ x$

7. $(x \mathbin{⫪_t} y)\mathbin{▫} z = x\mathbin{▫}z \mathbin{⫪_t} y\mathbin{▫}z$
8. $s\mathbin{▫}(x \mathbin{⫪_t} y) = s\mathbin{▫}x \mathbin{⫪_t} s\mathbin{▫}y$
9. $x \mathbin{⫪_t} (y \sqcup z) = (x \mathbin{⫪_t} y) \sqcup (x \mathbin{⫪_t} z)$
10. $x \sqcup (y \mathbin{⫪_t} z) = (x \sqcup y) \mathbin{⫪_t} (x \sqcup z)$
11. $1 \mathbin{⫪_s} t = s \mathbin{⫪} t$
12. $s \mathbin{⫪_t} u = t\mathbin{▫}s \mathbin{⫪} \neg t\mathbin{▫}u$
13. $x \mathbin{⫪_t} x = x$
14. $x \sqsubseteq y \implies x \mathbin{⫪_t} z \sqsubseteq y \mathbin{⫪_t} z$
15. $x \sqsubseteq y \implies z \mathbin{⫪_t} x \sqsubseteq z \mathbin{⫪_t} y$
16. $x \sqsubseteq y \iff t\mathbin{▫}x \sqsubseteq t\mathbin{▫}y \;\wedge\; \neg t\mathbin{▫}x \sqsubseteq \neg t\mathbin{▫}y$
17. $x = y \iff t\mathbin{▫}x = t\mathbin{▫}y \;\wedge\; \neg t\mathbin{▫}x = \neg t\mathbin{▫}y$
18. $x \sqsubseteq y \mathbin{⫪_t} z \iff x \sqsubseteq t\mathbin{▫}y \;\wedge\; x \sqsubseteq \neg t\mathbin{▫}z$
19. $(x_1 \mathbin{⫪_s} y_1) \mathbin{⫪_t} (x_2 \mathbin{⫪_s} y_2) = (x_1 \mathbin{⫪_t} x_2) \mathbin{⫪_s} (y_1 \mathbin{⫪_t} y_2)$
20. $\lceil(x \mathbin{⫪_t} y) = \lceil x \mathbin{⫪_t} \lceil y$
21. *The demonic meet of* $t\mathbin{▫}x$ *and* $\neg t\mathbin{▫}y$ *with respect to* $\sqsubseteq$ *exists and is equal to* $x \mathbin{⫪_t} y$.

Proof :

1. true
   $\iff$ $\langle\ \rangle$
   $x \mathbin{⫪_t} y = x \mathbin{⫪_t} y$
   $\iff$ $\langle$ by (3.23) $\rangle$
   $t\mathbin{▫}(x \mathbin{⫪_t} y) = t\mathbin{▫}x \;\wedge\; \neg t\mathbin{▫}(x \mathbin{⫪_t} y) = \neg t\mathbin{▫}y$
2. $x \mathbin{⫪_t} y = y \mathbin{⫪_{\neg t}} x$
   $\iff$ $\langle$ by (3.23) $\rangle$
   $t\mathbin{▫}x = t\mathbin{▫}(y \mathbin{⫪_{\neg t}} x) \;\wedge\; \neg t\mathbin{▫}y = \neg t\mathbin{▫}(y \mathbin{⫪_{\neg t}} x)$
   $\iff$ $\langle$ by Boolean algebra $\rangle$

$t▫x = \neg\neg t▫(y \pitchfork_{\neg t} x) \ \wedge \ \neg t▫y = \neg t▫(y \pitchfork_{\neg t} x)$

$\iff$ ⟨ by Proposition 3.20-1 ⟩

$t▫x = \neg\neg t▫x \ \wedge \ \neg t▫y = \neg t▫y$

$\iff$ ⟨ by Boolean algebra ⟩

true

3. $(t▫x) \pitchfork_t y = x \pitchfork_t y$

$\iff$ ⟨ by (3.23) ⟩

$t▫t▫x = t▫(x \pitchfork_t y) \ \wedge \ \neg t▫y = \neg t▫(x \pitchfork_t y)$

$\iff$ ⟨ by Proposition 3.20-1 ⟩

$t▫t▫x = t▫x \ \wedge \ \neg t▫y = \neg t▫y$

$\iff$ ⟨ by Boolean algebra ⟩

true

4. $x \pitchfork_t (\neg t▫y)$

$=$ ⟨ by Proposition 3.20-2 ⟩

$(\neg t▫y) \pitchfork_{\neg t} x$

$=$ ⟨ by Proposition 3.20-3 ⟩

$y \pitchfork_{\neg t} x$

$=$ ⟨ by Proposition 3.20-2 ⟩

$x \pitchfork_t y$

5. $x \pitchfork_t \top = t▫x$

$\iff$ ⟨ by (3.23) ⟩

$t▫x = t▫t▫x \ \wedge \ \neg t▫\top = \neg t▫t▫x$

$\iff$ ⟨ by Boolean algebra ⟩

$t▫x = t▫x \ \wedge \ \top = \top▫x$

$\iff$ ⟨ by (3.6) ⟩

true

6. $\top \pitchfork_t x$

$=$ ⟨ by Proposition 3.20-2 ⟩

$x \pitchfork_{\neg t} \top$

$=$ ⟨ by Proposition 3.20-5 ⟩

$\neg t \sqsubset x$

7. $x \sqsubset z \mathbin{⫐_t} y \sqsubset z = (x \mathbin{⫐_t} y) \sqsubset z$

$\iff$ ⟨ by (3.23) ⟩

$t \sqsubset x \sqsubset z = t \sqsubset (x \mathbin{⫐_t} y) \sqsubset z \ \wedge \ \neg t \sqsubset y \sqsubset z = \neg t \sqsubset (x \mathbin{⫐_t} y) \sqsubset z$

$\iff$ ⟨ by Proposition 3.20-1 ⟩

true

8. $s \sqsubset x \mathbin{⫐_t} s \sqsubset y = s \sqsubset (x \mathbin{⫐_t} y)$

$\iff$ ⟨ by (3.23) ⟩

$t \sqsubset s \sqsubset x = t \sqsubset s \sqsubset (x \mathbin{⫐_t} y) \ \wedge \ \neg t \sqsubset s \sqsubset y = \neg t \sqsubset s \sqsubset (x \mathbin{⫐_t} y)$

$\iff$ ⟨ by Boolean algebra ⟩

$s \sqsubset t \sqsubset x = s \sqsubset t \sqsubset (x \mathbin{⫐_t} y) \ \wedge \ s \sqsubset \neg t \sqsubset y = s \sqsubset \neg t \sqsubset (x \mathbin{⫐_t} y)$

$\iff$ ⟨ by Proposition 3.20-1 ⟩

true

9. $x \mathbin{⫐_t} (y \sqcup z) = (x \mathbin{⫐_t} y) \sqcup (x \mathbin{⫐_t} z)$

$\iff$ ⟨ by (3.23) ⟩

$t \sqsubset x = t \sqsubset ((x \mathbin{⫐_t} y) \sqcup (x \mathbin{⫐_t} z)) \ \wedge \ \neg t \sqsubset (y \sqcup z) = \neg t \sqsubset ((x \mathbin{⫐_t} y) \sqcup (x \mathbin{⫐_t} z))$

$\iff$ ⟨ by (3.8) ⟩

$t \sqsubset x = t \sqsubset (x \mathbin{⫐_t} y) \sqcup t \sqsubset (x \mathbin{⫐_t} z) \ \wedge \ \neg t \sqsubset y \sqcup \neg t \sqsubset z = \neg t \sqsubset (x \mathbin{⫐_t} y) \sqcup \neg t \sqsubset (x \mathbin{⫐_t} z)$

$\iff$ ⟨ by Proposition 3.20-1 and (3.3) ⟩

true

10. $(x \sqcup y) \mathbin{⫐_t} (x \sqcup z) = x \sqcup (y \mathbin{⫐_t} z)$

$\iff$ ⟨ by (3.23) ⟩

$t \sqsubset (x \sqcup y) = t \sqsubset (x \sqcup (y \mathbin{⫐_t} z)) \ \wedge \ \neg t \sqsubset (x \sqcup z) = \neg t \sqsubset (x \sqcup (y \mathbin{⫐_t} z))$

$\iff$ ⟨ by (3.8) ⟩

$t \sqsubset x \sqcup t \sqsubset y = t \sqsubset x \sqcup t \sqsubset (y \mathbin{⫐_t} z) \ \wedge \ \neg t \sqsubset x \sqcup \neg t \sqsubset z = \neg t \sqsubset x \sqcup \neg t \sqsubset (y \mathbin{⫐_t} z)$

$\iff$ ⟨ by Proposition 3.20-1 ⟩

true

11. $1 \mathbin{⫐_s} t = s \mathbin{⫐} t$

$\iff$ ⟨ by (3.23) and Boolean algebra ⟩

$s = s \circ (s \pitchfork t) \ \wedge \ \neg s \circ t = \neg s \circ (s \pitchfork t)$

$\iff$ ⟨ by Boolean algebra ⟩

true

12. $s \pitchfork_t u = t \circ s \pitchfork \neg t \circ u$

$\iff$ ⟨ by (3.23) ⟩

$t \circ s = t \circ (t \circ s \pitchfork \neg t \circ u) \ \wedge \ \neg t \circ u = \neg t \circ (t \circ s \pitchfork \neg t \circ u)$

$\iff$ ⟨ by Boolean algebra ⟩

true

13. This is direct from (3.23).

14. $x \sqsubseteq y$

$\iff$ ⟨ by (3.11) ⟩

$x \sqcup y = y$

$\implies$ ⟨ by Leibniz ⟩

$(x \sqcup y) \pitchfork_t z = y \pitchfork_t z$

$\iff$ ⟨ by Proposition 3.20-2 ⟩

$z \pitchfork_{\neg t} (x \sqcup y) = y \pitchfork_t z$

$\iff$ ⟨ by Proposition 3.20-9 ⟩

$(z \pitchfork_{\neg t} x) \sqcup (z \pitchfork_{\neg t} y) = y \pitchfork_t z$

$\iff$ ⟨ by Proposition 3.20-2 ⟩

$(x \pitchfork_t z) \sqcup (y \pitchfork_t z) = y \pitchfork_t z$

$\iff$ ⟨ by (3.11) ⟩

$x \pitchfork_t z \sqsubseteq y \pitchfork_t z$

15. $x \sqsubseteq y$

$\implies$ ⟨ by Proposition 3.20-14 ⟩

$x \pitchfork_{\neg t} z \sqsubseteq y \pitchfork_{\neg t} z$

$\iff$ ⟨ by Proposition 3.20-2 ⟩

$z \pitchfork_t x \sqsubseteq z \pitchfork_t y$

16. $x \sqsubseteq y$

$\implies$ ⟨ ⟩

$t{\circ}x \sqsubseteq t{\circ}y \ \wedge \ \neg t{\circ}x \sqsubseteq \neg t{\circ}y$

$\Longrightarrow$ ⟨ by Proposition 3.20-14 ⟩

$t{\circ}x \mathbin{⨽}_t \neg t{\circ}x \sqsubseteq t{\circ}y \mathbin{⨽}_t \neg t{\circ}x \ \wedge \ \neg t{\circ}x \mathbin{⨽}_{\neg t} t{\circ}y \sqsubseteq \neg t{\circ}y \mathbin{⨽}_{\neg t} t{\circ}y$

$\Longleftrightarrow$ ⟨ by Proposition 3.20-2 ⟩

$t{\circ}x \mathbin{⨽}_t \neg t{\circ}x \sqsubseteq t{\circ}y \mathbin{⨽}_t \neg t{\circ}x \ \wedge \ t{\circ}y \mathbin{⨽}_t \neg t{\circ}x \sqsubseteq t{\circ}y \mathbin{⨽}_t \neg t{\circ}y$

$\Longrightarrow$ ⟨ by transitivity of $\sqsubseteq$ ⟩

$t{\circ}x \mathbin{⨽}_t \neg t{\circ}x \sqsubseteq t{\circ}y \mathbin{⨽}_t \neg t{\circ}y$

$\Longleftrightarrow$ ⟨ by Propositions 3.20-3 and 3.20-4 ⟩

$x \mathbin{⨽}_t x \sqsubseteq y \mathbin{⨽}_t y$

$\Longleftrightarrow$ ⟨ by Proposition 3.20-13 ⟩

$x \sqsubseteq y$

17. $t{\circ}x = t{\circ}y \ \wedge \ \neg t{\circ}x = \neg t{\circ}y$

$\Longleftrightarrow$ ⟨ by (3.23) ⟩

$x \mathbin{⨽}_t x = y$

$\Longleftrightarrow$ ⟨ by Proposition 3.20-13 ⟩

$x = y$

18. $x \sqsubseteq y \mathbin{⨽}_t z$

$\Longleftrightarrow$ ⟨ by Proposition 3.20-16 ⟩

$t{\circ}x \sqsubseteq t{\circ}(y \mathbin{⨽}_t z) \ \wedge \ \neg t{\circ}x \sqsubseteq \neg t{\circ}(y \mathbin{⨽}_t z)$

$\Longleftrightarrow$ ⟨ by Proposition 3.20-1 ⟩

$t{\circ}x \sqsubseteq t{\circ}y \ \wedge \ \neg t{\circ}x \sqsubseteq \neg t{\circ}z$

$\Longleftrightarrow$ ⟨ by Proposition 3.14-6 ⟩

$x \sqsubseteq t{\circ}y \ \wedge \ x \sqsubseteq \neg t{\circ}z$

19. This is direct from (3.23) and Propositions 3.20-8 and 3.20-1.

20. $\lceil x \mathbin{⨽}_t \lceil y = \lceil(x \mathbin{⨽}_t y)$

$\Longleftrightarrow$ ⟨ by (3.23) ⟩

$t{\circ}\lceil x = t{\circ}\lceil(x \mathbin{⨽}_t y) \ \wedge \ \neg t{\circ}\lceil y = \neg t{\circ}\lceil(x \mathbin{⨽}_t y)$

$\Longleftrightarrow$ ⟨ by Proposition 3.14-9 ⟩

$\lceil(t{\circ}x) = \lceil(t{\circ}(x \mathbin{⨽}_t y)) \ \wedge \ \lceil(\neg t{\circ}y) = \lceil(\neg t{\circ}(x \mathbin{⨽}_t y))$

$\Longleftrightarrow$ ⟨ by Proposition 3.20-1 ⟩

true

21. By Proposition 3.20-18, $x \pitchfork_t y$ is the greatest lower bound of $t \boxdot x$ and $\neg t \boxdot y$. □

If we draw up what we got, tests have quite similar properties in KAT and DAT. But there are important differences as well. The first one is that $\sqcup$ and $\boxdot$ behave the same way on tests (Proposition 3.14-3). The second one concerns Laws 16 and 17 of Proposition 3.20, which show how a proof of refinement or equality can be done by *case analysis* by decomposing it with cases t and $\neg t$. The same is true in KAT. However, in KAT, this decomposition can also be done on the right side, since for instance the law

$$x \leq y \iff x \cdot t \leq y \cdot t \wedge x \cdot \neg t \leq y \cdot \neg t$$

holds (see Proposition 2.7-4), while the corresponding law does not hold in DAT. With the t-conditional operator, there is an asymmetry between left and right that can be traced back to Propositions 3.20-7 and 3.20-8. In Proposition 3.20-7, right distributivity holds for arbitrary elements, while left distributivity in Proposition 3.20-8 holds only for tests.

Propositions 3.20-14 and 3.20-15 simply express the monotonicity of $\pitchfork_t$ in its two arguments. On the other hand, $\pitchfork_\bullet$ is not monotonic with respect to its test argument. Indeed, $\top \pitchfork_1 1 = \top$ and $\top \pitchfork_\top 1 = 1$, so $1 \sqsubseteq \top \not\Longrightarrow \top \pitchfork_1 1 \sqsubseteq \top \pitchfork_\top 1$. Proposition 3.20-11 establishes the link between $\pitchfork_\bullet$ and $\pitchfork$ and makes it clear that the former is a generalisation of the latter. This is a generalisation since it has the same behaviour on demonic tests and it still calculates a meet with respect to $\sqsubseteq$ on other elements. Proposition 3.20-21 tells us that $x \pitchfork_t y$ is the demonic meet of $t \boxdot x$ and $\neg t \boxdot y$.

Note that the axiom for $\pitchfork_t$ (refer to (3.23)) is satisfied by the *conditional choice operator* $\_ \lhd t \rhd \_$ of Hoare et al. [HHJ+87, HJ98]. We list the correspondence between the axioms of DAD-$\pitchfork_\bullet$, the properties of the $\pitchfork_\bullet$ operator and the properties of Hoare et al.'s conditional choice operator in Table 3.1, using the same notation as the authors. The $\pitchfork_\bullet$ operator satisfies a lot of additional laws, as shown by Proposition 3.20. Note that the $\pitchfork_\bullet$ operator and the conditional choice operator of Hoare et al. are also related to the *conditional forms* of McCarthy presented in the precursor paper [McC63].

To simplify the notation when possible, we will use the abbreviation

$$x \pitchfork y = x \pitchfork_{\ulcorner x} y \quad . \tag{3.24}$$

It turns out that it is consistent with the demonic meet on demonic tests. Under special conditions, $\pitchfork$ has easy to use properties, as shown by the next corollary. The most useful cases are when $\pitchfork$ is used on tests and when $\ulcorner x \boxdot \ulcorner y = \top$.

DAD-$\pitchfork_\bullet$	Laws of programming [HHJ+87]	UTP [HJ98]
$x \sqsubseteq y \iff x \sqcup y = y$	$P \subseteq Q \iff P \cup Q = Q$	$[P \Rightarrow Q] \iff [P \sqcap Q = Q]$
$x \sqcup (y \sqcup z) = (x \sqcup y) \sqcup z$	$P \cup (Q \cup R) = (P \cup Q) \cup R$	$P \sqcap (Q \sqcap R) = (P \sqcap Q) \sqcap R$
$x \sqcup y = y \sqcup x$	$P \cup Q = Q \cup P$	$P \sqcap Q = Q \sqcap P$
$x \sqcup x = x$	$P \cup P = P$	$P \sqcap P = P$
$\top \sqcup x = \top$	$\bot \cup P = \bot$	$\mathsf{true} \sqcap P = \mathsf{true}$
$x \circ (y \circ z) = (x \circ y) \circ z$	$P; (Q; R) = (P; Q); R$	$P; (Q; R) = (P; Q); R$
$\top \circ x = x \circ \top = \top$	$\bot; P = P; \bot = \bot$	$\mathsf{true}; P = P; \mathsf{true} = \mathsf{true}$
$1 \circ x = x \circ 1 = x$	$I\!I; P = P; I\!I = P$	$I\!I_{\alpha P}; P = P; I\!I_{\alpha P} = P$
$x \circ (y \sqcup z) = x \circ y \sqcup x \circ z$	$P; (Q \cup R) = (P; Q) \cup (P; R)$	$P; (Q \sqcap R) = (P; Q) \sqcap (P; R)$
$(x \sqcup y) \circ z = x \circ z \sqcup y \circ z$	$(P \cup Q); R = (P; R) \cup (Q; R)$	$(P \sqcap Q); R = (P; R) \sqcap (Q; R)$
$x \pitchfork_t y = y \pitchfork_{\neg t} x$	$P \lhd b \rhd Q = Q \lhd \neg b \rhd P$	$P \lhd b \rhd Q = Q \lhd \neg b \rhd P$
$x \pitchfork_t x = x$	$P \lhd b \rhd P = P$	$P \lhd b \rhd P = P$
$(x \pitchfork_t y) \circ z = x \circ z \pitchfork_t y \circ z$	$(P \lhd b \rhd Q); R = (P; R) \lhd b \rhd (Q; R)$	$(P \lhd b \rhd Q); R = (P; R) \lhd b \rhd (Q; R)$
$x^\times = \mu_{\sqsubseteq}(y :: y \circ x \sqcup 1)$		$\nu R \bullet (P; R \sqcap I\!I_{\alpha(P;R)})$

Table 3.1: Correspondence between the axioms of DAD-$\pitchfork_\bullet$, the properties of the $\pitchfork_\bullet$ operator and the properties of Hoare et al.'s conditional choice operator.

Corollary 3.21. *Let $\mathcal{A}$ be a DAD-$\pitchfork_\bullet$. The following properties are true for all $x, y, z \in A$ and all $s, t, t_1, t_2, ..., t_n, u \in \mathsf{test}(A)$ $(n \geq 2)$.*

1. *$s \pitchfork t$ as defined by (3.24) is equal to the meet of s and t in the Boolean lattice of tests defined in Definition 3.4 (so there is no possible confusion).*
2. $x \pitchfork y = x \pitchfork \neg^{\Pi} x \circ y$
3. $\top \pitchfork x = x \pitchfork \top = x$
4. $t \circ (x \pitchfork y) = t \circ x \pitchfork t \circ y$
5. $(s \pitchfork t) \circ x = s \circ x \pitchfork t \circ x$
6. $x = t \circ x \pitchfork \neg t \circ x$
7. $^{\Pi} x \sqsubseteq t \implies t \circ (x \pitchfork y) = t \circ x$
8. $\neg^{\Pi} x \sqsubseteq t \implies t \circ (x \pitchfork y) = t \circ y$
9. $x \pitchfork_u y = u \circ x \pitchfork \neg u \circ y$
10. $^{\Pi} x \circ y = {}^{\Pi} y \circ x \implies x \pitchfork y = y \pitchfork x$
11. $x \pitchfork x = x$
12. $x \pitchfork y \sqsubseteq x$

13. $(x \pitchfork y) \pitchfork z = x \pitchfork (y \pitchfork z)$

14. $x \sqcup (y \pitchfork z) = (x \sqcup y) \pitchfork (x \sqcup z)$

15. $x \pitchfork (y \sqcup z) = (x \pitchfork y) \sqcup (x \pitchfork z)$

16. $\overline{\Gamma}(x \pitchfork y) = \overline{\Gamma}x \pitchfork \overline{\Gamma}y$

17. $\overline{\Gamma}x \circ \overline{\Gamma}y = \top \implies (x \pitchfork y) \circ z = x \circ z \pitchfork y \circ z$

18. $x \circ z = x \wedge y \circ z = y \implies (x \pitchfork_t y) \circ z = x \pitchfork_t y \wedge (x \pitchfork y) \circ z = x \pitchfork y$

19. If $t_1 \pitchfork t_2 \pitchfork \ldots \pitchfork t_n = 1$ *and* t_1, t_2, ..., t_n *are pairwise disjoint* ($n \geq 2$), *then*

$$x \sqsubseteq y \iff t_1 \circ x \sqsubseteq t_1 \circ y \wedge t_2 \circ x \sqsubseteq t_2 \circ y \wedge \ldots \wedge t_n \circ x \sqsubseteq t_n \circ y \ .$$

Proof :

1. From (3.24), we get

$$\begin{array}{ll} & s \pitchfork t \\ = & \quad \langle \text{ by (3.24) and Proposition 3.14-1 } \rangle \\ & s \pitchfork_s t \\ = & \quad \langle \text{ by Boolean algebra and Proposition 3.20-3 } \rangle \\ & 1 \pitchfork_s t. \end{array}$$

From Definition 3.4, we get

$$\begin{array}{ll} & s \pitchfork t \\ = & \quad \langle \text{ by Proposition 3.20-11 } \rangle \\ & 1 \pitchfork_s t. \end{array}$$

2. $$\begin{array}{ll} & x \pitchfork y = x \pitchfork \neg\overline{\Gamma}x \circ y \\ \iff & \quad \langle \text{ by (3.24) } \rangle \\ & x \pitchfork_{\overline{\Gamma}x} y = x \pitchfork_{\overline{\Gamma}x} \neg\overline{\Gamma}x \circ y \\ \iff & \quad \langle \text{ by Proposition 3.20-4 } \rangle \\ & \mathsf{true} \end{array}$$

3.
$$\begin{array}{ll} & \top \mathbin{⍐} x \\ = & \quad \langle \text{ by (3.24) and Proposition 3.14-1 } \rangle \\ & \top \mathbin{⍐_{\top}} x \\ = & \quad \langle \text{ by Proposition 3.20-6 } \rangle \\ & \neg \top \mathbin{▫} x \\ = & \quad \langle \text{ by Boolean algebra and (3.7) } \rangle \\ & x \\ = & \quad \langle \text{ by Propositions 3.20-5 and 3.14-7 } \rangle \\ & x \mathbin{⍐_{\overline{x}}} \top \\ = & \quad \langle \text{ by (3.24) } \rangle \\ & x \mathbin{⍐} \top \end{array}$$

4.
$$\begin{array}{ll} & t \mathbin{▫} x \mathbin{⍐} t \mathbin{▫} y = t \mathbin{▫} (x \mathbin{⍐} y) \\ \Longleftrightarrow & \quad \langle \text{ by (3.24) } \rangle \\ & t \mathbin{▫} x \mathbin{⍐_{\overline{(t \mathbin{▫} x)}}} t \mathbin{▫} y = t \mathbin{▫} (x \mathbin{⍐_{\overline{x}}} y) \\ \Longleftrightarrow & \quad \langle \text{ by (3.23) } \rangle \\ & \overline{\overline{(t \mathbin{▫} x)}} \mathbin{▫} t \mathbin{▫} x = \overline{\overline{(t \mathbin{▫} x)}} \mathbin{▫} t \mathbin{▫} (x \mathbin{⍐_{\overline{x}}} y) \ \wedge \ \neg \overline{\overline{(t \mathbin{▫} x)}} \mathbin{▫} t \mathbin{▫} y = \neg \overline{\overline{(t \mathbin{▫} x)}} \mathbin{▫} t \mathbin{▫} (x \mathbin{⍐_{\overline{x}}} y) \\ \Longleftrightarrow & \quad \langle \text{ by Propositions 3.14-9 and 3.14-7, and Boolean algebra } \rangle \\ & t \mathbin{▫} x = t \mathbin{▫} \overline{\overline{x}} \mathbin{▫} (x \mathbin{⍐_{\overline{x}}} y) \ \wedge \ t \mathbin{▫} \neg \overline{\overline{x}} \mathbin{▫} y = t \mathbin{▫} \neg \overline{\overline{x}} \mathbin{▫} (x \mathbin{⍐_{\overline{x}}} y) \\ \Longleftrightarrow & \quad \langle \text{ by Propositions 3.20-1 and 3.14-7 } \rangle \\ & \mathsf{true} \end{array}$$

5.
$$\begin{array}{ll} & (s \mathbin{⍐} t) \mathbin{▫} x = s \mathbin{▫} x \mathbin{⍐} t \mathbin{▫} x \\ \Longleftrightarrow & \quad \langle \text{ by Proposition 3.20-17 } \rangle \\ & s \mathbin{▫} (s \mathbin{⍐} t) \mathbin{▫} x = s \mathbin{▫} (s \mathbin{▫} x \mathbin{⍐} t \mathbin{▫} x) \ \wedge \ \neg s \mathbin{▫} (s \mathbin{⍐} t) \mathbin{▫} x = \neg s \mathbin{▫} (s \mathbin{▫} x \mathbin{⍐} t \mathbin{▫} x) \\ \Longleftrightarrow & \quad \langle \text{ Boolean algebra, Corollary 3.21-4 and (3.6) } \rangle \\ & s \mathbin{▫} x = s \mathbin{▫} (x \mathbin{⍐} t \mathbin{▫} x) \ \wedge \ \neg s \mathbin{▫} t \mathbin{▫} x = \top \mathbin{⍐} \neg s \mathbin{▫} t \mathbin{▫} x \\ \Longleftrightarrow & \quad \langle \text{ by Corollaries 3.21-2 and 3.21-3 } \rangle \\ & s \mathbin{▫} x = s \mathbin{▫} (x \mathbin{⍐} \neg \overline{\overline{x}} \mathbin{▫} t \mathbin{▫} x) \\ \Longleftrightarrow & \quad \langle \text{ by Boolean algebra, Proposition 3.14-17, (3.6) and Corollary 3.21-3 } \rangle \\ & \mathsf{true} \end{array}$$

6. $x = t \rhd x \between \neg t \rhd x$

$\iff$ ⟨ by Proposition 3.20-17 ⟩

$t \rhd x = t \rhd (t \rhd x \between \neg t \rhd x) \ \wedge \ \neg t \rhd x = \neg t \rhd (t \rhd x \between \neg t \rhd x)$

$\iff$ ⟨ by Corollary 3.21-4, Boolean algebra and (3.6) ⟩

$t \rhd x = t \rhd x \between \top \ \wedge \ \neg t \rhd x = \top \between \neg t \rhd x$

$\iff$ ⟨ by Corollary 3.21-3 ⟩

true

7. Suppose $\ulcorner x \sqsubseteq t$. Hence $t = t \rhd \ulcorner x$ by Boolean algebra.

$t \rhd (x \between y) = t \rhd x$

$\iff$ ⟨ by (3.24) and the hypothesis ⟩

$t \rhd \ulcorner x \rhd (x \between_{\ulcorner x} y) = t \rhd x$

$\iff$ ⟨ by Propositions 3.20-1 and 3.14-7 ⟩

true

8. Suppose $\neg \ulcorner x \sqsubseteq t$. Hence $t = t \rhd \neg \ulcorner x$ by Boolean algebra.

$t \rhd (x \between y) = t \rhd y$

$\iff$ ⟨ by (3.24) and the hypothesis ⟩

$t \rhd \neg \ulcorner x \rhd (x \between_{\ulcorner x} y) = t \rhd y$

$\iff$ ⟨ by Proposition 3.20-1 and the hypothesis ⟩

true

9. $x \between_u y = u \rhd x \between \neg u \rhd y$

$\iff$ ⟨ by (3.23) ⟩

$u \rhd x = u \rhd (u \rhd x \between \neg u \rhd y) \ \wedge \ \neg u \rhd y = \neg u \rhd (u \rhd x \between \neg u \rhd y)$

$\iff$ ⟨ by Corollary 3.21-4 and Boolean algebra ⟩

$u \rhd x = u \rhd x \between \top \rhd y \ \wedge \ \neg u \rhd y = \top \rhd x \between \neg u \rhd y$

$\iff$ ⟨ by (3.6) and Corollary 3.21-3 ⟩

true

10. Suppose $\ulcorner x \rhd y = \ulcorner y \rhd x$.

$x \pitchfork y = y \pitchfork x$

$\iff$ ⟨ by Proposition 3.20-17 and (3.24) ⟩

$\ulcorner x \urcorner (x \pitchfork y) = \ulcorner x \urcorner (y \pitchfork_{\ulcorner y \urcorner} x) \ \wedge \ \neg \ulcorner x \urcorner (x \pitchfork y) = \neg \ulcorner x \urcorner (y \pitchfork x)$

$\iff$ ⟨ by Proposition 3.20-8 and Corollaries 3.21-4, 3.21-7 and 3.21-8 ⟩

$\ulcorner x \urcorner x = \ulcorner x \urcorner y \pitchfork_{\ulcorner y \urcorner} \ulcorner x \urcorner x \ \wedge \ \neg \ulcorner x \urcorner y = \neg \ulcorner x \urcorner y \pitchfork \neg \ulcorner x \urcorner x$

$\iff$ ⟨ by Propositions 3.14-7 and 3.14-17 ⟩

$x = \ulcorner x \urcorner y \pitchfork_{\ulcorner y \urcorner} x \ \wedge \ \neg \ulcorner x \urcorner y = \neg \ulcorner x \urcorner y \pitchfork \top$

$\iff$ ⟨ by Corollary 3.21-3 ⟩

$x = \ulcorner x \urcorner y \pitchfork_{\ulcorner y \urcorner} x \ \wedge \ \mathsf{true}$

$\iff$ ⟨ by the hypothesis ⟩

$x = \ulcorner y \urcorner x \pitchfork_{\ulcorner y \urcorner} x$

$\iff$ ⟨ by Propositions 3.20-3 and 3.20-13 ⟩

true

11. $x \pitchfork x$

$=$ ⟨ by (3.24) ⟩

$x \pitchfork_{\ulcorner x \urcorner} x$

$=$ ⟨ by Proposition 3.20-13 ⟩

x

12. true

$\iff$ ⟨ by (3.14) ⟩

$y \sqsubseteq \top$

$\implies$ ⟨ by Proposition 3.20-15 ⟩

$x \pitchfork_{\ulcorner x \urcorner} y \sqsubseteq x \pitchfork_{\ulcorner x \urcorner} \top$

$\iff$ ⟨ by (3.24) and Propositions 3.20-5 and 3.14-7 ⟩

$x \pitchfork y \sqsubseteq x$

13. $x \pitchfork (y \pitchfork z) = (x \pitchfork y) \pitchfork z$

$\iff$ ⟨ by (3.24) ⟩

$x \pitchfork_{\ulcorner x \urcorner} (y \pitchfork z) = (x \pitchfork_{\ulcorner x \urcorner} y) \pitchfork z$

$\iff$ ⟨ by (3.23) and Proposition 3.14-7 ⟩

$x = {}^{\Gamma}x \rhd ((x \pitchfork_{{}^{\Gamma}x} y) \pitchfork z) \;\wedge\; \neg{}^{\Gamma}x \rhd (y \pitchfork z) = \neg{}^{\Gamma}x \rhd ((x \pitchfork_{{}^{\Gamma}x} y) \pitchfork z)$

$\Longleftrightarrow$ ⟨ by Corollaries 3.21-7 and 3.21-4, Proposition 3.20-20, (3.24) and Boolean algebra ⟩

$x = {}^{\Gamma}x \rhd (x \pitchfork_{{}^{\Gamma}x} y) \;\wedge\; \neg{}^{\Gamma}x \rhd y \pitchfork \neg{}^{\Gamma}x \rhd z = \neg{}^{\Gamma}x \rhd (x \pitchfork_{{}^{\Gamma}x} y) \pitchfork \neg{}^{\Gamma}x \rhd z$

$\Longleftrightarrow$ ⟨ by Propositions 3.20-1 and 3.14-7 ⟩

true

14. $(x \sqcup y) \pitchfork (x \sqcup z) = x \sqcup (y \pitchfork z)$

$\Longleftrightarrow$ ⟨ by (3.24), (3.21) and Proposition 3.14-3 ⟩

$(x \sqcup y) \pitchfork_{{}^{\Gamma}x \rhd {}^{\Gamma}y} (x \sqcup z) = x \sqcup (y \pitchfork z)$

$\Longleftrightarrow$ ⟨ by (3.23), Proposition 3.14-11 and De Morgan ⟩

$x \sqcup y = {}^{\Gamma}x \rhd {}^{\Gamma}y \rhd (x \sqcup (y \pitchfork z)) \;\wedge$
$(\neg{}^{\Gamma}x \pitchfork \neg{}^{\Gamma}y) \rhd (x \sqcup z) = (\neg{}^{\Gamma}x \pitchfork \neg{}^{\Gamma}y) \rhd (x \sqcup (y \pitchfork z))$

$\Longleftrightarrow$ ⟨ by (3.8), Corollary 3.21-7 and Propositions 3.14-11 and 3.14-7 ⟩

true $\wedge$ $(\neg{}^{\Gamma}x \pitchfork \neg{}^{\Gamma}y) \rhd (x \sqcup z) = (\neg{}^{\Gamma}x \pitchfork \neg{}^{\Gamma}y) \rhd (x \sqcup (y \pitchfork z))$

$\Longleftrightarrow$ ⟨ by Propositions 3.14-7 and 3.14-20, and Boolean algebra ⟩

$\neg{}^{\Gamma}y \rhd (x \sqcup z) = \neg{}^{\Gamma}y \rhd (x \sqcup (y \pitchfork z))$

$\Longleftrightarrow$ ⟨ by (3.8) and Corollary 3.21-8 ⟩

true

15. $x \pitchfork (y \sqcup z)$

$=$ ⟨ by (3.24) ⟩

$x \pitchfork_{{}^{\Gamma}x} (y \sqcup z)$

$=$ ⟨ by Proposition 3.20-9 ⟩

$(x \pitchfork_{{}^{\Gamma}x} y) \sqcup (x \pitchfork_{{}^{\Gamma}x} z)$

$=$ ⟨ by (3.24) ⟩

$(x \pitchfork y) \sqcup (x \pitchfork z)$

16. ${}^{\Gamma}(x \pitchfork y)$

$=$ ⟨ by (3.24) ⟩

${}^{\Gamma}(x \pitchfork_{{}^{\Gamma}x} y)$

$=$ ⟨ by Proposition 3.20-20 ⟩

${}^{\Gamma}x \pitchfork_{{}^{\Gamma}x} {}^{\Gamma}y$

$$
\begin{aligned}
&= && \langle \text{ by Proposition 3.14-1 and (3.24) } \rangle \\
&\quad {}^{\sqcap\!\!\sqcap}x \pitchfork {}^{\sqcap\!\!\sqcap}y
\end{aligned}
$$

17. Suppose ${}^{\sqcap\!\!\sqcap}x \circ {}^{\sqcap\!\!\sqcap}y = \top$, hence $\neg {}^{\sqcap\!\!\sqcap}x \circ {}^{\sqcap\!\!\sqcap}y = {}^{\sqcap\!\!\sqcap}y$ by Boolean algebra.

$$
\begin{aligned}
&\quad (x \pitchfork y) \circ z \\
&= && \langle \text{ by (3.24) } \rangle \\
&\quad (x \pitchfork_{{}^{\sqcap\!\!\sqcap}x} y) \circ z \\
&= && \langle \text{ by Proposition 3.20-7 } \rangle \\
&\quad x \circ z \pitchfork_{{}^{\sqcap\!\!\sqcap}x} y \circ z \\
&= && \langle \text{ by Corollary 3.21-9, Proposition 3.14-7 and the hypothesis } \rangle \\
&\quad x \circ z \pitchfork y \circ z
\end{aligned}
$$

18. Suppose $x \circ z = x$ and $y \circ z = y$.

$$
\begin{aligned}
&\quad (x \pitchfork_t y) \circ z \\
&= && \langle \text{ by Proposition 3.20-7 } \rangle \\
&\quad x \circ z \pitchfork_t y \circ z \\
&= && \langle \text{ by the hypothesis } \rangle \\
&\quad x \pitchfork_t y
\end{aligned}
$$

$$
\begin{aligned}
&\quad (x \pitchfork y) \circ z \\
&= && \langle \text{ by (3.24) } \rangle \\
&\quad (x \pitchfork_{{}^{\sqcap\!\!\sqcap}x} y) \circ z \\
&= && \langle \text{ see the previous derivation } \rangle \\
&\quad x \pitchfork_{{}^{\sqcap\!\!\sqcap}x} y \\
&= && \langle \text{ by (3.24) } \rangle \\
&\quad x \pitchfork y
\end{aligned}
$$

19. We prove Corollary 3.21-19 by induction.

    Basis case $n = 2$. For any t_1 and t_2 such that $t_1 \pitchfork t_2 = 1$ and $t_1 \circ t_2 = \top$, $t_2 = \neg t_1$ by Boolean algebra. Thus, Proposition 3.20-16 gives

$$x \sqsubseteq y \iff t_1 \circ x \sqsubseteq t_1 \circ y \wedge t_2 \circ x \sqsubseteq t_2 \circ y \ .$$

Induction hypothesis. Suppose that for any t_1, t_2, ..., t_{n-1} such that $t_1 \sqcap t_2 \sqcap ... \sqcap t_{n-1} = 1$ and t_1, t_2, ..., t_{n-1} are pairwise disjoint,

$$x \sqsubseteq y \iff t_1 \rhd x \sqsubseteq t_1 \rhd y \wedge t_2 \rhd x \sqsubseteq t_2 \rhd y \wedge ... \wedge t_{n-1} \rhd x \sqsubseteq t_{n-1} \rhd y \ .$$

Suppose now that $t_1 \sqcap t_2 \sqcap ... \sqcap t_n = 1$ and t_1, t_2, ..., t_n are pairwise disjoint. Then $(t_1 \sqcap t_2) \sqcap t_3 \sqcap ... \sqcap t_n = 1$ and $(t_1 \sqcap t_2)$, t_3, ..., t_n are pairwise disjoint by Boolean algebra.

$$\begin{array}{ll} & x \sqsubseteq y \\ \iff & \quad \langle \text{ by the induction hypothesis } \rangle \\ & (t_1 \sqcap t_2) \rhd x \sqsubseteq (t_1 \sqcap t_2) \rhd y \ \wedge \ t_3 \rhd x \sqsubseteq t_3 \rhd y \ \wedge \ ... \ \wedge \ t_n \rhd x \sqsubseteq t_n \rhd y \\ \iff & \quad \langle \text{ by Proposition 3.20-16, the hypothesis and Boolean algebra } \rangle \\ & t_1 \rhd x \sqsubseteq t_1 \rhd y \ \wedge \ t_2 \rhd x \sqsubseteq t_2 \rhd y \ \wedge \ ... \ \wedge \ t_n \rhd x \sqsubseteq t_n \rhd y \end{array}$$

□

By Corollary 3.21-14 and (3.2), $(x \sqcap y) \sqcup z = (x \sqcup z) \sqcap (y \sqcup z)$. However, $(x \sqcup y) \sqcap z = (x \sqcap z) \sqcup (y \sqcap z)$ is false in general. Take the relations $x = \{(0,0)\}$, $y = \{\}$ and $z = \{(0,1)\}$ as a counter-example.

Furthermore, the equality $(x \sqcap y) \rhd z = x \rhd z \sqcap y \rhd z$ is also false in general (compare with Proposition 3.20-7). Take the relations $x = \{(0,0),(0,1),(1,0),(1,1)\}$, $y = \{(0,1),(1,1)\}$ and $z = \{(1,1)\}$ as a counter-example. This counter-example shows that the hypothesis of Corollary 3.21-17 is welcome. Another way of getting $(x \sqcap y) \rhd z = x \rhd z \sqcap y \rhd z$ is to focus on tests, as in Corollary 3.21-5.

In order to demonstrate a refinement $x \sqsubseteq y$ for $x, y \in A$, rather than deriving it directly, it is sometimes easier to break it in more refinements $t_1 \rhd x \sqsubseteq t_1 \rhd y$, $t_2 \rhd x \sqsubseteq t_2 \rhd y$, ..., $t_n \rhd x \sqsubseteq t_n \rhd y$. This can be done under suitable hypotheses thanks to Corollary 3.21-19. This case analysis with many tests is going to be used several times in the proof of Theorem 4.31.

There is a trivial and very useful contraction of Proposition 3.14-21 and Corollary 3.21-10 which reads

$$\neg x \rhd \neg y = \top \implies x \sqcap y = y \sqcap x \ . \tag{3.25}$$

By Corollary 3.21-12, $x \sqcap y \sqsubseteq x$. In general, $x \sqcap y \sqsubseteq y$ does not hold. Take the relations $x = \{(0,0)\}$ and $y = \{(0,1)\}$ as a counter-example. However it is true under

suitable hypotheses. The following lemma presents hypotheses that help manipulating $⊓$ operators involved in different refinements.

Lemma 3.22. *Let $\mathcal{A}$ be a DAD-$⊓_•$. The following properties are true for all $x, y, z \in A$.*

1. $y \sqsubseteq z \implies x ⊓ y \sqsubseteq x ⊓ z$
2. $x \sqsubseteq y \implies x \sqsubseteq y ⊓ x$
3. $x \sqsubseteq y \wedge {}^{\sqcap}x = {}^{\sqcap}y \implies x ⊓ z \sqsubseteq y ⊓ z$
4. $x \sqsubseteq y \wedge {}^{\sqcap}x ▫ {}^{\sqcap}z = \top \implies x ⊓ z \sqsubseteq y ⊓ z$
5. ${}^{\sqcap}(x ⊓ y) = {}^{\sqcap}z \wedge x = {}^{\sqcap}x ▫ z \wedge y = {}^{\sqcap}y ▫ z \implies x ⊓ y = z$
6. $x \sqsubseteq y ⊓ z \iff x \sqsubseteq y \wedge x \sqsubseteq \neg {}^{\sqcap}y ▫ z$
7. ${}^{\sqcap}x ▫ {}^{\sqcap}y = {}^{\sqcap}w ▫ {}^{\sqcap}z = \top \implies (w ⊓ x) ⊔ (y ⊓ z) = (w ⊔ y) ⊓ (x ⊔ z)$

Proof :

1. This follows from (3.24) and Proposition 3.20-15.
2. Suppose $x \sqsubseteq y$

$$
\begin{array}{ll}
 & y ⊓ x \\
= & \quad \langle \text{ by Corollary 3.21-2 } \rangle \\
 & y ⊓ \neg {}^{\sqcap}y ▫ x \\
= & \quad \langle \text{ by Proposition 3.14-9 and Boolean algebra,} \\
 & \quad {}^{\sqcap}y ▫ {}^{\sqcap}(\neg {}^{\sqcap}y ▫ x) = \top, \\
 & \quad \text{then apply (3.25) } \rangle \\
 & \neg {}^{\sqcap}y ▫ x ⊓ y \\
= & \quad \langle \text{ by Proposition 3.14-7 } \rangle \\
 & \neg {}^{\sqcap}y ▫ x ⊓ {}^{\sqcap}y ▫ y \\
\sqsupseteq & \quad \langle \text{ by the hypothesis and Lemma 3.22-1 } \rangle \\
 & \neg {}^{\sqcap}y ▫ x ⊓ {}^{\sqcap}y ▫ x \\
= & \quad \langle \text{ by Corollary 3.21-6 } \rangle \\
 & x
\end{array}
$$

3. This follows from (3.24) and Proposition 3.20-14.

4. Assume $\ulcorner x \urcorner \ulcorner z = \top$.

$$
\begin{array}{ll}
& x \mathbin{⫤} z \sqsubseteq y \mathbin{⫤} z \\
\iff & \quad \langle \text{ by Proposition 3.20-16 } \rangle \\
& \ulcorner x \urcorner (x \mathbin{⫤} z) \sqsubseteq \ulcorner x \urcorner (y \mathbin{⫤} z) \ \wedge \ \neg \ulcorner x \urcorner (x \mathbin{⫤} z) \sqsubseteq \neg \ulcorner x \urcorner (y \mathbin{⫤} z) \\
\iff & \quad \langle \text{ by Corollaries 3.21-7, 3.21-8 and 3.21-4, and Proposition 3.14-7 } \rangle \\
& \ulcorner x \urcorner x \sqsubseteq \ulcorner x \urcorner y \mathbin{⫤} \ulcorner x \urcorner \ulcorner z \urcorner z \ \wedge \ \neg \ulcorner x \urcorner \ulcorner z \urcorner z \sqsubseteq \neg \ulcorner x \urcorner \ulcorner y \urcorner y \mathbin{⫤} \neg \ulcorner x \urcorner \ulcorner z \urcorner z \\
\iff & \quad \langle \text{ by the hypothesis, Boolean algebra, (3.6), Corollary 3.21-3 and Proposition 3.14-7 } \rangle \\
& \ulcorner x \urcorner x \sqsubseteq \ulcorner x \urcorner y \ \wedge \ z \sqsubseteq \neg \ulcorner x \urcorner y \mathbin{⫤} z \\
\impliedby & \quad \langle \text{ by Proposition 3.14-8, Boolean algebra, (3.6) and Corollary 3.21-3 } \rangle \\
& x \sqsubseteq y
\end{array}
$$

5. Assume $x = \ulcorner x \urcorner z$, $y = \ulcorner y \urcorner z$ and $\ulcorner (x \mathbin{⫤} y) = \ulcorner z$. Hence,

$$\neg \ulcorner x \urcorner \ulcorner y = \neg \ulcorner x \urcorner \ulcorner z \tag{3.26}$$

by Corollary 3.21-16 and Boolean algebra.

$$
\begin{array}{ll}
& x \mathbin{⫤} y = z \\
\iff & \quad \langle \text{ by (3.24) } \rangle \\
& x \mathbin{⫤_{\ulcorner x}} y = z \\
\iff & \quad \langle \text{ by (3.23) and Proposition 3.14-7 } \rangle \\
& x = \ulcorner x \urcorner z \ \wedge \ \neg \ulcorner x \urcorner y = \neg \ulcorner x \urcorner z \\
\iff & \quad \langle \text{ by the hypothesis } \rangle \\
& \mathsf{true} \ \wedge \ \neg \ulcorner x \urcorner \ulcorner y \urcorner z = \neg \ulcorner x \urcorner z \\
\iff & \quad \langle \text{ by Proposition 3.14-7 and (3.26) } \rangle \\
& \mathsf{true}
\end{array}
$$

6.

$$
\begin{array}{ll}
& x \sqsubseteq y \mathbin{⫤} z \\
\iff & \quad \langle \text{ by (3.24) } \rangle \\
& x \sqsubseteq y \mathbin{⫤_{\ulcorner y}} z \\
\iff & \quad \langle \text{ by Propositions 3.20-18 and 3.14-7 } \rangle \\
& x \sqsubseteq y \ \wedge \ x \sqsubseteq \neg \ulcorner y \urcorner z
\end{array}
$$

7. Assume $⌜x▫⌜y = \top$ and $⌜w▫⌜z = \top$.

$$
\begin{array}{ll}
 & (w \sqcap x) \sqcup (y \sqcap z) \\
= & \qquad \langle \text{ by Corollary 3.21-14 } \rangle \\
 & ((w \sqcap x) \sqcup y) \sqcap ((w \sqcap x) \sqcup z) \\
= & \qquad \langle \text{ by (3.2) and Corollary 3.21-14 } \rangle \\
 & (w \sqcup y) \sqcap (x \sqcup y) \sqcap (w \sqcup z) \sqcap (x \sqcup z) \\
= & \qquad \langle \text{ by Proposition 3.14-11, the hypothesis, (3.6) and} \\
 & \qquad \quad \text{Corollary 3.21-3 } \rangle \\
 & (w \sqcup y) \sqcap (x \sqcup z)
\end{array}
$$

□

Propositions 3.20-21 and 3.14-7 with Definition 3.24 imply that $x \sqcap y$ is the infimum of x and $\neg⌜x▫y$ with respect to $\sqsubseteq$.

Chapter 4

Definition of Angelic Operators in DAD

As mentioned at the beginning of Section 3.4, we are looking for a downward link — refer to Figure 1.4— from DAD-$\pitchfork$ to KAD for any model of KAD. The idea is to define angelic operators in the context of DAD-$\pitchfork$ and then demonstrate that the elements of a DAD-$\pitchfork$ together with those angelic operators form a KAD. This is exactly what is done in this chapter.

In Sections 4.1, 4.2 and 4.3, we respectively define angelic non-deterministic choice $+_D$, angelic sequential composition $\cdot_D$ and angelic finite iteration ^{*D}. In Section 4.2, we also define *decomposable elements*. These are indispensable for the definition of the $\cdot_D$ operator. In Section 4.4, we demonstrate many properties about decomposable elements. Finally, in Section 4.5, we demonstrate that the elements of a DAD-$\pitchfork$ together with those angelic operators form a KAD. This last result of the chapter is one of the most important of this thesis. Indeed, it is the second step toward the desired duality (refer to Section 1.3).

We add a subscript D to the angelic operators defined here, to denote that they are defined by demonic expressions.

4.1 Angelic Refinement and Angelic Choice

We start with the angelic partial order $\leq_D$. It is easy to see that this definition is the demonic version of Definition 2.9.

Definition 4.1 (Angelic refinement)**.** *Let $\mathcal{A}$ be a DAD-$\sqcap_\bullet$ and take $x, y \in A$. We say that $x \leq_D y$ when*

$$\sqcap y \sqsubseteq \sqcap x \ , \tag{4.1}$$

$$x \sqsubseteq \sqcap x \sqcup y \ . \tag{4.2}$$

Proposition 4.3 below states that $\leq_D$ is a partial order. Moreover, it gives a formula using demonic operators for the angelic supremum with respect to this partial order. In order to demonstrate this proposition, we need the following lemma.

Lemma 4.2. *Let $\mathcal{A}$ be a DAD-$\sqcap_\bullet$. The function*

$$\begin{array}{rcl} f : A \times A & \longrightarrow & A \\ (x, y) & \mapsto & (x \sqcup y) \sqcap \neg \sqcap y \sqcup x \sqcap \neg \sqcap x \sqcup y \end{array}$$

satisfies the following four properties for all $x, y, z \in A$. Note that f is well defined by Corollary 3.21-13.

1. $\sqcap f(x, y) = \sqcap x \sqcap \sqcap y$
2. $f(x, x) = x$
3. $f(x, y) = f(y, x)$
4. $f(x, f(y, z)) = f(f(x, y), z)$

Proof :

1. $\sqcap f(x, y)$

   $=$ $\quad \langle$ by definition of f $\rangle$

   $\sqcap((x \sqcup y) \sqcap \neg \sqcap y \sqcup x \sqcap \neg \sqcap x \sqcup y)$

   $=$ $\quad \langle$ by Corollary 3.21-16 $\rangle$

   $\sqcap(x \sqcup y) \sqcap \sqcap(\neg \sqcap y \sqcup x) \sqcap \sqcap(\neg \sqcap x \sqcup y)$

$$
\begin{array}{ll}
= & \langle \text{ by (3.21) and Propositions 3.14-3 and 3.14-9 } \rangle \\
& \Cap x \sqcap \Cap y \between \neg \Cap y \sqcap \Cap x \between \neg \Cap x \sqcap \Cap y \\
= & \langle \text{ by Boolean algebra } \rangle \\
& \Cap x \between \Cap y
\end{array}
$$

2.
$$
\begin{array}{ll}
& f(x,x) \\
= & \langle \text{ by definition of } f \rangle \\
& (x \sqcup x) \between \neg \Cap x \sqcap x \between \neg \Cap x \sqcap x \\
= & \langle \text{ by Proposition 3.14-17 } \rangle \\
& (x \sqcup x) \between \top \between \top \\
= & \langle \text{ by Corollary 3.21-3 and (3.3) } \rangle \\
& x
\end{array}
$$

3.
$$
\begin{array}{ll}
& f(x,y) \\
= & \langle \text{ by definition of } f \rangle \\
& (x \sqcup y) \between \neg \Cap y \sqcap x \between \neg \Cap x \sqcap y \\
= & \langle \text{ by Proposition 3.14-9 and Boolean algebra,} \\
& \quad \Cap(\neg \Cap y \sqcap x) \sqcap \Cap(\neg \Cap x \sqcap y) = \neg \Cap y \sqcap \Cap x \sqcap \neg \Cap x \sqcap \Cap y = \top, \\
& \quad \text{then apply (3.2) and (3.25) } \rangle \\
& (y \sqcup x) \between \neg \Cap x \sqcap y \between \neg \Cap y \sqcap x \\
= & \langle \text{ by definition of } f \rangle \\
& f(y,x)
\end{array}
$$

4. Here is the derivation. It repeatedly invokes (3.25). Using (3.21), Boolean algebra and Proposition 3.14-9, it is easy to check that the operands of the various $\between$ operators are pairwise disjoint, so that the condition $\Cap x \sqcap \Cap y = \top$ of (3.25) is satisfied. This is what allows permuting the operands.

$$
\begin{array}{ll}
& f(x, f(y,z)) \\
= & \langle \text{ by definition of } f \text{ and Lemma 4.2-1 } \rangle \\
& (x \sqcup ((y \sqcup z) \between \neg \Cap z \sqcap y \between \neg \Cap y \sqcap z)) \between \\
& \neg(\Cap y \between \Cap z) \sqcap x \between \neg \Cap x \sqcap ((y \sqcup z) \between \neg \Cap z \sqcap y \between \neg \Cap y \sqcap z) \\
= & \langle \text{ by Corollaries 3.21-14 and 3.21-4, and Boolean algebra } \rangle \\
& (x \sqcup y \sqcup z) \between (x \sqcup \neg \Cap z \sqcap y) \between (x \sqcup \neg \Cap y \sqcap z) \between \\
& \neg \Cap y \sqcap \neg \Cap z \sqcap x \between \neg \Cap x \sqcap (y \sqcup z) \between \neg \Cap x \sqcap \neg \Cap z \sqcap y \between \neg \Cap x \sqcap \neg \Cap y \sqcap z
\end{array}
$$

$$
\begin{array}{ll}
= & \langle \text{ by Proposition 3.14-20 and (3.25) } \rangle \\
& (x \sqcup y \sqcup z) \sqcap \neg\urcorner z \urcorner (x \sqcup y) \sqcap \neg\urcorner y \urcorner (x \sqcup z) \sqcap \neg\urcorner x \urcorner (y \sqcup z) \sqcap \\
& \neg\urcorner y \urcorner \neg\urcorner z \urcorner x \sqcap \neg\urcorner x \urcorner \neg\urcorner z \urcorner y \sqcap \neg\urcorner x \urcorner \neg\urcorner y \urcorner z \\
= & \langle \text{ by (3.2), (3.21), Proposition 3.14-9, (3.25) and Boolean algebra } \rangle \\
& (z \sqcup x \sqcup y) \sqcap \neg\urcorner y \urcorner (z \sqcup x) \sqcap \neg\urcorner x \urcorner (z \sqcup y) \sqcap \neg\urcorner z \urcorner (x \sqcup y) \sqcap \\
& \neg\urcorner x \urcorner \neg\urcorner y \urcorner z \sqcap \neg\urcorner z \urcorner \neg\urcorner y \urcorner x \sqcap \neg\urcorner z \urcorner \neg\urcorner x \urcorner y \\
= & \langle \text{ by Proposition 3.14-20 and (3.25) } \rangle \\
& (z \sqcup x \sqcup y) \sqcap (z \sqcup \neg\urcorner y \urcorner x) \sqcap (z \sqcup \neg\urcorner x \urcorner y) \sqcap \neg\urcorner x \urcorner \neg\urcorner y \urcorner z \sqcap \\
& \neg\urcorner z \urcorner (x \sqcup y) \sqcap \neg\urcorner z \urcorner \neg\urcorner y \urcorner x \sqcap \neg\urcorner z \urcorner \neg\urcorner x \urcorner y \\
= & \langle \text{ by Corollaries 3.21-14 and 3.21-4, and Boolean algebra } \rangle \\
& (z \sqcup ((x \sqcup y) \sqcap \neg\urcorner y \urcorner x \sqcap \neg\urcorner x \urcorner y)) \sqcap \neg(\urcorner x \sqcap \urcorner y) \urcorner z \sqcap \\
& \neg\urcorner z \urcorner ((x \sqcup y) \sqcap \neg\urcorner y \urcorner x \sqcap \neg\urcorner x \urcorner y) \\
= & \langle \text{ by definition of } f \text{ and Lemma 4.2-1 } \rangle \\
& f(z, f(x, y)) \\
= & \langle \text{ by Lemma 4.2-3 } \rangle \\
& f(f(x, y), z)
\end{array}
$$

□

Proposition 4.3 (Angelic choice)**.** *The angelic refinement of Definition 4.1 satisfies the following three properties.*

1. *For all* x, $\top \leq_D x$.
2. *For all* x, y,
$$x \leq_D y \iff f(x, y) = y \ ,$$
where f *is the function defined in Lemma 4.2.*
3. $\leq_D$ *is a partial order. Letting* $x +_D y$ *denote the supremum of* x *and* y *with respect to* $\leq_D$*, we have*
$$x +_D y = f(x, y) \ .$$

Proof :

1. From (3.14) and Proposition 3.14-8, we have $\ulcorner x \sqsubseteq \ulcorner\top$. Also, from Proposition 3.14-1 and (3.6), $\ulcorner\top \triangleleft x = \top$, so $\top \sqsubseteq \ulcorner\top \triangleleft x$. These two refinements are those from Definition 4.1, so $\top \leq_D x$.

2. $$\begin{array}{ll} & f(x,y) = y \\ \iff & \langle \text{ by Propositions 3.20-17, 3.14-7 and 3.14-17 } \rangle \\ & \ulcorner y \triangleleft f(x,y) = y \ \wedge\ \neg\ulcorner y \triangleleft f(x,y) = \top \\ \iff & \langle \text{ by Proposition 3.20-17 and (3.6) } \rangle \\ & \ulcorner x \triangleleft \ulcorner y \triangleleft f(x,y) = \ulcorner x \triangleleft y \ \wedge\ \ulcorner x \triangleleft \neg\ulcorner y \triangleleft f(x,y) = \top \ \wedge \\ & \neg\ulcorner x \triangleleft \ulcorner y \triangleleft f(x,y) = \neg\ulcorner x \triangleleft y \ \wedge\ \neg\ulcorner x \triangleleft \neg\ulcorner y \triangleleft f(x,y) = \top \\ \iff & \langle \text{ by definition of } f, \text{ Corollaries 3.21-4 and 3.21-3, Propositions} \\ & \quad \text{3.14-7, 3.14-17 and 3.14-11, Boolean algebra and (3.6) } \rangle \\ & \ulcorner x \triangleleft \ulcorner y \triangleleft (x \sqcup y) = \ulcorner x \triangleleft y \ \wedge\ \neg\ulcorner y \triangleleft x = \top \ \wedge\ \neg\ulcorner x \triangleleft y = \neg\ulcorner x \triangleleft y \ \wedge\ \top = \top \\ \iff & \langle \text{ by Proposition 3.14-11 and Boolean algebra } \rangle \\ & \ulcorner x \triangleleft (x \sqcup y) = \ulcorner x \triangleleft y \ \wedge\ \neg\ulcorner y \triangleleft x = \top \\ \iff & \langle \text{ by Propositions 3.14-20, 3.14-7, 3.14-19 and 3.14-9 } \rangle \\ & x \sqcup \ulcorner x \triangleleft y = \ulcorner x \triangleleft y \ \wedge\ \neg\ulcorner y \triangleleft \ulcorner x = \top \\ \iff & \langle \text{ by Proposition 3.14-16 } \rangle \\ & x \sqcup \ulcorner x \triangleleft y = \ulcorner x \triangleleft y \ \wedge\ \ulcorner y \sqsubseteq \ulcorner x \\ \iff & \langle \text{ by (3.11) and Definition 4.1 } \rangle \\ & x \leq_D y \end{array}$$

3. It follows from the previous point of the present proposition and by the fact that f is reflexive, symmetric and transitive (see Lemma 4.2). □

Proposition 4.3 and Lemma 4.2 show that $\leq_D$ and $+_D$ do what we expect them to do and the following corollary is a direct consequence of these results.

Corollary 4.4. *Let $\mathcal{A}$ be a DAD-$\pitchfork_\bullet$. For all $x, y, z \in A$,*

1. $x +_D y = (x \sqcup y) \pitchfork \neg\ulcorner y \triangleleft x \pitchfork \neg\ulcorner x \triangleleft y$,
2. $\leq_D$ *is a partial order and* $x +_D y = y \iff x \leq_D y$,
3. $\ulcorner(x +_D y) = \ulcorner x \pitchfork \ulcorner y$,
4. $(x +_D y) +_D z = x +_D (y +_D z)$,

5. $x +_D y = y +_D x$,

6. $x +_D x = x$,

7. $\top +_D x = x +_D \top = x$.

Remark 4.5. Note that for all $s, t \in \mathsf{test}(A)$,

$$s \leq_D t \iff t \sqsubseteq s$$

by Definition 4.1, Proposition 3.14-1 and Boolean algebra. This equivalence is the demonic version of the one of Remark 2.11.

Remark 4.6. Since the domains of $x \sqcup y$, $\neg^{\sqcap} x \triangleright y$ and $\neg^{\sqcap} y \triangleright x$ are pairwise disjoint by (3.21) and Proposition 3.14-9, the three terms in the definition of f (see Lemma 4.2) commute. In the next sections and chapters, we will use any of the following equalities by refering to Corollary 4.4-1.

$$\begin{aligned}
x +_D y &= (x \sqcup y) \sqcap \neg^{\sqcap} y \triangleright x \sqcap \neg^{\sqcap} x \triangleright y \\
x +_D y &= (x \sqcup y) \sqcap \neg^{\sqcap} x \triangleright y \sqcap \neg^{\sqcap} y \triangleright x \\
x +_D y &= \neg^{\sqcap} y \triangleright x \sqcap \neg^{\sqcap} x \triangleright y \sqcap (x \sqcup y) \\
x +_D y &= \neg^{\sqcap} y \triangleright x \sqcap (x \sqcup y) \sqcap \neg^{\sqcap} x \triangleright y \\
x +_D y &= \neg^{\sqcap} x \triangleright y \sqcap \neg^{\sqcap} y \triangleright x \sqcap (x \sqcup y) \\
x +_D y &= \neg^{\sqcap} x \triangleright y \sqcap (x \sqcup y) \sqcap \neg^{\sqcap} y \triangleright x
\end{aligned}$$

Other major properties of $+_D$ will be presented in Section 4.5.

4.2 Angelic Composition and Demonic Decomposition

We now turn to the definition of angelic composition. But things are not as simple as for $\leq_D$ or $+_D$. The difficulty is due to the asymmetry between left and right caused by the difference between Proposition 3.20-7 and 3.20-8, and by the absence of a *codomain operator* for "testing" the right-hand side of elements as can be done with the domain operator on the left. Consider the relations

$$\begin{aligned}
Q &= \{(0,0),(0,1),(1,2),(2,3)\} \ , \\
R &= \{(0,0),(2,2)\} \ .
\end{aligned}$$

The angelic composition of Q and R is $Q \cdot R = \{(0,0),(1,2)\}$, while their demonic composition is $Q \sqcap R = \{(1,2)\}$. There is no way to express $Q \cdot R$ only in terms of $Q \sqcap R$. What we could try to do is to decompose Q as follows using the conditional operator:

$$Q = Q \sqcap \Pi R \mathbin{⨅} Q \sqcap \neg \Pi R \mathbin{⨅} (Q_1 \sqcup Q_2) \ ,$$

where $Q_1 = \{(0,0)\}$ and $Q_2 = \{(0,1)\}$. Note that $Q \sqcap \Pi R = \{(1,2)\}$ and $Q \sqcap \neg \Pi R = \{(2,3)\}$, so that the domains of the three operands of $⨅$ are disjoint. The effect of $⨅$ is then just union. With these relations, it is possible to express the angelic composition as $Q \cdot R = Q \sqcap R \mathbin{⨅} Q_1 \sqcap R$. Now, it is possible to extract $Q_1 \sqcup Q_2$ from Q, since $Q_1 \sqcup Q_2 = \neg \Pi (Q \sqcap \Pi R) \sqcap \neg \Pi (Q \sqcap \neg \Pi R) \sqcap Q$. The problem is that it is not possible to extract Q_1 from $Q_1 \sqcup Q_2$. On the one hand, Q_1 and Q_2 have the same domain; on the other hand, there is no test t such that $Q_1 = (Q_1 \sqcup Q_2) \sqcap t$. This is what leads to the following definition.

Definition 4.7 (Decomposition)**.** *Let $\mathcal{A}$ be a DAD-$⨅$, and take $t \in \mathsf{test}(A)$. An element $x \in A$ is said to be* t-decomposable *if and only if there are* unique *elements x_t and $x_{\neg t}$ such that*

$$x = x \sqcap t \mathbin{⨅} x \sqcap \neg t \mathbin{⨅} (x_t \sqcup x_{\neg t}) \ , \tag{4.3}$$

$$\Pi(x_t) = \Pi(x_{\neg t}) = \neg \Pi (x \sqcap t) \sqcap \neg \Pi (x \sqcap \neg t) \sqcap \Pi x \ , \tag{4.4}$$

$$x_t = x_t \sqcap t \ , \tag{4.5}$$

$$x_{\neg t} = x_{\neg t} \sqcap \neg t \ . \tag{4.6}$$

Moreover, x is said to be decomposable *if and only if it is t-decomposable for all $t \in \mathsf{test}(A)$.*

Remark 4.8. The domains $\Pi(x \sqcap t)$, $\Pi(x \sqcap \neg t)$ and $\Pi(x_t)$ (or $\Pi(x_{\neg t})$) obtained by decomposing x as in Definition 4.7 are pairwise disjoint. That $\Pi(x_t)$ and $\Pi(x_{\neg t})$ are disjoint from $\Pi(x \sqcap t)$ and $\Pi(x \sqcap \neg t)$ is obvious from (4.4). By Lemma 3.17-4, $\Pi(x \sqcap t)$ and $\Pi(x \sqcap \neg t)$ are disjoint as well. This disjointness is often used in applications of (3.25) and Corollary 3.21-17.

Moreover,

$$\Pi x = \Pi(x \sqcap t) \mathbin{⨅} \Pi(x \sqcap \neg t) \mathbin{⨅} \Pi(x_t) \ , \tag{4.7}$$

since

$$\begin{array}{ll} & \Pi(x \sqcap t) \mathbin{⨅} \Pi(x \sqcap \neg t) \mathbin{⨅} \Pi(x_t) \\ = & \qquad \langle \text{ by (4.4) } \rangle \\ & \Pi(x \sqcap t) \mathbin{⨅} \Pi(x \sqcap \neg t) \mathbin{⨅} \neg \Pi (x \sqcap t) \sqcap \neg \Pi (x \sqcap \neg t) \sqcap \Pi x \end{array}$$

$$
\begin{aligned}
&= && \langle \text{ by Boolean algebra } \rangle \\
&\quad \ulcorner(x \circ t) \sqcap \ulcorner(x \circ \neg t) \sqcap \ulcorner x \\
&= && \langle \text{ by Proposition 3.14-18 and Boolean algebra } \rangle \\
&\quad \ulcorner x \ .
\end{aligned}
$$

Then from Corollary 3.21-16, Boolean algebra and Remark 4.8, it is easy to see that

$$\ulcorner(x \circ t \sqcap x_t) = \neg\ulcorner(x \circ \neg t) \circ \ulcorner x \ , \tag{4.8}$$

$$\ulcorner x \sqsubseteq \ulcorner(x \circ t \sqcap x_t) \ , \tag{4.9}$$

$$\neg\ulcorner x \circ x_t = \top \ . \tag{4.10}$$

Remark 4.9. Any element $x \in A$ is 1-decomposable and $\top$-decomposable. Indeed,

$$x_1 = x_\top = \top$$

by (4.4), Boolean algebra, (3.6) and Propositions 3.14-1 and 3.14-19.

Looking at Definition 4.7, many questions arise. Before defining angelic composition, we answer them.

- Are demonic tests all decomposable?

  Indeed they are, the t-decomposition of a test s is

  $$s = s \circ t \sqcap s \circ \neg t \sqcap (\top \sqcup \top) \tag{4.11}$$

  by (4.4), Boolean algebra and Propositions 3.14-1 and 3.14-19.

- Is there a DAD-$\sqcap_\bullet$ containing an element that is not decomposable?

  The following example presents such a scenario.

  Example 4.10. For this example, we consider the following nine relations defined on $S_2 = \{1, 2\}$.

$$\top = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \quad \mathsf{s} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \quad \mathsf{t} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \quad \mathsf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\mathsf{a} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \quad \mathsf{b} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \mathsf{c} = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \quad \mathsf{d} = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \quad \mathsf{e} = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$$

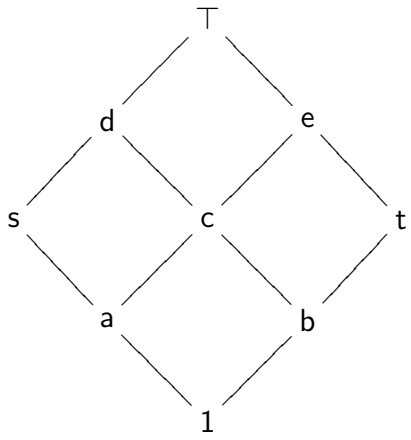


Figure 4.1: Hasse diagram of Example 4.10.

Take $A = \{\top, \mathsf{s}, \mathsf{t}, 1, \mathsf{a}, \mathsf{b}, \mathsf{c}, \mathsf{d}, \mathsf{e}\}$, $\mathsf{test}(A) = \{\top, \mathsf{s}, \mathsf{t}, 1\}$ and the demonic operators defined by the following tables, omitting $\sqcap_{\bullet}$.

⊔	⊤	s	t	1	a	b	c	d	e
⊤	⊤	⊤	⊤	⊤	⊤	⊤	⊤	⊤	⊤
s	⊤	s	⊤	s	s	d	d	d	⊤
t	⊤	⊤	t	t	e	t	e	⊤	e
1	⊤	s	t	1	a	b	c	d	e
a	⊤	s	e	a	a	c	c	d	e
b	⊤	d	t	b	c	b	c	d	e
c	⊤	d	e	c	c	c	c	d	e
d	⊤	d	⊤	d	d	d	d	d	⊤
e	⊤	⊤	e	e	e	e	e	⊤	e

▫	⊤	s	t	1	a	b	c	d	e
⊤	⊤	⊤	⊤	⊤	⊤	⊤	⊤	⊤	⊤
s	⊤	s	⊤	s	s	d	d	d	⊤
t	⊤	⊤	t	t	e	t	e	⊤	e
1	⊤	s	t	1	a	b	c	d	e
a	⊤	s	⊤	a	a	c	c	d	⊤
b	⊤	⊤	t	b	c	b	c	⊤	e
c	⊤	⊤	⊤	c	c	c	c	⊤	⊤
d	⊤	⊤	⊤	d	d	d	d	⊤	⊤
e	⊤	⊤	⊤	e	e	e	e	⊤	⊤

×	
⊤	⊤
s	s
t	t
1	1
a	a
b	b
c	c
d	⊤
e	⊤

⊓	
⊤	⊤
s	s
t	t
1	1
a	1
b	1
c	1
d	s
e	t

¬	
⊤	1
s	t
t	s
1	⊤

The demonic refinement ordering corresponding to ⊔ is represented in the semi-lattice of Figure 4.1. It is easy to convince oneself that it is a DAD-$\sqcap_{\bullet}$. Look at Figure 2.3. The present example is simply a subalgebra of that figure. The

elements $\mathsf{a}, \mathsf{b}, \mathsf{c}, \mathsf{d}$ and e are not decomposable. For instance, to decompose c with respect to s would require the existence of the relations

$$\mathsf{f} = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad \mathsf{g} = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \ ,$$

which are not there.

- Let t be a demonic test. May an element of a DAD-$\boxplus_\bullet$ have more than one t-decomposition? In other words, is it relevant to ask for uniqueness in Definition 4.7?

  Example 4.12 is one where there is an element with *nine* different t-decompositions. This example is constructed from the general structure introduced in the following lemma.

  Lemma 4.11. *Let* $(A, \mathsf{test}(A), \sqcup, \circ, ^\times, \top, 1, \neg, \boxplus, \ulcorner, \boxplus_\bullet)$ *be a DAD-*$\boxplus_\bullet$*. Consider* $E = \{(x,t) : A \times \mathsf{test}(A) \mid \ulcorner x \sqsubseteq t\}$ *and* $T = \{(t,t) : \mathsf{test}(A) \times \mathsf{test}(A)\}$ *and define the following operations for elements of* E*, where* $x, y \in A$ *and* $s, t, u \in \mathsf{test}(A)$*.*

$$\begin{aligned}
(x,s) \oplus (y,t) &= (x \sqcup y, s \sqcup t) \\
(x,s) \odot (y,t) &= (x \circ y, \ulcorner(s \circ x \circ t)) \\
(x,s)^{\circledast} &= (x^\times, \ulcorner(x^\times \circ s)) \\
\overline{(s,s)} &= (\neg s, \neg s) \\
(s,s) \mathbin{\Cap} (t,t) &= (s \boxplus t, s \boxplus t) \\
\ulcorner(x,s) &= (\ulcorner x, \ulcorner x) \\
(x,s) \mathbin{\Cap_{(u,u)}} (y,t) &= (x \boxplus_u y, s \boxplus_u t)
\end{aligned}$$

  Then $(E, T, \oplus, \odot, ^{\circledast}, (\top, \top), (1,1), \overline{}, \Cap, \ulcorner, \Cap_\bullet)$ *is a DAD-*$\Cap_\bullet$ *and the partial order related to* $\oplus$ *satisfies*

$$(x,s) \sqsubseteq (y,t) \iff x \sqsubseteq y \wedge s \sqsubseteq t \ .$$

  Proof : The proof of Lemma 4.11 contains no new idea and is ten pages long. Therefore, it is postponed to Appendix A. □

  Here is a DAD-$\boxplus_\bullet$ where the t-decomposition of x is not unique.

  Example 4.12. Take the structure constructed in Lemma 4.11 with relations on the set $S_2 = \{1, 2\}$ as carrier set A. Take the following relations

$$\top = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \quad \mathsf{s} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \quad \mathsf{t} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \quad 1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$
$$\mathsf{f} = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \quad \mathsf{g} = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \quad \mathsf{c} = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

and define $\mathbb{T} = (\top, \top)$. Then $(c, \top)$ admits nine different (s, s)-decompositions.

$$(c, \top) = \mathbb{T} \Cap \mathbb{T} \Cap ((\mathsf{f}, \top) \oplus (\mathsf{g}, \top)) \tag{4.12}$$
$$(c, \top) = \mathbb{T} \Cap \mathbb{T} \Cap ((\mathsf{f}, \mathsf{s}) \oplus (\mathsf{g}, \mathsf{t})) \tag{4.13}$$
$$(c, \top) = \mathbb{T} \Cap \mathbb{T} \Cap ((\mathsf{f}, \mathsf{t}) \oplus (\mathsf{g}, \mathsf{s})) \tag{4.14}$$
$$(c, \top) = \mathbb{T} \Cap \mathbb{T} \Cap ((\mathsf{f}, \mathsf{s}) \oplus (\mathsf{g}, \top)) \tag{4.15}$$
$$(c, \top) = \mathbb{T} \Cap \mathbb{T} \Cap ((\mathsf{f}, \mathsf{t}) \oplus (\mathsf{g}, \top)) \tag{4.16}$$
$$(c, \top) = \mathbb{T} \Cap \mathbb{T} \Cap ((\mathsf{f}, \top) \oplus (\mathsf{g}, \mathsf{s})) \tag{4.17}$$
$$(c, \top) = \mathbb{T} \Cap \mathbb{T} \Cap ((\mathsf{f}, \top) \oplus (\mathsf{g}, \mathsf{t})) \tag{4.18}$$
$$(c, \top) = \mathbb{T} \Cap \mathbb{T} \Cap ((\mathsf{f}, 1) \oplus (\mathsf{g}, \top)) \tag{4.19}$$
$$(c, \top) = \mathbb{T} \Cap \mathbb{T} \Cap ((\mathsf{f}, \top) \oplus (\mathsf{g}, 1)) \tag{4.20}$$

Lemma 4.11 is going to be used in Section 6.1 in order to give a possible semantics for DAD-⊓ containing nondecomposable elements.

- Do the decomposable elements of a DAD-⊓ $\mathcal{A}$ together with the demonic operators form a subalgebra of $\mathcal{A}$?

  The answer is no and here is a counter-example. Go back to Example 4.12. It is easy to see that the elements (f, s) and (g, t) are (s, s)-decomposable, because

  $$\begin{aligned} (\mathsf{f}, \mathsf{s}) &= (\mathsf{f}, \mathsf{s}) \Cap \mathbb{T} \Cap (\mathbb{T} \oplus \mathbb{T}) \\ (\mathsf{g}, \mathsf{t}) &= \mathbb{T} \Cap (\mathsf{g}, \mathsf{t}) \Cap (\mathbb{T} \oplus \mathbb{T}) \end{aligned}$$

  since

  $$\begin{aligned} (\mathsf{f}, \mathsf{s}) &= (\mathsf{f}, \mathsf{s}) \odot (\mathsf{s}, \mathsf{s}) \\ (\mathsf{g}, \mathsf{t}) &= (\mathsf{g}, \mathsf{t}) \odot \overline{(\mathsf{s}, \mathsf{s})} \ . \end{aligned}$$

  For the same reason, (f, s) and (g, t) are (t, t)-decomposable. Also, (f, s) and (g, t) are $(1, 1)$-decomposable and $\mathbb{T}$-decomposable by Remark 4.9. Therefore, (f, s) and (g, t) are decomposable.

  However, $(\mathsf{f}, \mathsf{s}) \oplus (\mathsf{g}, \mathsf{t})$ has two possible (s, s)-decompositions (see (4.13) and (4.14)):

  $$\begin{aligned} (\mathsf{f}, \mathsf{s}) \oplus (\mathsf{g}, \mathsf{t}) &= (\mathsf{c}, \top) = \mathbb{T} \Cap \mathbb{T} \Cap ((\mathsf{f}, \mathsf{s}) \oplus (\mathsf{g}, \mathsf{t})) \\ (\mathsf{f}, \mathsf{s}) \oplus (\mathsf{g}, \mathsf{t}) &= (\mathsf{c}, \top) = \mathbb{T} \Cap \mathbb{T} \Cap ((\mathsf{f}, \mathsf{t}) \oplus (\mathsf{g}, \mathsf{s})) \ . \end{aligned}$$

  So $(\mathsf{f}, \mathsf{s}) \oplus (\mathsf{g}, \mathsf{t})$ is not decomposable, while (f, s) and (g, t) are.

- Therefore, are there maximal subalgebras of decomposable elements?

  Fortunately, the answer is yes. It is the subject of the following proposition.

Proposition 4.13 (Maximal subalgebra of decomposable elements)**.** *Let $\mathcal{A}$ be a DAD-⍈. There is a maximal subalgebra (not necessarily unique) of decomposable elements containing* $\mathsf{test}(A)$*.*

The proof of Proposition 4.13 involves Zorn's Lemma (which is equivalent to the axiom of choice, see [Jec73]) and here is how it reads.

Lemma 4.14 (Zorn's Lemma)**.** *Every non-empty partially ordered set in which every chain has an upper bound contains at least one maximal element.*

Now let us prove Proposition 4.13. To ease the presentation of the proof, we make no distinction between a DAD-⍈ and its carrier set.
Proof : Consider

$$E = \{I : \wp(A) \mid \mathsf{test}(A) \subseteq I \wedge I \text{ is a subalgebra of decomposable elements}\} \ .$$

Since all tests are decomposable (see (4.11)), $\mathsf{test}(A) \in E$ so E is not empty. Trivially, E is partially ordered by inclusion.

Let $C \subseteq E$ be a chain. We will demonstrate that

$$I_C = \bigcup_{I \in C} I$$

is an upper bound for C. Then, by Zorn's Lemma, the proof is done.

Take $x, y, t \in I_C$. There are $I', I'', I''' \in C$ such that $x \in I'$, $y \in I''$ and $t \in I'''$. Without loss of generality, $I' \subseteq I'' \subseteq I'''$ so $x, y, t \in I'''$. Then, since I''' is a subalgebra of decomposable elements, $x \boxplus y$, $x \boxdot y$, $x^\times$ and $x \boxplus_t y$ are decomposable and belong to I''' and thus to I_C. Since, for all $I \in C$, $\mathsf{test}(A) \subseteq I$, then $\mathsf{test}(A) \subseteq I_C$. Therefore, I_C is an upper bound for C. □

That proposition brings back confidence in the concept of decomposition. Indeed, considering any DAD-⍈ $\mathcal{A}$, Proposition 4.13 guarantees that there is a part of $\mathcal{A}$ containing $\mathsf{test}(A)$ that is a subalgebra of decomposable elements. If $\mathcal{A}$ is itself a subalgebra of decomposable elements containing $\mathsf{test}(A)$, then we say that $\mathcal{A}$ is an algebra of decomposable elements.

Definition 4.15 (Algebra of decomposable elements)**.** *A DAD-⍈ $\mathcal{A}$ is an* algebra of decomposable elements *if x is decomposable for all $x \in A$.*

In Section 4.4, we will consider algebras of decomposable elements and study many of their properties. In Section 4.5, we will show that the elements of an algebra of decomposable elements together with the angelic operators defined in Sections 4.1, 4.2 and 4.3 form a KAD. In Chapter 5, we will demonstrate that this result of Section 4.5 can only be valid within algebras of decomposable elements. We will also demonstrate that all KAD-based DAD-⍈s are algebras of decomposable elements.

We are now ready to define angelic composition.

Definition 4.16 (Angelic composition)**.** *Let x and y be elements of a DAD-$\boldsymbol{\sqcap}$ such that x is $\sqcap y$-decomposable. The* angelic composition $x \cdot_D y$ *is defined by*

$$x \cdot_D y = x \sqcup y \sqcap x_{\sqcap y} \sqcup y \ .$$

Proposition 4.17. *Let x, y, z be elements of a DAD-$\boldsymbol{\sqcap}$ $\mathcal{A}$. Then*

1. $1 \cdot_D x = x \cdot_D 1 = x$,
2. $\top \cdot_D x = x \cdot_D \top = \top$,
3. $t \cdot_D x = t \sqcup x$,
4. $\sqcap y = 1 \implies x \cdot_D y = x \sqcup y$.
5. *If x is $\sqcap y$-decomposable, then* $\sqcap(x \cdot_D y) = \sqcap x \sqcup \neg \sqcap (x \sqcup \neg \sqcap y)$.
6. *If x is $\sqcap y$-decomposable and $\sqcap(y \cdot_D z)$-decomposable, y is $\sqcap z$-decomposable and $x \cdot_D y$ is $\sqcap z$-decomposable, then* $\sqcap(x \cdot_D (y \cdot_D z)) = \sqcap((x \cdot_D y) \cdot_D z)$.
7. *If x is $\sqcap y$-decomposable, then* $x \cdot_D y = (x \sqcup \sqcap y \sqcap x_{\sqcap y}) \sqcup y$.

The hypotheses of Propositions 4.17-5, 4.17-6 and 4.17-7 ensure that each angelic composition involved is well defined. There is no need for such assumptions for Propositions 4.17-1, 4.17-2, 4.17-3 and 4.17-4 since all tests are decomposable by (4.11) and any element is 1-decomposable and $\top$-decomposable by Remark 4.9.

These comments illustrate how careful one must be when dealing with angelic composition. However, in further sections, when decomposition is involved, we will suppose that A is an algebra of decomposable elements. Therefore, all angelic compositions will be well defined.

Proof :

1.
$$\begin{aligned} & 1 \cdot_D x \\ = & \qquad \langle \text{ by Definition 4.16 } \rangle \\ & 1 \sqcup x \sqcap 1_{\sqcap x} \sqcup x \\ = & \qquad \langle \text{ by (4.11) } \rangle \\ & 1 \sqcup x \sqcap \top \sqcup x \end{aligned}$$

$=$ ⟨ by (3.7), (3.6) and Corollary 3.21-3 ⟩

x

$=$ ⟨ by (3.7) and Corollary 3.21-3 ⟩

$x \circ 1 \mathbin{\square} \top \circ 1$

$=$ ⟨ by Remark 4.9 and Proposition 3.14-1 ⟩

$x \circ 1 \mathbin{\square} x_{\lceil 1 \rceil} \circ 1$

$=$ ⟨ by Definition 4.16 ⟩

$x \mathrel{\triangleright_D} 1$

2. $\top \mathrel{\triangleright_D} x$

$=$ ⟨ by Definition 4.16 ⟩

$\top \circ x \mathbin{\square} \top_{\lceil x \rceil} \circ x$

$=$ ⟨ by (4.11) ⟩

$\top \circ x \mathbin{\square} \top \circ x$

$=$ ⟨ by (3.6) and Corollary 3.21-11 ⟩

$\top$

$=$ ⟨ by (3.6) and Corollary 3.21-11 ⟩

$x \circ \top \mathbin{\square} \top \circ \top$

$=$ ⟨ by Remark 4.9 and Proposition 3.14-1 ⟩

$x \circ \top \mathbin{\square} x_{\lceil \top \rceil} \circ \top$

$=$ ⟨ by Definition 4.16 ⟩

$x \mathrel{\triangleright_D} \top$

3. $t \mathrel{\triangleright_D} x$

$=$ ⟨ by Definition 4.16 ⟩

$t \circ x \mathbin{\square} t_{\lceil x \rceil} \circ x$

$=$ ⟨ by (4.11) ⟩

$t \circ x \mathbin{\square} \top \circ x$

$=$ ⟨ by (3.6) and Corollary 3.21-3 ⟩

$t \circ x$

4. Suppose $\lceil y = 1$

$x \mathrel{\triangleright_D} y$

$$
\begin{aligned}
= & \quad \langle \text{ by Definition 4.16, the hypothesis and Remark 4.9 } \rangle \\
& x \square y \sqcap x_1 \square y \\
= & \quad \langle \text{ by Remark 4.9 } \rangle \\
& x \square y \sqcap \top \square y \\
= & \quad \langle \text{ by (3.6) and Corollary 3.21-3 } \rangle \\
& x \square y
\end{aligned}
$$

5. Suppose x is $\ulcorner y$-decomposable.

$$
\begin{aligned}
& \ulcorner(x \cdot_D y) \\
= & \quad \langle \text{ by Definition 4.16, Corollary 3.21-16 and (3.20) } \rangle \\
& \ulcorner(x \square \ulcorner y) \sqcap \ulcorner(x_{\ulcorner y} \square \ulcorner y) \\
= & \quad \langle \text{ by (4.5) with } x, t := x, \ulcorner y \ \rangle \\
& \ulcorner(x \square \ulcorner y) \sqcap \ulcorner(x_{\ulcorner y}) \\
= & \quad \langle \text{ by (4.4) with } x, t := x, \ulcorner y \ \rangle \\
& \ulcorner(x \square \ulcorner y) \sqcap \neg\ulcorner(x \square \ulcorner y) \square \neg\ulcorner(x \square \neg\ulcorner y) \square \ulcorner x \\
= & \quad \langle \text{ by Boolean algebra } \rangle \\
& \ulcorner(x \square \ulcorner y) \sqcap \neg\ulcorner(x \square \neg\ulcorner y) \square \ulcorner x \\
= & \quad \langle \text{ by Boolean algebra, Lemma 3.17-5 and Proposition 3.14-18,} \\
& \quad\ \ \neg\ulcorner(x \square \neg\ulcorner y) \square \ulcorner x \sqsubseteq \ulcorner(x \square \ulcorner y) \iff \\
& \quad\ \ \neg\ulcorner(x \square \neg\ulcorner y) \sqsubseteq \ulcorner(x \square \ulcorner y) \wedge \ulcorner x \sqsubseteq \ulcorner(x \square \ulcorner y) \iff \mathsf{true}, \\
& \quad\ \ \text{then apply Boolean algebra } \rangle \\
& \ulcorner x \square \neg\ulcorner(x \square \neg\ulcorner y)
\end{aligned}
$$

6. Suppose x is $\ulcorner y$-decomposable and $\ulcorner(y \cdot_D z)$-decomposable, y is $\ulcorner z$-decomposable and $x \cdot_D y$ is $\ulcorner z$-decomposable.

$$
\begin{aligned}
& \ulcorner(x \cdot_D (y \cdot_D z)) \\
= & \quad \langle \text{ by Proposition 4.17-5 } \rangle \\
& \ulcorner x \square \neg\ulcorner(x \square \neg(\ulcorner y \square \neg\ulcorner(y \square \neg\ulcorner z))) \\
= & \quad \langle \text{ by De Morgan } \rangle \\
& \ulcorner x \square \neg\ulcorner(x \square (\neg\ulcorner y \sqcap \ulcorner(y \square \neg\ulcorner z))) \\
= & \quad \langle \text{ by (4.3) with } x, t := x, \ulcorner y \ \rangle \\
& \ulcorner x \square \neg\ulcorner((x \square \ulcorner y \sqcap x \square \neg\ulcorner y \sqcap (x_{\ulcorner y} \sqcup x_{\neg\ulcorner y})) \square (\neg\ulcorner y \sqcap \ulcorner(y \square \neg\ulcorner z)))
\end{aligned}
$$

$$
\begin{array}{ll}
= & \langle \text{ by Corollary 3.21-17 and Remark 4.8 } \rangle \\
& \lceil x \rceil \cdot \neg \lceil \neg \lceil y \rceil \sqcap \lceil y \cdot \neg \lceil z \rceil \rceil \sqcap x \cdot \neg \lceil y \cdot \neg \lceil \neg \lceil y \rceil \sqcap \lceil y \cdot \neg \lceil z \rceil \rceil \sqcap \\
& \qquad (x_{\lceil y \rceil} \sqcup x_{\neg \lceil y \rceil}) \cdot (\neg \lceil y \rceil \sqcap \lceil y \cdot \neg \lceil z \rceil)) \\
= & \langle \text{ by Corollaries 3.21-8 and 3.21-7, and Boolean algebra } \rangle \\
& \lceil x \rceil \cdot \neg \lceil x \cdot \lceil y \rceil \cdot \lceil y \cdot \neg \lceil z \rceil \rceil \sqcap x \cdot \neg \lceil y \rceil \sqcap (x_{\lceil y \rceil} \sqcup x_{\neg \lceil y \rceil}) \cdot (\neg \lceil y \rceil \sqcap \lceil y \cdot \neg \lceil z \rceil)) \\
= & \langle \text{ by Proposition 3.14-18 and Boolean algebra } \rangle \\
& \lceil x \rceil \cdot \neg \lceil x \cdot \lceil y \cdot \neg \lceil z \rceil \rceil \sqcap x \cdot \neg \lceil y \rceil \sqcap (x_{\lceil y \rceil} \sqcup x_{\neg \lceil y \rceil}) \cdot (\neg \lceil y \rceil \sqcap \lceil y \cdot \neg \lceil z \rceil)) \\
= & \langle \text{ by Corollary 3.21-16 and (3.20) } \rangle \\
& \lceil x \rceil \cdot \neg \lceil x \cdot y \cdot \neg \lceil z \rceil \sqcap x \cdot \neg \lceil y \rceil \sqcap (x_{\lceil y \rceil} \sqcup x_{\neg \lceil y \rceil}) \cdot (\neg \lceil y \rceil \sqcap \lceil y \cdot \neg \lceil z \rceil)) \\
= & \langle \text{ by (4.5) with } x, t := x, \lceil y \rceil, \text{ (4.6) with } x, t := x, \lceil y \rceil \text{ and (3.9) } \rangle \\
& \lceil x \rceil \cdot \neg \lceil x \cdot y \cdot \neg \lceil z \rceil \sqcap x \cdot \neg \lceil y \rceil \sqcap \\
& \qquad (x_{\lceil y \rceil} \cdot \lceil y \rceil \cdot (\neg \lceil y \rceil \sqcap \lceil y \cdot \neg \lceil z \rceil) \sqcup x_{\neg \lceil y \rceil} \cdot \neg \lceil y \rceil \cdot (\neg \lceil y \rceil \sqcap \lceil y \cdot \neg \lceil z \rceil))) \\
= & \langle \text{ by Corollaries 3.21-8 and 3.21-7, and Boolean algebra } \rangle \\
& \lceil x \rceil \cdot \neg \lceil x \cdot y \cdot \neg \lceil z \rceil \sqcap x \cdot \neg \lceil y \rceil \sqcap (x_{\lceil y \rceil} \cdot \lceil y \rceil \cdot \lceil y \cdot \neg \lceil z \rceil \sqcup x_{\neg \lceil y \rceil} \cdot \neg \lceil y \rceil)) \\
= & \langle \text{ by Proposition 3.14-18 and (4.6) with } x, t := x, \lceil y \rceil \rangle \\
& \lceil x \rceil \cdot \neg \lceil x \cdot y \cdot \neg \lceil z \rceil \sqcap x \cdot \neg \lceil y \rceil \sqcap (x_{\lceil y \rceil} \cdot \lceil y \cdot \neg \lceil z \rceil \sqcup x_{\neg \lceil y \rceil})) \\
= & \langle \text{ by Corollary 3.21-16 and (3.21) } \rangle \\
& \lceil x \rceil \cdot \neg (\lceil x \cdot y \cdot \neg \lceil z \rceil \rceil \sqcap \lceil x \cdot \neg \lceil y \rceil \rceil \sqcap (\lceil x_{\lceil y \rceil} \cdot \lceil y \cdot \neg \lceil z \rceil \rceil \sqcup \lceil x_{\neg \lceil y \rceil} \rceil)) \\
= & \langle \text{ by (4.4) with } x, t := x, \lceil y \rceil \text{ and Proposition 3.14-18,} \\
& \qquad \lceil x_{\neg \lceil y \rceil} \rceil = \lceil x_{\lceil y \rceil} \rceil \sqsubseteq \lceil x_{\lceil y \rceil} \cdot \lceil y \cdot \neg \lceil z \rceil \rceil \rangle \\
& \lceil x \rceil \cdot \neg (\lceil x \cdot y \cdot \neg \lceil z \rceil \rceil \sqcap \lceil x \cdot \neg \lceil y \rceil \rceil \sqcap \lceil x_{\lceil y \rceil} \cdot \lceil y \cdot \neg \lceil z \rceil \rceil) \\
= & \langle \text{ by Boolean algebra and (3.20) } \rangle \\
& \lceil x \rceil \cdot \neg \lceil x \cdot \neg \lceil y \rceil \rceil \cdot \neg \lceil x \cdot y \cdot \neg \lceil z \rceil \rceil \cdot \neg \lceil x_{\lceil y \rceil} \cdot y \cdot \neg \lceil z \rceil \\
= & \langle \text{ by Boolean algebra and Corollary 3.21-16 } \rangle \\
& \lceil x \rceil \cdot \neg \lceil x \cdot \neg \lceil y \rceil \rceil \cdot \neg \lceil x \cdot y \cdot \neg \lceil z \rceil \sqcap x_{\lceil y \rceil} \cdot y \cdot \neg \lceil z \rceil \\
= & \langle \text{ by Corollary 3.21-17 and Remark 4.8 } \rangle \\
& \lceil x \rceil \cdot \neg \lceil x \cdot \neg \lceil y \rceil \rceil \cdot \neg \lceil (x \cdot y \sqcap x_{\lceil y \rceil} \cdot y) \cdot \neg \lceil z \rceil \\
= & \langle \text{ by Proposition 4.17-5 and Definition 4.16 } \rangle \\
& \lceil (x \mathbin{;_D} y) \mathbin{;_D} z \rceil
\end{array}
$$

7. Suppose x is $\lceil y \rceil$-decomposable.

$$
\begin{array}{ll}
& x \mathbin{;_D} y
\end{array}
$$

$$
\begin{aligned}
&= && \langle \text{ by Definition 4.16 } \rangle \\
&x \mathbin{\square} y \mathbin{⨅} x_{\overline{\top}_y} \mathbin{\square} y \\
&= && \langle \text{ by Proposition 3.14-7 } \rangle \\
&x \mathbin{\square} \overline{\top} y \mathbin{\square} y \mathbin{⨅} x_{\overline{\top}_y} \mathbin{\square} y \\
&= && \langle \text{ by Remark 4.8 and Corollary 3.21-17 } \rangle \\
&(x \mathbin{\square} \overline{\top} y \mathbin{⨅} x_{\overline{\top}_y}) \mathbin{\square} y
\end{aligned}
$$

□

Knowing the main result we are looking for (refer to Section 1.3), one would expect us to demonstrate the associativity of $\cdot_D$ and its distributivity over $+_D$. We postpone these demonstrations and many others until Section 4.5 since we need more properties about decomposition before being able to get these results. These properties about decomposition are gathered in Section 4.4.

Remark 4.18. By Definition 2.8 and Proposition 2.13-4,

$$\ulcorner(x \mathbin{\square_A} y) = \ulcorner x \cdot \neg \ulcorner(x \cdot \neg \ulcorner y) \ .$$

Comparing this expression with the one given in Proposition 4.17-5, namely

$$\overline{\top}(x \mathbin{\cdot_D} y) = \overline{\top} x \mathbin{\square} \neg \overline{\top}(x \mathbin{\square} \neg \overline{\top} y) \ ,$$

reveals a nice duality.

4.3 Kleene Star

The last angelic operator that we define here is the *angelic iteration operator* that corresponds to the Kleene star.

Definition 4.19 (Angelic iteration operator)**.** *Let x be an element of a DAD-⨅. The* angelic iteration operator ^{*_D} *is defined by*

$$x^{*_D} = (x \mathbin{⨅} 1)^{\times} \ .$$

The following laws are technical results needed in Section 4.5.

Lemma 4.20. *Let $\mathcal{A}$ be a DAD-⨅. The following laws hold for all $x, y \in A$.*

1. $\top(x^{*_D}) = \top((x \barwedge 1)^\times) = 1$
2. $\top(1 \sqcup x \circ (x \barwedge 1)^\times) = \top x$
3. $\top y \sqsubseteq \top((x \barwedge 1)^\times \circ y)$

PROOF :

1. $\top(x \barwedge 1)$
   $=$ ⟨ by Corollary 3.21-16 ⟩
   $\top x \barwedge \top 1$
   $=$ ⟨ by Proposition 3.14-1 and Boolean algebra ⟩
   1

   So $\top(x^{*_D}) = \top((x \barwedge 1)^\times) = 1$ by Definition 4.19 and Proposition 3.14-22.

2. $\top(1 \sqcup x \circ (x \barwedge 1)^\times)$
   $=$ ⟨ by (3.21), Proposition 3.14-1 and (3.20) ⟩
   $1 \sqcup \top(x \circ \top((x \barwedge 1)^\times))$
   $=$ ⟨ by Boolean algebra, Lemma 4.20-1 and (3.7) ⟩
   $\top x$

3. By (3.7) and Proposition 3.3-1, $\top y = \top(1 \circ y) \sqsubseteq \top((x \barwedge 1)^\times \circ y)$. □

Major results about the ^{*_D} operator will be presented in Section 4.5. As for the $\cdot_D$ operator, the proof of these results requires many properties about decomposition that are presented in Section 4.4.

4.4 Crucial Identities

In this section, we present many properties about t-decomposition. Without them, it would be highly difficult, if not impossible, to demonstrate the main theorem of Section 4.5 stating that, under a suitable hypothesis, the definition of $+_D$, $\cdot_D$ and ^{*_D} lead to angelic operators that satisfy the laws of KAD. We already mentioned in the introduction of Chapter 4 that this theorem is one of the most important of this thesis. The *suitable hypothesis* previously mentioned is that the algebra $\mathcal{A}$ must be an algebra of

decomposable elements. In Chapter 5, it will be shown that this hypothesis is necessary and sufficient.

We spread the results among three theorems and several intermediate results. Theorems 4.23, 4.27 and 4.29 respectively give algebraic expressions for $(x \sqcup y)_t$, $(x \boxdot y)_t$ and $(x \barwedge_u y)_t$. The other results of the section are meant to facilitate the demonstration of Theorems 4.23, 4.27 and 4.29, and to help for the demonstration of the results of Section 4.5. Note that we do not give any algebraic expression for $(x^\times)_t$ since it is not necessary for the demonstrations to come. Also, we did not find any compact expression for it.

In this section, the proofs involve new ideas and illustrate how the theory developped until now can be used. Although the results are easy to understand, some proofs are long while others are subtle. For these reasons, at first reading, one might just concentrate on results rather than verify all the details of each demonstration.

Let us present a general scheme of argumentation that will be used throughout this section. As mentioned previously, this section deals with t-decomposition. Therefore, Definition 4.7 is involved in many derivations. Let $\mathcal{A}$ be a DAD-$\barwedge$ and take $x \in A$ and $t \in \mathsf{test}(A)$. Suppose we have to demonstrate $y = x_t$ and $z = x_{\neg t}$ for some $y, z \in A$. According to Definition 4.7, we have to establish

$$\begin{aligned} x &= x \boxdot t \barwedge x \boxdot \neg t \barwedge (y \sqcup z) \ , \\ \tilde{\neg} y &= \tilde{\neg} z = \neg\tilde{\neg}(x \boxdot t) \boxdot \neg\tilde{\neg}(x \boxdot \neg t) \boxdot \tilde{\neg} x \ , \\ y &= y \boxdot t \ , \\ z &= z \boxdot \neg t \ . \end{aligned}$$

In such a situation (Proposition 4.22-4 for example), we will say that *we have to show that y and z satisfy (4.3), (4.4), (4.5) and (4.6).* Once we have established these previous four equalities, we can conclude that $y = x_t$ and $z = x_{\neg t}$ since the t-decomposition of x is unique (see Definition 4.7).

Remark 4.21. If we succeed in proving that y and z satisfy (4.4), there is a way to simplify the proof that y and z satisfy (4.3). Indeed, suppose y and z satisfy (4.4).

$$\begin{aligned} & x = x \boxdot t \barwedge x \boxdot \neg t \barwedge (y \sqcup z) \\ \iff & \qquad \langle \text{ by Proposition 3.20-17 and Corollary 3.21-4 } \rangle \\ & \tilde{\neg}(x_t) \boxdot x = \tilde{\neg}(x_t) \boxdot x \boxdot t \barwedge \tilde{\neg}(x_t) \boxdot x \boxdot \neg t \barwedge \tilde{\neg}(x_t) \boxdot (y \sqcup z) \ \wedge \\ & \neg\tilde{\neg}(x_t) \boxdot x = \neg\tilde{\neg}(x_t) \boxdot x \boxdot t \barwedge \neg\tilde{\neg}(x_t) \boxdot x \boxdot \neg t \barwedge \neg\tilde{\neg}(x_t) \boxdot (y \sqcup z) \end{aligned}$$

$$
\begin{array}{ll}
\iff & \langle \text{ by Proposition 3.14-7, the hypothesis, (3.8), Remark 4.8 and (3.6) } \rangle \\
& \pi(x_t)\cdot x = \top \sqcap \top \sqcap (y \sqcup z) \ \wedge \ \neg\pi(x_t)\cdot x = \neg\pi(x_t)\cdot x\cdot t \sqcap \neg\pi(x_t)\cdot x\cdot\neg t \sqcap \top \\
\iff & \langle \text{ by Corollary 3.21-3 } \rangle \\
& \pi(x_t)\cdot x = y \sqcup z \ \wedge \ \neg\pi(x_t)\cdot x = \neg\pi(x_t)\cdot x\cdot t \sqcap \neg\pi(x_t)\cdot x\cdot\neg t \\
\iff & \langle \text{ by Proposition 3.14-7, (4.4), De Morgan and Boolean algebra } \rangle \\
& \pi(x_t)\cdot x = y \sqcup z \ \wedge \ (\pi(x\cdot t) \sqcap \pi(x\cdot\neg t))\cdot x = x\cdot t \sqcap x\cdot\neg t \\
\iff & \langle \text{ by Lemma 3.17-4, Corollary 3.21-17 and (3.19) } \rangle \\
& \pi(x_t)\cdot x = y \sqcup z
\end{array}
$$

At some places (Proposition 4.25 for example), when we need to show that y and z satisfy (4.3), we will rather work on $\pi(x_t)\cdot x = y \sqcup z$.

The following laws are useful in what comes next.

Proposition 4.22. *If $\mathcal{A}$ is an algebra of decomposable elements, then the following equalities are valid for all $x, y, z \in A$ and all $s, t \in \mathsf{test}(A)$.*

1. $x\cdot(y \sqcap z) = x\cdot y \sqcap x\cdot\neg\pi y\cdot z \sqcap (x_{\pi y}\cdot y \sqcup x_{\neg\pi y}\cdot z)$
2. $\pi(x_t)\cdot x = x_t \sqcup x_{\neg t}$
3. $\pi(x_t)\cdot x\cdot t = \top$
4. $(x\cdot s)_t = \pi(x\cdot s)\cdot x_t$
5. $(s\cdot x)_t = s\cdot x_t$
6. $\pi(x\cdot s)\cdot x_t\cdot s = \pi(x\cdot s)\cdot x_t$
7. $(x_s)_t\cdot s = (x_s)_t$
8. $\pi(x_s\cdot t) = \pi(x_s)\cdot\pi(x\cdot(\neg s \sqcap t))$
9. $\pi(x_s\cdot t) = \neg\pi(x\cdot s\cdot t)\cdot\neg\pi(x\cdot\neg s)\cdot\pi(x\cdot(\neg s \sqcap t))$
10. $\pi((x_s)_t) = \neg\pi(x\cdot(\neg s \sqcap t))\cdot\neg\pi(x\cdot(\neg s \sqcap \neg t))\cdot\neg\pi(x\cdot s)\cdot\pi x$

Proof :

1. $x \mathbin{\square} (y \mathbin{\sqcap} z)$

   $=$ $\langle$ by (4.3) with $x, t := x, \Gamma y$ $\rangle$

   $(x \mathbin{\square} \Gamma y \mathbin{\sqcap} x \mathbin{\square} \neg \Gamma y \mathbin{\sqcap} (x_{\Gamma y} \sqcup x_{\neg \Gamma y})) \mathbin{\square} (y \mathbin{\sqcap} z)$

   $=$ $\langle$ by Remark 4.8, Corollary 3.21-17 and (3.9) $\rangle$

   $x \mathbin{\square} \Gamma y \mathbin{\square} (y \mathbin{\sqcap} z) \mathbin{\sqcap} x \mathbin{\square} \neg \Gamma y \mathbin{\square} (y \mathbin{\sqcap} z) \mathbin{\sqcap} (x_{\Gamma y} \mathbin{\square} (y \mathbin{\sqcap} z) \sqcup x_{\neg \Gamma y} \mathbin{\square} (y \mathbin{\sqcap} z))$

   $=$ $\langle$ by Corollaries 3.21-7 and 3.21-8, (4.5) with $x, t := x, \Gamma y$, (4.6) with $x, t := x, \Gamma y$ and Proposition 3.14-7 $\rangle$

   $x \mathbin{\square} y \mathbin{\sqcap} x \mathbin{\square} \neg \Gamma y \mathbin{\square} z \mathbin{\sqcap} (x_{\Gamma y} \mathbin{\square} y \sqcup x_{\neg \Gamma y} \mathbin{\square} z)$

2. $\Gamma(x_t) \mathbin{\square} x$

   $=$ $\langle$ by (4.3) $\rangle$

   $\Gamma(x_t) \mathbin{\square} (x \mathbin{\square} t \mathbin{\sqcap} x \mathbin{\square} \neg t \mathbin{\sqcap} (x_t \sqcup x_{\neg t}))$

   $=$ $\langle$ by Corollary 3.21-4, Proposition 3.14-7, Remark 4.8, Boolean algebra and (3.6) $\rangle$

   $(\top \mathbin{\sqcap} \top \mathbin{\sqcap} \Gamma(x_t) \mathbin{\square} (x_t \sqcup x_{\neg t}))$

   $=$ $\langle$ by Corollary 3.21-3 $\rangle$

   $\Gamma(x_t) \mathbin{\square} (x_t \sqcup x_{\neg t})$

   $=$ $\langle$ by Propositions 3.14-20 and 3.14-7 $\rangle$

   $x_t \sqcup x_{\neg t}$

3. This is direct from Proposition 3.14-7, Remark 4.8, Boolean algebra and (3.6).

4. We have to show that $\Gamma(x \mathbin{\square} s) \mathbin{\square} x_t$ and $\Gamma(x \mathbin{\square} s) \mathbin{\square} x_{\neg t}$ satisfy (4.3), (4.4), (4.5) and (4.6) with $x, t := x \mathbin{\square} s, t$ (see Definition 4.7).

   (4.5) and (4.6) are easily obtained from (4.5) and (4.6) with $x, t := x, t$.

   Here is the proof for (4.4). First note that

   $\Gamma(\Gamma(x \mathbin{\square} s) \mathbin{\square} x_t)$

   $=$ $\langle$ by Proposition 3.14-9 $\rangle$

   $\Gamma(x \mathbin{\square} s) \mathbin{\square} \Gamma(x_t)$

   $=$ $\langle$ by (4.4) $\rangle$

   $\Gamma(x \mathbin{\square} s) \mathbin{\square} \Gamma(x_{\neg t})$

   $=$ $\langle$ by Proposition 3.14-9 $\rangle$

   $\Gamma(\Gamma(x \mathbin{\square} s) \mathbin{\square} x_{\neg t})$.

   And here is the main derivation.

$$
\begin{array}{ll}
& \Pi(\Pi(x \triangleright s) \triangleright x_t) \\
= & \qquad \langle \text{ by Proposition 3.14-9 and (4.4) } \rangle \\
& \Pi(x \triangleright s) \triangleright \neg \Pi(x \triangleright t) \triangleright \neg \Pi(x \triangleright \neg t) \triangleright \Pi x \\
= & \qquad \langle \text{ by Boolean algebra and Lemma 3.17-1 } \rangle \\
& \neg \Pi(x \triangleright t) \triangleright \neg \Pi(x \triangleright \neg t) \triangleright \Pi(x \triangleright s) \\
= & \qquad \langle \text{ by Boolean algebra } \rangle \\
& (\neg \Pi(x \triangleright s) \sqcap \neg \Pi(x \triangleright t)) \triangleright (\neg \Pi(x \triangleright s) \sqcap \neg \Pi(x \triangleright \neg t)) \triangleright \Pi(x \triangleright s) \\
= & \qquad \langle \text{ by De Morgan } \rangle \\
& \neg(\Pi(x \triangleright s) \triangleright \Pi(x \triangleright t)) \triangleright \neg(\Pi(x \triangleright s) \triangleright \Pi(x \triangleright \neg t)) \triangleright \Pi(x \triangleright s) \\
= & \qquad \langle \text{ by Proposition 3.14-12 } \rangle \\
& \neg \Pi(x \triangleright s \triangleright t) \triangleright \neg \Pi(x \triangleright s \triangleright \neg t) \triangleright \Pi(x \triangleright s) \\
= & \qquad \langle \text{ by (4.4) with } x, t := x \triangleright s, t \rangle \\
& \Pi((x \triangleright s)_t)
\end{array}
$$

Finally, we conclude with the proof of (4.3).

$$
\begin{array}{ll}
& \mathsf{true} \\
\Longrightarrow & \qquad \langle \text{ by (4.3) } \rangle \\
& x = x \triangleright t \sqcap x \triangleright \neg t \sqcap (x_t \sqcup x_{\neg t}) \\
\Longrightarrow & \qquad \langle \text{ by Corollary 3.21-4 and (3.8) } \rangle \\
& \Pi(x \triangleright s) \triangleright x = \Pi(x \triangleright s) \triangleright x \triangleright t \sqcap \Pi(x \triangleright s) \triangleright x \triangleright \neg t \sqcap (\Pi(x \triangleright s) \triangleright x_t \sqcup \Pi(x \triangleright s) \triangleright x_{\neg t}) \\
\Longleftrightarrow & \qquad \langle \text{ by (3.19) } \rangle \\
& x \triangleright s = x \triangleright s \triangleright t \sqcap x \triangleright s \triangleright \neg t \sqcap (\Pi(x \triangleright s) \triangleright x_t \sqcup \Pi(x \triangleright s) \triangleright x_{\neg t})
\end{array}
$$

5. We have to show that $s \triangleright x_t$ and $s \triangleright x_{\neg t}$ satisfy (4.3), (4.4), (4.5) and (4.6) with $x, t := s \triangleright x, t$ (see Definition 4.7).

   (4.5) and (4.6) are easily obtained from (4.5) and (4.6) with $x, t := x, t$.

   Here is the proof for (4.4). First note that

$$
\begin{array}{ll}
& \Pi(s \triangleright x_t) \\
= & \qquad \langle \text{ by Proposition 3.14-9 } \rangle \\
& s \triangleright \Pi(x_t) \\
= & \qquad \langle \text{ by (4.4) } \rangle
\end{array}
$$

$$
\begin{array}{ll}
& s \mathbin{\square} \Pi(x_{\neg t}) \\
= & \qquad \langle \text{ by Proposition 3.14-9 } \rangle \\
& \Pi(s \mathbin{\square} x_{\neg t}) \ .
\end{array}
$$

And here is the main derivation.

$$
\begin{array}{ll}
& \Pi(s \mathbin{\square} x_t) \\
= & \qquad \langle \text{ by Proposition 3.14-9 } \rangle \\
& s \mathbin{\square} \Pi(x_t) \\
= & \qquad \langle \text{ by (4.4) } \rangle \\
& s \mathbin{\square} \neg \Pi(x \mathbin{\square} t) \mathbin{\square} \neg \Pi(x \mathbin{\square} \neg t) \mathbin{\square} \Pi x \\
= & \qquad \langle \text{ by Boolean algebra } \rangle \\
& (\neg s \sqcap \neg \Pi(x \mathbin{\square} t)) \mathbin{\square} (\neg s \sqcap \neg \Pi(x \mathbin{\square} \neg t)) \mathbin{\square} s \mathbin{\square} \Pi x \\
= & \qquad \langle \text{ by De Morgan } \rangle \\
& \neg(s \mathbin{\square} \Pi(x \mathbin{\square} t)) \mathbin{\square} \neg(s \mathbin{\square} \Pi(x \mathbin{\square} \neg t)) \mathbin{\square} s \mathbin{\square} \Pi x \\
= & \qquad \langle \text{ by Proposition 3.14-9 } \rangle \\
& \neg \Pi(s \mathbin{\square} x \mathbin{\square} t) \mathbin{\square} \neg \Pi(s \mathbin{\square} x \mathbin{\square} \neg t) \mathbin{\square} \Pi(s \mathbin{\square} x) \\
= & \qquad \langle \text{ by (4.4) with } x, t := s \mathbin{\square} x, t \ \rangle \\
& \Pi((s \mathbin{\square} x)_t)
\end{array}
$$

Finally, we conclude with the proof of (4.3).

$$
\begin{array}{ll}
& \mathsf{true} \\
\Longrightarrow & \qquad \langle \text{ by (4.3) } \rangle \\
& x = x \mathbin{\square} t \sqcap x \mathbin{\square} \neg t \sqcap (x_t \sqcup x_{\neg t}) \\
\Longrightarrow & \qquad \langle \text{ by Corollary 3.21-4 and (3.8) } \rangle \\
& s \mathbin{\square} x = s \mathbin{\square} x \mathbin{\square} t \sqcap s \mathbin{\square} x \mathbin{\square} \neg t \sqcap (s \mathbin{\square} x_t \sqcup s \mathbin{\square} x_{\neg t})
\end{array}
$$

6. If we demonstrate that $\Pi(x \mathbin{\square} s) \mathbin{\square} x_t \mathbin{\square} s = (x \mathbin{\square} s)_t$, then we are finished thanks to Proposition 4.22-4.

   Hence, we have to show that $\Pi(x \mathbin{\square} s) \mathbin{\square} x_t \mathbin{\square} s$ and $\Pi(x \mathbin{\square} s) \mathbin{\square} x_{\neg t} \mathbin{\square} s$ satisfy (4.3), (4.4), (4.5) and (4.6) with $x, t := x \mathbin{\square} s, t$ (see Definition 4.7).

   (4.5) and (4.6) are easily obtained from (4.5), (4.6) with $x, t := x, t$ and Boolean algebra.

   Here is the proof of (4.3).

$$
\begin{array}{ll}
& \mathsf{true} \\
\Longrightarrow & \quad \langle \text{ by (4.3) with } x,t := x \mathbin{\triangledown} s, t \rangle \\
& x \mathbin{\triangledown} s = x \mathbin{\triangledown} s \mathbin{\triangledown} t \sqcap x \mathbin{\triangledown} s \mathbin{\triangledown} \neg t \sqcap ((x \mathbin{\triangledown} s)_t \sqcup (x \mathbin{\triangledown} s)_{\neg t}) \\
\Longrightarrow & \quad \langle \text{ by Corollary 3.21-17, Remark 4.8 and (3.9)} \rangle \\
& x \mathbin{\triangledown} s \mathbin{\triangledown} s = x \mathbin{\triangledown} s \mathbin{\triangledown} t \mathbin{\triangledown} s \sqcap x \mathbin{\triangledown} s \mathbin{\triangledown} \neg t \mathbin{\triangledown} s \sqcap ((x \mathbin{\triangledown} s)_t \mathbin{\triangledown} s \sqcup (x \mathbin{\triangledown} s)_{\neg t} \mathbin{\triangledown} s) \\
\Longrightarrow & \quad \langle \text{ by Boolean algebra} \rangle \\
& x \mathbin{\triangledown} s = x \mathbin{\triangledown} s \mathbin{\triangledown} t \sqcap x \mathbin{\triangledown} s \mathbin{\triangledown} \neg t \sqcap ((x \mathbin{\triangledown} s)_t \mathbin{\triangledown} s \sqcup (x \mathbin{\triangledown} s)_{\neg t} \mathbin{\triangledown} s) \\
\Longrightarrow & \quad \langle \text{ by Proposition 4.22-4} \rangle \\
& x \mathbin{\triangledown} s = x \mathbin{\triangledown} s \mathbin{\triangledown} t \sqcap x \mathbin{\triangledown} s \mathbin{\triangledown} \neg t \sqcap (\Pi(x \mathbin{\triangledown} s) \mathbin{\triangledown} x_t \mathbin{\triangledown} s \sqcup \Pi(x \mathbin{\triangledown} s) \mathbin{\triangledown} x_{\neg t} \mathbin{\triangledown} s)
\end{array}
$$

Finally, we conclude with the proof of (4.4).

$$
\begin{array}{ll}
& \mathsf{true} \\
\Longrightarrow & \quad \langle \text{ see the last derivation} \rangle \\
& x \mathbin{\triangledown} s = x \mathbin{\triangledown} s \mathbin{\triangledown} t \sqcap x \mathbin{\triangledown} s \mathbin{\triangledown} \neg t \sqcap (\Pi(x \mathbin{\triangledown} s) \mathbin{\triangledown} x_t \mathbin{\triangledown} s \sqcup \Pi(x \mathbin{\triangledown} s) \mathbin{\triangledown} x_{\neg t} \mathbin{\triangledown} s) \\
\Longrightarrow & \quad \langle \text{ by Proposition 3.14-7, Remark 4.8, Corollary 3.21-4, Boolean} \\
& \qquad \text{algebra and (3.6)} \rangle \\
& \Pi((x \mathbin{\triangledown} s)_t) \mathbin{\triangledown} x \mathbin{\triangledown} s = \top \sqcap \top \sqcap \Pi((x \mathbin{\triangledown} s)_t) \mathbin{\triangledown} (\Pi(x \mathbin{\triangledown} s) \mathbin{\triangledown} x_t \mathbin{\triangledown} s \sqcup \Pi(x \mathbin{\triangledown} s) \mathbin{\triangledown} x_{\neg t} \mathbin{\triangledown} s) \\
\Longleftrightarrow & \quad \langle \text{ by Corollary 3.21-3} \rangle \\
& \Pi((x \mathbin{\triangledown} s)_t) \mathbin{\triangledown} x \mathbin{\triangledown} s = \Pi((x \mathbin{\triangledown} s)_t) \mathbin{\triangledown} (\Pi(x \mathbin{\triangledown} s) \mathbin{\triangledown} x_t \mathbin{\triangledown} s \sqcup \Pi(x \mathbin{\triangledown} s) \mathbin{\triangledown} x_{\neg t} \mathbin{\triangledown} s) \\
\Longrightarrow & \quad \langle \text{ by Propositions 3.14-9 and 3.14-3, and (3.21)} \rangle \\
& \Pi((x \mathbin{\triangledown} s)_t) \mathbin{\triangledown} \Pi(x \mathbin{\triangledown} s) = \Pi((x \mathbin{\triangledown} s)_t) \mathbin{\triangledown} \Pi(\Pi(x \mathbin{\triangledown} s) \mathbin{\triangledown} x_t \mathbin{\triangledown} s) \mathbin{\triangledown} \Pi(\Pi(x \mathbin{\triangledown} s) \mathbin{\triangledown} x_{\neg t} \mathbin{\triangledown} s) \\
\Longrightarrow & \quad \langle \text{ by (4.4) with } x,t := x \mathbin{\triangledown} s, t \text{ and Boolean algebra} \rangle \\
& \Pi((x \mathbin{\triangledown} s)_t) = \Pi((x \mathbin{\triangledown} s)_t) \mathbin{\triangledown} \Pi(\Pi(x \mathbin{\triangledown} s) \mathbin{\triangledown} x_t \mathbin{\triangledown} s) \mathbin{\triangledown} \Pi(\Pi(x \mathbin{\triangledown} s) \mathbin{\triangledown} x_{\neg t} \mathbin{\triangledown} s) \\
\Longrightarrow & \quad \langle \text{ by Boolean algebra} \rangle \\
& \Pi(\Pi(x \mathbin{\triangledown} s) \mathbin{\triangledown} x_t \mathbin{\triangledown} s) \mathbin{\triangledown} \Pi(\Pi(x \mathbin{\triangledown} s) \mathbin{\triangledown} x_{\neg t} \mathbin{\triangledown} s) \sqsubseteq \Pi((x \mathbin{\triangledown} s)_t)
\end{array}
$$

We note that last refinement

$$
\Pi(\Pi(x \mathbin{\triangledown} s) \mathbin{\triangledown} x_t \mathbin{\triangledown} s) \mathbin{\triangledown} \Pi(\Pi(x \mathbin{\triangledown} s) \mathbin{\triangledown} x_{\neg t} \mathbin{\triangledown} s) \sqsubseteq \Pi((x \mathbin{\triangledown} s)_t) \quad . \tag{4.21}
$$

The following derivation will establish $\Pi(\Pi(x \mathbin{\triangledown} s) \mathbin{\triangledown} x_t \mathbin{\triangledown} s) = \Pi((x \mathbin{\triangledown} s)_t)$.

$$
\Pi(\Pi(x \mathbin{\triangledown} s) \mathbin{\triangledown} x_t \mathbin{\triangledown} s)
$$

$$
\begin{array}{ll}
\sqsubseteq & \langle \text{ by Boolean algebra } \rangle \\
& \Pi(\Pi(x \sqcap s) \sqcap x_t \sqcap s) \sqcap \Pi(\Pi(x \sqcap s) \sqcap x_{\neg t} \sqcap s) \\
\sqsubseteq & \langle \text{ by (4.21) } \rangle \\
& \Pi((x \sqcap s)_t) \\
\sqsubseteq & \langle \text{ by Proposition 3.14-18 } \rangle \\
& \Pi((x \sqcap s)_t \sqcap s) \\
= & \langle \text{ by Proposition 4.22-4 } \rangle \\
& \Pi(\Pi(x \sqcap s) \sqcap x_t \sqcap s)
\end{array}
$$

Since, in the proof of (4.4), t may be replaced by $\neg t$ and $\neg t$ may be replaced by t without affecting the refinements, the proof is complete.

7. We have to show that $(x_s)_t \sqcap s$ and $(x_s)_{\neg t} \sqcap s$ satisfy (4.3), (4.4), (4.5) and (4.6) with $x, t := x_s, t$ (see Definition 4.7).

   (4.5) and (4.6) are easily obtained from (4.5), (4.6) with $x, t := x_s, t$ and Boolean algebra.

   Here is the proof for (4.3).

$$
\begin{array}{ll}
& \mathsf{true} \\
\Longrightarrow & \langle \text{ by (4.3) with } x, t := x_s, t \rangle \\
& x_s = x_s \sqcap t \sqcap x_s \sqcap \neg t \sqcap ((x_s)_t \sqcup (x_s)_{\neg t}) \\
\Longrightarrow & \langle \text{ by Corollary 3.21-17, Remark 4.8 and (3.9) } \rangle \\
& x_s \sqcap s = x_s \sqcap t \sqcap s \sqcap x_s \sqcap \neg t \sqcap s \sqcap ((x_s)_t \sqcap s \sqcup (x_s)_{\neg t} \sqcap s) \\
\Longleftrightarrow & \langle \text{ by (4.5) with } x, t := x, s \text{ and Boolean algebra } \rangle \\
& x_s = x_s \sqcap t \sqcap x_s \sqcap \neg t \sqcap ((x_s)_t \sqcap s \sqcup (x_s)_{\neg t} \sqcap s)
\end{array}
$$

   Finally, we conclude with the proof of (4.4).

$$
\begin{array}{ll}
& \mathsf{true} \\
\Longrightarrow & \langle \text{ see the last derivation } \rangle \\
& x_s = x_s \sqcap t \sqcap x_s \sqcap \neg t \sqcap ((x_s)_t \sqcap s \sqcup (x_s)_{\neg t} \sqcap s) \\
\Longrightarrow & \langle \text{ by Proposition 3.14-7, Remark 4.8, Corollary 3.21-4, Boolean} \\
& \quad \text{algebra and (3.6) } \rangle \\
& \Pi((x_s)_t) \sqcap x_s = \top \sqcap \top \sqcap \Pi((x_s)_t) \sqcap ((x_s)_t \sqcap s \sqcup (x_s)_{\neg t} \sqcap s)
\end{array}
$$

$$
\begin{array}{ll}
\iff & \langle \text{ by Corollary 3.21-3 } \rangle \\
& \top((x_s)_t) \triangleright x_s = \top((x_s)_t) \triangleright ((x_s)_t \triangleright s \sqcup (x_s)_{\neg t} \triangleright s) \\
\implies & \langle \text{ by Propositions 3.14-9 and 3.14-3, and (3.21) } \rangle \\
& \top((x_s)_t) \triangleright \top(x_s) = \top((x_s)_t) \triangleright \top((x_s)_t \triangleright s) \triangleright \top((x_s)_{\neg t} \triangleright s) \\
\iff & \langle \text{ by (4.4) with } x, t := x_s, t \text{ and Boolean algebra } \rangle \\
& \top((x_s)_t) = \top((x_s)_t) \triangleright \top((x_s)_t \triangleright s) \triangleright \top((x_s)_{\neg t} \triangleright s) \\
\implies & \langle \text{ by Boolean algebra } \rangle \\
& \top((x_s)_t \triangleright s) \triangleright \top((x_s)_{\neg t} \triangleright s) \sqsubseteq \top((x_s)_t)
\end{array}
$$

We note this last refinement

$$\top((x_s)_t \triangleright s) \triangleright \top((x_s)_{\neg t} \triangleright s) \sqsubseteq \top((x_s)_t) \ . \tag{4.22}$$

The following derivation will establish $\top((x_s)_t \triangleright s) = \top((x_s)_t)$.

$$
\begin{array}{ll}
& \top((x_s)_t \triangleright s) \\
\sqsubseteq & \langle \text{ by Boolean algebra } \rangle \\
& \top((x_s)_t \triangleright s) \triangleright \top((x_s)_{\neg t} \triangleright s) \\
\sqsubseteq & \langle \text{ by (4.22) } \rangle \\
& \top((x_s)_t) \\
\sqsubseteq & \langle \text{ by Proposition 3.14-18 } \rangle \\
& \top((x_s)_t \triangleright s)
\end{array}
$$

Since, in the proof of (4.4), t may be replaced by $\neg t$ and $\neg t$ may be replaced by t without affecting the refinements, the proof is complete.

8.
$$
\begin{array}{ll}
& \top(x_s) \triangleright \top(x \triangleright (\neg s \sqcap t)) \\
= & \langle \text{ by Proposition 3.14-9 } \rangle \\
& \top(\top(x_s) \triangleright x \triangleright (\neg s \sqcap t)) \\
= & \langle \text{ by Proposition 4.22-2 } \rangle \\
& \top((x_s \sqcup x_{\neg s}) \triangleright (\neg s \sqcap t)) \\
= & \langle \text{ by (4.5) and (4.6) with } x, t := x, s \ \rangle \\
& \top((x_s \triangleright s \sqcup x_{\neg s} \triangleright \neg s) \triangleright (\neg s \sqcap t)) \\
= & \langle \text{ by (3.9) and Boolean algebra } \rangle
\end{array}
$$

$$
\begin{array}{ll}
& \Pi(x_s \sqcap s \sqcap t \sqcup x_{\neg s} \sqcap \neg s) \\
= & \quad \langle \text{ by (4.5) and (4.6) with } x, t := x, s \ \rangle \\
& \Pi(x_s \sqcap t \sqcup x_{\neg s}) \\
= & \quad \langle \text{ by (3.21) and Proposition 3.14-3 } \rangle \\
& \Pi(x_s \sqcap t) \sqcap \Pi(x_{\neg s}) \\
= & \quad \langle \text{ by (4.4) with } x, t := x, s \ \rangle \\
& \Pi(x_s \sqcap t) \sqcap \Pi(x_s) \\
= & \quad \langle \text{ by Proposition 3.14-18 and Boolean algebra } \rangle \\
& \Pi(x_s \sqcap t)
\end{array}
$$

9.

$$
\begin{array}{ll}
& \neg\Pi(x \sqcap s \sqcap t) \sqcap \neg\Pi(x \sqcap \neg s) \sqcap \Pi(x \sqcap (\neg s \sqcap t)) \\
= & \quad \langle \text{ by Boolean algebra } \rangle \\
& \neg\Pi(x \sqcap (\neg s \sqcap t) \sqcap s) \sqcap \neg\Pi(x \sqcap (\neg s \sqcap t) \sqcap \neg s) \sqcap \Pi(x \sqcap (\neg s \sqcap t)) \\
= & \quad \langle \text{ by (4.4) with } x, t := x \sqcap (\neg s \sqcap t), s \ \rangle \\
& \Pi((x \sqcap (\neg s \sqcap t))_s) \\
= & \quad \langle \text{ by Proposition 4.22-4 } \rangle \\
& \Pi(\Pi(x \sqcap (\neg s \sqcap t)) \sqcap x_s) \\
= & \quad \langle \text{ by Proposition 3.14-9 and Boolean algebra } \rangle \\
& \Pi(x_s) \sqcap \Pi(x \sqcap (\neg s \sqcap t)) \\
= & \quad \langle \text{ by Proposition 4.22-8 } \rangle \\
& \Pi(x_s \sqcap t)
\end{array}
$$

10.

$$
\begin{array}{ll}
& \Pi((x_s)_t) \\
= & \quad \langle \text{ by (4.4) with } x, t := x_s, t \ \rangle \\
& \neg\Pi(x_s \sqcap t) \sqcap \neg\Pi(x_s \sqcap \neg t) \sqcap \Pi(x_s) \\
= & \quad \langle \text{ by Proposition 4.22-8 } \rangle \\
& \neg(\Pi(x_s) \sqcap \Pi(x \sqcap (\neg s \sqcap t))) \sqcap \neg(\Pi(x_s) \sqcap \Pi(x \sqcap (\neg s \sqcap \neg t))) \sqcap \Pi(x_s) \\
= & \quad \langle \text{ by De Morgan } \rangle \\
& (\neg\Pi(x_s) \sqcap \neg\Pi(x \sqcap (\neg s \sqcap t))) \sqcap (\neg\Pi(x_s) \sqcap \neg\Pi(x \sqcap (\neg s \sqcap \neg t))) \sqcap \Pi(x_s) \\
= & \quad \langle \text{ by Boolean algebra } \rangle \\
& \neg\Pi(x \sqcap (\neg s \sqcap t)) \sqcap \neg\Pi(x \sqcap (\neg s \sqcap \neg t)) \sqcap \Pi(x_s) \\
= & \quad \langle \text{ by (4.4) with } x, t := x, s \ \rangle
\end{array}
$$

$$\begin{array}{ll} & \neg\Pi(x\sqcap(\neg s\sqcap t))\sqcap\neg\Pi(x\sqcap(\neg s\sqcap\neg t))\sqcap\neg\Pi(x\sqcap s)\sqcap\neg\Pi(x\sqcap\neg s)\sqcap\Pi x \\ = & \qquad\langle \text{ by Lemma 3.17-6 and Boolean algebra } \rangle \\ & \neg\Pi(x\sqcap(\neg s\sqcap t))\sqcap\neg\Pi(x\sqcap(\neg s\sqcap\neg t))\sqcap\neg\Pi(x\sqcap s)\sqcap\Pi x \end{array}$$

□

Theorem 4.23. *Suppose $\mathcal{A}$ is an algebra of decomposable elements. The following equality is valid for all $x, y \in A$ and all $t \in \mathsf{test}(A)$.*

$$\begin{array}{rl} (x \sqcup y)_t = & \Pi(y\sqcap\neg t)\sqcap x\sqcap t \sqcap \Pi(y\sqcap\neg t)\sqcap x_t \sqcap (x\sqcap t \sqcup y_t) \sqcap \\ & \Pi(x\sqcap\neg t)\sqcap y\sqcap t \sqcap \Pi(x\sqcap\neg t)\sqcap y_t \sqcap (x_t \sqcup y\sqcap t) \sqcap (x_t \sqcup y_t) \end{array}$$

Proof : We use the notation

$$\begin{array}{rl} L_t = & \Pi(y\sqcap\neg t)\sqcap x\sqcap t \sqcap \Pi(y\sqcap\neg t)\sqcap x_t \sqcap (x\sqcap t \sqcup y_t) \sqcap \\ & \Pi(x\sqcap\neg t)\sqcap y\sqcap t \sqcap \Pi(x\sqcap\neg t)\sqcap y_t \sqcap (x_t \sqcup y\sqcap t) \sqcap (x_t \sqcup y_t) \ . \end{array}$$

Substituting $\neg t$ for t, we find

$$\begin{array}{rl} L_{\neg t} = & \Pi(y\sqcap t)\sqcap x\sqcap\neg t \sqcap \Pi(y\sqcap t)\sqcap x_{\neg t} \sqcap (x\sqcap\neg t \sqcup y_{\neg t}) \sqcap \\ & \Pi(x\sqcap t)\sqcap y\sqcap\neg t \sqcap \Pi(x\sqcap t)\sqcap y_{\neg t} \sqcap (x_{\neg t} \sqcup y\sqcap\neg t) \sqcap (x_{\neg t} \sqcup y_{\neg t}) \ . \end{array}$$

Hence, we have to establish $L_t = (x \sqcup y)_t$. In order to do so, we have to show that L_t and $L_{\neg t}$ satisfy (4.3), (4.4), (4.5) and (4.6) with $x, t := x \sqcup y, t$ (see Definition 4.7).

(4.5) and (4.6) follow from (3.9), (4.5), (4.6), (4.5) with $x, t := y, t$, (4.6) with $x, t := y, t$, Boolean algebra and Corollary 3.21-18.

Here is the proof of (4.4). Note that

$$\begin{array}{rcl} \Pi(L_t) & = & \Pi(y\sqcap\neg t)\sqcap\Pi(x\sqcap t) \sqcap \Pi(y\sqcap\neg t)\sqcap\Pi(x_t) \sqcap \Pi(x\sqcap t)\sqcap\Pi(y_t) \sqcap \\ & & \Pi(x\sqcap\neg t)\sqcap\Pi(y\sqcap t) \sqcap \Pi(x\sqcap\neg t)\sqcap\Pi(y_t) \sqcap \Pi(x_t)\sqcap\Pi(y\sqcap t) \sqcap \Pi(x_t)\sqcap\Pi(y_t) \\ \Pi(L_{\neg t}) & = & \Pi(y\sqcap t)\sqcap\Pi(x\sqcap\neg t) \sqcap \Pi(y\sqcap t)\sqcap\Pi(x_{\neg t}) \sqcap \Pi(x\sqcap\neg t)\sqcap\Pi(y_{\neg t}) \sqcap \\ & & \Pi(x\sqcap t)\sqcap\Pi(y\sqcap\neg t) \sqcap \Pi(x\sqcap t)\sqcap\Pi(y_{\neg t}) \sqcap \Pi(x_{\neg t})\sqcap\Pi(y\sqcap\neg t) \sqcap \Pi(x_{\neg t})\sqcap\Pi(y_{\neg t}) \ . \end{array}$$

by Corollary 3.21-16, (3.21), and Propositions 3.14-3 and 3.14-9. Also, we have $\Pi(L_t) = \Pi(L_{\neg t})$ by Boolean algebra, (4.4) and (4.4) with $x, t := y, t$.

$$\begin{array}{ll} & \Pi(L_t) \\ = & \qquad\langle \text{ just established } \rangle \\ & \Pi(y\sqcap\neg t)\sqcap\Pi(x\sqcap t) \sqcap \Pi(y\sqcap\neg t)\sqcap\Pi(x_t) \sqcap \Pi(x\sqcap t)\sqcap\Pi(y_t) \sqcap \end{array}$$

$$
\begin{array}{ll}
& \Cap(x \cup \neg t) \cup \Cap(y \cup t) \sqcap \Cap(x \cup \neg t) \cup \Cap(y_t) \sqcap \Cap(x_t) \cup \Cap(y \cup t) \sqcap \Cap(x_t) \cup \Cap(y_t) \\
= & \qquad \langle \text{ by Boolean algebra } \rangle \\
& \Cap(x_t) \cup \Cap(y \cup t) \sqcap \Cap(x_t) \cup \Cap(y_t) \sqcap \Cap(x_t) \cup \Cap(y \cup \neg t) \sqcap \\
& \Cap(x \cup t) \cup \Cap(y_t) \sqcap \Cap(x_t) \cup \Cap(y_t) \sqcap \Cap(x \cup \neg t) \cup \Cap(y_t) \sqcap \\
& \Cap(x \cup \neg t) \cup \Cap(y \cup t) \sqcap \Cap(x \cup \neg t) \cup \Cap(y_t) \sqcap \\
& \Cap(x \cup t) \cup \Cap(y \cup \neg t) \sqcap \Cap(x_t) \cup \Cap(y \cup \neg t) \\
= & \qquad \langle \text{ by Boolean algebra, Lemmas 3.17-5 and 3.17-1, (4.4) and (4.4) with } \\
& \qquad\quad x, t := y, t \rangle \\
& (\Cap(y \cup t) \sqcap \neg \Cap(y \cup t)) \cup \Cap(x_t) \cup \neg \Cap(y \cup \neg t) \cup \Cup y \sqcap \Cap(x_t) \cup \Cap(y \cup \neg t) \sqcap \\
& (\Cap(x \cup t) \sqcap \neg \Cap(x \cup t)) \cup \neg \Cap(x \cup \neg t) \cup \Cup x \cup \Cap(y_t) \sqcap \Cap(x \cup \neg t) \cup \Cup x \cup \Cap(y_t) \sqcap \\
& (\Cap(y \cup t) \sqcap \neg \Cap(y \cup t)) \cup \Cap(x \cup \neg t) \cup \neg \Cap(y \cup \neg t) \cup \Cup y \sqcap \\
& (\Cap(x \cup t) \sqcap \neg \Cap(x \cup t)) \cup \neg \Cap(x \cup \neg t) \cup \Cup x \cup \Cap(y \cup \neg t) \\
= & \qquad \langle \text{ by Boolean algebra } \rangle \\
& \Cap(x_t) \cup \neg \Cap(y \cup \neg t) \cup \Cup y \sqcap \Cap(x_t) \cup \Cap(y \cup \neg t) \sqcap \\
& \neg \Cap(x \cup \neg t) \cup \Cup x \cup \Cap(y_t) \sqcap \Cap(x \cup \neg t) \cup \Cup x \cup \Cap(y_t) \sqcap \\
& \Cap(x \cup \neg t) \cup \neg \Cap(y \cup \neg t) \cup \Cup y \sqcap \Cap(x_t) \cup \neg \Cap(y \cup \neg t) \cup \Cup y \sqcap \\
& \neg \Cap(x \cup \neg t) \cup \Cup x \cup \Cap(y \cup \neg t) \sqcap \neg \Cap(x \cup \neg t) \cup \Cup x \cup \Cap(y_t) \\
= & \qquad \langle \text{ by Boolean algebra, Lemmas 3.17-1 and 3.17-5, (4.4) and (4.4) with } \\
& \qquad\quad x, t := y, t \rangle \\
& (\Cap(y \cup \neg t) \sqcap \neg \Cap(y \cup \neg t)) \cup \Cap(x_t) \cup \Cup y \sqcap \\
& (\Cap(x \cup \neg t) \sqcap \neg \Cap(x \cup \neg t)) \cup \Cup x \cup \Cap(y_t) \sqcap \\
& (\Cap(x \cup \neg t) \sqcap \neg \Cap(x \cup \neg t)) \cup \neg \Cap(x \cup t) \cup \Cup x \cup \neg \Cap(y \cup \neg t) \cup \Cup y \sqcap \\
& (\Cap(y \cup \neg t) \sqcap \neg \Cap(y \cup \neg t)) \cup \neg \Cap(x \cup \neg t) \cup \Cup x \cup \neg \Cap(y \cup t) \cup \Cup y \\
= & \qquad \langle \text{ by Boolean algebra } \rangle \\
& \Cap(x_t) \cup \Cup y \sqcap \Cup x \cup \Cap(y_t) \sqcap \\
& \neg \Cap(x \cup t) \cup \Cup x \cup \neg \Cap(y \cup \neg t) \cup \Cup y \sqcap \neg \Cap(x \cup \neg t) \cup \Cup x \cup \neg \Cap(y \cup t) \cup \Cup y \\
= & \qquad \langle \text{ by Boolean algebra, (4.4) and (4.4) with } x, t := y, t \rangle \\
& \neg \Cap(x \cup t) \cup \neg \Cap(x \cup \neg t) \cup \Cup x \cup \Cup y \sqcap \Cup x \cup \neg \Cap(y \cup t) \cup \neg \Cap(y \cup \neg t) \cup \Cup y \sqcap \\
& \neg \Cap(x \cup t) \cup \Cup x \cup \neg \Cap(y \cup \neg t) \cup \Cup y \sqcap \neg \Cap(x \cup \neg t) \cup \Cup x \cup \neg \Cap(y \cup t) \cup \Cup y \\
= & \qquad \langle \text{ by Boolean algebra } \rangle \\
& (\neg \Cap(x \cup t) \sqcap \neg \Cap(y \cup t)) \cup (\neg \Cap(x \cup \neg t) \sqcap \neg \Cap(y \cup \neg t)) \cup \Cup x \cup \Cup y \\
= & \qquad \langle \text{ by De Morgan and Proposition 3.14-3 } \rangle \\
& \neg(\Cap(x \cup t) \sqcup \Cap(y \cup t)) \cup \neg(\Cap(x \cup \neg t) \sqcup \Cap(y \cup \neg t)) \cup (\Cup x \sqcup \Cup y)
\end{array}
$$

$$
\begin{array}{ll}
= & \langle \text{ by (3.21) and (3.9) } \rangle \\
\multicolumn{2}{l}{\neg\Pi(\neg\Pi((x \sqcup y)\triangleright t)\triangleright\neg\Pi((x \sqcup y)\triangleright\neg t)\triangleright\Pi(x \sqcup y)}
\end{array}
$$

We just established

$$\Pi(L_t) = \Pi(L_{\neg t}) = \Pi((x \sqcup y)_t) \ . \tag{4.23}$$

Also, from (4.4) with $x, t := x \sqcup y, t$ and the last three equalities of this derivation, one finds

$$
\begin{array}{rcl}
\Pi((x \sqcup y)_t) & = & \neg\Pi(x\triangleright t)\triangleright\neg\Pi(x\triangleright\neg t)\triangleright\Pi x\triangleright\Pi y \between \neg\Pi(x\triangleright\neg t)\triangleright\Pi x\triangleright\neg\Pi(y\triangleright t)\triangleright\Pi y \between \\
& & \Pi x\triangleright\neg\Pi(y\triangleright t)\triangleright\neg\Pi(y\triangleright\neg t)\triangleright\Pi y \between \Pi x\triangleright\neg\Pi(x\triangleright t)\triangleright\neg\Pi(y\triangleright\neg t)\triangleright\Pi y \ .
\end{array} \tag{4.24}
$$

To finish the demonstration, it remains to show that L_t and $L_{\neg t}$ satisfy (4.3). The following derivation repeatedly invokes Lemma 3.22-7. Using Proposition 3.14-9, (3.21), Corollary 3.21-16, Remark 4.8 and Boolean algebra, it is easy to check that the appropriate pairs of operands of the various $\sqcup$ and $\between$ operators are disjoint, so that the condition $\Pi x\triangleright\Pi y = \Pi w\triangleright\Pi z = \top$ of Lemma 3.22-7 is satisfied.

$$
\begin{array}{ll}
 & x \sqcup y \\
= & \langle \text{ by (3.2), (4.3) and (4.3) with } x, t := y, t \ \rangle \\
 & (y\triangleright t \between y\triangleright\neg t \between (y_t \sqcup y_{\neg t})) \sqcup (x\triangleright t \between x\triangleright\neg t \between (x_t \sqcup x_{\neg t})) \\
= & \langle \text{ by Corollary 3.21-14 and (3.2) } \rangle \\
 & (x\triangleright t \sqcup (y\triangleright t \between y\triangleright\neg t \between (y_t \sqcup y_{\neg t}))) \between \\
 & (x\triangleright\neg t \sqcup (y\triangleright t \between y\triangleright\neg t \between (y_t \sqcup y_{\neg t}))) \between \\
 & ((x_t \sqcup x_{\neg t}) \sqcup (y\triangleright t \between y\triangleright\neg t \between (y_t \sqcup y_{\neg t}))) \\
= & \langle \text{ by Corollary 3.21-14 and (3.2) } \rangle \\
 & (x\triangleright t \sqcup y\triangleright t) \between (x\triangleright t \sqcup y\triangleright\neg t) \between (x\triangleright t \sqcup y_t \sqcup y_{\neg t}) \between \\
 & (y\triangleright t \sqcup x\triangleright\neg t) \between (x\triangleright\neg t \sqcup y\triangleright\neg t) \between (y_t \sqcup x\triangleright\neg t \sqcup y_{\neg t}) \between \\
 & (x_t \sqcup y\triangleright t \sqcup x_{\neg t}) \between (x_t \sqcup x_{\neg t} \sqcup y\triangleright\neg t) \between (x_t \sqcup y_t \sqcup x_{\neg t} \sqcup y_{\neg t}) \\
= & \langle \text{ by (3.21), Remark 4.8 and Boolean algebra,} \\
 & \quad \text{the domains of } x\triangleright t \sqcup y\triangleright\neg t,\ x\triangleright t \sqcup y_t \sqcup y_{\neg t},\ y\triangleright t \sqcup x\triangleright\neg t \\
 & \quad \text{and } x\triangleright\neg t \sqcup y\triangleright\neg t \text{ are pairwise disjoint,} \\
 & \quad \text{then apply (3.25) and (3.9) } \rangle \\
 & (x \sqcup y)\triangleright t \between (x \sqcup y)\triangleright\neg t \between (x\triangleright t \sqcup y\triangleright\neg t) \between
\end{array}
$$

$$
\begin{array}{ll}
& (x \triangleleft t \sqcup y_t \sqcup y_{\neg t}) \pitchfork (y \triangleleft t \sqcup x \triangleleft \neg t) \pitchfork (y_t \sqcup x \triangleleft \neg t \sqcup y_{\neg t}) \pitchfork \\
& (x_t \sqcup y \triangleleft t \sqcup x_{\neg t}) \pitchfork (x_t \sqcup x_{\neg t} \sqcup y \triangleleft \neg t) \pitchfork (x_t \sqcup y_t \sqcup x_{\neg t} \sqcup y_{\neg t}) \\
= & \quad \langle \text{ by (3.21), Remark 4.8 and Boolean algebra,} \\
& \quad \text{the domains of } x \triangleleft t \sqcup y_t \sqcup y_{\neg t},\ y \triangleleft t \sqcup x \triangleleft \neg t,\ x \triangleleft \neg t \sqcup y_t \sqcup y_{\neg t}, \\
& \quad x_t \sqcup x_{\neg t} \sqcup y \triangleleft t \text{ and } x_t \sqcup x_{\neg t} \sqcup y \triangleleft \neg t \text{ are pairwise disjoint,} \\
& \quad \text{then apply (3.25)} \rangle \\
& (x \sqcup y) \triangleleft t \pitchfork (x \sqcup y) \triangleleft \neg t \pitchfork (x \triangleleft t \sqcup y \triangleleft \neg t) \pitchfork \\
& (x_t \sqcup x_{\neg t} \sqcup y \triangleleft \neg t) \pitchfork (x \triangleleft t \sqcup y_t \sqcup y_{\neg t}) \pitchfork (y \triangleleft t \sqcup x \triangleleft \neg t) \pitchfork \\
& (y_t \sqcup x \triangleleft \neg t \sqcup y_{\neg t}) \pitchfork (x_t \sqcup y \triangleleft t \sqcup x_{\neg t}) \pitchfork (x_t \sqcup y_t \sqcup x_{\neg t} \sqcup y_{\neg t}) \\
= & \quad \langle \text{ by Propositions 3.14-7 and 3.14-20, and (3.2)} \rangle \\
& (x \sqcup y) \triangleleft t \pitchfork (x \sqcup y) \triangleleft \neg t \pitchfork \\
& (\Pi(y \triangleleft \neg t) \triangleleft x \triangleleft t \sqcup \Pi(x \triangleleft t) \triangleleft y \triangleleft \neg t) \pitchfork (\Pi(y \triangleleft \neg t) \triangleleft x_t \sqcup x_{\neg t} \sqcup y \triangleleft \neg t) \pitchfork \\
& (x \triangleleft t \sqcup y_t \sqcup \Pi(x \triangleleft t) \triangleleft y_{\neg t}) \pitchfork (\Pi(x \triangleleft \neg t) \triangleleft y \triangleleft t \sqcup \Pi(y \triangleleft t) \triangleleft x \triangleleft \neg t) \pitchfork \\
& (\Pi(x \triangleleft \neg t) \triangleleft y_t \sqcup x \triangleleft \neg t \sqcup y_{\neg t}) \pitchfork (x_t \sqcup y \triangleleft t \sqcup \Pi(y \triangleleft t) \triangleleft x_{\neg t}) \pitchfork \\
& (x_t \sqcup y_t \sqcup x_{\neg t} \sqcup y_{\neg t}) \\
= & \quad \langle \text{ by Lemma 3.22-7} \rangle \\
& (x \sqcup y) \triangleleft t \pitchfork (x \sqcup y) \triangleleft \neg t \pitchfork \\
& ((\Pi(y \triangleleft \neg t) \triangleleft x \triangleleft t \pitchfork \Pi(y \triangleleft \neg t) \triangleleft x_t) \sqcup (\Pi(x \triangleleft t) \triangleleft y \triangleleft \neg t \pitchfork x_{\neg t} \sqcup y \triangleleft \neg t)) \pitchfork \\
& (x \triangleleft t \sqcup y_t \sqcup \Pi(x \triangleleft t) \triangleleft y_{\neg t}) \pitchfork (\Pi(x \triangleleft \neg t) \triangleleft y \triangleleft t \sqcup \Pi(y \triangleleft t) \triangleleft x \triangleleft \neg t) \pitchfork \\
& (\Pi(x \triangleleft \neg t) \triangleleft y_t \sqcup x \triangleleft \neg t \sqcup y_{\neg t}) \pitchfork (x_t \sqcup y \triangleleft t \sqcup \Pi(y \triangleleft t) \triangleleft x_{\neg t}) \pitchfork \\
& (x_t \sqcup y_t \sqcup x_{\neg t} \sqcup y_{\neg t}) \\
= & \quad \langle \text{ by Lemma 3.22-7} \rangle \\
& (x \sqcup y) \triangleleft t \pitchfork (x \sqcup y) \triangleleft \neg t \pitchfork \\
& ((\Pi(y \triangleleft \neg t) \triangleleft x \triangleleft t \pitchfork \Pi(y \triangleleft \neg t) \triangleleft x_t \pitchfork (x \triangleleft t \sqcup y_t)) \sqcup \\
& \ (\Pi(x \triangleleft t) \triangleleft y \triangleleft \neg t \pitchfork x_{\neg t} \sqcup y \triangleleft \neg t \pitchfork \Pi(x \triangleleft t) \triangleleft y_{\neg t}) \pitchfork \\
& (\Pi(x \triangleleft \neg t) \triangleleft y \triangleleft t \sqcup \Pi(y \triangleleft t) \triangleleft x \triangleleft \neg t) \pitchfork (\Pi(x \triangleleft \neg t) \triangleleft y_t \sqcup x \triangleleft \neg t \sqcup y_{\neg t}) \pitchfork \\
& (x_t \sqcup y \triangleleft t \sqcup \Pi(y \triangleleft t) \triangleleft x_{\neg t}) \pitchfork (x_t \sqcup y_t \sqcup x_{\neg t} \sqcup y_{\neg t}) \\
= & \quad \langle \text{ by Lemma 3.22-7} \rangle \\
& (x \sqcup y) \triangleleft t \pitchfork (x \sqcup y) \triangleleft \neg t \pitchfork \\
& ((\Pi(y \triangleleft \neg t) \triangleleft x \triangleleft t \pitchfork \Pi(y \triangleleft \neg t) \triangleleft x_t \pitchfork (x \triangleleft t \sqcup y_t) \pitchfork \Pi(x \triangleleft \neg t) \triangleleft y \triangleleft t) \sqcup \\
& \ (\Pi(x \triangleleft t) \triangleleft y \triangleleft \neg t \pitchfork x_{\neg t} \sqcup y \triangleleft \neg t \pitchfork \Pi(x \triangleleft t) \triangleleft y_{\neg t} \pitchfork \Pi(y \triangleleft t) \triangleleft x \triangleleft \neg t) \pitchfork \\
& (\Pi(x \triangleleft \neg t) \triangleleft y_t \sqcup x \triangleleft \neg t \sqcup y_{\neg t}) \pitchfork (x_t \sqcup y \triangleleft t \sqcup \Pi(y \triangleleft t) \triangleleft x_{\neg t}) \pitchfork \\
& (x_t \sqcup y_t \sqcup x_{\neg t} \sqcup y_{\neg t})
\end{array}
$$

$$
\begin{aligned}
&= \quad \langle \text{ by Lemma 3.22-7 } \rangle \\
&\quad (x \sqcup y)\triangleright t \pitchfork (x \sqcup y)\triangleright \neg t \pitchfork \\
&\quad ((\Pi(y\triangleright\neg t)\triangleright x\triangleright t \pitchfork \Pi(y\triangleright\neg t)\triangleright x_t \pitchfork (x\triangleright t \sqcup y_t) \pitchfork \Pi(x\triangleright\neg t)\triangleright y\triangleright t \pitchfork \Pi(x\triangleright\neg t)\triangleright y_t) \sqcup \\
&\quad (\Pi(x\triangleright t)\triangleright y\triangleright\neg t \pitchfork x_{\neg t} \sqcup y\triangleright\neg t \pitchfork \Pi(x\triangleright t)\triangleright y_{\neg t} \pitchfork \Pi(y\triangleright t)\triangleright x\triangleright\neg t \pitchfork (x\triangleright\neg t \sqcup y_{\neg t})) \pitchfork \\
&\quad (x_t \sqcup y\triangleright t \sqcup \Pi(y\triangleright t)\triangleright x_{\neg t}) \pitchfork (x_t \sqcup y_t \sqcup x_{\neg t} \sqcup y_{\neg t}) \\
&= \quad \langle \text{ by Lemma 3.22-7 } \rangle \\
&\quad (x \sqcup y)\triangleright t \pitchfork (x \sqcup y)\triangleright \neg t \pitchfork \\
&\quad ((\Pi(y\triangleright\neg t)\triangleright x\triangleright t \pitchfork \Pi(y\triangleright\neg t)\triangleright x_t \pitchfork (x\triangleright t \sqcup y_t) \pitchfork \\
&\quad \Pi(x\triangleright\neg t)\triangleright y\triangleright t \pitchfork \Pi(x\triangleright\neg t)\triangleright y_t \pitchfork (x_t \sqcup y\triangleright t)) \sqcup \\
&\quad (\Pi(x\triangleright t)\triangleright y\triangleright\neg t \pitchfork x_{\neg t} \sqcup y\triangleright\neg t \pitchfork \Pi(x\triangleright t)\triangleright y_{\neg t} \pitchfork \\
&\quad \Pi(y\triangleright t)\triangleright x\triangleright\neg t \pitchfork (x\triangleright\neg t \sqcup y_{\neg t}) \pitchfork \Pi(y\triangleright t)\triangleright x_{\neg t}) \pitchfork \\
&\quad (x_t \sqcup y_t \sqcup x_{\neg t} \sqcup y_{\neg t}) \\
&= \quad \langle \text{ by Lemma 3.22-7 } \rangle \\
&\quad (x \sqcup y)\triangleright t \pitchfork (x \sqcup y)\triangleright \neg t \pitchfork \\
&\quad ((\Pi(y\triangleright\neg t)\triangleright x\triangleright t \pitchfork \Pi(y\triangleright\neg t)\triangleright x_t \pitchfork (x\triangleright t \sqcup y_t) \pitchfork \\
&\quad \Pi(x\triangleright\neg t)\triangleright y\triangleright t \pitchfork \Pi(x\triangleright\neg t)\triangleright y_t \pitchfork (x_t \sqcup y\triangleright t) \pitchfork (x_t \sqcup y_t)) \sqcup \\
&\quad (\Pi(x\triangleright t)\triangleright y\triangleright\neg t \pitchfork x_{\neg t} \sqcup y\triangleright\neg t \pitchfork \Pi(x\triangleright t)\triangleright y_{\neg t} \pitchfork \\
&\quad \Pi(y\triangleright t)\triangleright x\triangleright\neg t \pitchfork (x\triangleright\neg t \sqcup y_{\neg t}) \pitchfork \Pi(y\triangleright t)\triangleright x_{\neg t} \pitchfork (x_{\neg t} \sqcup y_{\neg t})) \\
&= \quad \langle \text{ by Proposition 3.14-9, (3.21), Lemma 3.17-4, Remark 4.8} \\
&\qquad \text{and Boolean algebra,} \\
&\qquad \text{the domains of } \Pi(x\triangleright t)\triangleright y\triangleright\neg t,\ x_{\neg t} \sqcup y\triangleright\neg t,\ \Pi(x\triangleright t)\triangleright y_{\neg t}, \\
&\qquad \Pi(y\triangleright t)\triangleright x\triangleright\neg t,\ x\triangleright\neg t \sqcup y_{\neg t},\ \Pi(y\triangleright t)\triangleright x_{\neg t} \text{ and } x_{\neg t} \sqcup y_{\neg t} \text{ are pairwise disjoint,} \\
&\qquad \text{then apply (3.25) } \rangle \\
&\quad (x \sqcup y)\triangleright t \pitchfork (x \sqcup y)\triangleright \neg t \pitchfork (L_t \sqcup L_{\neg t})
\end{aligned}
$$

□

Corollary 4.24. *Suppose $\mathcal{A}$ is an algebra of decomposable elements. Then, for all $x, y \in A$ and all $t \in \mathsf{test}(A)$,*

$$
\begin{aligned}
(x \sqcup y)_t = \ & \Pi(y\triangleright\neg t)\triangleright x\triangleright t \pitchfork \Pi(y\triangleright\neg t)\triangleright x_t \pitchfork (x\triangleright t \sqcup y_t) \pitchfork \\
& \Pi(x\triangleright\neg t)\triangleright y\triangleright t \pitchfork \Pi(x\triangleright\neg t)\triangleright y_t \pitchfork (x_t \sqcup y\triangleright t) \pitchfork (x_t \sqcup y_t)
\end{aligned}
$$

and any of the seven operands of the $\pitchfork$ operators can be permuted with another.

Proof : The equality is the one of Theorem 4.23.

By Propositions 3.14-9 and 3.14-3, (3.21), Lemma 3.17-4, Remark 4.8 and Boolean algebra, the domains of the seven operands of the $\sqcap$ operators are pairwise disjoint. Then apply (3.25). □

Proposition 4.25. *Suppose $\mathcal{A}$ is an algebra of decomposable elements. The following equalities are valid for all $x \in A$ and all $s, t \in \mathsf{test}(A)$.*

1. $x_{s \sqcap t} = \neg^{\sqcap}(x \triangleright (s \sqcap t)) \triangleright ((x_s \sqcup x_t) \sqcap \neg^{\sqcap}(x_s) \triangleright x_t \sqcap \neg^{\sqcap}(x_t) \triangleright x_s)$
2. $x_{s \triangleright t} = {}^{\sqcap}(x \triangleright s) \triangleright x_t \sqcap (x_s)_t \sqcap x_s \triangleright t$

One might understand Proposition 4.25-1 intuitively by noting that

$$x_{s \sqcap t} = \neg^{\sqcap}(x \triangleright (s +_D t)) \cdot_D (x_s +_D x_t)$$

by Corollary 4.4-1, Proposition 4.17-3 and Boolean algebra.

Proof : Part 1 of the proposition is an expression for $x_{s \sqcap t}$, but what is the corresponding expression for $x_{\neg(s \sqcap t)}$? Actually, $x_{\neg(s \sqcap t)} = x_{\neg s \triangleright \neg t}$ by Boolean algebra and part 2 of the proposition gives an expression for that. So in order to demonstrate the proposition, we need to work on both parts at the same time. These expressions must satisfy (4.3), (4.4), (4.5) and (4.6) with $x, t := x, s \sqcap t$ (see Definition 4.7).

For these reasons, the demonstration is divided in five steps. We show that the candidate for $x_{s \sqcap t}$

$$\neg^{\sqcap}(x \triangleright (s \sqcap t)) \triangleright ((x_s \sqcup x_t) \sqcap \neg^{\sqcap}(x_s) \triangleright x_t \sqcap \neg^{\sqcap}(x_t) \triangleright x_s)$$

satisfies (4.5) and (4.4) with $x, t := x, s \sqcap t$, then we show that the candidate for $x_{\neg s \triangleright \neg t}$

$${}^{\sqcap}(x \triangleright \neg s) \triangleright x_{\neg t} \sqcap (x_{\neg s})_{\neg t} \sqcap x_{\neg s} \triangleright \neg t$$

satisfies (4.6) and (4.4) with $x, t := x, s \sqcap t$ and we conclude with the demonstration that

$$\neg^{\sqcap}(x \triangleright (s \sqcap t)) \triangleright ((x_s \sqcup x_t) \sqcap \neg^{\sqcap}(x_s) \triangleright x_t \sqcap \neg^{\sqcap}(x_t) \triangleright x_s)$$

and

$${}^{\sqcap}(x \triangleright \neg s) \triangleright x_{\neg t} \sqcap (x_{\neg s})_{\neg t} \sqcap x_{\neg s} \triangleright \neg t$$

satisfy (4.3) with $x, t := x, s \sqcap t$.

1. We begin with the proof that

   $$\neg^{\sqcap}(x \triangleright (s \sqcap t)) \triangleright ((x_s \sqcup x_t) \sqcap \neg^{\sqcap}(x_s) \triangleright x_t \sqcap \neg^{\sqcap}(x_t) \triangleright x_s)$$

   satisfies (4.5) with $x, t := x, s \sqcap t$. Firstly we have

$$
\begin{array}{ll}
& (x_s \sqcup x_t)\vartriangleright(s \sqcap t) \\
= & \qquad \langle \text{ by (3.9) } \rangle \\
& x_s\vartriangleright(s \sqcap t) \sqcup x_t\vartriangleright(s \sqcap t) \\
= & \qquad \langle \text{ by (4.5) with } x,t := x,s \text{ and (4.5) } \rangle \\
& x_s\vartriangleright s\vartriangleright(s \sqcap t) \sqcup x_t\vartriangleright t\vartriangleright(s \sqcap t) \\
= & \qquad \langle \text{ by Boolean algebra, (4.5) with } x,t := x,s \text{ and (4.5) } \rangle \\
& x_s \sqcup x_t \ ,
\end{array}
$$

secondly

$$
\begin{array}{ll}
& \neg^{\sqcap}(x_s)\vartriangleright x_t\vartriangleright(s \sqcap t) \\
= & \qquad \langle \text{ by (4.5) } \rangle \\
& \neg^{\sqcap}(x_s)\vartriangleright x_t\vartriangleright t\vartriangleright(s \sqcap t) \\
= & \qquad \langle \text{ by Boolean algebra and (4.5) } \rangle \\
& \neg^{\sqcap}(x_s)\vartriangleright x_t
\end{array}
$$

and finally

$$
\begin{array}{ll}
& \neg^{\sqcap}(x_t)\vartriangleright x_s\vartriangleright(s \sqcap t) \\
= & \qquad \langle \text{ by (4.5) with } x,t := x,s \ \rangle \\
& \neg^{\sqcap}(x_t)\vartriangleright x_s\vartriangleright s\vartriangleright(s \sqcap t) \\
= & \qquad \langle \text{ by Boolean algebra and (4.5) with } x,t := x,s \ \rangle \\
& \neg^{\sqcap}(x_t)\vartriangleright x_s \ .
\end{array}
$$

Hence

$$((x_s \sqcup x_t) \sqcap \neg^{\sqcap}(x_s)\vartriangleright x_t \sqcap \neg^{\sqcap}(x_t)\vartriangleright x_s)\vartriangleright(s \sqcap t) = (x_s \sqcup x_t) \sqcap \neg^{\sqcap}(x_s)\vartriangleright x_t \sqcap \neg^{\sqcap}(x_t)\vartriangleright x_s$$

by Corollary 3.21-18, so

$$
\begin{array}{l}
\neg^{\sqcap}(x\vartriangleright(s \sqcap t))\vartriangleright((x_s \sqcup x_t) \sqcap \neg^{\sqcap}(x_s)\vartriangleright x_t \sqcap \neg^{\sqcap}(x_t)\vartriangleright x_s)\vartriangleright(s \sqcap t) \\
\qquad = \neg^{\sqcap}(x\vartriangleright(s \sqcap t))\vartriangleright((x_s \sqcup x_t) \sqcap \neg^{\sqcap}(x_s)\vartriangleright x_t \sqcap \neg^{\sqcap}(x_t)\vartriangleright x_s)
\end{array}
$$

and (4.5) is established.

2. Now we show that

$$\neg^{\sqcap}(x\vartriangleright(s \sqcap t))\vartriangleright((x_s \sqcup x_t) \sqcap \neg^{\sqcap}(x_s)\vartriangleright x_t \sqcap \neg^{\sqcap}(x_t)\vartriangleright x_s)$$

satisfies (4.4) with $x,t := x, s \sqcap t$.

$$
\begin{array}{ll}
& \Pi(\neg\Pi(x\rhd(s \between t))\rhd((x_s \sqcup x_t) \between \neg\Pi(x_s)\rhd x_t \between \neg\Pi(x_t)\rhd x_s)) \\
= & \qquad \langle \text{ by Corollary 4.4-1 } \rangle \\
& \Pi(\neg\Pi(x\rhd(s \between t))\rhd(x_s +_D x_t)) \\
= & \qquad \langle \text{ by Proposition 3.14-9 and Corollary 4.4-3 } \rangle \\
& \neg\Pi(x\rhd(s \between t))\rhd(\Pi(x_s) \between \Pi(x_t)) \\
= & \qquad \langle \text{ by Boolean algebra, (4.4) with } x,t := x,s \text{ and (4.4) } \rangle \\
& \neg\Pi(x\rhd(s \between t))\rhd\neg\Pi(x\rhd s)\rhd\neg\Pi(x\rhd\neg s)\rhd\Pi x \between \\
& \neg\Pi(x\rhd(s \between t))\rhd\neg\Pi(x\rhd t)\rhd\neg\Pi(x\rhd\neg t)\rhd\Pi x \\
= & \qquad \langle \text{ by Lemma 3.17-6 and Boolean algebra } \rangle \\
& \neg\Pi(x\rhd(s \between t))\rhd\neg\Pi(x\rhd\neg s)\rhd\Pi x \between \neg\Pi(x\rhd(s \between t))\rhd\neg\Pi(x\rhd\neg t)\rhd\Pi x \\
= & \qquad \langle \text{ by Boolean algebra } \rangle \\
& \neg\Pi(x\rhd(s \between t))\rhd\Pi x\rhd(\neg\Pi(x\rhd\neg s) \between \neg\Pi(x\rhd\neg t)) \\
= & \qquad \langle \text{ by De Morgan } \rangle \\
& \neg\Pi(x\rhd(s \between t))\rhd\Pi x\rhd\neg(\Pi(x\rhd\neg s)\rhd\Pi(x\rhd\neg t)) \\
= & \qquad \langle \text{ by Proposition 3.14-12 } \rangle \\
& \neg\Pi(x\rhd(s \between t))\rhd\Pi x\rhd\neg\Pi(x\rhd\neg s\rhd\neg t) \\
= & \qquad \langle \text{ by De Morgan and Boolean algebra } \rangle \\
& \neg\Pi(x\rhd(s \between t))\rhd\neg\Pi(x\rhd\neg(s \between t))\rhd\Pi x
\end{array}
$$

3. Here comes the proof that

$$\Pi(x\rhd\neg s)\rhd x_{\neg t} \between (x_{\neg s})_{\neg t} \between x_{\neg s}\rhd\neg t$$

satisfies (4.6) with $x,t := x, s \between t$. Firstly we have

$$
\begin{array}{ll}
& \Pi(x\rhd\neg s)\rhd x_{\neg t}\rhd\neg s\rhd\neg t \\
= & \qquad \langle \text{ by Proposition 4.22-6 } \rangle \\
& \Pi(x\rhd\neg s)\rhd x_{\neg t}\rhd\neg t \\
= & \qquad \langle \text{ by (4.6) } \rangle \\
& \Pi(x\rhd\neg s)\rhd x_{\neg t} \quad ,
\end{array}
$$

secondly

$$(x_{\neg s})_{\neg t}\rhd\neg s\rhd\neg t$$

$$
\begin{array}{ll}
= & \quad \langle \text{ by Proposition 4.22-7 } \rangle \\
& (x_{\neg s})_{\neg t} \mathbin{\square} \neg t \\
= & \quad \langle \text{ by (4.6) with } x, t := x_{\neg s}, t \rangle \\
& (x_{\neg s})_{\neg t}
\end{array}
$$

and finally

$$
\begin{array}{ll}
& x_{\neg s} \mathbin{\square} \neg t \mathbin{\square} \neg s \mathbin{\square} \neg t \\
= & \quad \langle \text{ by (4.6) with } x, t := x, s \text{ and Boolean algebra } \rangle \\
& x_{\neg s} \mathbin{\square} \neg t \quad .
\end{array}
$$

Hence

$$(\Pi(x \mathbin{\square} \neg s) \mathbin{\square} x_{\neg t} \mathbin{\sqcap} (x_{\neg s})_{\neg t} \mathbin{\sqcap} x_{\neg s} \mathbin{\square} \neg t) \mathbin{\square} \neg s \mathbin{\square} \neg t = \Pi(x \mathbin{\square} \neg s) \mathbin{\square} x_{\neg t} \mathbin{\sqcap} (x_{\neg s})_{\neg t} \mathbin{\sqcap} x_{\neg s} \mathbin{\square} \neg t$$

by Corollary 3.21-18, so (4.6) is established.

4. Now we show that

$$\Pi(x \mathbin{\square} \neg s) \mathbin{\square} x_{\neg t} \mathbin{\sqcap} (x_{\neg s})_{\neg t} \mathbin{\sqcap} x_{\neg s} \mathbin{\square} \neg t$$

satisfies (4.4) with $x, t := x, s \mathbin{\sqcap} t$. We want to establish

$$\Pi(\Pi(x \mathbin{\square} \neg s) \mathbin{\square} x_{\neg t} \mathbin{\sqcap} (x_{\neg s})_{\neg t} \mathbin{\sqcap} x_{\neg s} \mathbin{\square} \neg t) = \neg \Pi(x \mathbin{\square} (s \mathbin{\sqcap} t)) \mathbin{\square} \neg \Pi(x \mathbin{\square} \neg (s \mathbin{\sqcap} t)) \mathbin{\square} \Pi x$$

but we will rather work to demonstrate

$$\neg \Pi(\Pi(x \mathbin{\square} \neg s) \mathbin{\square} x_{\neg t} \mathbin{\sqcap} (x_{\neg s})_{\neg t} \mathbin{\sqcap} x_{\neg s} \mathbin{\square} \neg t) = \neg(\neg \Pi(x \mathbin{\square} (s \mathbin{\sqcap} t)) \mathbin{\square} \neg \Pi(x \mathbin{\square} \neg s \mathbin{\square} \neg t) \mathbin{\square} \Pi x) \quad ,$$

which is equivalent by Boolean algebra and De Morgan.

$$
\begin{array}{ll}
& \neg \Pi(\Pi(x \mathbin{\square} \neg s) \mathbin{\square} x_{\neg t} \mathbin{\sqcap} (x_{\neg s})_{\neg t} \mathbin{\sqcap} x_{\neg s} \mathbin{\square} \neg t) \\
= & \quad \langle \text{ by Corollary 3.21-16 } \rangle \\
& \neg(\Pi(\Pi(x \mathbin{\square} \neg s) \mathbin{\square} x_{\neg t}) \mathbin{\sqcap} \Pi((x_{\neg s})_{\neg t}) \mathbin{\sqcap} \Pi(x_{\neg s} \mathbin{\square} \neg t)) \\
= & \quad \langle \text{ by Proposition 3.14-9 } \rangle \\
& \neg(\Pi(x \mathbin{\square} \neg s) \mathbin{\square} \Pi(x_{\neg t}) \mathbin{\sqcap} \Pi((x_{\neg s})_{\neg t}) \mathbin{\sqcap} \Pi(x_{\neg s} \mathbin{\square} \neg t)) \\
= & \quad \langle \text{ by (4.4) and (4.4) with } x, t := x_{\neg s}, t \rangle \\
& \neg(\Pi(x \mathbin{\square} \neg s) \mathbin{\square} \neg \Pi(x \mathbin{\square} \neg t) \mathbin{\square} \neg \Pi(x \mathbin{\square} t) \mathbin{\square} \Pi x \mathbin{\sqcap} \\
& \quad \neg \Pi(x_{\neg s} \mathbin{\square} \neg t) \mathbin{\square} \neg \Pi(x_{\neg s} \mathbin{\square} t) \mathbin{\square} \Pi(x_{\neg s}) \mathbin{\sqcap} \Pi(x_{\neg s} \mathbin{\square} \neg t)) \\
= & \quad \langle \text{ by Boolean algebra } \rangle
\end{array}
$$

$$
\begin{array}{ll}
 & \neg(\Cap(x \cup \neg s) \cup \neg\Cap(x \cup \neg t) \cup \neg\Cap(x \cup t) \cup \Cap x \mathbin{\Cup} \neg\Cap(x_{\neg s} \cup t) \cup \Cap(x_{\neg s}) \mathbin{\Cup} \Cap(x_{\neg s} \cup \neg t)) \\
= & \quad \langle \text{ by Lemmas 3.17-5 and 3.17-1, and Boolean algebra } \rangle \\
 & \neg(\Cap(x \cup \neg s) \cup \neg\Cap(x \cup \neg t) \cup \neg\Cap(x \cup t) \cup \Cap x \mathbin{\Cup} \neg\Cap(x_{\neg s} \cup t) \cup \Cap(x_{\neg s})) \\
= & \quad \langle \text{ by Boolean algebra, Lemma 3.17-1 and (4.4) with } x, t := x, s \rangle \\
 & \neg(\Cap(x \cup \neg s) \cup \neg\Cap(x \cup \neg t) \cup \neg\Cap(x \cup t) \mathbin{\Cup} \neg\Cap(x_{\neg s} \cup t) \cup \neg\Cap(x \cup \neg s) \cup \neg\Cap(x \cup s) \cup \Cap x) \\
= & \quad \langle \text{ by De Morgan } \rangle \\
 & (\neg\Cap(x \cup \neg s) \mathbin{\Cup} \Cap(x \cup \neg t) \mathbin{\Cup} \Cap(x \cup t)) \cup (\Cap(x_{\neg s} \cup t) \mathbin{\Cup} \Cap(x \cup \neg s) \mathbin{\Cup} \Cap(x \cup s) \mathbin{\Cup} \neg\Cap x) \\
= & \quad \langle \text{ by Boolean algebra and Lemmas 3.17-5, 3.17-3 and 3.17-2 } \rangle \\
 & \neg\Cap(x \cup \neg s) \cup \Cap(x_{\neg s} \cup t) \mathbin{\Cup} \Cap(x \cup s) \mathbin{\Cup} \neg\Cap x \mathbin{\Cup} \\
 & \Cap(x \cup \neg t) \cup \Cap(x_{\neg s} \cup t) \mathbin{\Cup} \Cap(x \cup \neg s) \cup \Cap(x \cup \neg t) \mathbin{\Cup} \Cap(x \cup s) \cup \Cap(x \cup \neg t) \mathbin{\Cup} \\
 & \Cap(x \cup t) \cup \Cap(x_{\neg s} \cup t) \mathbin{\Cup} \Cap(x \cup \neg s) \cup \Cap(x \cup t) \mathbin{\Cup} \Cap(x \cup s) \cup \Cap(x \cup t) \\
= & \quad \langle \text{ by Propositions 3.14-9 and 3.14-12 } \rangle \\
 & \Cap(\neg\Cap(x \cup \neg s) \cup x_{\neg s} \cup t) \mathbin{\Cup} \Cap(x \cup s) \mathbin{\Cup} \neg\Cap x \mathbin{\Cup} \\
 & \Cap(\Cap(x \cup \neg t) \cup x_{\neg s} \cup t) \mathbin{\Cup} \Cap(x \cup \neg s \cup \neg t) \mathbin{\Cup} \Cap(x \cup \neg t) \cup \Cap(x \cup s) \mathbin{\Cup} \\
 & \Cap(x \cup t) \cup \Cap(x_{\neg s} \cup t) \mathbin{\Cup} \Cap(x \cup \neg s \cup t) \mathbin{\Cup} \Cap(x \cup t) \cup \Cap(x \cup s) \\
= & \quad \langle \text{ by Propositions 3.14-7, 4.22-6 and 3.14-1, (4.4) with } \\
 & \qquad x, t := x, s, \text{ Boolean algebra and (3.6) } \rangle \\
 & \Cap(x_{\neg s} \cup t) \mathbin{\Cup} \Cap(x \cup s) \mathbin{\Cup} \neg\Cap x \mathbin{\Cup} \\
 & \Cap(x \cup \neg s \cup \neg t) \mathbin{\Cup} \Cap(x \cup \neg t) \cup \Cap(x \cup s) \mathbin{\Cup} \\
 & \Cap(x \cup t) \cup \Cap(x_{\neg s} \cup t) \mathbin{\Cup} \Cap(x \cup \neg s \cup t) \mathbin{\Cup} \Cap(x \cup t) \cup \Cap(x \cup s) \\
= & \quad \langle \text{ by Boolean algebra } \rangle \\
 & \Cap(x_{\neg s} \cup t) \mathbin{\Cup} \Cap(x \cup s) \mathbin{\Cup} \neg\Cap x \mathbin{\Cup} \Cap(x \cup \neg s \cup \neg t) \mathbin{\Cup} \Cap(x \cup \neg s \cup t) \\
= & \quad \langle \text{ by Proposition 4.22-8, Lemma 3.17-1 and (4.4) with } x, t := x, s \rangle \\
 & \neg\Cap(x \cup \neg s) \cup \neg\Cap(x \cup s) \cup \Cap(x \cup (s \mathbin{\Cap} t)) \mathbin{\Cup} \Cap(x \cup s) \mathbin{\Cup} \neg\Cap x \mathbin{\Cup} \Cap(x \cup \neg s \cup \neg t) \mathbin{\Cup} \Cap(x \cup \neg s \cup t) \\
= & \quad \langle \text{ by Proposition 3.14-12 and Boolean algebra } \rangle \\
 & \neg\Cap(x \cup \neg s) \cup \neg\Cap(x \cup s) \cup \Cap(x \cup (s \mathbin{\Cap} t)) \mathbin{\Cup} \Cap(x \cup s) \cup \Cap(x \cup (s \mathbin{\Cap} t)) \mathbin{\Cup} \neg\Cap x \mathbin{\Cup} \\
 & \Cap(x \cup \neg s \cup \neg t) \mathbin{\Cup} \Cap(x \cup \neg s) \cup \Cap(x \cup (s \mathbin{\Cap} t)) \\
= & \quad \langle \text{ by Boolean algebra } \rangle \\
 & (\neg\Cap(x \cup \neg s) \cup \neg\Cap(x \cup s) \mathbin{\Cup} \Cap(x \cup s) \mathbin{\Cup} \Cap(x \cup \neg s)) \cup \Cap(x \cup (s \mathbin{\Cap} t)) \mathbin{\Cup} \neg\Cap x \mathbin{\Cup} \Cap(x \cup \neg s \cup \neg t) \\
= & \quad \langle \text{ by Boolean algebra } \rangle \\
 & \Cap(x \cup (s \mathbin{\Cap} t)) \mathbin{\Cup} \neg\Cap x \mathbin{\Cup} \Cap(x \cup \neg s \cup \neg t)
\end{array}
$$

$$
\begin{array}{ll}
= & \langle \text{ by De Morgan and Boolean algebra } \rangle \\
& \neg(\neg\Pi(x\,\square\,(s \sqcap t))\,\square\,\neg\Pi(x\,\square\,\neg s\,\square\,\neg t)\,\square\,\Pi x)
\end{array}
$$

5. It remains to demonstrate that the two candidates

$$\neg\Pi(x\,\square\,(s \sqcap t))\,\square\,((x_s \sqcup x_t) \sqcap \neg\Pi(x_s)\,\square\,x_t \sqcap \neg\Pi(x_t)\,\square\,x_s)$$

and

$$\Pi(x\,\square\,\neg s)\,\square\,x_{\neg t} \sqcap (x_{\neg s})_{\neg t} \sqcap x_{\neg s}\,\square\,\neg t$$

satisfy (4.3). To be more precise, we need to demonstrate that

$$
\begin{array}{rcl}
x & = & x\,\square\,(s \sqcap t) \sqcap x\,\square\,(\neg s\,\square\,\neg t) \sqcap \\
& & (\neg\Pi(x\,\square\,(s \sqcap t))\,\square\,((x_s \sqcup x_t) \sqcap \neg\Pi(x_s)\,\square\,x_t \sqcap \neg\Pi(x_t)\,\square\,x_s) \sqcup \\
& & (\Pi(x\,\square\,\neg s)\,\square\,x_{\neg t} \sqcap (x_{\neg s})_{\neg t} \sqcap x_{\neg s}\,\square\,\neg t)) \ .
\end{array}
$$

Thanks to Remark 4.21, it is sufficient to work on

$$
\begin{array}{rcl}
\Pi(x_{s \sqcap t})\,\square\,x & = & \neg\Pi(x\,\square\,(s \sqcap t))\,\square\,((x_s \sqcup x_t) \sqcap \neg\Pi(x_s)\,\square\,x_t \sqcap \neg\Pi(x_t)\,\square\,x_s) \sqcup \\
& & (\Pi(x\,\square\,\neg s)\,\square\,x_{\neg t} \sqcap (x_{\neg s})_{\neg t} \sqcap x_{\neg s}\,\square\,\neg t) \ .
\end{array}
$$

Before working on this equality, we first work on each side of it.

$$
\begin{array}{ll}
& \Pi(x_{s \sqcap t})\,\square\,x \\
= & \langle \text{ by (4.4) with } x, t := x, s \sqcap t, \text{ Proposition 3.14-7 and Boolean algebra } \rangle \\
& \neg\Pi(x\,\square\,(s \sqcap t))\,\square\,\neg\Pi(x\,\square\,\neg s\,\square\,\neg t)\,\square\,x \\
= & \langle \text{ by Proposition 3.14-12 and De Morgan } \rangle \\
& \neg\Pi(x\,\square\,(s \sqcap t))\,\square\,(\neg\Pi(x\,\square\,\neg s) \sqcap \neg\Pi(x\,\square\,\neg t))\,\square\,x
\end{array}
$$

We note

$$L = \neg\Pi(x\,\square\,(s \sqcap t))\,\square\,(\neg\Pi(x\,\square\,\neg s) \sqcap \neg\Pi(x\,\square\,\neg t))\,\square\,x \ .$$

$$
\begin{array}{ll}
& \neg\Pi(x\,\square\,(s \sqcap t))\,\square\,((x_s \sqcup x_t) \sqcap \neg\Pi(x_s)\,\square\,x_t \sqcap \neg\Pi(x_t)\,\square\,x_s) \sqcup \\
& (\Pi(x\,\square\,\neg s)\,\square\,x_{\neg t} \sqcap (x_{\neg s})_{\neg t} \sqcap x_{\neg s}\,\square\,\neg t) \\
= & \langle \text{ by (4.4) with } x, t := x, s, \text{ (4.4), Proposition 3.14-7 and Boolean algebra } \rangle \\
& \neg\Pi(x\,\square\,(s \sqcap t))\,\square\,((x_s \sqcup x_t) \sqcap \neg(\neg\Pi(x\,\square\,s)\,\square\,\neg\Pi(x\,\square\,\neg s)\,\square\,\Pi x)\,\square\,\Pi x\,\square\,x_t \sqcap
\end{array}
$$

$$
\begin{array}{ll}
 & \qquad\qquad \neg(\neg\Pi(x\triangleright t)\triangleright\neg\Pi(x\triangleright\neg t)\triangleright\Pi x)\triangleright\Pi x\triangleright x_s)\sqcup \\
 & (\Pi(x\triangleright\neg s)\triangleright x_{\neg t}\sqcap(x_{\neg s})_{\neg t}\sqcap x_{\neg s}\triangleright\neg t) \\
= & \qquad \langle \text{ by De Morgan } \rangle \\
 & \neg\Pi(x\triangleright(s\sqcap t))\triangleright((x_s\sqcup x_t)\sqcap(\Pi(x\triangleright s)\sqcap\Pi(x\triangleright\neg s)\sqcap\neg\Pi x)\triangleright\Pi x\triangleright x_t\sqcap \\
 & \qquad\qquad (\Pi(x\triangleright t)\sqcap\Pi(x\triangleright\neg t)\sqcap\neg\Pi x)\triangleright\Pi x\triangleright x_s)\sqcup \\
 & (\Pi(x\triangleright\neg s)\triangleright x_{\neg t}\sqcap(x_{\neg s})_{\neg t}\sqcap x_{\neg s}\triangleright\neg t) \\
= & \qquad \langle \text{ by Lemmas 3.17-6 and 3.17-1, (3.8), Corollary 3.21-4 and} \\
 & \quad \text{Boolean algebra } \rangle \\
 & (\neg\Pi(x\triangleright(s\sqcap t))\triangleright(x_s\sqcup x_t)\sqcap\neg\Pi(x\triangleright(s\sqcap t))\triangleright\Pi(x\triangleright\neg s)\triangleright x_t\sqcap \\
 & \neg\Pi(x\triangleright(s\sqcap t))\triangleright\Pi(x\triangleright\neg t)\triangleright x_s)\sqcup \\
 & (\Pi(x\triangleright\neg s)\triangleright x_{\neg t}\sqcap(x_{\neg s})_{\neg t}\sqcap x_{\neg s}\triangleright\neg t) \\
= & \qquad \langle \text{ by Proposition 3.14-20 } \rangle \\
 & \neg\Pi(x\triangleright(s\sqcap t))\triangleright(((x_s\sqcup x_t)\sqcap\Pi(x\triangleright\neg s)\triangleright x_t\sqcap\Pi(x\triangleright\neg t)\triangleright x_s)\sqcup \\
 & \qquad\qquad (\Pi(x\triangleright\neg s)\triangleright x_{\neg t}\sqcap(x_{\neg s})_{\neg t}\sqcap x_{\neg s}\triangleright\neg t))
\end{array}
$$

We note

$$
\begin{array}{rcl}
R & = & \neg\Pi(x\triangleright(s\sqcap t))\triangleright(((x_s\sqcup x_t)\sqcap\Pi(x\triangleright\neg s)\triangleright x_t\sqcap\Pi(x\triangleright\neg t)\triangleright x_s)\sqcup \\
 & & \qquad (\Pi(x\triangleright\neg s)\triangleright x_{\neg t}\sqcap(x_{\neg s})_{\neg t}\sqcap x_{\neg s}\triangleright\neg t))
\end{array}
$$

and we are looking for $L = R$. By Proposition 3.20-17,

$$
L = R \iff \Pi(x\triangleright\neg s)\triangleright L = \Pi(x\triangleright\neg s)\triangleright R \wedge \neg\Pi(x\triangleright\neg s)\triangleright L = \neg\Pi(x\triangleright\neg s)\triangleright R \ .
$$

The derivation of $\Pi(x\triangleright\neg s)\triangleright L = \Pi(x\triangleright\neg s)\triangleright R$ is straightforward.

$$
\begin{array}{ll}
 & \Pi(x\triangleright\neg s)\triangleright L \\
= & \qquad \langle \text{ by Boolean algebra } \rangle \\
 & \Pi(x\triangleright\neg s)\triangleright\neg\Pi(x\triangleright(s\sqcap t))\triangleright\neg\Pi(x\triangleright\neg t)\triangleright x \\
= & \qquad \langle \text{ by Lemma 3.17-6, Proposition 3.14-7 and Boolean algebra } \rangle \\
 & \Pi(x\triangleright\neg s)\triangleright\neg\Pi(x\triangleright(s\sqcap t))\triangleright\neg\Pi(x\triangleright t)\triangleright\neg\Pi(x\triangleright\neg t)\triangleright\Pi x\triangleright x \\
= & \qquad \langle \text{ by (4.4), Proposition 4.22-2, Boolean algebra and (3.8) } \rangle \\
 & \neg\Pi(x\triangleright(s\sqcap t))\triangleright(\Pi(x\triangleright\neg s)\triangleright x_t\sqcup\Pi(x\triangleright\neg s)\triangleright x_{\neg t}) \\
= & \qquad \langle \text{ by Propositions 3.14-7 and 4.22-10, Lemma 3.17-6, Boolean} \\
 & \quad \text{algebra, (3.6) and Corollary 3.21-3 } \rangle \\
 & \neg\Pi(x\triangleright(s\sqcap t))\triangleright(\Pi(x\triangleright\neg s)\triangleright x_t\sqcup(\Pi(x\triangleright\neg s)\triangleright x_{\neg t}\sqcap\Pi(x\triangleright\neg s)\triangleright(x_{\neg s})_{\neg t}))
\end{array}
$$

$$
\begin{array}{ll}
= & \langle \text{ by Propositions 3.14-7 and 3.14-20, (4.4) with } x,t := x,s, \\
& \quad \text{Boolean algebra, (3.6) and Corollary 3.21-3 } \rangle \\
& \neg\Pi(x \triangleright (s \sqcap t)) \triangleright \\
& ((\Pi(x \triangleright \neg s) \triangleright (x_s \sqcup x_t) \sqcap \Pi(x \triangleright \neg s) \triangleright x_t \sqcap \Pi(x \triangleright \neg s) \triangleright \Pi(x \triangleright \neg t) \triangleright x_s) \sqcup \\
& \ (\Pi(x \triangleright \neg s) \triangleright x_{\neg t} \sqcap \Pi(x \triangleright \neg s) \triangleright (x_{\neg s})_{\neg t} \sqcap \Pi(x \triangleright \neg s) \triangleright x_{\neg s} \triangleright \neg t)) \\
= & \langle \text{ by Boolean algebra, Corollary 3.21-4 and (3.8) } \rangle \\
& \Pi(x \triangleright \neg s) \triangleright R
\end{array}
$$

To derive $\neg\Pi(x \triangleright \neg s) \triangleright L = \neg\Pi(x \triangleright \neg s) \triangleright R$, we use Proposition 3.20-17 with $t := \Pi(x \triangleright \neg t)$. Therefore, we will derive the following two equalities.

$$\Pi(x \triangleright \neg t) \triangleright \neg\Pi(x \triangleright \neg s) \triangleright L = \Pi(x \triangleright \neg t) \triangleright \neg\Pi(x \triangleright \neg s) \triangleright R \tag{4.25}$$

$$\neg\Pi(x \triangleright \neg t) \triangleright \neg\Pi(x \triangleright \neg s) \triangleright L = \neg\Pi(x \triangleright \neg t) \triangleright \neg\Pi(x \triangleright \neg s) \triangleright R \tag{4.26}$$

It will conclude the proof.

Before working on (4.25) and (4.26), first note the following two useful laws.

$$\neg\Pi(x \triangleright \neg s) \triangleright \neg\Pi(x \triangleright (s \sqcap t)) \triangleright \Pi x = \neg\Pi(x \triangleright (s \sqcap t)) \triangleright \Pi(x_s) \tag{4.27}$$

$$\Pi x \triangleright R = R \tag{4.28}$$

(4.27) follows from Lemma 3.17-6, Boolean algebra and (4.4) with $x,t := x,s$. (4.28) follows Propositions 3.14-20 and 3.14-7, (4.4) and Boolean algebra.

Proof of (4.25).

$$
\begin{array}{ll}
& \Pi(x \triangleright \neg t) \triangleright \neg\Pi(x \triangleright \neg s) \triangleright L \\
= & \langle \text{ by Boolean algebra } \rangle \\
& \neg\Pi(x \triangleright \neg s) \triangleright \neg\Pi(x \triangleright (s \sqcap t)) \triangleright \Pi(x \triangleright \neg t) \triangleright x \\
= & \langle \text{ by Propositions 3.14-7 and 4.22-2, Boolean algebra, (4.27) and} \\
& \quad (3.8) \rangle \\
& \neg\Pi(x \triangleright (s \sqcap t)) \triangleright \Pi(x_s) \triangleright (\Pi(x \triangleright \neg t) \triangleright x_s \sqcup \Pi(x \triangleright \neg t) \triangleright x_{\neg s}) \\
= & \langle \text{ by Propositions 3.14-7, 4.22-10 and 4.22-6, Lemma 3.17-6,} \\
& \quad \text{Boolean algebra, (3.6) and Corollary 3.21-3 } \rangle \\
& \neg\Pi(x \triangleright (s \sqcap t)) \triangleright \Pi(x_s) \triangleright (\Pi(x \triangleright \neg t) \triangleright x_s \sqcup (\Pi(x \triangleright \neg t) \triangleright (x_{\neg s})_{\neg t} \sqcap \Pi(x \triangleright \neg t) \triangleright x_{\neg s} \triangleright \neg t)) \\
= & \langle \text{ by Propositions 3.14-7 and 3.14-20, (4.4), Boolean algebra,} \\
& \quad (3.6) \text{ and Corollary 3.21-3 } \rangle \\
& \neg\Pi(x \triangleright (s \sqcap t)) \triangleright \Pi(x_s) \triangleright \\
& ((\Pi(x \triangleright \neg t) \triangleright (x_s \sqcup x_t) \sqcap \Pi(x \triangleright \neg t) \triangleright \Pi(x \triangleright \neg s) \triangleright x_t \sqcap \Pi(x \triangleright \neg t) \triangleright x_s) \sqcup
\end{array}
$$

$$
\begin{array}{ll}
 & (\Pi(x \rhd \neg t) \rhd \Pi(x \rhd \neg s) \rhd x_{\neg t} \sqcap \Pi(x \rhd \neg t) \rhd (x_{\neg s})_{\neg t} \sqcap \Pi(x \rhd \neg t) \rhd x_{\neg s} \rhd \neg t)) \\
= & \quad \langle \text{ by Boolean algebra, Corollary 3.21-4 and (3.8) } \rangle \\
 & \neg\Pi(x \rhd (s \sqcap t)) \rhd \Pi(x_s) \rhd \Pi(x \rhd \neg t) \rhd R \\
= & \quad \langle \text{ by Boolean algebra, (4.27) and (4.28) } \rangle \\
 & \Pi(x \rhd \neg t) \rhd \neg\Pi(x \rhd \neg s) \rhd R
\end{array}
$$

Proof of (4.26).

$$
\begin{array}{ll}
 & \neg\Pi(x \rhd \neg t) \rhd \neg\Pi(x \rhd \neg s) \rhd L \\
= & \quad \langle \text{ by (4.27) and Boolean algebra } \rangle \\
 & \neg\Pi(x \rhd (s \sqcap t)) \rhd \Pi(x_s) \rhd \Pi(x_t) \rhd x \\
= & \quad \langle \text{ by (3.15), Proposition 4.22-2 and Boolean algebra,} \\
 & \quad \Pi(x_t) \rhd x_s \sqsubseteq \Pi(x_t) \rhd (x_s \sqcup x_{\neg s}) = \Pi(x_t) \rhd \Pi(x_s) \rhd x = \Pi(x_s) \rhd (x_t \sqcup x_{\neg t}), \\
 & \quad \text{then apply Proposition 4.22-2 and (3.11) } \rangle \\
 & \neg\Pi(x \rhd (s \sqcap t)) \rhd (\Pi(x_s) \rhd (x_t \sqcup x_{\neg t}) \sqcup \Pi(x_t) \rhd x_s) \\
= & \quad \langle \text{ by Propositions 3.14-7 and 3.14-20, and (3.2) } \rangle \\
 & \neg\Pi(x \rhd (s \sqcap t)) \rhd (x_s \sqcup x_t \sqcup \Pi(x_s) \rhd x_{\neg t}) \\
= & \quad \langle \text{ by Propositions 4.22-5 and 4.22-2 } \rangle \\
 & \neg\Pi(x \rhd (s \sqcap t)) \rhd (x_s \sqcup x_t \sqcup (x_s \sqcup x_{\neg s})_{\neg t}) \\
= & \quad \langle \text{ by Corollary 4.24 } \rangle \\
 & \neg\Pi(x \rhd (s \sqcap t)) \rhd \\
 & (x_s \sqcup x_t \sqcup \\
 & (\Pi(x_{\neg s} \rhd t) \rhd x_s \rhd \neg t \sqcap \Pi(x_{\neg s} \rhd t) \rhd (x_s)_{\neg t} \sqcap \Pi(x_s \rhd t) \rhd (x_{\neg s})_{\neg t} \sqcap \\
 & (x_s \rhd \neg t \sqcup (x_{\neg s})_{\neg t}) \sqcap ((x_s)_{\neg t} \sqcup (x_{\neg s})_{\neg t}) \sqcap \Pi(x_s \rhd t) \rhd x_{\neg s} \rhd \neg t \sqcap \\
 & ((x_s)_{\neg t} \sqcup x_{\neg s} \rhd \neg t))) \\
= & \quad \langle \text{ by (3.8), Corollaries 3.21-4 and 3.21-3, Proposition 4.22-9,} \\
 & \quad \text{Boolean algebra, (3.6) and (3.4) } \rangle \\
 & \neg\Pi(x \rhd (s \sqcap t)) \rhd \\
 & (x_s \sqcup x_t \sqcup (\Pi(x_s \rhd t) \rhd (x_{\neg s})_{\neg t} \sqcap (x_s \rhd \neg t \sqcup (x_{\neg s})_{\neg t}) \sqcap ((x_s)_{\neg t} \sqcup (x_{\neg s})_{\neg t}) \sqcap \\
 & \quad \Pi(x_s \rhd t) \rhd x_{\neg s} \rhd \neg t \sqcap ((x_s)_{\neg t} \sqcup x_{\neg s} \rhd \neg t))) \\
= & \quad \langle \text{ by (3.2) and Corollary 3.21-14 } \rangle \\
 & \neg\Pi(x \rhd (s \sqcap t)) \rhd \\
 & (x_t \sqcup ((x_s \sqcup \Pi(x_s \rhd t) \rhd (x_{\neg s})_{\neg t}) \sqcap (x_s \sqcup x_s \rhd \neg t \sqcup (x_{\neg s})_{\neg t}) \sqcap \\
 & \quad (x_s \sqcup (x_s)_{\neg t} \sqcup (x_{\neg s})_{\neg t}) \sqcap (x_s \sqcup \Pi(x_s \rhd t) \rhd x_{\neg s} \rhd \neg t) \sqcap
\end{array}
$$

$$
\begin{array}{ll}
 & (x_s \sqcup (x_s)_{\neg t} \sqcup x_{\neg s} \triangleright \neg t))) \\
= & \quad \langle \text{ by Lemma 3.7-1, (3.11) and Propositions 3.14-7 and 3.14-20 } \rangle \\
 & \neg\, ⟙(x \triangleright (s \sqcap t)) \triangleright \\
 & (x_t \sqcup ((⟙(x_s \triangleright t) \triangleright x_s \sqcup (x_{\neg s})_{\neg t}) \sqcap (x_s \triangleright \neg t \sqcup (x_{\neg s})_{\neg t}) \sqcap \\
 & \qquad (⟙((x_s)_{\neg t}) \triangleright x_s \sqcup (x_s)_{\neg t} \sqcup (x_{\neg s})_{\neg t}) \sqcap (⟙(x_s \triangleright t) \triangleright x_s \sqcup x_{\neg s} \triangleright \neg t) \sqcap \\
 & \qquad (⟙((x_s)_{\neg t}) \triangleright x_s \sqcup (x_s)_{\neg t} \sqcup x_{\neg s} \triangleright \neg t))) \\
= & \quad \langle \text{ by (3.19), Proposition 4.22-2, (3.2) and (3.3) } \rangle \\
 & \neg\, ⟙(x \triangleright (s \sqcap t)) \triangleright \\
 & (x_t \sqcup ((x_s \triangleright t \sqcup (x_{\neg s})_{\neg t}) \sqcap (x_s \triangleright \neg t \sqcup (x_{\neg s})_{\neg t}) \sqcap \\
 & \qquad ((x_s)_t \sqcup (x_s)_{\neg t} \sqcup (x_{\neg s})_{\neg t}) \sqcap (x_s \triangleright t \sqcup x_{\neg s} \triangleright \neg t) \sqcap \\
 & \qquad ((x_s)_t \sqcup (x_s)_{\neg t} \sqcup x_{\neg s} \triangleright \neg t))) \\
= & \quad \langle \text{ by Proposition 4.22-6, Boolean algebra and (3.6),} \\
 & \quad\ ⟙(x_t) \triangleright x_s \triangleright \neg t = ⟙(x_t) \triangleright x_s \triangleright t \triangleright \neg t = ⟙(x_t) \triangleright x_s \triangleright \top = \top, \\
 & \quad\ \text{then apply (3.4) and Corollary 3.21-3 } \rangle \\
 & \neg\, ⟙(x \triangleright (s \sqcap t)) \triangleright \\
 & (x_t \sqcup ((x_s \triangleright t \sqcup (x_{\neg s})_{\neg t}) \sqcap (x_s \triangleright \neg t \sqcup (x_{\neg s})_{\neg t}) \sqcap \\
 & \qquad ((x_s)_t \sqcup (x_s)_{\neg t} \sqcup (x_{\neg s})_{\neg t}) \sqcap (x_s \triangleright t \sqcup x_{\neg s} \triangleright \neg t) \sqcap \\
 & \qquad (⟙(x_t) \triangleright x_s \triangleright \neg t \sqcup x_{\neg s} \triangleright \neg t) \sqcap ((x_s)_t \sqcup (x_s)_{\neg t} \sqcup x_{\neg s} \triangleright \neg t))) \\
= & \quad \langle \text{ by Proposition 3.14-20 and Corollary 3.21-4 } \rangle \\
 & \neg\, ⟙(x \triangleright (s \sqcap t)) \triangleright \\
 & (x_t \sqcup ((x_s \triangleright t \sqcup (x_{\neg s})_{\neg t}) \sqcap (x_s \triangleright \neg t \sqcup (x_{\neg s})_{\neg t}) \sqcap \\
 & \qquad ((x_s)_t \sqcup (x_s)_{\neg t} \sqcup (x_{\neg s})_{\neg t}) \sqcap (x_s \triangleright t \sqcup x_{\neg s} \triangleright \neg t) \sqcap \\
 & \qquad (x_s \triangleright \neg t \sqcup x_{\neg s} \triangleright \neg t) \sqcap ((x_s)_t \sqcup (x_s)_{\neg t} \sqcup x_{\neg s} \triangleright \neg t))) \\
= & \quad \langle \text{ by (3.2) and Corollary 3.21-14 } \rangle \\
 & \neg\, ⟙(x \triangleright (s \sqcap t)) \triangleright (x_t \sqcup (((x_s \triangleright t \sqcap x_s \triangleright \neg t \sqcap ((x_s)_t \sqcup (x_s)_{\neg t})) \sqcup (x_{\neg s})_{\neg t}) \sqcap \\
 & \qquad\qquad ((x_s \triangleright t \sqcap x_s \triangleright \neg t \sqcap ((x_s)_t \sqcup (x_s)_{\neg t})) \sqcup x_{\neg s} \triangleright \neg t)) \\
= & \quad \langle \text{ by (4.3) with } x, t := x_s, t \rangle \\
 & \neg\, ⟙(x \triangleright (s \sqcap t)) \triangleright (x_t \sqcup ((x_s \sqcup (x_{\neg s})_{\neg t}) \sqcap (x_s \sqcup x_{\neg s} \triangleright \neg t))) \\
= & \quad \langle \text{ by Corollary 3.21-14, (3.2) and Propositions 3.14-7 and 3.14-20 } \rangle \\
 & \neg\, ⟙(x \triangleright (s \sqcap t)) \triangleright ⟙(x_s) \triangleright ⟙(x_t) \triangleright (x_s \sqcup x_t \sqcup ((x_{\neg s})_{\neg t} \sqcap x_{\neg s} \triangleright \neg t)) \\
= & \quad \langle \text{ by (3.8), Corollaries 3.21-4 and 3.21-3, Remark 4.8 and (3.6) } \rangle \\
 & \neg\, ⟙(x \triangleright (s \sqcap t)) \triangleright ⟙(x_s) \triangleright ⟙(x_t) \triangleright R
\end{array}
$$

$$
\begin{array}{ll}
= & \langle \text{ by (4.27) and (4.28) } \rangle \\
& \neg\sqcap(x\circ\neg t)\circ\neg\sqcap(x\circ\neg s)\circ R
\end{array}
$$

This completes the demonstration. □

Corollary 4.26. *Suppose $\mathcal{A}$ is an algebra of decomposable elements. The following equalities are valid for all $x, y, z \in A$ and all $r, s, t \in \mathsf{test}(A)$.*

1. $t \sqsubseteq s \implies (x\circ s)_t = (x\circ s)_{\neg t} = \top$
2. $\sqcap(x\circ(s \sqcap t))\circ\sqcap(x_s)\circ\sqcap(x_t)\circ x = \sqcap(x\circ(s \sqcap t))\circ(x_s \sqcup x_t)$
3. $\sqcap(x\circ\neg s)\circ x_{s\sqcap t} = \sqcap(x\circ\neg s)\circ x_t$
4. $s\circ t = \top \implies x_{s\sqcap t}\circ t \sqsubseteq \sqcap(x_{s\sqcap t}\circ t)\circ x_{r\sqcap t}$
5. $t \sqsubseteq s \implies (x\circ s \sqcup y\circ\neg s)_t = \sqcap(y\circ\neg t)\circ x\circ s \sqcap (x\circ s \sqcup (y\circ\neg s)_t)$
6. $t \sqsubseteq s \implies (x_s \sqcup x_{\neg s})_t = \sqcap(x_{\neg s}\circ\neg t)\circ x_s \sqcap (x_s \sqcup (x_{\neg s})_t)$
7. $s \sqsubseteq t \implies (x\circ s \sqcup y\circ\neg s)_t = \sqcap(y\circ\neg s)\circ x\circ t \sqcap \sqcap(y\circ\neg s)\circ(x\circ s)_t$
8. $s \sqsubseteq t \implies (x_s \sqcup x_{\neg s})_t = x_s\circ t \sqcap (x_s)_t$
9. $(x\circ t \sqcup y\circ\neg t)_t = \sqcap(y\circ\neg t)\circ x\circ t$
10. $x\circ t \sqsubseteq y\circ t \sqcup z\circ\neg t \iff x\circ t \sqsubseteq \sqcap(z\circ\neg t)\circ y\circ t$

Proof :

1. Assume $t \sqsubseteq s$. By (4.4) with $x, t := x\circ s, t$, the assumption and Boolean algebra, $\sqcap((x\circ s)_{\neg t}) = \sqcap((x\circ s)_t) \sqsupseteq \neg\sqcap(x\circ s\circ t)\circ\sqcap(x\circ s) = \neg\sqcap(x\circ s)\circ\sqcap(x\circ s) = \top$. Thus, by Proposition 3.14-19, $(x\circ s)_{\neg t} = (x\circ s)_t = \top$.
2. First, we derive an intermediate result.

$$
\begin{array}{ll}
& \sqcap(x\circ(s \sqcap t))\circ\sqcap(x_s)\circ x_t \\
= & \langle \text{ by Proposition 4.22-5 } \rangle \\
& (\sqcap(x\circ(s \sqcap t))\circ\sqcap(x_s)\circ x)_t \\
= & \langle \text{ by Boolean algebra and (3.19) } \rangle
\end{array}
$$

$$
\begin{array}{ll}
& (\sqcap(x_s)\triangleright x\triangleright(s \sqcap t))_t \\
= & \qquad \langle \text{ by Proposition 4.22-2 } \rangle \\
& ((x_s \sqcup x_{\neg s})\triangleright(s \sqcap t))_t \\
= & \qquad \langle \text{ by (3.9), (4.5) with } x,t := x,s, \text{ (4.6) with } x,t := x,s \text{ and} \\
& \quad \text{Boolean algebra } \rangle \\
& (x_s \sqcup x_{\neg s}\triangleright t)_t \\
= & \qquad \langle \text{ by Theorem 4.23 } \rangle \\
& \sqcap(x_{\neg s}\triangleright t\triangleright\neg t)\triangleright x_s\triangleright t \sqcap \sqcap(x_{\neg s}\triangleright t\triangleright\neg t)\triangleright(x_s)_t \sqcap (x_s\triangleright t \sqcup (x_{\neg s}\triangleright t)_t) \sqcap \\
& \sqcap(x_s\triangleright\neg t)\triangleright x_{\neg s}\triangleright t\triangleright t \sqcap \sqcap(x_s\triangleright\neg t)\triangleright(x_{\neg s}\triangleright t)_t \sqcap ((x_s)_t \sqcup x_{\neg s}\triangleright t\triangleright t) \sqcap \\
& ((x_s)_t \sqcup (x_{\neg s}\triangleright t)_t) \\
= & \qquad \langle \text{ by Boolean algebra, (3.6), Proposition 3.14-1, (3.4) and} \\
& \quad \text{Corollary 4.26-1 } \rangle \\
& \top \sqcap \top \sqcap \top \sqcap \sqcap(x_s\triangleright\neg t)\triangleright x_{\neg s}\triangleright t \sqcap \top \sqcap ((x_s)_t \sqcup x_{\neg s}\triangleright t) \sqcap \top \\
= & \qquad \langle \text{ by Corollaries 3.21-3 and 3.21-15 } \rangle \\
& (\sqcap(x_s\triangleright\neg t)\triangleright x_{\neg s}\triangleright t \sqcap (x_s)_t) \sqcup (\sqcap(x_s\triangleright\neg t)\triangleright x_{\neg s}\triangleright t \sqcap x_{\neg s}\triangleright t) \\
= & \qquad \langle \text{ by (3.7), Corollary 3.21-5 and Boolean algebra } \rangle \\
& (\sqcap(x_s\triangleright\neg t)\triangleright x_{\neg s}\triangleright t \sqcap (x_s)_t) \sqcup x_{\neg s}\triangleright t \\
\sqsupseteq & \qquad \langle \text{ by (3.15) } \rangle \\
& x_{\neg s}\triangleright t
\end{array}
$$

We note

$$x_{\neg s}\triangleright t \sqsubseteq \sqcap(x\triangleright(s \sqcap t))\triangleright\sqcap(x_s)\triangleright x_t \ . \tag{4.29}$$

And now the main proof.

$$
\begin{array}{ll}
& \sqcap(x\triangleright(s \sqcap t))\triangleright\sqcap(x_s)\triangleright\sqcap(x_t)\triangleright x \\
= & \qquad \langle \text{ by (3.3) } \rangle \\
& \sqcap(x\triangleright(s \sqcap t))\triangleright\sqcap(x_s)\triangleright\sqcap(x_t)\triangleright(x \sqcup x) \\
= & \qquad \langle \text{ by Boolean algebra and Proposition 3.14-20 } \rangle \\
& \sqcap(x\triangleright(s \sqcap t))\triangleright\sqcap(x_s)\triangleright\sqcap(x_t)\triangleright(\sqcap(x_s)\triangleright x \sqcup \sqcap(x_t)\triangleright x) \\
= & \qquad \langle \text{ by Proposition 4.22-2 } \rangle \\
& \sqcap(x\triangleright(s \sqcap t))\triangleright\sqcap(x_s)\triangleright\sqcap(x_t)\triangleright(x_s \sqcup x_{\neg s} \sqcup x_t \sqcup x_{\neg t}) \\
= & \qquad \langle \text{ by Boolean algebra and Proposition 3.14-20 } \rangle
\end{array}
$$

$$
\begin{array}{ll}
& \Pi(x \triangleright (s \sqcap t)) \triangleright (\Pi(x_t) \triangleright x_s \sqcup \Pi(x \triangleright (s \sqcap t)) \triangleright x_{\neg s} \sqcup \Pi(x_s) \triangleright x_t \sqcup \Pi(x \triangleright (s \sqcap t)) \triangleright x_{\neg t}) \\
= & \quad \langle \text{ by Proposition 4.22-6, (4.6) with } x, t := x, s \text{ and (4.6) } \rangle \\
& \Pi(x \triangleright (s \sqcap t)) \triangleright (\Pi(x_t) \triangleright x_s \sqcup \Pi(x \triangleright (s \sqcap t)) \triangleright x_{\neg s} \triangleright \neg s \triangleright (s \sqcap t) \sqcup \\
& \qquad \Pi(x_s) \triangleright x_t \sqcup \Pi(x \triangleright (s \sqcap t)) \triangleright x_{\neg t} \triangleright \neg t \triangleright (s \sqcap t)) \\
= & \quad \langle \text{ by Boolean algebra, (4.6) and Proposition 3.14-20 } \rangle \\
& \Pi(x \triangleright (s \sqcap t)) \triangleright \Pi(x_t) \triangleright x_s \sqcup x_{\neg s} \triangleright t \sqcup \Pi(x \triangleright (s \sqcap t)) \triangleright \Pi(x_s) \triangleright x_t \sqcup x_{\neg t} \triangleright s \\
= & \quad \langle \text{ by (4.29) and (3.11) } \rangle \\
& \Pi(x \triangleright (s \sqcap t)) \triangleright \Pi(x_t) \triangleright x_s \sqcup \Pi(x \triangleright (s \sqcap t)) \triangleright \Pi(x_s) \triangleright x_t \\
= & \quad \langle \text{ by (3.8) and Propositions 3.14-20 and 3.14-11 } \rangle \\
& \Pi(x \triangleright (s \sqcap t)) \triangleright (x_s \sqcup x_t)
\end{array}
$$

3.

$$
\begin{array}{ll}
& \Pi(x \triangleright \neg s) \triangleright x_{s \sqcap t} \\
= & \quad \langle \text{ by Proposition 4.22-4 } \rangle \\
& (x \triangleright \neg s)_{s \sqcap t} \\
= & \quad \langle \text{ by Proposition 4.25-1 } \rangle \\
& \neg \Pi(x \triangleright \neg s \triangleright (s \sqcap t)) \triangleright (((x \triangleright \neg s)_s \sqcup (x \triangleright \neg s)_t) \sqcap \neg \Pi((x \triangleright \neg s)_s) \triangleright (x \triangleright \neg s)_t \sqcap \\
& \qquad \neg \Pi((x \triangleright \neg s)_t) \triangleright (x \triangleright \neg s)_s) \\
= & \quad \langle \text{ by (4.4) with } x, t := x \triangleright \neg s, s, \text{ Propositions 3.14-7 and 3.14-1,} \\
& \quad \text{Boolean algebra, (3.6) and (3.7) } \rangle \\
& \neg \Pi(x \triangleright \neg s \triangleright t) \triangleright ((\top \sqcup (x \triangleright \neg s)_t) \sqcap (x \triangleright \neg s)_t \sqcap \top) \\
= & \quad \langle \text{ by (3.4) and Corollary 3.21-3 } \rangle \\
& \neg \Pi(x \triangleright \neg s \triangleright t) \triangleright (x \triangleright \neg s)_t \\
= & \quad \langle \text{ by (4.4) with } x, t := x \triangleright \neg s, t, \text{ Proposition 3.14-7 and Boolean} \\
& \quad \text{algebra } \rangle \\
& (x \triangleright \neg s)_t \\
= & \quad \langle \text{ by Proposition 4.22-4 } \rangle \\
& \Pi(x \triangleright \neg s) \triangleright x_t
\end{array}
$$

4. Assume $s \triangleright t = \top$.

$$
\begin{array}{ll}
& \Pi(x_{s \sqcap t} \triangleright t) \triangleright x_{r \sqcap t} \\
= & \quad \langle \text{ by Proposition 4.25-1 } \rangle \\
& \Pi(\neg \Pi(x \triangleright (s \sqcap t)) \triangleright ((x_s \sqcup x_t) \sqcap \neg \Pi(x_s) \triangleright x_t \sqcap \neg \Pi(x_t) \triangleright x_s) \triangleright t) \triangleright \\
& \neg \Pi(x \triangleright (r \sqcap t)) \triangleright ((x_r \sqcup x_t) \sqcap \neg \Pi(x_r) \triangleright x_t \sqcap \neg \Pi(x_t) \triangleright x_r)
\end{array}
$$

$=$ ⟨ by (3.21), Boolean algebra and Propositions 3.14-9 and 3.14-3,
the domains of $x_s \sqcup x_t$, $\neg\Pi(x_s)\triangleright x_t$ and $\neg\Pi(x_t)\triangleright x_s$
are pairwise disjoint,
then apply Corollary 3.21-17 and (3.9) ⟩

$\Pi(\neg\Pi(x\triangleright(s \sqcap t))\triangleright((x_s\triangleright t \sqcup x_t\triangleright t) \sqcap \neg\Pi(x_s)\triangleright x_t\triangleright t \sqcap \neg\Pi(x_t)\triangleright x_s\triangleright t))\triangleright$
$\neg\Pi(x\triangleright(r \sqcap t))\triangleright((x_r \sqcup x_t) \sqcap \neg\Pi(x_r)\triangleright x_t \sqcap \neg\Pi(x_t)\triangleright x_r)$

$=$ ⟨ by (4.5) with $x, t := x, s$, (4.5), the hypothesis, (3.4), (3.6)
and Corollary 3.21-3 ⟩

$\Pi(\neg\Pi(x\triangleright(s \sqcap t))\triangleright\neg\Pi(x_s)\triangleright x_t)\triangleright$
$\neg\Pi(x\triangleright(r \sqcap t))\triangleright((x_r \sqcup x_t) \sqcap \neg\Pi(x_r)\triangleright x_t \sqcap \neg\Pi(x_t)\triangleright x_r)$

$\sqsupseteq$ ⟨ by Proposition 3.14-9 and Lemma 3.7-1 ⟩

$\neg\Pi(x\triangleright(s \sqcap t))\triangleright\neg\Pi(x_s)\triangleright\Pi(x_t)\triangleright((x_r \sqcup x_t) \sqcap \neg\Pi(x_r)\triangleright x_t \sqcap \neg\Pi(x_t)\triangleright x_r)$

$=$ ⟨ by Corollaries 3.21-4 and 3.21-3, Boolean algebra and (3.6) ⟩

$\neg\Pi(x\triangleright(s \sqcap t))\triangleright\neg\Pi(x_s)\triangleright\Pi(x_t)\triangleright((x_r \sqcup x_t) \sqcap \neg\Pi(x_r)\triangleright x_t)$

$\sqsupseteq$ ⟨ by (3.15) and Propositions 3.14-20 and 3.14-7,
$\Pi(x_r)\triangleright x_t \sqsubseteq x_r \sqcup \Pi(x_r)\triangleright x_t = x_r \sqcup x_t$,
by (3.21) and Propositions 3.14-3 and 3.14-9,
$\Pi(\Pi(x_r)\triangleright x_t) = \Pi(x_r \sqcup x_t)$,
then apply Lemma 3.22-3 ⟩

$\neg\Pi(x\triangleright(s \sqcap t))\triangleright\neg\Pi(x_s)\triangleright\Pi(x_t)\triangleright(\Pi(x_r)\triangleright x_t \sqcap \neg\Pi(x_r)\triangleright x_t)$

$=$ ⟨ by Corollary 3.21-6 and Proposition 3.14-7 ⟩

$\neg\Pi(x\triangleright(s \sqcap t))\triangleright\neg\Pi(x_s)\triangleright x_t$

$=$ ⟨ by (4.5) with $x, t := x, s$, (4.5), the hypothesis, (3.4), (3.6)
and Corollary 3.21-3 ⟩

$\neg\Pi(x\triangleright(s \sqcap t))\triangleright((x_s\triangleright t \sqcup x_t\triangleright t) \sqcap \neg\Pi(x_s)\triangleright x_t\triangleright t \sqcap \neg\Pi(x_t)\triangleright x_s\triangleright t)$

$=$ ⟨ by (3.21), Boolean algebra and Propositions 3.14-9 and 3.14-3,
the domains of $x_s \sqcup x_t$, $\neg\Pi(x_s)\triangleright x_t$ and $\neg\Pi(x_t)\triangleright x_s$
are pairwise disjoint,
then apply Corollary 3.21-17 and (3.9) ⟩

$\neg\Pi(x\triangleright(s \sqcap t))\triangleright((x_s \sqcup x_t) \sqcap \neg\Pi(x_s)\triangleright x_t \sqcap \neg\Pi(x_t)\triangleright x_s)\triangleright t$

$=$ ⟨ by Proposition 4.25-1 ⟩

$x_{s \sqcap t}\triangleright t$

5. Assume $t \sqsubseteq s$.

$(x\triangleright s \sqcup y\triangleright\neg s)_t$

$$
\begin{array}{ll}
= & \langle \text{ by Theorem 4.23, the hypothesis and Boolean algebra } \rangle \\
& \Cap(y \sqcup \neg t) \sqcup x \sqcup s \sqcap \Cap(y \sqcup \neg t) \sqcup (x \sqcup s)_t \sqcap (x \sqcup s \sqcup (y \sqcup \neg s)_t) \sqcap \\
& \Cap(x \sqcup \top) \sqcup y \sqcup \neg s \sqcup t \sqcap \Cap(x \sqcup \top) \sqcup (y \sqcup \neg s)_t \sqcap ((x \sqcup s)_t \sqcup y \sqcup \neg s \sqcup t) \sqcap \\
& ((x \sqcup s)_t \sqcup (y \sqcup \neg s)_t) \\
= & \langle \text{ by (3.6), Proposition 3.14-19 and Corollary 3.21-3 } \rangle \\
& \Cap(y \sqcup \neg t) \sqcup x \sqcup s \sqcap \Cap(y \sqcup \neg t) \sqcup (x \sqcup s)_t \sqcap (x \sqcup s \sqcup (y \sqcup \neg s)_t) \sqcap \\
& ((x \sqcup s)_t \sqcup y \sqcup \neg s \sqcup t) \sqcap ((x \sqcup s)_t \sqcup (y \sqcup \neg s)_t) \\
= & \langle \text{ by Corollaries 4.26-1 and 3.21-3, (3.6) and (3.4) } \rangle \\
& \Cap(y \sqcup \neg t) \sqcup x \sqcup s \sqcap (x \sqcup s \sqcup (y \sqcup \neg s)_t)
\end{array}
$$

6. Assume $t \sqsubseteq s$.

$$
\begin{array}{ll}
& (x_s \sqcup x_{\neg s})_t \\
= & \langle \text{ by (4.5) with } x, t := x, s \text{ and (4.6) with } x, t := x, s \ \rangle \\
& (x_s \sqcup s \sqcup x_{\neg s} \sqcup \neg s)_t \\
= & \langle \text{ by Corollary 4.26-5, (4.5) with } x, t := x, s, \text{ (4.6) with} \\
& \quad x, t := x, s, \text{ the hypothesis and Boolean algebra } \rangle \\
& \Cap(x_{\neg s} \sqcup \neg t) \sqcup x_s \sqcap (x_s \sqcup (x_{\neg s})_t)
\end{array}
$$

7. Assume $s \sqsubseteq t$, then $\neg t \sqsubseteq \neg s$ by Boolean algebra.

$$
\begin{array}{ll}
& (x \sqcup s \sqcup y \sqcup \neg s)_t \\
= & \langle \text{ by Theorem 4.23, the hypothesis and Boolean algebra } \rangle \\
& \Cap(y \sqcup \neg s) \sqcup x \sqcup t \sqcap \Cap(y \sqcup \neg s) \sqcup (x \sqcup s)_t \sqcap (x \sqcup t \sqcup (y \sqcup \neg s)_t) \sqcap \\
& \Cap(x \sqcup s \sqcup \neg t) \sqcup y \sqcup \top \sqcap \Cap(x \sqcup s \sqcup \neg t) \sqcup (y \sqcup \neg s)_t \sqcap ((x \sqcup s)_t \sqcup y \sqcup \top) \sqcap \\
& ((x \sqcup s)_t \sqcup (y \sqcup \neg s)_t) \\
= & \langle \text{ by (3.6), (3.4) and Corollary 3.21-3 } \rangle \\
& \Cap(y \sqcup \neg s) \sqcup x \sqcup t \sqcap \Cap(y \sqcup \neg s) \sqcup (x \sqcup s)_t \sqcap (x \sqcup t \sqcup (y \sqcup \neg s)_t) \sqcap \\
& \Cap(x \sqcup s \sqcup \neg t) \sqcup (y \sqcup \neg s)_t \sqcap ((x \sqcup s)_t \sqcup (y \sqcup \neg s)_t) \\
= & \langle \text{ by Corollaries 4.26-1 and 3.21-3, (3.4) and (3.6) } \rangle \\
& \Cap(y \sqcup \neg s) \sqcup x \sqcup t \sqcap \Cap(y \sqcup \neg s) \sqcup (x \sqcup s)_t
\end{array}
$$

8. Assume $s \sqsubseteq t$.

$(x_s \sqcup x_{\neg s})_t$

$=$ $\langle$ by (4.5) with $x,t := x,s$ and (4.6) with $x,t := x,s$ $\rangle$

$(x_s \mathbin{;} s \sqcup x_{\neg s} \mathbin{;} \neg s)_t$

$=$ $\langle$ by Corollary 4.26-7, (4.5) with $x,t := x,s$, (4.6) with $x,t := x,s$, the hypothesis and Boolean algebra $\rangle$

$\Pi(x_{\neg s}) \mathbin{;} x_s \mathbin{;} t \sqcap \Pi(x_{\neg s}) \mathbin{;} (x_s)_t$

$=$ $\langle$ by Proposition 3.14-7, (4.4) with $x,t := x,s$, (4.4) with $x,t := x_s,t$ and Boolean algebra $\rangle$

$x_s \mathbin{;} t \sqcap (x_s)_t$

9. $(x \mathbin{;} t \sqcup y \mathbin{;} \neg t)_t$

$=$ $\langle$ by Corollary 4.26-5 $\rangle$

$\Pi(y \mathbin{;} \neg t) \mathbin{;} x \mathbin{;} t \sqcap (x \mathbin{;} t \sqcup (y \mathbin{;} \neg t)_t)$

$=$ $\langle$ by Corollaries 4.26-1 and 3.21-3, and (3.4) $\rangle$

$\Pi(y \mathbin{;} \neg t) \mathbin{;} x \mathbin{;} t$

10. $x \mathbin{;} t \sqsubseteq y \mathbin{;} t \sqcup z \mathbin{;} \neg t$

$\iff$ $\langle$ by (3.11) $\rangle$

$x \mathbin{;} t \sqcup y \mathbin{;} t \sqcup z \mathbin{;} \neg t = y \mathbin{;} t \sqcup z \mathbin{;} \neg t$

$\implies$ $\langle$ by Leibniz $\rangle$

$(x \mathbin{;} t \sqcup y \mathbin{;} t \sqcup z \mathbin{;} \neg t)_t = (y \mathbin{;} t \sqcup z \mathbin{;} \neg t)_t$

$\iff$ $\langle$ by (3.9) and Corollary 4.26-9 $\rangle$

$\Pi(z \mathbin{;} \neg t) \mathbin{;} (x \mathbin{;} t \sqcup y \mathbin{;} t) = \Pi(z \mathbin{;} \neg t) \mathbin{;} y \mathbin{;} t$

$\iff$ $\langle$ by (3.8) and (3.11) $\rangle$

$\Pi(z \mathbin{;} \neg t) \mathbin{;} x \mathbin{;} t \sqsubseteq \Pi(z \mathbin{;} \neg t) \mathbin{;} y \mathbin{;} t$

$\iff$ $\langle$ by Proposition 3.14-6 $\rangle$

$x \mathbin{;} t \sqsubseteq \Pi(z \mathbin{;} \neg t) \mathbin{;} y \mathbin{;} t$

$\implies$ $\langle$ by Propositions 3.14-20 and 3.14-7 $\rangle$

$x \mathbin{;} t \sqsubseteq y \mathbin{;} t \sqcup z \mathbin{;} \neg t$

□

Theorem 4.27. *Suppose $\mathcal{A}$ is an algebra of decomposable elements. The following equality is valid for all $x, y \in A$ and all $t \in \mathsf{test}(A)$.*

$$(x \mathbin{;} y)_t = \Pi((x \mathbin{;} y)_t) \mathbin{;} (x \mathbin{;} (y \mathbin{;} t \sqcap y_t) \sqcap x_{\Pi(y \mathbin{;} t \sqcap y_t)} \mathbin{;} (y \mathbin{;} t \sqcap y_t))$$

Remark 4.28. One might understand Theorem 4.27 intuitively by noting that

$$\pi((x\triangleright y)_t)\triangleright(x\triangleright(y\triangleright t\mathbin{⫪} y_t)\mathbin{⫪} x_{\pi(y\triangleright t\mathbin{⫪} y_t)}\triangleright(y\triangleright t\mathbin{⫪} y_t)) = \pi((x\triangleright y)_t)\mathbin{\cdot_{\mathcal{D}}}(x\mathbin{\cdot_{\mathcal{D}}}(y\mathbin{\cdot_{\mathcal{D}}} t))$$

by Proposition 4.17-3, (4.5) with $x,t := y,t$ and Definition 4.16.

Proof : Since $\pi((x\triangleright y)_t) = \neg\pi(x\triangleright y\triangleright t)\triangleright\neg\pi(x\triangleright y\triangleright\neg t)\triangleright\pi(x\triangleright y)$ according to (4.4) with $x,t := x\triangleright y,t$, we will rather demonstrate

$$(x\triangleright y)_t = \neg\pi(x\triangleright y\triangleright t)\triangleright\neg\pi(x\triangleright y\triangleright\neg t)\triangleright\pi(x\triangleright y)\triangleright(x\triangleright(y\triangleright t\mathbin{⫪} y_t)\mathbin{⫪} x_{\pi(y\triangleright t\mathbin{⫪} y_t)}\triangleright(y\triangleright t\mathbin{⫪} y_t))\ .$$

In this proof, the following abbreviations are used.

$$\begin{aligned}
A :=&\ \neg\pi(x\triangleright y\triangleright t)\triangleright\neg\pi(x\triangleright y\triangleright\neg t)\triangleright\pi(x\triangleright y)\\
B :=&\ x\triangleright(y\triangleright t\mathbin{⫪} y_t)\mathbin{⫪} x_{\pi(y\triangleright t\mathbin{⫪} y_t)}\triangleright(y\triangleright t\mathbin{⫪} y_t)\\
C :=&\ x\triangleright(y\triangleright t\mathbin{⫪} y_t)\mathbin{⫪} x_{\neg\pi(y\triangleright t\mathbin{⫪} y_t)}\triangleright y\triangleright\neg t\\
D :=&\ x\triangleright(y\triangleright\neg t\mathbin{⫪} y_{\neg t})\mathbin{⫪} x_{\pi(y\triangleright\neg t\mathbin{⫪} y_{\neg t})}\triangleright(y\triangleright\neg t\mathbin{⫪} y_{\neg t})\\
E :=&\ x\triangleright(y\triangleright\neg t\mathbin{⫪} y_{\neg t})\mathbin{⫪} x_{\neg\pi(y\triangleright\neg t\mathbin{⫪} y_{\neg t})}\triangleright y\triangleright t
\end{aligned}$$

Hence, we have to show $(x\triangleright y)_t = A\triangleright B$. By symmetry, $(x\triangleright y)_{\neg t} = A\triangleright D$. Therefore, we verify that $A\triangleright B$ and $A\triangleright D$ satisfy (4.4), (4.5), (4.6) and (4.3) with $x,t := x\triangleright y,t$ (see definition 4.7), in this order.

1. Proof of (4.4). We have to show $\pi(A\triangleright B) = \pi(A\triangleright D) = A$. We begin by showing $\pi B \sqsubseteq A$.

$$\begin{array}{ll}
& \pi B \sqsubseteq A\\
\iff & \quad\langle\ \text{by Corollary 3.21-16, (3.20) and (4.5) with } x,t := x,\pi(y\triangleright t\mathbin{⫪} y_t)\ \rangle\\
& \pi(x\triangleright(y\triangleright t\mathbin{⫪} y_t))\mathbin{⫪}\pi(x_{\pi(y\triangleright t\mathbin{⫪} y_t)}) \sqsubseteq \neg\pi(x\triangleright y\triangleright t)\triangleright\neg\pi(x\triangleright y\triangleright\neg t)\triangleright\pi(x\triangleright y)\\
\iff & \quad\langle\ \text{by Boolean algebra}\ \rangle\\
& \pi(x\triangleright(y\triangleright t\mathbin{⫪} y_t))\mathbin{⫪}\pi(x\triangleright y\triangleright t)\mathbin{⫪}\pi(x\triangleright y\triangleright\neg t) \sqsubseteq \pi(x\triangleright y)\triangleright\neg\pi(x_{\pi(y\triangleright t\mathbin{⫪} y_t)})\\
\iff & \quad\langle\ \text{by Corollary 3.21-12 and Proposition 3.14-8,}\\
& \quad\ \mathsf{true} \Longrightarrow y\triangleright t\mathbin{⫪} y_t \sqsubseteq y\triangleright t \Longrightarrow x\triangleright(y\triangleright t\mathbin{⫪} y_t) \sqsubseteq x\triangleright y\triangleright t\\
& \quad\ \Longrightarrow \pi(x\triangleright(y\triangleright t\mathbin{⫪} y_t)) \sqsubseteq \pi(x\triangleright y\triangleright t),\\
& \quad\ \text{then apply Boolean algebra and (4.4) with } x,t := x,\pi(y\triangleright t\mathbin{⫪} y_t)\\
& \quad\rangle\\
& \pi(x\triangleright(y\triangleright t\mathbin{⫪} y_t))\mathbin{⫪}\pi(x\triangleright y\triangleright\neg t)\\
& \sqsubseteq \pi(x\triangleright y)\triangleright\neg(\neg\pi(x\triangleright\pi(y\triangleright t\mathbin{⫪} y_t))\triangleright\neg\pi(x\triangleright\neg\pi(y\triangleright t\mathbin{⫪} y_t))\triangleright\pi x)
\end{array}$$

$$
\begin{array}{ll}
\Longleftrightarrow & \langle \text{ by De Morgan, Boolean algebra and (3.20) } \rangle \\
& \ulcorner(x \sqsubset (y \sqsubset t \sqcap y_t)) \sqcap \ulcorner(x \sqsubset y \sqsubset \neg t) \\
& \sqsubseteq \ulcorner(x \sqsubset \ulcorner y) \sqsubset \ulcorner(x \sqsubset \ulcorner(y \sqsubset t \sqcap y_t)) \sqcap \ulcorner(x \sqsubset y) \sqsubset \ulcorner(x \sqsubset \neg \ulcorner(y \sqsubset t \sqcap y_t)) \sqcap \ulcorner(x \sqsubset y) \sqsubset \neg \ulcorner x \\
\Longleftrightarrow & \langle \text{ by Propositions 3.14-9 and 3.14-7, (3.19), Corollaries 3.21-4} \\
& \quad \text{and 3.21-3, (4.4) with } x, t := y, t \text{ and Boolean algebra } \rangle \\
& \ulcorner(x \sqsubset (y \sqsubset t \sqcap y_t)) \sqcap \ulcorner(x \sqsubset y \sqsubset \neg t) \\
& \sqsubseteq \ulcorner(x \sqsubset (y \sqsubset t \sqcap y_t)) \sqcap \ulcorner(x \sqsubset y) \sqsubset \ulcorner(x \sqsubset \neg \ulcorner(y \sqsubset t \sqcap y_t)) \\
\Longleftarrow & \langle \text{ by Lemma 3.22-1 } \rangle \\
& \ulcorner(x \sqsubset y \sqsubset \neg t) \sqsubseteq \ulcorner(x \sqsubset y) \sqsubset \ulcorner(x \sqsubset \neg \ulcorner(y \sqsubset t \sqcap y_t)) \\
\Longleftrightarrow & \langle \text{ by Proposition 3.14-9 and (3.20) } \rangle \\
& \ulcorner(x \sqsubset y \sqsubset \neg t) \sqsubseteq \ulcorner(\ulcorner(x \sqsubset \ulcorner y) \sqsubset x \sqsubset \neg \ulcorner(y \sqsubset t \sqcap y_t)) \\
\Longleftrightarrow & \langle \text{ by (3.19), (4.8) and De Morgan } \rangle \\
& \ulcorner(x \sqsubset y \sqsubset \neg t) \sqsubseteq \ulcorner(x \sqsubset \ulcorner y \sqsubset (\ulcorner(y \sqsubset \neg t) \sqcap \neg \ulcorner y)) \\
\Longleftrightarrow & \langle \text{ by Boolean algebra } \rangle \\
& \ulcorner(x \sqsubset y \sqsubset \neg t) \sqsubseteq \ulcorner(x \sqsubset \ulcorner y \sqsubset \ulcorner(y \sqsubset \neg t)) \\
\Longleftrightarrow & \langle \text{ Proposition 3.14-18, Boolean algebra and (3.20) } \rangle \\
& \mathsf{true}
\end{array}
$$

Using this result with $t := \neg t$ yields $\ulcorner D \sqsubseteq A$. Hence, also Proposition 3.14-9 and Boolean algebra,

$$\ulcorner(A \sqsubset B) = A \sqsubset \ulcorner B = A = A \sqsubset \ulcorner D = \ulcorner(A \sqsubset D) \ .$$

2. Proof of (4.5).

$$
\begin{array}{ll}
& A \sqsubset B \sqsubset t \\
= & \langle \text{ by (3.24) } \rangle \\
& A \sqsubset \left(x \sqsubset (y \sqsubset t \sqcap_{\ulcorner(y \sqsubset t)} y_t) \sqcap_{\ulcorner(x \sqsubset (y \sqsubset t \sqcap y_t))} x_{\ulcorner(y \sqsubset t \sqcap y_t)} \sqsubset (y \sqsubset t \sqcap_{\ulcorner(y \sqsubset t)} y_t)\right) \sqsubset t \\
= & \langle \text{ by Proposition 3.20-7, Boolean algebra and (4.4) with} \\
& \quad x, t := y, t \ \rangle \\
& A \sqsubset \left(x \sqsubset (y \sqsubset t \sqcap_{\ulcorner(y \sqsubset t)} y_t) \sqcap_{\ulcorner(x \sqsubset (y \sqsubset t \sqcap y_t))} x_{\ulcorner(y \sqsubset t \sqcap y_t)} \sqsubset (y \sqsubset t \sqcap_{\ulcorner(y \sqsubset t)} y_t)\right) \\
= & \langle \text{ by (3.24) } \rangle \\
& A \sqsubset B
\end{array}
$$

3. Proof of (4.6). This follows from the proof of (4.5) with the substitution $t := \neg t$.

4. Proof of (4.3). We have to show

$$x \circledcirc y = x \circledcirc y \circledcirc t \sqcap x \circledcirc y \circledcirc \neg t \sqcap (A \circledcirc B \sqcup A \circledcirc D) \ .$$

It is sufficient to show that

$$\sqcap((x \circledcirc y)_t) \circledcirc x \circledcirc y = A \circledcirc B \sqcup A \circledcirc D$$

by Remark 4.21.

So here is the proof of

$$A \circledcirc x \circledcirc y = A \circledcirc (B \sqcup D) \ .$$

$$\begin{array}{ll}
& A \circledcirc x \circledcirc y \\
= & \qquad \langle \text{ by (4.3) with } x, t := y, t \ \rangle \\
& A \circledcirc x \circledcirc (y \circledcirc t \sqcap y \circledcirc \neg t \sqcap (y_t \sqcup y_{\neg t})) \\
= & \qquad \langle \text{ by Corollary 3.21-15 and (3.8)} \ \rangle \\
& A \circledcirc (x \circledcirc (y \circledcirc t \sqcap y \circledcirc \neg t \sqcap y_t) \sqcup x \circledcirc (y \circledcirc t \sqcap y \circledcirc \neg t \sqcap y_{\neg t})) \\
= & \qquad \langle \text{ by Remark 4.8, (3.25), Proposition 4.22-1 twice:} \\
& \quad \text{(1) with } x, y, z := x, y \circledcirc t \sqcap y_t, y \circledcirc \neg t, \\
& \quad \text{(2) with } x, y, z := x, y \circledcirc \neg t \sqcap y_{\neg t}, y \circledcirc t, \\
& \quad \text{and Boolean algebra} \ \rangle \\
& A \circledcirc \Big((x \circledcirc (y \circledcirc t \sqcap y_t) \sqcap x \circledcirc y \circledcirc \neg t \sqcap \\
& \quad (x_{\sqcap(y \circledcirc t \sqcap y_t)} \circledcirc (y \circledcirc t \sqcap y_t) \sqcup x_{\neg \sqcap(y \circledcirc t \sqcap y_t)} \circledcirc y \circledcirc \neg t)) \sqcup \\
& \quad (x \circledcirc (y \circledcirc \neg t \sqcap y_{\neg t}) \sqcap x \circledcirc y \circledcirc t \sqcap \\
& \quad (x_{\sqcap(y \circledcirc \neg t \sqcap y_{\neg t})} \circledcirc (y \circledcirc \neg t \sqcap y_{\neg t}) \sqcup x_{\neg \sqcap(y \circledcirc \neg t \sqcap y_{\neg t})} \circledcirc y \circledcirc t) \Big) \\
= & \qquad \langle \text{ by (3.8), Corollary 3.21-4, Propositions 3.14-7 and 3.14-17,} \\
& \quad \text{and Corollary 3.21-3} \ \rangle \\
& A \circledcirc \Big((x \circledcirc (y \circledcirc t \sqcap y_t) \sqcap \\
& \quad (x_{\sqcap(y \circledcirc t \sqcap y_t)} \circledcirc (y \circledcirc t \sqcap y_t) \sqcup x_{\neg \sqcap(y \circledcirc t \sqcap y_t)} \circledcirc y \circledcirc \neg t)) \sqcup \\
& \quad (x \circledcirc (y \circledcirc \neg t \sqcap y_{\neg t}) \sqcap \\
& \quad (x_{\sqcap(y \circledcirc \neg t \sqcap y_{\neg t})} \circledcirc (y \circledcirc \neg t \sqcap y_{\neg t}) \sqcup x_{\neg \sqcap(y \circledcirc \neg t \sqcap y_{\neg t})} \circledcirc y \circledcirc t) \Big) \\
= & \qquad \langle \text{ by Corollary 3.21-15} \ \rangle \\
& A \circledcirc \Big((x \circledcirc (y \circledcirc t \sqcap y_t) \sqcap x_{\sqcap(y \circledcirc t \sqcap y_t)} \circledcirc (y \circledcirc t \sqcap y_t)) \sqcup \\
& \quad (x \circledcirc (y \circledcirc t \sqcap y_t) \sqcap x_{\neg \sqcap(y \circledcirc t \sqcap y_t)} \circledcirc y \circledcirc \neg t) \sqcup
\end{array}$$

$$
\begin{array}{ll}
& (x \mathbin{\square} (y \mathbin{\square} \neg t \mathbin{\sqcap} y_{\neg t}) \mathbin{\sqcap} x_{\ulcorner (y \mathbin{\square} \neg t \sqcap y_{\neg t}) \urcorner} \mathbin{\square} (y \mathbin{\square} \neg t \mathbin{\sqcap} y_{\neg t})) \sqcup \\
& (x \mathbin{\square} (y \mathbin{\square} \neg t \mathbin{\sqcap} y_{\neg t}) \mathbin{\sqcap} x_{\neg \ulcorner (y \mathbin{\square} \neg t \sqcap y_{\neg t}) \urcorner} \mathbin{\square} y \mathbin{\square} t)\Big) \\
= & \quad \langle \text{ by the definitions of } A,\ B,\ C,\ D \text{ and } E \ \rangle \\
& A \mathbin{\square} (B \sqcup C \sqcup D \sqcup E)
\end{array}
$$

We have to show that the last expression is equal to $A \mathbin{\square} (B \sqcup D)$.

$$
\begin{array}{ll}
& A \mathbin{\square} (B \sqcup C \sqcup D \sqcup E) = A \mathbin{\square} (B \sqcup D) \\
\Longleftarrow & \quad \langle \text{ by (3.8) and (3.11) } \rangle \\
& A \mathbin{\square} C \sqsubseteq A \mathbin{\square} (B \sqcup D) \ \wedge \ A \mathbin{\square} E \sqsubseteq A \mathbin{\square} (B \sqcup D) \\
\Longleftrightarrow & \quad \langle \text{ since the second conjunct follows from the first by symmetry,} \\
& \quad \text{using the substitution } t := \neg t \ \rangle \\
& A \mathbin{\square} C \sqsubseteq A \mathbin{\square} (B \sqcup D) \\
\Longleftrightarrow & \quad \langle \text{ by Proposition 3.14-6 } \rangle \\
& C \sqsubseteq A \mathbin{\square} (B \sqcup D) \\
\Longleftarrow & \quad \langle \text{ by Lemma 3.7-1 } \rangle \\
& C \sqsubseteq \sqcap (x \mathbin{\square} y) \mathbin{\square} (B \sqcup D) \\
\Longleftrightarrow & \quad \langle \text{ by Proposition 3.14-20 } \rangle \\
& C \sqsubseteq B \sqcup \sqcap (x \mathbin{\square} y) \mathbin{\square} D \\
\Longleftrightarrow & \quad \langle \text{ by Proposition 3.20-16 } \rangle \\
& \sqcap (x \mathbin{\square} (y \mathbin{\square} t \mathbin{\sqcap} y_t)) \mathbin{\square} C \sqsubseteq \sqcap (x \mathbin{\square} (y \mathbin{\square} t \mathbin{\sqcap} y_t)) \mathbin{\square} (B \sqcup \sqcap (x \mathbin{\square} y) \mathbin{\square} D) \ \wedge \\
& \neg \sqcap (x \mathbin{\square} (y \mathbin{\square} t \mathbin{\sqcap} y_t)) \mathbin{\square} C \sqsubseteq \neg \sqcap (x \mathbin{\square} (y \mathbin{\square} t \mathbin{\sqcap} y_t)) \mathbin{\square} (B \sqcup \sqcap (x \mathbin{\square} y) \mathbin{\square} D) \\
\Longleftrightarrow & \quad \langle \text{ by Corollaries 3.21-7 and 3.21-8, Proposition 3.14-7, (4.4) with} \\
& \quad x, t := x, \sqcap (y \mathbin{\square} t \mathbin{\sqcap} y_t) \text{ and Boolean algebra } \rangle \\
& x \mathbin{\square} (y \mathbin{\square} t \mathbin{\sqcap} y_t) \sqsubseteq \sqcap (x \mathbin{\square} (y \mathbin{\square} t \mathbin{\sqcap} y_t)) \mathbin{\square} (B \sqcup \sqcap (x \mathbin{\square} y) \mathbin{\square} D) \ \wedge \\
& x_{\neg \ulcorner (y \mathbin{\square} t \sqcap y_t) \urcorner} \mathbin{\square} y \mathbin{\square} \neg t \sqsubseteq \neg \sqcap (x \mathbin{\square} (y \mathbin{\square} t \mathbin{\sqcap} y_t)) \mathbin{\square} (B \sqcup \sqcap (x \mathbin{\square} y) \mathbin{\square} D) \\
\Longleftrightarrow & \quad \langle \text{ by (3.8), Corollary 3.21-7 and Proposition 3.14-7 } \rangle \\
& x \mathbin{\square} (y \mathbin{\square} t \mathbin{\sqcap} y_t) \sqsubseteq x \mathbin{\square} (y \mathbin{\square} t \mathbin{\sqcap} y_t) \sqcup \sqcap (x \mathbin{\square} (y \mathbin{\square} t \mathbin{\sqcap} y_t)) \mathbin{\square} \sqcap (x \mathbin{\square} y) \mathbin{\square} D) \ \wedge \\
& x_{\neg \ulcorner (y \mathbin{\square} t \sqcap y_t) \urcorner} \mathbin{\square} y \mathbin{\square} \neg t \sqsubseteq \neg \sqcap (x \mathbin{\square} (y \mathbin{\square} t \mathbin{\sqcap} y_t)) \mathbin{\square} (B \sqcup \sqcap (x \mathbin{\square} y) \mathbin{\square} D) \\
\Longleftrightarrow & \quad \langle \text{ by (3.15) } \rangle \\
& x_{\neg \ulcorner (y \mathbin{\square} t \sqcap y_t) \urcorner} \mathbin{\square} y \mathbin{\square} \neg t \sqsubseteq \neg \sqcap (x \mathbin{\square} (y \mathbin{\square} t \mathbin{\sqcap} y_t)) \mathbin{\square} (B \sqcup \sqcap (x \mathbin{\square} y) \mathbin{\square} D)
\end{array}
$$

The proof of the last refinement follows.

$$
\begin{array}{ll}
& \neg{}^{\Pi}(x \triangleright (y \triangleright t \mathbin{\overline{\wedge}} y_t)) \triangleright (B \sqcup {}^{\Pi}(x \triangleright y) \triangleright D) \\
= & \quad \langle \text{ by (3.8), Corollary 3.21-8, Proposition 3.14-7, (4.4) with } \\
& \quad\ x, t := x, {}^{\Pi}(y \triangleright t \mathbin{\overline{\wedge}} y_t) \text{ and Boolean algebra } \rangle \\
& x_{\Gamma(y \triangleright t \overline{\wedge} y_t)} \triangleright (y \triangleright t \mathbin{\overline{\wedge}} y_t) \sqcup \neg{}^{\Pi}(x \triangleright (y \triangleright t \mathbin{\overline{\wedge}} y_t)) \triangleright {}^{\Pi}(x \triangleright y) \triangleright D \\
= & \quad \langle \text{ by Propositions 3.14-7 and 3.14-20, (3.20) and (4.5) with } \\
& \quad\ x, t := x, {}^{\Pi}(y \triangleright t \mathbin{\overline{\wedge}} y_t) \rangle \\
& x_{\Gamma(y \triangleright t \overline{\wedge} y_t)} \triangleright (y \triangleright t \mathbin{\overline{\wedge}} y_t) \sqcup {}^{\Pi}(x_{\Gamma(y \triangleright t \overline{\wedge} y_t)}) \triangleright \neg{}^{\Pi}(x \triangleright (y \triangleright t \mathbin{\overline{\wedge}} y_t)) \triangleright {}^{\Pi}(x \triangleright y) \triangleright D \\
\sqsupseteq & \quad \langle \text{ by (3.15) } \rangle \\
& {}^{\Pi}(x_{\Gamma(y \triangleright t \overline{\wedge} y_t)}) \triangleright \neg{}^{\Pi}(x \triangleright (y \triangleright t \mathbin{\overline{\wedge}} y_t)) \triangleright {}^{\Pi}(x \triangleright y) \triangleright D \\
= & \quad \langle \text{ by (3.20), (4.4) with } x, t := x, {}^{\Pi}(y \triangleright t \mathbin{\overline{\wedge}} y_t) \text{ and Boolean algebra } \\
& \quad\ \rangle \\
& {}^{\Pi}(x_{\Gamma(y \triangleright t \overline{\wedge} y_t)}) \triangleright {}^{\Pi}(x \triangleright y) \triangleright D \\
= & \quad \langle \text{ by the definition of } D \rangle \\
& {}^{\Pi}(x_{\Gamma(y \triangleright t \overline{\wedge} y_t)}) \triangleright {}^{\Pi}(x \triangleright y) \triangleright (x \triangleright (y \triangleright \neg t \mathbin{\overline{\wedge}} y_{\neg t}) \mathbin{\overline{\wedge}} x_{\Gamma(y \triangleright \neg t \overline{\wedge} y_{\neg t})} \triangleright (y \triangleright \neg t \mathbin{\overline{\wedge}} y_{\neg t})) \\
= & \quad \langle \text{ by Corollary 3.21-4, (3.19) and (3.20) } \rangle \\
& {}^{\Pi}(x_{\Gamma(y \triangleright t \overline{\wedge} y_t)}) \triangleright (x \triangleright {}^{\Pi}y \triangleright (y \triangleright \neg t \mathbin{\overline{\wedge}} y_{\neg t}) \mathbin{\overline{\wedge}} {}^{\Pi}(x \triangleright y) \triangleright x_{\Gamma(y \triangleright \neg t \overline{\wedge} y_{\neg t})} \triangleright (y \triangleright \neg t \mathbin{\overline{\wedge}} y_{\neg t})) \\
= & \quad \langle \text{ by Proposition 3.14-7, (4.9) and Boolean algebra } \rangle \\
& {}^{\Pi}(x_{\Gamma(y \triangleright t \overline{\wedge} y_t)}) \triangleright (x \triangleright (y \triangleright \neg t \mathbin{\overline{\wedge}} y_{\neg t}) \mathbin{\overline{\wedge}} {}^{\Pi}(x \triangleright y) \triangleright x_{\Gamma(y \triangleright \neg t \overline{\wedge} y_{\neg t})} \triangleright (y \triangleright \neg t \mathbin{\overline{\wedge}} y_{\neg t})) \\
= & \quad \langle \text{ by Corollary 3.21-4 and Proposition 3.14-9 } \rangle \\
& {}^{\Pi}(x_{\Gamma(y \triangleright t \overline{\wedge} y_t)}) \triangleright x \triangleright (y \triangleright \neg t \mathbin{\overline{\wedge}} y_{\neg t}) \mathbin{\overline{\wedge}} \\
& {}^{\Pi}({}^{\Pi}(x_{\Gamma(y \triangleright t \overline{\wedge} y_t)}) \triangleright x \triangleright y) \triangleright x_{\Gamma(y \triangleright \neg t \overline{\wedge} y_{\neg t})} \triangleright (y \triangleright \neg t \mathbin{\overline{\wedge}} y_{\neg t}) \\
= & \quad \langle \text{ by Proposition 4.22-2 } \rangle \\
& {}^{\Pi}(x_{\Gamma(y \triangleright t \overline{\wedge} y_t)}) \triangleright x \triangleright (y \triangleright \neg t \mathbin{\overline{\wedge}} y_{\neg t}) \mathbin{\overline{\wedge}} \\
& {}^{\Pi}((x_{\Gamma(y \triangleright t \overline{\wedge} y_t)} \sqcup x_{\neg \Gamma(y \triangleright t \overline{\wedge} y_t)}) \triangleright y) \triangleright x_{\Gamma(y \triangleright \neg t \overline{\wedge} y_{\neg t})} \triangleright (y \triangleright \neg t \mathbin{\overline{\wedge}} y_{\neg t}) \\
\sqsupseteq & \quad \langle \text{ by (3.15) and Proposition 3.14-8, } \\
& \quad\ x_{\neg \Gamma(y \triangleright t \overline{\wedge} y_t)} \sqsubseteq x_{\Gamma(y \triangleright t \overline{\wedge} y_t)} \sqcup x_{\neg \Gamma(y \triangleright t \overline{\wedge} y_t)} \\
& \quad\ \Longrightarrow x_{\neg \Gamma(y \triangleright t \overline{\wedge} y_t)} \triangleright y \sqsubseteq (x_{\Gamma(y \triangleright t \overline{\wedge} y_t)} \sqcup x_{\neg \Gamma(y \triangleright t \overline{\wedge} y_t)}) \triangleright y \\
& \quad\ \Longrightarrow {}^{\Pi}(x_{\neg \Gamma(y \triangleright t \overline{\wedge} y_t)} \triangleright y) \sqsubseteq {}^{\Pi}((x_{\Gamma(y \triangleright t \overline{\wedge} y_t)} \sqcup x_{\neg \Gamma(y \triangleright t \overline{\wedge} y_t)}) \triangleright y), \\
& \quad\ \text{then apply Lemma 3.22-1 } \rangle \\
& {}^{\Pi}(x_{\Gamma(y \triangleright t \overline{\wedge} y_t)}) \triangleright x \triangleright (y \triangleright \neg t \mathbin{\overline{\wedge}} y_{\neg t}) \mathbin{\overline{\wedge}} \\
& {}^{\Pi}(x_{\neg \Gamma(y \triangleright t \overline{\wedge} y_t)} \triangleright y) \triangleright x_{\Gamma(y \triangleright \neg t \overline{\wedge} y_{\neg t})} \triangleright (y \triangleright \neg t \mathbin{\overline{\wedge}} y_{\neg t}) \\
= & \quad \langle \text{ by Proposition 3.14-9, (3.20), (4.4) with } x, t := x, {}^{\Pi}(y \triangleright \neg t \overline{\wedge} y_{\neg t}), \\
& \quad\ \text{Remark 4.8 and Boolean algebra, } \\
& \quad\ \text{the domains of the two operands of the main } \overline{\wedge} \text{ are disjoint, } \\
& \quad\ \text{then apply (3.25) } \rangle
\end{array}
$$

$$
\begin{array}{ll}
& \sqcap(x_{\neg\lceil(y\sqcup t\sqcap y_t)}\sqcup y)\sqcup x_{\lceil(y\sqcup\neg t\sqcap y_{\neg t})}\sqcup(y\sqcup\neg t\sqcap y_{\neg t})\sqcap \\
& \sqcap(x_{\lceil(y\sqcup t\sqcap y_t)})\sqcup x\sqcup(y\sqcup\neg t\sqcap y_{\neg t}) \\
= & \quad \langle \text{ by Proposition 4.22-2 } \rangle \\
& \sqcap(x_{\neg\lceil(y\sqcup t\sqcap y_t)}\sqcup y)\sqcup x_{\lceil(y\sqcup\neg t\sqcap y_{\neg t})}\sqcup(y\sqcup\neg t\sqcap y_{\neg t})\sqcap \\
& (x_{\lceil(y\sqcup t\sqcap y_t)}\sqcup x_{\neg\lceil(y\sqcup t\sqcap y_t)})\sqcup(y\sqcup\neg t\sqcap y_{\neg t}) \\
\sqsupseteq & \quad \langle \text{ by (3.15) and Lemma 3.22-1 } \rangle \\
& \sqcap(x_{\neg\lceil(y\sqcup t\sqcap y_t)}\sqcup y)\sqcup x_{\lceil(y\sqcup\neg t\sqcap y_{\neg t})}\sqcup(y\sqcup\neg t\sqcap y_{\neg t})\sqcap \\
& x_{\neg\lceil(y\sqcup t\sqcap y_t)}\sqcup(y\sqcup\neg t\sqcap y_{\neg t}) \\
= & \quad \langle \text{ by (4.6) with } x,t := x,\sqcap(y\sqcup t\sqcap y_t),\text{ (4.8) and De Morgan } \rangle \\
& \sqcap(x_{\lceil(y\sqcup\neg t)\sqcap\neg\lceil y}\sqcup(\sqcap(y\sqcup\neg t)\sqcap\neg\sqcap y)\sqcup y)\sqcup x_{\lceil(y\sqcup\neg t\sqcap y_{\neg t})}\sqcup(y\sqcup\neg t\sqcap y_{\neg t})\sqcap \\
& x_{\neg\lceil(y\sqcup t\sqcap y_t)}\sqcup(\sqcap(y\sqcup\neg t)\sqcap\neg\sqcap y)\sqcup(y\sqcup\neg t\sqcap y_{\neg t}) \\
= & \quad \langle \text{ by Corollaries 3.21-5 and 3.21-3, (3.19) and Proposition} \\
& \quad \text{3.14-17 } \rangle \\
& \sqcap(x_{\lceil(y\sqcup\neg t)\sqcap\neg\lceil y}\sqcup y\sqcup\neg t)\sqcup x_{\lceil(y\sqcup\neg t\sqcap y_{\neg t})}\sqcup(y\sqcup\neg t\sqcap y_{\neg t})\sqcap \\
& x_{\neg\lceil(y\sqcup t\sqcap y_t)}\sqcup(\sqcap(y\sqcup\neg t)\sqcap\neg\sqcap y)\sqcup(y\sqcup\neg t\sqcap y_{\neg t}) \\
= & \quad \langle \text{ by Corollaries 3.21-5, 3.21-4 and 3.21-3, Propositions 3.14-7} \\
& \quad \text{and 3.14-17, (4.4) with } x,t := y,t,\text{ (3.6) and Boolean algebra} \\
& \quad \rangle \\
& \sqcap(x_{\lceil(y\sqcup\neg t)\sqcap\neg\lceil y}\sqcup y\sqcup\neg t)\sqcup x_{\lceil(y\sqcup\neg t\sqcap y_{\neg t})}\sqcup(y\sqcup\neg t\sqcap y_{\neg t})\sqcap x_{\neg\lceil(y\sqcup t\sqcap y_t)}\sqcup y\sqcup\neg t \\
\sqsupseteq & \quad \langle \text{ It is shown immediately after this derivation that} \\
& \quad x_{\neg\lceil(y\sqcup t\sqcap y_t)}\sqcup y\sqcup\neg t \text{ refines the first operand of the main } \sqcap. \\
& \quad \text{The result then follows from Lemma 3.22-2. } \rangle \\
& x_{\neg\lceil(y\sqcup t\sqcap y_t)}\sqcup y\sqcup\neg t
\end{array}
$$

Thus, all what remains to do is prove the assertion in the justification of the last equality.

$$
\begin{array}{ll}
& \sqcap(x_{\lceil(y\sqcup\neg t)\sqcap\neg\lceil y}\sqcup y\sqcup\neg t)\sqcup x_{\lceil(y\sqcup\neg t\sqcap y_{\neg t})}\sqcup(y\sqcup\neg t\sqcap y_{\neg t}) \\
\sqsupseteq & \quad \langle \text{ by Lemma 3.17-2, } \neg\sqcap y\sqcup\sqcap(y\sqcup\neg t)=\top, \\
& \quad \text{then by Boolean algebra} \\
& \quad \text{and Corollary 4.26-4 with } r,s,t := \sqcap(y_{\neg t}),\neg\sqcap y,\sqcap(y\sqcup\neg t), \\
& \quad x_{\lceil(y\sqcup\neg t)\sqcap\neg\lceil y}\sqcup\sqcap(y\sqcup\neg t) \\
& \quad = x_{\neg\lceil y\sqcap\lceil(y\sqcup\neg t)}\sqcup\sqcap(y\sqcup\neg t) \\
& \quad \sqsubseteq \sqcap(x_{\neg\lceil y\sqcap\lceil(y\sqcup\neg t)}\sqcup\sqcap(y\sqcup\neg t))\sqcup x_{\lceil(y_{\neg t})\sqcap\lceil(y\sqcup\neg t)} \\
& \quad = \sqcap(x_{\lceil(y\sqcup\neg t)\sqcap\neg\lceil y}\sqcup\sqcap(y\sqcup\neg t))\sqcup x_{\lceil(y_{\neg t})\sqcap\lceil(y\sqcup\neg t)}, \\
& \quad \text{then apply Corollary 3.21-16 and (3.20) } \rangle
\end{array}
$$

$$
\begin{array}{ll}
 & x_{\ulcorner(y\,\square\,\neg t)\,\sqcap\,\neg\ulcorner y\,\square\,\sqcap(y\,\square\,\neg t)\,\square\,(y\,\square\,\neg t\,\sqcap\,y_{\neg t})} \\
= & \qquad \langle \text{ by (4.8), De Morgan, Corollaries 3.21-4 and 3.21-3,} \\
 & \qquad \text{Proposition 3.14-7, (4.4) with } x,t := y,t \text{, Boolean algebra and} \\
 & \qquad (3.6) \ \rangle \\
 & x_{\neg\ulcorner(y\,\square\,t\,\sqcap\,y_t)\,\square\,y\,\square\,\neg t}
\end{array}
$$

□

Theorem 4.29. *Suppose $\mathcal{A}$ is an algebra of decomposable elements. The following equality is valid for all $x, y \in A$ and all $t, u \in \mathsf{test}(A)$.*

$$(x \sqcap_u y)_t = x_t \sqcap_u y_t$$

Proof : We have to show that $x_t \sqcap_u y_t$ and $x_{\neg t} \sqcap_u y_{\neg t}$ satisfy (4.3), (4.4), (4.5) and (4.6) with $x, t := x \sqcap_u y, t$ (see Definition 4.7).

With (4.5), (4.6), (4.5) with $x, t := y, t$, (4.6) with $x, t := y, t$ and Corollary 3.21-18, one gets (4.5) and (4.6).

Let us work now on (4.3). We have to demonstrate that

$$x \sqcap_u y = (x \sqcap_u y)\square t \sqcap (x \sqcap_u y)\square\neg t \sqcap ((x_t \sqcap_u y_t) \sqcup (x_{\neg t} \sqcap_u y_{\neg t})) \ .$$

This equality can be established by comparing the two members with the tests u and $\neg u$ and invoking Proposition 3.20-17.

Case u

$$
\begin{array}{ll}
 & u\square(x \sqcap_u y) \\
= & \qquad \langle \text{ by Proposition 3.20-1 } \rangle \\
 & u\square x \\
= & \qquad \langle \text{ by (4.3) } \rangle \\
 & u\square(x\square t \sqcap x\square\neg t \sqcap (x_t \sqcup x_{\neg t})) \\
= & \qquad \langle \text{ by Corollary 3.21-4 and (3.8) } \rangle \\
 & u\square x\square t \sqcap u\square x\square\neg t \sqcap (u\square x_t \sqcup u\square x_{\neg t}) \\
= & \qquad \langle \text{ by Proposition 3.20-1 } \rangle \\
 & u\square(x \sqcap_u y)\square t \sqcap u\square(x \sqcap_u y)\square\neg t \sqcap (u\square(x_t \sqcap_u y_t) \sqcup u\square(x_{\neg t} \sqcap_u y_{\neg t})) \\
= & \qquad \langle \text{ by Corollary 3.21-4 and (3.8) } \rangle \\
 & u\square((x \sqcap_u y)\square t \sqcap (x \sqcap_u y)\square\neg t \sqcap ((x_t \sqcap_u y_t) \sqcup (x_{\neg t} \sqcap_u y_{\neg t})))
\end{array}
$$

Case $\neg u$

$$
\begin{array}{ll}
& \neg u \triangleright (x \mathbin{⫪_u} y) \\
= & \qquad \langle \text{ by Proposition 3.20-1 } \rangle \\
& \neg u \triangleright y \\
= & \qquad \langle \text{ by (4.3) with } x, t := y, t \ \rangle \\
& \neg u \triangleright (y \triangleright t \mathbin{⫪} y \triangleright \neg t \mathbin{⫪} (y_t \sqcup y_{\neg t})) \\
= & \qquad \langle \text{ by Corollary 3.21-4 and (3.8) } \rangle \\
& \neg u \triangleright y \triangleright t \mathbin{⫪} \neg u \triangleright y \triangleright \neg t \mathbin{⫪} (\neg u \triangleright y_t \sqcup \neg u \triangleright y_{\neg t}) \\
= & \qquad \langle \text{ by Proposition 3.20-1 } \rangle \\
& \neg u \triangleright (x \mathbin{⫪_u} y) \triangleright t \mathbin{⫪} \neg u \triangleright (x \mathbin{⫪_u} y) \triangleright \neg t \mathbin{⫪} (\neg u \triangleright (x_t \mathbin{⫪_u} y_t) \sqcup \neg u \triangleright (x_{\neg t} \mathbin{⫪_u} y_{\neg t})) \\
= & \qquad \langle \text{ by Corollary 3.21-4 and (3.8) } \rangle \\
& \neg u \triangleright ((x \mathbin{⫪_u} y) \triangleright t \mathbin{⫪} (x \mathbin{⫪_u} y) \triangleright \neg t \mathbin{⫪} ((x_t \mathbin{⫪_u} y_t) \sqcup (x_{\neg t} \mathbin{⫪_u} y_{\neg t})))
\end{array}
$$

It remains to derive (4.4). First note that

$$
\begin{array}{ll}
& \top\!\!\top (x_t \mathbin{⫪_u} y_t) \\
= & \qquad \langle \text{ by Proposition 3.20-20 } \rangle \\
& \top\!\!\top (x_t) \mathbin{⫪_u} \top\!\!\top (y_t) \\
= & \qquad \langle \text{ by (4.4) and (4.4) with } x, t := y, t \ \rangle \\
& \top\!\!\top (x_{\neg t}) \mathbin{⫪_u} \top\!\!\top (y_{\neg t}) \\
= & \qquad \langle \text{ by Proposition 3.20-20 } \rangle \\
& \top\!\!\top (x_{\neg t} \mathbin{⫪_u} y_{\neg t}) \ .
\end{array}
$$

And here is the main derivation.

$$
\begin{array}{ll}
& \neg \top\!\!\top ((x \mathbin{⫪_u} y) \triangleright t) \triangleright \neg \top\!\!\top ((x \mathbin{⫪_u} y) \triangleright \neg t) \triangleright \top\!\!\top (x \mathbin{⫪_u} y) \\
= & \qquad \langle \text{ by Propositions 3.20-7 and 3.20-20 } \rangle \\
& \neg (\top\!\!\top (x \triangleright t) \mathbin{⫪_u} \top\!\!\top (y \triangleright t)) \triangleright \neg (\top\!\!\top (x \triangleright \neg t) \mathbin{⫪_u} \top\!\!\top (y \triangleright \neg t)) \triangleright (\top\!\!\top x \mathbin{⫪_u} \top\!\!\top y) \\
= & \qquad \langle \text{ by Proposition 3.20-12 } \rangle
\end{array}
$$

$$
\begin{array}{ll}
& \neg(u\sqcap{}^{\sqcap}(x\sqcap t)\mathbin{⫪}\neg u\sqcap{}^{\sqcap}(y\sqcap t))\sqcap\neg(u\sqcap{}^{\sqcap}(x\sqcap\neg t)\mathbin{⫪}\neg u\sqcap{}^{\sqcap}(y\sqcap\neg t))\sqcap(u\sqcap{}^{\sqcap}x\mathbin{⫪}\neg u\sqcap{}^{\sqcap}y) \\
= & \qquad \langle \text{ by De Morgan } \rangle \\
& (\neg u\mathbin{⫪}\neg{}^{\sqcap}(x\sqcap t))\sqcap(u\mathbin{⫪}\neg{}^{\sqcap}(y\sqcap t))\sqcap \\
& (\neg u\mathbin{⫪}\neg{}^{\sqcap}(x\sqcap\neg t))\sqcap(u\mathbin{⫪}\neg{}^{\sqcap}(y\sqcap\neg t))\sqcap(u\sqcap{}^{\sqcap}x\mathbin{⫪}\neg u\sqcap{}^{\sqcap}y) \\
= & \qquad \langle \text{ by Boolean algebra } \rangle \\
& (\neg u\mathbin{⫪}u\sqcap\neg{}^{\sqcap}(x\sqcap t))\sqcap(u\mathbin{⫪}\neg u\sqcap\neg{}^{\sqcap}(y\sqcap t))\sqcap \\
& (\neg u\mathbin{⫪}u\sqcap\neg{}^{\sqcap}(x\sqcap\neg t))\sqcap(u\mathbin{⫪}\neg u\sqcap\neg{}^{\sqcap}(y\sqcap\neg t))\sqcap(u\sqcap{}^{\sqcap}x\mathbin{⫪}\neg u\sqcap{}^{\sqcap}y) \\
= & \qquad \langle \text{ by Boolean algebra } \rangle \\
& u\sqcap\neg{}^{\sqcap}(x\sqcap t)\sqcap\neg{}^{\sqcap}(x\sqcap\neg t)\sqcap{}^{\sqcap}x\mathbin{⫪}\neg u\sqcap\neg{}^{\sqcap}(y\sqcap t)\sqcap\neg{}^{\sqcap}(y\sqcap\neg t)\sqcap{}^{\sqcap}y \\
= & \qquad \langle \text{ by Proposition 3.20-12, (4.4) and (4.4) with } x,t := y,t \rangle \\
& {}^{\sqcap}(x_t)\mathbin{⫪}_u{}^{\sqcap}(y_t) \\
= & \qquad \langle \text{ by Proposition 3.20-20 } \rangle \\
& {}^{\sqcap}(x_t\mathbin{⫪}_u y_t)
\end{array}
$$

□

Corollary 4.30. *Suppose $\mathcal{A}$ is an algebra of decomposable elements. The following equalities are valid for all $x, y \in A$ and all $r, s, t \in \mathsf{test}(A)$.*

1. $(x \mathbin{⫪} y)_t = x_t \mathbin{⫪} \neg{}^{\sqcap}x\sqcap y_t$
2. ${}^{\sqcap}x\sqcap{}^{\sqcap}y = \top \implies (x \mathbin{⫪} y)_t = x_t \mathbin{⫪} y_t$
3. $r \sqsubseteq t \sqsubseteq s \implies {}^{\sqcap}(x_r\sqcap s)\sqcap x_t = x_r\sqcap s$

Proof :

1. $$
\begin{array}{ll}
& (x \mathbin{⫪} y)_t \\
= & \qquad \langle \text{ by (3.24) } \rangle \\
& (x \mathbin{⫪}_{\lceil x} y)_t \\
= & \qquad \langle \text{ by Theorem 4.29 } \rangle \\
& x_t \mathbin{⫪}_{\lceil x} y_t \\
= & \qquad \langle \text{ by Corollary 3.21-9, Proposition 3.14-7, (4.4) and Boolean algebra } \rangle \\
& x_t \mathbin{⫪} \neg{}^{\sqcap}x\sqcap y_t
\end{array}
$$

2. Suppose $\sqcap x \sqcup \sqcap y = \top$.

$$
\begin{array}{ll}
& (x \sqcap y)_t \\
= & \quad \langle \text{ by Corollary 4.30-1 } \rangle \\
& x_t \sqcap \neg \sqcap x \sqcup y_t \\
= & \quad \langle \text{ by Proposition 3.14-7, (4.4) with } x, t := y, t, \text{ the hypothesis and Boolean algebra } \rangle \\
& x_t \sqcap y_t
\end{array}
$$

3. First, we derive an intermediate result. Assume $r \sqsubseteq t$.

$$
\begin{array}{ll}
& x_t \\
= & \quad \langle \text{ by (4.3) with } x, t := x, r \rangle \\
& (x \sqcup r \sqcap x \sqcup \neg r \sqcap (x_r \sqcup x_{\neg r}))_t \\
= & \quad \langle \text{ by Corollaries 4.30-1, 3.21-4 and 3.21-13 } \rangle \\
& (x \sqcup r)_t \sqcap \neg \sqcap (x \sqcup r) \sqcup (x \sqcup \neg r)_t \sqcap \neg \sqcap (x \sqcup r) \sqcup \neg \sqcap (x \sqcup \neg r) \sqcup (x_r \sqcup x_{\neg r})_t \\
= & \quad \langle \text{ by Propositions 3.14-7 and 3.14-3, (4.4) with } x, t := x \sqcup \neg r, t, \text{ (4.4) with } x, t := x_r \sqcup x_{\neg r}, t, \text{ (4.4) with } x, t := x, r, \text{ Lemma 3.17-5, (3.21) and Boolean algebra } \rangle \\
& (x \sqcup r)_t \sqcap (x \sqcup \neg r)_t \sqcap (x_r \sqcup x_{\neg r})_t \\
= & \quad \langle \text{ by Proposition 3.14-7, (4.4) with } x, t := x \sqcup \neg r, t, \text{ Boolean algebra and Theorem 4.23 } \rangle \\
& (x \sqcup r)_t \sqcap \neg \sqcap (x \sqcup \neg r \sqcup \neg t) \sqcup \sqcap (x \sqcup \neg r) \sqcup (x \sqcup \neg r)_t \sqcap \sqcap (x_{\neg r} \sqcup \neg t) \sqcup x_r \sqcup t \sqcap \\
& \sqcap (x_{\neg r} \sqcup \neg t) \sqcup (x_r)_t \sqcap (x_r \sqcup t \sqcup (x_{\neg r})_t) \sqcap \sqcap (x_r \sqcup \neg t) \sqcup x_{\neg r} \sqcup t \sqcap \\
& \sqcap (x_r \sqcup \neg t) \sqcup (x_{\neg r})_t \sqcap ((x_r)_t \sqcup x_{\neg r} \sqcup t) \sqcap ((x_r)_t \sqcup (x_{\neg r})_t) \\
= & \quad \langle \text{ by the hypothesis and Boolean algebra, } \neg r \sqcup \neg t = \neg r, \text{ then by (4.6) with } x, t := x, r, \\
& \quad x_{\neg r} \sqcup \neg t = x_{\neg r} \sqcup \neg r \sqcup \neg t = x_{\neg r} \sqcup \neg r = x_{\neg r} \rangle \\
& (x \sqcup r)_t \sqcap \neg \sqcap (x \sqcup \neg r) \sqcup \sqcap (x \sqcup \neg r) \sqcup (x \sqcup \neg r)_t \sqcap \sqcap (x_{\neg r}) \sqcup x_r \sqcup t \sqcap \\
& \sqcap (x_{\neg r}) \sqcup (x_r)_t \sqcap (x_r \sqcup t \sqcup (x_{\neg r})_t) \sqcap \sqcap (x_r \sqcup \neg t) \sqcup x_{\neg r} \sqcup t \sqcap \\
& \sqcap (x_r \sqcup \neg t) \sqcup (x_{\neg r})_t \sqcap ((x_r)_t \sqcup x_{\neg r} \sqcup t) \sqcap ((x_r)_t \sqcup (x_{\neg r})_t)
\end{array}
$$

$=$ $\langle$ by (4.6) with $x,t := x,r$, the hypothesis, Boolean algebra and (3.6),
$x_{\neg r}\triangleright t = x_{\neg r}\triangleright\neg r\triangleright t = \top$;
by Proposition 4.22-7, (4.5) with $x,t := x_{\neg r},t$, the hypothesis, Boolean algebra and (3.6)
$(x_{\neg r})_t = (x_{\neg r})_t\triangleright\neg r = (x_{\neg r})_t\triangleright t\triangleright\neg r = \top$;
apply Boolean algebra too $\rangle$

$(x\triangleright r)_t \between \top\triangleright(x\triangleright\neg r)_t \between \Pi(x_{\neg r})\triangleright x_r\triangleright t \between$
$\Pi(x_{\neg r})\triangleright(x_r)_t \between (x_r\triangleright t \sqcup \top) \between \Pi(x_r\triangleright\neg t)\triangleright\top \between$
$\Pi(x_r\triangleright\neg t)\triangleright\top \between ((x_r)_t \sqcup \top) \between ((x_r)_t \sqcup \top)$

$=$ $\langle$ Boolean algebra, (3.6), (3.4) and Corollary 3.21-3 $\rangle$

$(x\triangleright r)_t \between \Pi(x_{\neg r})\triangleright x_r\triangleright t \between \Pi(x_{\neg r})\triangleright(x_r)_t$

$=$ $\langle$ by (4.4) with $x,t := x,r$, (4.4) with $x,t := x_r,t$, Proposition 3.14-7 and Boolean algebra $\rangle$

$(x\triangleright r)_t \between x_r\triangleright t \between (x_r)_t$

So $r \sqsubseteq t \Longrightarrow x_t = (x\triangleright r)_t \between x_r\triangleright t \between (x_r)_t$.

And now the main proof. Assume $r \sqsubseteq t \sqsubseteq s$.

$\Pi(x_r\triangleright s)\triangleright x_t$

$=$ $\langle$ by the hypothesis and the intermediate result above $\rangle$

$\Pi(x_r\triangleright s)\triangleright((x\triangleright r)_t \between x_r\triangleright t \between (x_r)_t)$

$=$ $\langle$ by Corollary 3.21-4 $\rangle$

$\Pi(x_r\triangleright s)\triangleright(x\triangleright r)_t \between \Pi(x_r\triangleright s)\triangleright x_r\triangleright t \between \Pi(x_r\triangleright s)\triangleright(x_r)_t$

$=$ $\langle$ by the hypothesis, (4.4) with $x,t := x_r,t$, Proposition 3.14-8 and Boolean algebra,
$\mathsf{true} \Longrightarrow t \sqsubseteq s \Longrightarrow x_r\triangleright t \sqsubseteq x_r\triangleright s \Longrightarrow \Pi(x_r\triangleright t) \sqsubseteq \Pi(x_r\triangleright s)$
$\Longrightarrow \Pi(x_r\triangleright t)\triangleright\neg\Pi(x_r\triangleright t) \sqsubseteq \Pi(x_r\triangleright s)\triangleright\Pi(x_r)_t$
$\Longrightarrow \Pi(x_r\triangleright s)\triangleright\Pi(x_r)_t = \top$ $\rangle$

$\Pi(x_r\triangleright s)\triangleright(x\triangleright r)_t \between \Pi(x_r\triangleright s)\triangleright x_r\triangleright t \between \top$

$=$ $\langle$ by (4.4) with $x,t := x,r$, by (4.4) with $x,t := x\triangleright r,t$, Propositions 3.14-7 and 3.14-9, Boolean algebra and (3.6),
$\Pi(x_r\triangleright s)\triangleright(x\triangleright r)_t = \Pi(\neg\Pi(x\triangleright r)\triangleright x_r\triangleright s)\triangleright\Pi(x\triangleright r)\triangleright(x\triangleright r)_t$
$= \neg\Pi(x\triangleright r)\triangleright\Pi(x_r\triangleright s)\triangleright\Pi(x\triangleright r)\triangleright(x\triangleright r)_t = \top\triangleright(x\triangleright r)_t = \top$ $\rangle$

$\top \between \Pi(x_r\triangleright s)\triangleright x_r\triangleright t \between \top$

$=$ $\langle$ by Corollary 3.21-3, (3.19), the hypothesis and Boolean algebra $\rangle$

$$x_r \,\square\, s$$

□

4.5 A Framework for KAD Within DAD-⌐•

In this section, we present three theorems. Theorems 4.31, 4.32 and 4.33 respectively state that, under suitable hypotheses, the elements of a DAD-⌐• together with the angelic operators form a KA, a KAT and a KAD. They make up a downward link from DAD-⌐• to KAD for any model of KAD —refer to Figure 1.4. These theorems are the demonic versions of Theorems 2.20, 2.21, 2.22 and 2.23.

We give the same advices as at the beginning of Section 4.4. Firstly, in order to demonstrate Theorems 4.31, 4.32 and 4.33, we need the algebra $\mathcal{A}$ to be an algebra of decomposable elements. In Chapter 5, it will be shown that this hypothesis is necessary and sufficient. Secondly, although the results are easy to understand, some proofs are long while others are subtle. For these reasons, at first reading, one might just concentrate on results rather than verify all the details of each demonstration.

Here is the first theorem of the section.

Theorem 4.31. *Suppose $\mathcal{A}$ is an algebra of decomposable elements. For all $x, y, z \in A$, the following laws are true, hence $(A, +_D, \cdot_D, ^{*_D}, \top, 1)$ is a KA.*

1. $(x +_D y) +_D z = x +_D (y +_D z)$
2. $x +_D y = y +_D x$
3. $x +_D x = x$
4. $\top +_D x = x$
5. $(x \cdot_D y) \cdot_D z = x \cdot_D (y \cdot_D z)$
6. $\top \cdot_D x = x \cdot_D \top = \top$
7. $1 \cdot_D x = x \cdot_D 1 = x$
8. $x \cdot_D (y + z) = x \cdot_D y +_D x \cdot_D z$
9. $(x +_D y) \cdot_D z = x \cdot_D z +_D y \cdot_D z$

10. $x^{*_D} = x^{*_D} \cdot_D x +_D 1$

11. $x \leq_D y \iff x +_D y = y$

12. $x \cdot_D z +_D y \leq_D z \implies x^{*_D} \cdot_D y \leq_D z$

13. $z \cdot_D x +_D y \leq_D z \implies y \cdot_D x^{*_D} \leq_D z$

Proof :

1. This is direct from Corollary 4.4-4.
2. This is firect from Corollary 4.4-5.
3. This is direct from Corollary 4.4-6.
4. This is direct from Corollary 4.4-7.
5. $$\begin{array}{ll} & (x \cdot_D y) \cdot_D z = x \cdot_D (y \cdot_D z) \\ \iff & \quad \langle \text{ by Proposition 4.17-7 } \rangle \\ & ((x \cdot_D y)\barwedge^{\sqcap} z \barwedge (x \cdot_D y)_{\sqcap z}) \barwedge z = (x \barwedge^{\sqcap}(y \cdot_D z) \barwedge x_{\sqcap(y \cdot_D z)}) \barwedge (y \cdot_D z) \\ \iff & \quad \langle \text{ by Proposition 4.17-7 } \rangle \\ & ((x \cdot_D y)\barwedge^{\sqcap} z \barwedge (x \cdot_D y)_{\sqcap z}) \barwedge z = (x \barwedge^{\sqcap}(y \cdot_D z) \barwedge x_{\sqcap(y \cdot_D z)}) \barwedge (y \barwedge^{\sqcap} z \barwedge y_{\sqcap z}) \barwedge z \\ \Longleftarrow & \quad \langle \text{ by Leibniz } \rangle \\ & (x \cdot_D y)\barwedge^{\sqcap} z \barwedge (x \cdot_D y)_{\sqcap z} = (x \barwedge^{\sqcap}(y \cdot_D z) \barwedge x_{\sqcap(y \cdot_D z)}) \barwedge (y \barwedge^{\sqcap} z \barwedge y_{\sqcap z}) \\ \iff & \quad \langle \text{ by Proposition 4.17-5 } \rangle \\ & (x \cdot_D y)\barwedge^{\sqcap} z \barwedge (x \cdot_D y)_{\sqcap z} = (x \barwedge^{\sqcap} y \barwedge \neg^{\sqcap}(y \barwedge \neg^{\sqcap} z) \barwedge x_{\sqcap y \barwedge \neg^{\sqcap}(y \barwedge \neg^{\sqcap} z)}) \barwedge (y \barwedge^{\sqcap} z \barwedge y_{\sqcap z}) \end{array}$$

   Since in the last formula z appears only as ${}^{\sqcap}z$, it suffices to show $(x \cdot_D y) \cdot_D t = x \cdot_D (y \cdot_D t)$ for an arbitrary test t.

$$\begin{array}{ll} & (x \cdot_D y) \cdot_D t \\ = & \quad \langle \text{ by Definition 4.16 and Proposition 3.14-1 } \rangle \\ & (x \barwedge y \barwedge x_{\sqcap y} \barwedge y) \barwedge t \barwedge (x \barwedge y \barwedge x_{\sqcap y} \barwedge y)_t \barwedge t \\ = & \quad \langle \text{ by (4.5) with } x, t := x \barwedge y \barwedge x_{\sqcap y} \barwedge y, t \rangle \\ & (x \barwedge y \barwedge x_{\sqcap y} \barwedge y) \barwedge t \barwedge (x \barwedge y \barwedge x_{\sqcap y} \barwedge y)_t \\ = & \quad \langle \text{ by (3.20), (4.4) with } x, t := x, {}^{\sqcap}y, \text{ Remark 4.8} \\ & \quad \text{and Boolean algebra,} \\ & \quad {}^{\sqcap}(x \barwedge y) \barwedge {}^{\sqcap}(x_{\sqcap y} \barwedge y) = {}^{\sqcap}(x \barwedge y) \barwedge {}^{\sqcap}(x_{\sqcap y} \barwedge {}^{\sqcap}y) = {}^{\sqcap}(x \barwedge y) \barwedge {}^{\sqcap}(x_{\sqcap y}) = \top, \\ & \quad \text{then apply Corollaries 3.21-17 and 4.30-1 } \rangle \end{array}$$

$$
\begin{array}{ll}
& x \barwedge y \barwedge t \barwedge x_{\overline{\top}y} \barwedge y \barwedge t \barwedge (x \barwedge y)_t \barwedge \neg \overline{\top}(x \barwedge y) \barwedge (x_{\overline{\top}y} \barwedge y)_t \\
= & \quad \langle \text{ by (4.4) with } x,t := x_{\overline{\top}y} \barwedge y, t, \text{ (4.4) with } x,t := x, \overline{\top}y, \text{ (3.20)}, \\
& \quad \text{(4.5) with } x,t := x, \overline{\top}y, \text{ Proposition 3.14-7 and Boolean algebra} \\
& \quad \rangle \\
& x \barwedge y \barwedge t \barwedge x_{\overline{\top}y} \barwedge y \barwedge t \barwedge (x \barwedge y)_t \barwedge (x_{\overline{\top}y} \barwedge y)_t
\end{array}
$$

Hence, by Proposition 4.17-6,

$$\overline{\top}(x \barwedge y \barwedge t \barwedge x_{\overline{\top}y} \barwedge y \barwedge t \barwedge (x \barwedge y)_t \barwedge (x_{\overline{\top}y} \barwedge y)_t) = \overline{\top}(x \mathbin{\cdot_{\mathcal{D}}} (y \mathbin{\cdot_{\mathcal{D}}} t)) \ .$$

Thus, by Lemma 3.22-5, it suffices to prove

$$
\begin{aligned}
x \barwedge y \barwedge t &= \overline{\top}(x \barwedge y \barwedge t) \barwedge (x \mathbin{\cdot_{\mathcal{D}}} (y \mathbin{\cdot_{\mathcal{D}}} t)) && (4.30)\\
x_{\overline{\top}y} \barwedge y \barwedge t &= \overline{\top}(x_{\overline{\top}y} \barwedge y \barwedge t) \barwedge (x \mathbin{\cdot_{\mathcal{D}}} (y \mathbin{\cdot_{\mathcal{D}}} t)) && (4.31)\\
(x \barwedge y)_t &= \overline{\top}((x \barwedge y)_t) \barwedge (x \mathbin{\cdot_{\mathcal{D}}} (y \mathbin{\cdot_{\mathcal{D}}} t)) && (4.32)\\
(x_{\overline{\top}y} \barwedge y)_t &= \overline{\top}((x_{\overline{\top}y} \barwedge y)_t) \barwedge (x \mathbin{\cdot_{\mathcal{D}}} (y \mathbin{\cdot_{\mathcal{D}}} t)) && (4.33)
\end{aligned}
$$

to show

$$x \barwedge y \barwedge t \barwedge x_{\overline{\top}y} \barwedge y \barwedge t \barwedge (x \barwedge y)_t \barwedge (x_{\overline{\top}y} \barwedge y)_t = x \mathbin{\cdot_{\mathcal{D}}} (y \mathbin{\cdot_{\mathcal{D}}} t) \ ,$$

which completes the proof of associativity of $\cdot_{\mathcal{D}}$.

(a) Proof of (4.30).

$$
\begin{array}{ll}
& \overline{\top}(x \barwedge y \barwedge t) \barwedge (x \mathbin{\cdot_{\mathcal{D}}} (y \mathbin{\cdot_{\mathcal{D}}} t)) \\
= & \quad \langle \text{ by Definition 4.16, Proposition 3.14-1 and (4.5) with} \\
& \quad x,t := y,t \ \rangle \\
& \overline{\top}(x \barwedge y \barwedge t) \barwedge (x \barwedge (y \barwedge t \barwedge y_t) \barwedge x_{\overline{\top}(y \barwedge t \barwedge y_t)} \barwedge (y \barwedge t \barwedge y_t)) \\
= & \quad \langle \text{ by Corollary 3.21-4 } \rangle \\
& \overline{\top}(x \barwedge y \barwedge t) \barwedge x \barwedge (y \barwedge t \barwedge y_t) \barwedge \overline{\top}(x \barwedge y \barwedge t) \barwedge x_{\overline{\top}(y \barwedge t \barwedge y_t)} \barwedge (y \barwedge t \barwedge y_t) \\
= & \quad \langle \text{ by (3.20), Proposition 3.14-7, (4.4) with} \\
& \quad x,t := x, \overline{\top}(y \barwedge t \barwedge y_t), \text{ Boolean algebra and (3.19) } \rangle \\
& x \barwedge \overline{\top}(y \barwedge t) \barwedge (y \barwedge t \barwedge y_t) \barwedge \overline{\top}(x \barwedge y \barwedge t) \barwedge \neg \overline{\top}(x \barwedge (y \barwedge t \barwedge y_t)) \barwedge x_{\overline{\top}(y \barwedge t \barwedge y_t)} \barwedge (y \barwedge t \barwedge y_t) \\
= & \quad \langle \text{ by Corollary 3.21-12, Proposition 3.14-8} \\
& \quad \text{and Boolean algebra,} \\
& \quad \mathsf{true} \Longrightarrow y \barwedge t \barwedge y_t \sqsubseteq y \barwedge t \Longrightarrow x \barwedge (y \barwedge t \barwedge y_t) \sqsubseteq x \barwedge y \barwedge t \\
& \quad \Longrightarrow \overline{\top}(x \barwedge (y \barwedge t \barwedge y_t)) \sqsubseteq \overline{\top}(x \barwedge y \barwedge t) \\
& \quad \Longrightarrow \overline{\top}(x \barwedge y \barwedge t) \barwedge \neg \overline{\top}(x \barwedge (y \barwedge t \barwedge y_t)) = \top; \\
& \quad \text{apply Corollary 3.21-4 too } \rangle \\
& x \barwedge (\overline{\top}(y \barwedge t) \barwedge y \barwedge t \barwedge \overline{\top}(y \barwedge t) \barwedge y_t) \barwedge \top \barwedge x_{\overline{\top}(y \barwedge t \barwedge y_t)} \barwedge (y \barwedge t \barwedge y_t)
\end{array}
$$

$$
\begin{array}{ll}
= & \quad \langle \text{ by Proposition 3.14-7, Remark 4.8, Boolean algebra, (3.6) and Corollary 3.21-3 } \rangle \\
& x \mathbin{\square} y \mathbin{\square} t
\end{array}
$$

(b) Proof of (4.31). First, we derive an intermediate result.

$$
\begin{array}{ll}
& \mathbb{\Pi}(\mathbb{\Pi}(x_{\mathbb{\Pi} y} \mathbin{\square} y \mathbin{\square} t) \mathbin{\square} x \mathbin{\square} (y \mathbin{\square} t \mathbin{\sqcap} y_t)) \\
= & \quad \langle \text{ by Proposition 3.14-9 } \rangle \\
& \mathbb{\Pi}(x_{\mathbb{\Pi} y} \mathbin{\square} y \mathbin{\square} t) \mathbin{\square} \mathbb{\Pi}(x \mathbin{\square} (y \mathbin{\square} t \mathbin{\sqcap} y_t)) \\
\sqsupseteq & \quad \langle \text{ by (4.9) and Proposition 3.14-8,} \\
& \quad \mathsf{true} \Longrightarrow {}^{\mathbb{\Pi}} y \sqsubseteq \mathbb{\Pi}(y \mathbin{\square} t \mathbin{\sqcap} y_t) \Longrightarrow x \mathbin{\square} {}^{\mathbb{\Pi}} y \sqsubseteq x \mathbin{\square} \mathbb{\Pi}(y \mathbin{\square} t \mathbin{\sqcap} y_t) \\
& \quad \Longrightarrow \mathbb{\Pi}(x \mathbin{\square} {}^{\mathbb{\Pi}} y) \sqsubseteq \mathbb{\Pi}(x \mathbin{\square} \mathbb{\Pi}(y \mathbin{\square} t \mathbin{\sqcap} y_t)), \\
& \quad \text{then apply (3.20) and Proposition 3.14-18 } \rangle \\
& \mathbb{\Pi}(x_{\mathbb{\Pi} y}) \mathbin{\square} \mathbb{\Pi}(x \mathbin{\square} {}^{\mathbb{\Pi}} y) \\
\sqsupseteq & \quad \langle \text{ by (4.4) with } x, t := x, {}^{\mathbb{\Pi}} y \text{ and Boolean algebra } \rangle \\
& \neg \mathbb{\Pi}(x \mathbin{\square} {}^{\mathbb{\Pi}} y) \mathbin{\square} \mathbb{\Pi}(x \mathbin{\square} {}^{\mathbb{\Pi}} y) \\
= & \quad \langle \text{ by Boolean algebra } \rangle \\
& \top
\end{array}
$$

And now the main proof.

$$
\begin{array}{ll}
& \mathbb{\Pi}(x_{\mathbb{\Pi} y} \mathbin{\square} y \mathbin{\square} t) \mathbin{\square} (x \mathbin{\cdot_{\mathcal{D}}} (y \mathbin{\cdot_{\mathcal{D}}} t)) \\
= & \quad \langle \text{ by Definition 4.16, Proposition 3.14-1 and (4.5) with } x, t := y, t \rangle \\
& \mathbb{\Pi}(x_{\mathbb{\Pi} y} \mathbin{\square} y \mathbin{\square} t) \mathbin{\square} (x \mathbin{\square} (y \mathbin{\square} t \mathbin{\sqcap} y_t) \mathbin{\sqcap} x_{\mathbb{\Pi}(y \mathbin{\square} t \mathbin{\sqcap} y_t)} \mathbin{\square} (y \mathbin{\square} t \mathbin{\sqcap} y_t)) \\
= & \quad \langle \text{ by Corollary 3.21-4 } \rangle \\
& \mathbb{\Pi}(x_{\mathbb{\Pi} y} \mathbin{\square} y \mathbin{\square} t) \mathbin{\square} x \mathbin{\square} (y \mathbin{\square} t \mathbin{\sqcap} y_t) \mathbin{\sqcap} \mathbb{\Pi}(x_{\mathbb{\Pi} y} \mathbin{\square} y \mathbin{\square} t) \mathbin{\square} x_{\mathbb{\Pi}(y \mathbin{\square} t \mathbin{\sqcap} y_t)} \mathbin{\square} (y \mathbin{\square} t \mathbin{\sqcap} y_t) \\
= & \quad \langle \text{ by the intermediate result above, Proposition 3.14-19 and (3.20) } \rangle \\
& \top \mathbin{\sqcap} \mathbb{\Pi}(x_{\mathbb{\Pi} y} \mathbin{\square} \mathbb{\Pi}(y \mathbin{\square} t)) \mathbin{\square} x_{\mathbb{\Pi}(y \mathbin{\square} t \mathbin{\sqcap} y_t)} \mathbin{\square} (y \mathbin{\square} t \mathbin{\sqcap} y_t) \\
= & \quad \langle \text{ by (4.9), Corollary 3.21-16 and Boolean algebra,} \\
& \quad {}^{\mathbb{\Pi}} y \sqsubseteq \mathbb{\Pi}(y \mathbin{\square} t \mathbin{\sqcap} y_t) \sqsubseteq \mathbb{\Pi}(y \mathbin{\square} t), \\
& \quad \text{then apply Corollaries 3.21-3 and 4.30-3 with} \\
& \quad r, s, t := {}^{\mathbb{\Pi}} y, \mathbb{\Pi}(y \mathbin{\square} t), \mathbb{\Pi}(y \mathbin{\square} t \mathbin{\sqcap} y_t) \rangle \\
& x_{\mathbb{\Pi} y} \mathbin{\square} \mathbb{\Pi}(y \mathbin{\square} t) \mathbin{\square} (y \mathbin{\square} t \mathbin{\sqcap} y_t) \\
= & \quad \langle \text{ by Corollary 3.21-4 } \rangle \\
& x_{\mathbb{\Pi} y} \mathbin{\square} (\mathbb{\Pi}(y \mathbin{\square} t) \mathbin{\square} y \mathbin{\square} t \mathbin{\sqcap} \mathbb{\Pi}(y \mathbin{\square} t) \mathbin{\square} y_t)
\end{array}
$$

$$
\begin{array}{ll}
= & \langle \text{ by Proposition 3.14-7, Remark 4.8 and (3.6) } \rangle \\
x_{\overline{\sqcap}_y} \mathbin{\square} (y \mathbin{\square} t \mathbin{\sqcap} \top) & \\
= & \langle \text{ by Corollary 3.21-3 } \rangle \\
x_{\overline{\sqcap}_y} \mathbin{\square} y \mathbin{\square} t &
\end{array}
$$

(c) Proof of (4.32).

$$
\begin{array}{ll}
\overline{\sqcap}((x \mathbin{\square} y)_t) \mathbin{\square} (x \mathbin{\cdot_{\mathcal{D}}} (y \mathbin{\cdot_{\mathcal{D}}} t)) & \\
= & \langle \text{ by Definition 4.16, Proposition 3.14-1 and (4.5) with } \\
& \quad x, t := y, t \ \rangle \\
\overline{\sqcap}((x \mathbin{\square} y)_t) \mathbin{\square} (x \mathbin{\square} (y \mathbin{\square} t \mathbin{\sqcap} y_t) \mathbin{\sqcap} x_{\overline{\sqcap}(y \mathbin{\square} t \mathbin{\sqcap} y_t)} \mathbin{\square} (y \mathbin{\square} t \mathbin{\sqcap} y_t)) & \\
= & \langle \text{ by Theorem 4.27 } \rangle \\
(x \mathbin{\square} y)_t &
\end{array}
$$

(d) Proof of (4.33). Again, we start with intermediate results.

$$
\begin{array}{ll}
\overline{\sqcap}(\overline{\sqcap}(x_{\overline{\sqcap}_y} \mathbin{\square} y)_t \mathbin{\square} x \mathbin{\square} (y \mathbin{\square} t \mathbin{\sqcap} y_t)) & \\
= & \langle \text{ by Proposition 3.14-9 } \rangle \\
\overline{\sqcap}((x_{\overline{\sqcap}_y} \mathbin{\square} y)_t) \mathbin{\square} \overline{\sqcap}(x \mathbin{\square} (y \mathbin{\square} t \mathbin{\sqcap} y_t)) & \\
\sqsupseteq & \langle \text{ by (4.9) and Proposition 3.14-8, } \\
& \quad \mathsf{true} \Longrightarrow \overline{\sqcap} y \sqsubseteq \overline{\sqcap}(y \mathbin{\square} t \mathbin{\sqcap} y_t) \Longrightarrow x \mathbin{\square} \overline{\sqcap} y \sqsubseteq x \mathbin{\square} \overline{\sqcap}(y \mathbin{\square} t \mathbin{\sqcap} y_t)) \\
& \quad \Longrightarrow \overline{\sqcap}(x \mathbin{\square} \overline{\sqcap} y) \sqsubseteq \overline{\sqcap}(x \mathbin{\square} \overline{\sqcap}(y \mathbin{\square} t \mathbin{\sqcap} y_t))), \\
& \quad \text{then apply (3.20) } \rangle \\
\overline{\sqcap}((x_{\overline{\sqcap}_y} \mathbin{\square} y)_t) \mathbin{\square} \overline{\sqcap}(x \mathbin{\square} \overline{\sqcap} y) & \\
\sqsupseteq & \langle \text{ by (4.4) with } x, t := x_{\overline{\sqcap}_y} \mathbin{\square} y, t \text{ and Boolean algebra } \rangle \\
\overline{\sqcap}(x_{\overline{\sqcap}_y} \mathbin{\square} y) \mathbin{\square} \overline{\sqcap}(x \mathbin{\square} \overline{\sqcap} y) & \\
= & \langle \text{ by (3.20) and (4.5) with } x, t := x, \overline{\sqcap} y \ \rangle \\
\overline{\sqcap}(x_{\overline{\sqcap}_y}) \mathbin{\square} \overline{\sqcap}(x \mathbin{\square} \overline{\sqcap} y) & \\
\sqsupseteq & \langle \text{ by (4.4) with } x, t := x, \overline{\sqcap} y \text{ and Boolean algebra } \rangle \\
\neg \overline{\sqcap}(x \mathbin{\square} \overline{\sqcap} y) \mathbin{\square} \overline{\sqcap}(x \mathbin{\square} \overline{\sqcap} y) & \\
= & \langle \text{ by Boolean algebra } \rangle \\
\top &
\end{array}
$$

Proposition 3.14-19 then yields

$$\overline{\sqcap}(x_{\overline{\sqcap}_y} \mathbin{\square} y)_t \mathbin{\square} x \mathbin{\square} (y \mathbin{\square} t \mathbin{\sqcap} y_t) = \top \ . \tag{4.34}$$

Looking at the previous derivation from the third step down to the last, we also get

$$\Pi(x_{\Pi y} \circ y)_t \circ \Pi(x \circ \Pi y) = \top \ . \tag{4.35}$$

There is a similar proof for

$$\Pi(x_{\Pi y} \circ y)_t \circ \Pi(x \circ \neg \Pi y) = \top \ . \tag{4.36}$$

And here is the main proof.

$$\begin{array}{ll}
& \Pi((x_{\Pi y} \circ y)_t) \circ (x \mathbin{;_{\mathcal{D}}} (y \mathbin{;_{\mathcal{D}}} t)) \\
= & \qquad \langle \text{ by Definition 4.16, Proposition 3.14-1 and (4.5) with } x, t := y, t \ \rangle \\
& \Pi((x_{\Pi y} \circ y)_t) \circ (x \circ (y \circ t \sqcap y_t) \sqcap x_{\Gamma(y \circ t \sqcap y_t)} \circ (y \circ t \sqcap y_t)) \\
= & \qquad \langle \text{ by Corollary 3.21-4 } \rangle \\
& \Pi((x_{\Pi y} \circ y)_t) \circ x \circ (y \circ t \sqcap y_t) \sqcap \Pi((x_{\Pi y} \circ y)_t) \circ x_{\Gamma(y \circ t \sqcap y_t)} \circ (y \circ t \sqcap y_t) \\
= & \qquad \langle \text{ by (4.34) and (4.3) with } x, t := x, \Pi y \ \rangle \\
& \top \sqcap \Pi((x_{\Pi y} \circ y)_t) \circ (x \circ \Pi y \sqcap x \circ \neg \Pi y \sqcap (x_{\Pi y} \sqcup x_{\neg \Pi y})) \Gamma(y \circ t \sqcap y_t) \circ (y \circ t \sqcap y_t) \\
= & \qquad \langle \text{ by Corollaries 3.21-3, 3.21-13, 4.30-1 and 3.21-4 } \rangle \\
& \Pi((x_{\Pi y} \circ y)_t) \circ ((x \circ \Pi y)_{\Gamma(y \circ t \sqcap y_t)} \sqcap \neg \Pi(x \circ \Pi y) \circ (x \circ \neg \Pi y)_{\Gamma(y \circ t \sqcap y_t)} \sqcap \\
& \qquad \neg \Pi(x \circ \Pi y) \circ \neg \Pi(x \circ \neg \Pi y) \circ (x_{\Pi y} \sqcup x_{\neg \Pi y})_{\Gamma(y \circ t \sqcap y_t)}) \circ (y \circ t \sqcap y_t) \\
= & \qquad \langle \text{ by Propositions 3.14-7 and 3.14-3, (4.4) with } \\
& \qquad x, t := x \circ \neg \Pi y, \Pi(y \circ t \sqcap y_t), \text{ (4.4) with } \\
& \qquad x, t := x_{\Pi y} \sqcup x_{\neg \Pi y}, \Pi(y \circ t \sqcap y_t), \text{ (4.4) with } x, t := x, \Pi y, \\
& \qquad \text{Lemma 3.17-5, (3.21) and Boolean algebra } \rangle \\
& \Pi((x_{\Pi y} \circ y)_t) \circ ((x \circ \Pi y)_{\Gamma(y \circ t \sqcap y_t)} \sqcap (x \circ \neg \Pi y)_{\Gamma(y \circ t \sqcap y_t)} \sqcap (x_{\Pi y} \sqcup x_{\neg \Pi y})_{\Gamma(y \circ t \sqcap y_t)}) \circ \\
& (y \circ t \sqcap y_t) \\
= & \qquad \langle \text{ by Corollary 3.21-4, Proposition 3.14-7, (4.4) with } \\
& \qquad x, t := x \circ \Pi y, \Pi(y \circ t \sqcap y_t), \text{ (4.4) with } x, t := x \circ \neg \Pi y, \Pi(y \circ t \sqcap y_t) \\
& \qquad \text{and Boolean algebra } \rangle \\
& \Big(\Pi((x_{\Pi y} \circ y)_t) \circ \Pi(x \circ \Pi y) \circ (x \circ \Pi y)_{\Gamma(y \circ t \sqcap y_t)} \sqcap \\
& \ \Pi((x_{\Pi y} \circ y)_t) \circ \Pi(x \circ \neg \Pi y) \circ (x \circ \neg \Pi y)_{\Gamma(y \circ t \sqcap y_t)} \sqcap \\
& \ \Pi((x_{\Pi y} \circ y)_t) \circ (x_{\Pi y} \sqcup x_{\neg \Pi y})_{\Gamma(y \circ t \sqcap y_t)} \Big) \circ (y \circ t \sqcap y_t) \\
= & \qquad \langle \text{ by (4.35), (4.36), (3.6) and Corollary 3.21-3 } \rangle \\
& \Pi((x_{\Pi y} \circ y)_t) \circ (x_{\Pi y} \sqcup x_{\neg \Pi y})_{\Gamma(y \circ t \sqcap y_t)} \circ (y \circ t \sqcap y_t) \\
= & \qquad \langle \text{ by Theorem 4.23 } \rangle \\
& \Pi((x_{\Pi y} \circ y)_t) \circ \Big(\Pi(x_{\neg \Pi y} \circ \neg \Pi(y \circ t \sqcap y_t)) \circ x_{\Pi y} \circ \Pi(y \circ t \sqcap y_t) \sqcap
\end{array}$$

$$\ulcorner(x_{\neg\ulcorner y}\Box\neg\ulcorner(y\Box t \sqcap y_t))\Box(x_{\ulcorner y})_{\ulcorner(y\Box t\sqcap y_t)} \sqcap$$
$$(x_{\ulcorner y}\Box\ulcorner(y\Box t \sqcap y_t) \sqcup (x_{\neg\ulcorner y})_{\ulcorner(y\Box t\sqcap y_t)}) \sqcap$$
$$\ulcorner(x_{\ulcorner y}\Box\neg\ulcorner(y\Box t \sqcap y_t))\Box x_{\neg\ulcorner y}\Box\ulcorner(y\Box t \sqcap y_t) \sqcap$$
$$\ulcorner(x_{\ulcorner y}\Box\neg\ulcorner(y\Box t \sqcap y_t))\Box(x_{\neg\ulcorner y})_{\ulcorner(y\Box t\sqcap y_t)} \sqcap$$
$$((x_{\ulcorner y})_{\ulcorner(y\Box t\sqcap y_t)} \sqcup x_{\neg\ulcorner y}\Box\ulcorner(y\Box t \sqcap y_t)) \sqcap$$
$$((x_{\ulcorner y})_{\ulcorner(y\Box t\sqcap y_t)} \sqcup (x_{\neg\ulcorner y})_{\ulcorner(y\Box t\sqcap y_t)})\Big)\Box(y\Box t \sqcap y_t)$$

$=$ ⟨ by (4.9) and Boolean algebra, $\neg\ulcorner(y\Box t \sqcap y_t) \sqsubseteq \neg\ulcorner y$, then apply (4.6) with $x, t := x, \ulcorner y$ and Corollary 4.26-1 ⟩

$$\ulcorner((x_{\ulcorner y}\Box y)_t)\Box\Big(\ulcorner(x_{\neg\ulcorner y})\Box x_{\ulcorner y}\Box\ulcorner(y\Box t \sqcap y_t) \sqcap \ulcorner(x_{\neg\ulcorner y})\Box(x_{\ulcorner y})_{\ulcorner(y\Box t\sqcap y_t)} \sqcap$$
$$(x_{\ulcorner y}\Box\ulcorner(y\Box t \sqcap y_t) \sqcup \top) \sqcap \ulcorner(x_{\ulcorner y}\Box\neg\ulcorner(y\Box t \sqcap y_t))\Box x_{\neg\ulcorner y}\Box\top \sqcap$$
$$\ulcorner(x_{\ulcorner y}\Box\neg\ulcorner(y\Box t \sqcap y_t))\Box\top \sqcap ((x_{\ulcorner y})_{\ulcorner(y\Box t\sqcap y_t)} \sqcup \top) \sqcap$$
$$((x_{\ulcorner y})_{\ulcorner(y\Box t\sqcap y_t)} \sqcup \top)\Big)\Box(y\Box t \sqcap y_t)$$

$=$ ⟨ by (4.4) with $x, t := x, \ulcorner y$, (3.4), (3.6) and Corollary 3.21-3 ⟩

$$\ulcorner((x_{\ulcorner y}\Box y)_t)\Box(\ulcorner(x_{\ulcorner y})\Box x_{\ulcorner y}\Box\ulcorner(y\Box t \sqcap y_t) \sqcap \ulcorner(x_{\ulcorner y})\Box(x_{\ulcorner y})_{\ulcorner(y\Box t\sqcap y_t)})\Box(y\Box t \sqcap y_t)$$

$=$ ⟨ by Proposition 3.14-7, (4.4) with $x, t := x_{\ulcorner y}, \ulcorner(y\Box t \sqcap y_t)$ and Boolean algebra ⟩

$$\ulcorner((x_{\ulcorner y}\Box y)_t)\Box(x_{\ulcorner y}\Box\ulcorner(y\Box t \sqcap y_t) \sqcap (x_{\ulcorner y})_{\ulcorner(y\Box t\sqcap y_t)})\Box(y\Box t \sqcap y_t)$$

$=$ ⟨ by (4.4) and Boolean algebra, $\ulcorner(x_{\ulcorner y}\Box\ulcorner(y\Box t \sqcap y_t))\Box\ulcorner((x_{\ulcorner y})_{\ulcorner(y\Box t\sqcap y_t)}) = \top$, then apply Corollary 3.21-17 and Proposition 3.14-7 ⟩

$$\ulcorner((x_{\ulcorner y}\Box y)_t)\Box(x_{\ulcorner y}\Box(y\Box t \sqcap y_t) \sqcap (x_{\ulcorner y})_{\ulcorner(y\Box t\sqcap y_t)}\Box(y\Box t \sqcap y_t))$$

$=$ ⟨ by Theorem 4.27 ⟩

$$(x_{\ulcorner y}\Box y)_t$$

6. This is direct from Proposition 4.17-2.

7. This is direct from Proposition 4.17-1.

8. First, we prove $\ulcorner(x \cdot_D (y +_D z)) = \ulcorner(x \cdot_D y +_D x \cdot_D z)$.

$$\ulcorner(x \cdot_D (y +_D z))$$

$=$ ⟨ by Proposition 4.17-5 ⟩

$$\ulcorner x\Box\neg\ulcorner(x\Box\neg\ulcorner(y +_D z))$$

$=$ ⟨ by Corollary 4.4-3 ⟩

$$
\begin{array}{ll}
& \Cap x \cdot \neg \Cap (x \cdot \neg (\Cap y \sqcap \Cap z)) \\
= & \qquad \langle \text{ by De Morgan } \rangle \\
& \Cap x \cdot \neg \Cap (x \cdot \neg \Cap y \cdot \neg \Cap z) \\
= & \qquad \langle \text{ by Proposition 3.14-12 } \rangle \\
& \Cap x \cdot \neg (\Cap (x \cdot \neg \Cap y) \cdot \Cap (x \cdot \neg \Cap z)) \\
= & \qquad \langle \text{ by De Morgan } \rangle \\
& \Cap x \cdot (\neg \Cap (x \cdot \neg \Cap y) \sqcap \neg \Cap (x \cdot \neg \Cap z)) \\
= & \qquad \langle \text{ by Boolean algebra } \rangle \\
& \Cap x \cdot \neg \Cap (x \cdot \neg \Cap y) \sqcap \Cap x \cdot \neg \Cap (x \cdot \neg \Cap z) \\
= & \qquad \langle \text{ by Proposition 4.17-5 } \rangle \\
& \Cap (x \mathbin{;_D} y) \sqcap \Cap (x \mathbin{;_D} z) \\
= & \qquad \langle \text{ by Corollary 4.4-3 } \rangle \\
& \Cap (x \mathbin{;_D} y +_D x \mathbin{;_D} z)
\end{array}
$$

Now,

$$
\begin{array}{ll}
& x \mathbin{;_D} y +_D x \mathbin{;_D} z \\
= & \qquad \langle \text{ by Corollary 4.4-1 } \rangle \\
& \neg \Cap (x \mathbin{;_D} z) \cdot (x \mathbin{;_D} y) \sqcap \neg \Cap (x \mathbin{;_D} y) \cdot (x \mathbin{;_D} z) \sqcap ((x \mathbin{;_D} y) \sqcup (x \mathbin{;_D} z)) \\
= & \qquad \langle \text{ by Definition 4.16 } \rangle \\
& \neg \Cap (x \mathbin{;_D} z) \cdot (x \mathbin{;_D} y) \sqcap \neg \Cap (x \mathbin{;_D} y) \cdot (x \mathbin{;_D} z) \sqcap \\
& ((x \cdot y \sqcap x_{\Cap y} \cdot y) \sqcup (x \cdot z \sqcap x_{\Cap z} \cdot z)) \\
= & \qquad \langle \text{ by Corollary 3.21-14 } \rangle \\
& \neg \Cap (x \mathbin{;_D} z) \cdot (x \mathbin{;_D} y) \sqcap \neg \Cap (x \mathbin{;_D} y) \cdot (x \mathbin{;_D} z) \sqcap \\
& (x \cdot y \sqcup x \cdot z) \sqcap (x \cdot y \sqcup x_{\Cap z} \cdot z) \sqcap (x_{\Cap y} \cdot y \sqcup x \cdot z) \sqcap (x_{\Cap y} \cdot y \sqcup x_{\Cap z} \cdot z) \quad .
\end{array}
$$

Because $\Cap (x \mathbin{;_D} (y +_D z)) = \Cap (x \mathbin{;_D} y +_D x \mathbin{;_D} z)$, it thus suffices, by Lemma 3.22-5, to prove the following six equations.

$$
\Cap (\neg \Cap (x \mathbin{;_D} z) \cdot (x \mathbin{;_D} y)) \cdot (x \mathbin{;_D} (y +_D z)) = \neg \Cap (x \mathbin{;_D} z) \cdot (x \mathbin{;_D} y) \tag{4.37}
$$

$$
\Cap (\neg \Cap (x \mathbin{;_D} y) \cdot (x \mathbin{;_D} z)) \cdot (x \mathbin{;_D} (y +_D z)) = \neg \Cap (x \mathbin{;_D} y) \cdot (x \mathbin{;_D} z) \tag{4.38}
$$

$$
\Cap (x \cdot y \sqcup x \cdot z) \cdot (x \mathbin{;_D} (y +_D z)) = x \cdot y \sqcup x \cdot z \tag{4.39}
$$

$$
\Cap (x \cdot y \sqcup x_{\Cap z} \cdot z) \cdot (x \mathbin{;_D} (y +_D z)) = x \cdot y \sqcup x_{\Cap z} \cdot z \tag{4.40}
$$

$$
\Cap (x_{\Cap y} \cdot y \sqcup x \cdot z) \cdot (x \mathbin{;_D} (y +_D z)) = x_{\Cap y} \cdot y \sqcup x \cdot z \tag{4.41}
$$

$$
\Cap (x_{\Cap y} \cdot y \sqcup x_{\Cap z} \cdot z) \cdot (x \mathbin{;_D} (y +_D z)) = x_{\Cap y} \cdot y \sqcup x_{\Cap z} \cdot z \tag{4.42}
$$

Because $\sqcup$ and $+_D$ are commutative (by (3.2) and Corollary 4.4-5), equations (4.37) and (4.38) are symmetric in y and z, and similarly for (4.40) and (4.41). Thus, we only need to prove (4.37), (4.39), (4.40) and (4.42).

(a) Proof of (4.37). Since

$$
\begin{array}{ll}
& \Pi(\neg\Pi(x \mathbin{;_D} z)\sqcap(x \mathbin{;_D} y))\sqcap(x \mathbin{;_D} (y +_D z)) = \neg\Pi(x \mathbin{;_D} z)\sqcap(x \mathbin{;_D} y) \\
\Longleftrightarrow & \quad \langle \text{ by Propositions 3.14-9 and 3.14-7 } \rangle \\
& \neg\Pi(x \mathbin{;_D} z)\sqcap\Pi(x \mathbin{;_D} y)\sqcap(x \mathbin{;_D} (y +_D z)) = \neg\Pi(x \mathbin{;_D} z)\sqcap\Pi(x \mathbin{;_D} y)\sqcap(x \mathbin{;_D} y) \\
\Longleftarrow & \quad \langle \text{ by Boolean algebra and Leibniz } \rangle \\
& \neg\Pi(x \mathbin{;_D} z)\sqcap(x \mathbin{;_D} (y +_D z)) = \neg\Pi(x \mathbin{;_D} z)\sqcap(x \mathbin{;_D} y) \ ,
\end{array}
$$

we only prove the last equation.

$$
\begin{array}{ll}
& \neg\Pi(x \mathbin{;_D} z)\sqcap(x \mathbin{;_D} (y +_D z)) \\
= & \quad \langle \text{ by Proposition 4.17-7 } \rangle \\
& \neg\Pi(x \mathbin{;_D} z)\sqcap(x\sqcap\Pi(y +_D z) \sqcap x_{\Gamma(y+_D z)})\sqcap(y +_D z) \\
= & \quad \langle \text{ by Proposition 4.17-5, Corollary 4.4-3 and De Morgan } \rangle \\
& (\neg\Gamma x \sqcap \Pi(x\sqcap\neg\Pi z))\sqcap(x\sqcap(\Pi y \sqcap \Pi z) \sqcap x_{\Pi y\sqcap\Pi z})\sqcap(y +_D z) \\
= & \quad \langle \text{ by Corollary 3.21-5 } \rangle \\
& \neg\Gamma x\sqcap(x\sqcap(\Pi y \sqcap \Pi z) \sqcap x_{\Pi y\sqcap\Pi z})\sqcap(y +_D z) \sqcap \\
& \Pi(x\sqcap\neg\Pi z)\sqcap(x\sqcap(\Pi y \sqcap \Pi z) \sqcap x_{\Pi y\sqcap\Pi z})\sqcap(y +_D z) \\
= & \quad \langle \text{ by Proposition 3.14-7, (4.9), Boolean algebra, (3.6) and} \\
& \quad \text{Corollary 3.21-3 } \rangle \\
& \Pi(x\sqcap\neg\Pi z)\sqcap(x\sqcap(\Pi y \sqcap \Pi z) \sqcap x_{\Pi y\sqcap\Pi z})\sqcap(y +_D z) \\
= & \quad \langle \text{ by Corollary 3.21-4 } \rangle \\
& (\Pi(x\sqcap\neg\Pi z)\sqcap x\sqcap(\Pi y \sqcap \Pi z) \sqcap \Pi(x\sqcap\neg\Pi z)\sqcap x_{\Pi y\sqcap\Pi z})\sqcap(y +_D z) \\
= & \quad \langle \text{ by (3.19), Boolean algebra and Corollary 4.26-3 } \rangle \\
& (x\sqcap\neg\Pi z\sqcap(\Pi y \sqcap \Pi z) \sqcap \Pi(x\sqcap\neg\Pi z)\sqcap x_{\Pi y})\sqcap(y +_D z) \\
= & \quad \langle \text{ by Boolean algebra and Proposition 4.22-6 } \rangle \\
& (x\sqcap\Pi y\sqcap\neg\Pi z \sqcap \Pi(x\sqcap\neg\Pi z)\sqcap x_{\Pi y}\sqcap\neg\Pi z)\sqcap(y +_D z) \\
= & \quad \langle \text{ by Remark 4.8, Proposition 3.14-9 and Boolean algebra,} \\
& \quad \Pi(x\sqcap\Pi y)\sqcap\Pi(\Pi(x\sqcap\neg\Pi z)\sqcap x_{\Pi y}) = \Pi(x\sqcap\neg\Pi z)\sqcap\Pi(x\sqcap\Pi y)\sqcap\Pi(x_{\Pi y}) = \top \\
& \quad \text{then apply Corollaries 3.21-17 and 4.4-1 } \rangle \\
& (x\sqcap\Pi y \sqcap \Pi(x\sqcap\neg\Pi z)\sqcap x_{\Pi y})\sqcap\neg\Pi z\sqcap(\neg\Pi z\sqcap y \sqcap \neg\Pi y\sqcap z \sqcap (y \sqcup z))
\end{array}
$$

$=$ ⟨ by Corollaries 3.21-4 and 3.21-3, Propositions 3.14-17 and 3.14-11, Boolean algebra and (3.6) ⟩

$$(x \Box \ulcorner y \sqcap \ulcorner(x \Box \neg\ulcorner z) \Box x_{\ulcorner y}) \Box \neg\ulcorner z \Box y$$

$=$ ⟨ by Remark 4.8, Proposition 3.14-9 and Boolean algebra, $\ulcorner(x \Box \ulcorner y) \Box \ulcorner(\ulcorner(x \Box \neg\ulcorner z) \Box x_{\ulcorner y}) = \ulcorner(x \Box \neg\ulcorner z) \Box \ulcorner(x \Box \ulcorner y) \Box \ulcorner(x_{\ulcorner y}) = \top$, then apply Corollary 3.21-17 and Boolean algebra ⟩

$$x \Box \neg\ulcorner z \Box \ulcorner y \Box y \sqcap \ulcorner(x \Box \neg\ulcorner z) \Box x_{\ulcorner y} \Box \neg\ulcorner z \Box y$$

$=$ ⟨ by (3.19) and Propositions 3.14-7 and 4.22-6 ⟩

$$\ulcorner(x \Box \neg\ulcorner z) \Box x \Box y \sqcap \ulcorner(x \Box \neg\ulcorner z) \Box x_{\ulcorner y} \Box y$$

$=$ ⟨ by Corollary 3.21-4 ⟩

$$\ulcorner(x \Box \neg\ulcorner z) \Box (x \Box y \sqcap x_{\ulcorner y} \Box y)$$

$=$ ⟨ by Corollaries 3.21-4 and 3.21-3, Proposition 3.14-7, (4.4) with $x, t := x, \ulcorner y$, Boolean algebra and (3.6) ⟩

$$\neg\ulcorner x \Box (x \Box y \sqcap x_{\ulcorner y} \Box y) \sqcap \ulcorner(x \Box \neg\ulcorner z) \Box (x \Box y \sqcap x_{\ulcorner y} \Box y)$$

$=$ ⟨ by Corollary 3.21-5 ⟩

$$(\neg\ulcorner x \sqcap \ulcorner(x \Box \neg\ulcorner z)) \Box (x \Box y \sqcap x_{\ulcorner y} \Box y)$$

$=$ ⟨ by De Morgan, Proposition 4.17-5 and Definition 4.16 ⟩

$$\neg\ulcorner(x \cdot_D z) \Box (x \cdot_D y)$$

(b) Proof of (4.39).

$$\ulcorner(x \Box y \sqcup x \Box z) \Box (x \cdot_D (y +_D z))$$

$=$ ⟨ by (3.21), (3.20), Proposition 3.14-3 and Definition 4.16 ⟩

$$\ulcorner(x \Box \ulcorner y) \Box \ulcorner(x \Box \ulcorner z) \Box (x \Box (y +_D z) \sqcap x_{\ulcorner(y +_D z)} \Box (y +_D z))$$

$=$ ⟨ by Corollary 3.21-4 ⟩

$$\ulcorner(x \Box \ulcorner y) \Box \ulcorner(x \Box \ulcorner z) \Box x \Box (y +_D z) \sqcap \ulcorner(x \Box \ulcorner y) \Box \ulcorner(x \Box \ulcorner z) \Box x_{\ulcorner(y +_D z)} \Box (y +_D z)$$

$=$ ⟨ by (4.4) with $x, t := x, \ulcorner(y +_D z)$, Corollary 4.4-3, Lemma 3.17-6 and Boolean algebra,

$\ulcorner(x \Box \ulcorner z) \Box \ulcorner(x_{\ulcorner(y +_D z)})$

$\sqsupseteq \ulcorner(x \Box \ulcorner z) \Box \neg\ulcorner(x \Box \ulcorner(y +_D z)) = \ulcorner(x \Box \ulcorner z) \Box \neg\ulcorner(x \Box (\ulcorner y \sqcap \ulcorner z))$

$\sqsupseteq \ulcorner(x \Box \ulcorner z) \Box \neg\ulcorner(x \Box \ulcorner z) = \top$,

then apply (3.19) twice, Corollary 4.4-1 and Proposition 3.14-7 ⟩

$$x \Box \ulcorner y \Box \ulcorner z \Box (\neg\ulcorner z \Box y \sqcap \neg\ulcorner y \Box z \sqcap (y \sqcup z)) \sqcap \ulcorner(x \Box \ulcorner y) \Box \top \Box x_{\ulcorner(y +_D z)} \Box (y +_D z)$$

$=$ ⟨ by Corollaries 3.21-4 and 3.21-3, Boolean algebra and (3.6) ⟩

$$
\begin{array}{ll}
& x \mathbin{\triangleright} {}^{\sqcap}y \mathbin{\triangleright} {}^{\sqcap}z \mathbin{\triangleright} (y \sqcup z) \\
= & \qquad \langle \text{ by Proposition 3.14-11 and (3.8) } \rangle \\
& x \mathbin{\triangleright} y \sqcup x \mathbin{\triangleright} z
\end{array}
$$

(c) Proof of (4.40).

$$
\begin{array}{ll}
& {}^{\sqcap}(x \mathbin{\triangleright} y \sqcup x_{\Gamma z} \mathbin{\triangleright} z) \mathbin{\triangleright} (x \cdot_D (y +_D z)) \\
= & \qquad \langle \text{ by (3.21), (3.20), Proposition 3.14-3, Definition 4.16 and Boolean algebra } \rangle \\
& {}^{\sqcap}(x_{\Gamma z} \mathbin{\triangleright} {}^{\sqcap}z) \mathbin{\triangleright} {}^{\sqcap}(x \mathbin{\triangleright} {}^{\sqcap}y) \mathbin{\triangleright} (x \mathbin{\triangleright} (y +_D z) \sqcap x_{\Gamma(y +_D z)} \mathbin{\triangleright} (y +_D z)) \\
= & \qquad \langle \text{ by (4.5) with } x, t := x, {}^{\sqcap}z \text{ and Corollaries 3.21-4 and 4.4-3 } \rangle \\
& {}^{\sqcap}(x_{\Gamma z}) \mathbin{\triangleright} ({}^{\sqcap}(x \mathbin{\triangleright} {}^{\sqcap}y) \mathbin{\triangleright} x \mathbin{\triangleright} (y +_D z) \sqcap {}^{\sqcap}(x \mathbin{\triangleright} {}^{\sqcap}y) \mathbin{\triangleright} x_{\Gamma y \sqcap \Gamma z} \mathbin{\triangleright} (y +_D z)) \\
= & \qquad \langle \text{ by (4.4) with } x, t := x, {}^{\sqcap}(y +_D z), \text{ Corollary 4.4-3, Lemma 3.17-6 and Boolean algebra,} \\
& \qquad {}^{\sqcap}(x \mathbin{\triangleright} {}^{\sqcap}z) \mathbin{\triangleright} {}^{\sqcap}(x_{\Gamma(y +_D z)}) \\
& \qquad \sqsupseteq {}^{\sqcap}(x \mathbin{\triangleright} {}^{\sqcap}z) \mathbin{\triangleright} \neg {}^{\sqcap}(x \mathbin{\triangleright} {}^{\sqcap}(y +_D z)) = {}^{\sqcap}(x \mathbin{\triangleright} {}^{\sqcap}z) \mathbin{\triangleright} \neg {}^{\sqcap}(x \mathbin{\triangleright} ({}^{\sqcap}y \sqcap {}^{\sqcap}z)) \\
& \qquad \sqsupseteq {}^{\sqcap}(x \mathbin{\triangleright} {}^{\sqcap}z) \mathbin{\triangleright} \neg {}^{\sqcap}(x \mathbin{\triangleright} {}^{\sqcap}z) = \top, \\
& \qquad \text{then apply (3.19) twice, Corollary 4.4-1 and Proposition 3.14-7 } \rangle \\
& {}^{\sqcap}(x_{\Gamma z}) \mathbin{\triangleright} (x \mathbin{\triangleright} {}^{\sqcap}y \mathbin{\triangleright} (y +_D z) \sqcap \top \mathbin{\triangleright} (y +_D z)) \\
= & \qquad \langle \text{ by Corollary 4.4-1, (3.6) and Corollary 3.21-3 } \rangle \\
& {}^{\sqcap}(x_{\Gamma z}) \mathbin{\triangleright} x \mathbin{\triangleright} {}^{\sqcap}y \mathbin{\triangleright} (\neg {}^{\sqcap}z \mathbin{\triangleright} y \sqcap \neg {}^{\sqcap}y \mathbin{\triangleright} z \sqcap (y \sqcup z)) \\
= & \qquad \langle \text{ by Corollaries 3.21-4 and 3.21-3, Boolean algebra, Propositions 3.14-7 and 3.14-11, and (3.6) } \rangle \\
& {}^{\sqcap}(x_{\Gamma z}) \mathbin{\triangleright} x \mathbin{\triangleright} (\neg {}^{\sqcap}z \mathbin{\triangleright} y \sqcap (y \sqcup z)) \\
= & \qquad \langle \text{ by Proposition 4.22-2 } \rangle \\
& (x_{\Gamma z} \sqcup x_{\neg \Gamma z}) \mathbin{\triangleright} (\neg {}^{\sqcap}z \mathbin{\triangleright} y \sqcap (y \sqcup z)) \\
= & \qquad \langle \text{ by (3.9), (4.5) with } x, t := x, {}^{\sqcap}z \text{ and (4.6) with } x, t := x, {}^{\sqcap}z \\
& \qquad \rangle \\
& x_{\Gamma z} \mathbin{\triangleright} {}^{\sqcap}z \mathbin{\triangleright} (\neg {}^{\sqcap}z \mathbin{\triangleright} y \sqcap (y \sqcup z)) \sqcup x_{\neg \Gamma z} \mathbin{\triangleright} \neg {}^{\sqcap}z \mathbin{\triangleright} (\neg {}^{\sqcap}z \mathbin{\triangleright} y \sqcap (y \sqcup z)) \\
= & \qquad \langle \text{ by Corollaries 3.21-4 and 3.21-3, Proposition 3.14-11, Boolean algebra, (3.6) and (4.6) with } x, t := x, {}^{\sqcap}z \rangle \\
& x_{\Gamma z} \mathbin{\triangleright} (y \sqcup z) \sqcup x_{\neg \Gamma z} \mathbin{\triangleright} y \\
= & \qquad \langle \text{ by (3.8) and (3.9) } \rangle \\
& (x_{\Gamma z} \sqcup x_{\neg \Gamma z}) \mathbin{\triangleright} y \sqcup x_{\Gamma z} \mathbin{\triangleright} z \\
= & \qquad \langle \text{ by Proposition 4.22-2 } \rangle
\end{array}
$$

$$
\begin{array}{ll}
& {}^{\sqcap\!\!\sqcap}(x_{{}^{\sqcap\!\!\sqcap}z})\mathbin{\square} x \mathbin{\square} y \sqcup x_{{}^{\sqcap\!\!\sqcap}z} \mathbin{\square} z \\
= & \qquad \langle \text{ by Propositions 3.14-20 and 3.14-7 } \rangle \\
& x \mathbin{\square} y \sqcup x_{{}^{\sqcap\!\!\sqcap}z} \mathbin{\square} z
\end{array}
$$

(d) Proof of (4.42). The proof uses the following abbreviations.

$$
\begin{array}{lcl}
r & := & {}^{\sqcap\!\!\sqcap}y \mathbin{\square} {}^{\sqcap\!\!\sqcap}z \\
s & := & {}^{\sqcap\!\!\sqcap}y \mathbin{\square} \neg {}^{\sqcap\!\!\sqcap}z \\
t & := & \neg {}^{\sqcap\!\!\sqcap}y \mathbin{\square} {}^{\sqcap\!\!\sqcap}z \\
A & := & \neg {}^{\sqcap\!\!\sqcap}(x \mathbin{\square} y) \mathbin{\square} ({}^{\sqcap\!\!\sqcap}(x_r) \mathbin{\square} {}^{\sqcap\!\!\sqcap}(x_s) \mathbin{\square} (x_r \mathbin{\square} z \sqcup x_s \mathbin{\square} y) \sqcap \neg {}^{\sqcap\!\!\sqcap}(x_r) \mathbin{\square} x_s \mathbin{\square} y \sqcap \neg {}^{\sqcap\!\!\sqcap}(x_s) \mathbin{\square} x_r \mathbin{\square} z) \\
B & := & \neg {}^{\sqcap\!\!\sqcap}(x \mathbin{\square} y) \mathbin{\square} \neg {}^{\sqcap\!\!\sqcap}(x \mathbin{\square} z) \mathbin{\square} \\
& & \Big(({}^{\sqcap\!\!\sqcap}(x_r) \mathbin{\square} {}^{\sqcap\!\!\sqcap}(x_s) \mathbin{\square} (x_r \mathbin{\square} y \sqcup x_s \mathbin{\square} y) \sqcap \neg {}^{\sqcap\!\!\sqcap}(x_r) \mathbin{\square} x_s \mathbin{\square} y \sqcap \neg {}^{\sqcap\!\!\sqcap}(x_s) \mathbin{\square} x_r \mathbin{\square} y) \sqcup \\
& & ({}^{\sqcap\!\!\sqcap}(x_r) \mathbin{\square} {}^{\sqcap\!\!\sqcap}(x_t) \mathbin{\square} (x_r \mathbin{\square} z \sqcup x_t \mathbin{\square} z) \sqcap \neg {}^{\sqcap\!\!\sqcap}(x_r) \mathbin{\square} x_t \mathbin{\square} z \sqcap \neg {}^{\sqcap\!\!\sqcap}(x_t) \mathbin{\square} x_r \mathbin{\square} z) \Big)
\end{array}
$$

Before getting to the main proof, we need some intermediate results. The first one is $A = x_{{}^{\sqcap\!\!\sqcap}y} \mathbin{\square} (\neg {}^{\sqcap\!\!\sqcap}z \mathbin{\square} y \sqcap {}^{\sqcap\!\!\sqcap}y \mathbin{\square} z)$.

$$
\begin{array}{ll}
& x_{{}^{\sqcap\!\!\sqcap}y} \mathbin{\square} (\neg {}^{\sqcap\!\!\sqcap}z \mathbin{\square} y \sqcap {}^{\sqcap\!\!\sqcap}y \mathbin{\square} z) \\
= & \qquad \langle \text{ by Boolean algebra } \rangle \\
& x_{r \sqcap s} \mathbin{\square} (\neg {}^{\sqcap\!\!\sqcap}z \mathbin{\square} y \sqcap {}^{\sqcap\!\!\sqcap}y \mathbin{\square} z) \\
= & \qquad \langle \text{ by Proposition 4.25-1 } \rangle \\
& \neg {}^{\sqcap\!\!\sqcap}(x \mathbin{\square} (r \sqcap s)) \mathbin{\square} ((x_r \sqcup x_s) \sqcap \neg {}^{\sqcap\!\!\sqcap}(x_r) \mathbin{\square} x_s \sqcap \neg {}^{\sqcap\!\!\sqcap}(x_s) \mathbin{\square} x_r) \mathbin{\square} (\neg {}^{\sqcap\!\!\sqcap}z \mathbin{\square} y \sqcap {}^{\sqcap\!\!\sqcap}y \mathbin{\square} z) \\
= & \qquad \langle \text{ by Boolean algebra, (3.20) and Proposition 3.14-11 } \rangle \\
& \neg {}^{\sqcap\!\!\sqcap}(x \mathbin{\square} y) \mathbin{\square} ({}^{\sqcap\!\!\sqcap}(x_r) \mathbin{\square} {}^{\sqcap\!\!\sqcap}(x_s) \mathbin{\square} (x_r \sqcup x_s) \sqcap \neg {}^{\sqcap\!\!\sqcap}(x_r) \mathbin{\square} x_s \sqcap \neg {}^{\sqcap\!\!\sqcap}(x_s) \mathbin{\square} x_r) \mathbin{\square} \\
& (\neg {}^{\sqcap\!\!\sqcap}z \mathbin{\square} y \sqcap {}^{\sqcap\!\!\sqcap}y \mathbin{\square} z) \\
= & \qquad \langle \text{ by Proposition 3.14-9 and Boolean algebra,} \\
& \quad \text{the domains of } {}^{\sqcap\!\!\sqcap}(x_r) \mathbin{\square} {}^{\sqcap\!\!\sqcap}(x_s) \mathbin{\square} (x_r \sqcup x_s),\ \neg {}^{\sqcap\!\!\sqcap}(x_r) \mathbin{\square} x_s \\
& \quad \text{and } \neg {}^{\sqcap\!\!\sqcap}(x_s) \mathbin{\square} x_r \text{ are pairwise disjoint,} \\
& \quad \text{then apply Corollary 3.21-17, (3.9), (4.5) with } x, t := x, r \\
& \quad \text{and (4.5) with } x, t := x, s \ \rangle \\
& \neg {}^{\sqcap\!\!\sqcap}(x \mathbin{\square} y) \mathbin{\square} ({}^{\sqcap\!\!\sqcap}(x_r) \mathbin{\square} {}^{\sqcap\!\!\sqcap}(x_s) \mathbin{\square} (x_r \mathbin{\square} r \mathbin{\square} (\neg {}^{\sqcap\!\!\sqcap}z \mathbin{\square} y \sqcap {}^{\sqcap\!\!\sqcap}y \mathbin{\square} z) \sqcup \\
& \qquad\qquad x_s \mathbin{\square} s \mathbin{\square} (\neg {}^{\sqcap\!\!\sqcap}z \mathbin{\square} y \sqcap {}^{\sqcap\!\!\sqcap}y \mathbin{\square} z)) \sqcap \\
& \qquad \neg {}^{\sqcap\!\!\sqcap}(x_r) \mathbin{\square} x_s \mathbin{\square} s \mathbin{\square} (\neg {}^{\sqcap\!\!\sqcap}z \mathbin{\square} y \sqcap {}^{\sqcap\!\!\sqcap}y \mathbin{\square} z) \sqcap \\
& \qquad \neg {}^{\sqcap\!\!\sqcap}(x_s) \mathbin{\square} x_r \mathbin{\square} r \mathbin{\square} (\neg {}^{\sqcap\!\!\sqcap}z \mathbin{\square} y \sqcap {}^{\sqcap\!\!\sqcap}y \mathbin{\square} z)) \\
= & \qquad \langle \text{ by Corollaries 3.21-4 and 3.21-3, Boolean algebra, (3.6),} \\
& \quad \text{Proposition 3.14-17, (4.5) with } x, t := x, r \text{ and (4.5) with} \\
& \quad x, t := x, s \ \rangle
\end{array}
$$

A

The second one is $B = x_{\Pi y} \rhd y \sqcup x_{\Pi z} \rhd z$.

$x_{\Pi y} \rhd y \sqcup x_{\Pi z} \rhd z$

$=$ ⟨ by Boolean algebra ⟩

$x_{r \sqcap s} \rhd y \sqcup x_{r \sqcap t} \rhd z$

$=$ ⟨ by Proposition 4.25-1 ⟩

$\neg\Pi(x \rhd (r \sqcap s)) \rhd ((x_r \sqcup x_s) \sqcap \neg\Pi(x_r) \rhd x_s \sqcap \neg\Pi(x_s) \rhd x_r) \rhd y \sqcup$
$\neg\Pi(x \rhd (r \sqcap t)) \rhd ((x_r \sqcup x_t) \sqcap \neg\Pi(x_r) \rhd x_t \sqcap \neg\Pi(x_t) \rhd x_r) \rhd z$

$=$ ⟨ by Proposition 3.14-9 and Boolean algebra, the domains of $(x_r \sqcup x_s)$, $\neg\Pi(x_r) \rhd x_s$ and $\neg\Pi(x_s) \rhd x_r$ are pairwise disjoint and the domains of $(x_r \sqcup x_t)$, $\neg\Pi(x_r) \rhd x_t$ and $\neg\Pi(x_t) \rhd x_r$ are pairwise disjoint, then apply Corollary 3.21-17, Propositions 3.14-11 and 3.14-20, (3.9) and Boolean algebra ⟩

B

Next, we show

$$x_{\Pi y} \rhd (\neg\Pi z \rhd y \sqcap \Pi y \rhd z) \sqsubseteq x_{\Pi y} \rhd y \sqcup x_{\Pi z} \rhd z. \tag{4.43}$$

By the previous two derivations, this is equivalent to $A \sqsubseteq B$. This will be shown by using case analysis (Corollary 3.21-19) with the four disjoint tests $\Pi(x_r) \rhd \Pi(x_s)$, $\Pi(x_r) \rhd \neg\Pi(x_s)$, $\neg\Pi(x_r) \rhd \Pi(x_s)$ and $\neg\Pi(x_r) \rhd \neg\Pi(x_s)$, which satisfy

$$\Pi(x_r) \rhd \Pi(x_s) \sqcap \Pi(x_r) \rhd \neg\Pi(x_s) \sqcap \neg\Pi(x_r) \rhd \Pi(x_s) \sqcap \neg\Pi(x_r) \rhd \neg\Pi(x_s) = 1$$

by Boolean algebra.

i. Test $\Pi(x_r) \rhd \Pi(x_s)$.

$\Pi(x_r) \rhd \Pi(x_s) \rhd B$

$=$ ⟨ by Boolean algebra, (3.8), Corollaries 3.21-4 and 3.21-3, and (3.6) ⟩

$\Pi(x_r) \rhd \Pi(x_s) \rhd \neg\Pi(x \rhd y) \rhd \neg\Pi(x \rhd z) \rhd$
$(x_r \rhd y \sqcup x_s \rhd y \sqcup (\Pi(x_r) \rhd \Pi(x_t) \rhd (x_r \rhd z \sqcup x_t \rhd z) \sqcap \neg\Pi(x_t) \rhd x_r \rhd z))$

$\sqsupseteq$ ⟨ by Propositions 3.14-9 and 3.14-3, (3.21), (3.20), (4.5), the definition of t and Boolean algebra,
$\Pi(\Pi(x_r)\circ\Pi(x_t)\circ(x_r\circ z \sqcup x_t\circ z))$
$= \Pi(x_r)\circ\Pi(x_t)\circ\Pi(x_r\circ z \sqcup x_t\circ z)$
$= \Pi(x_r)\circ\Pi(x_t)\circ\Pi(x_r\circ z)\circ\Pi(x_t\circ z)$
$= \Pi(x_r)\circ\Pi(x_t)\circ\Pi(x_r\circ z)\circ\Pi(x_t\circ \Pi z)$
$= \Pi(x_r)\circ\Pi(x_t)\circ\Pi(x_r\circ z)$
$= \Pi(\Pi(x_r)\circ\Pi(x_t)\circ x_r\circ z)$,
then apply (3.15) and Lemmas 3.22-3 and 3.7-1 ⟩

$\Pi(x_r)\circ\Pi(x_s)\circ\neg\Pi(x\circ y)\circ$
$(x_s\circ y \sqcup (\Pi(x_r)\circ\Pi(x_t)\circ x_r\circ z \sqcap \neg\Pi(x_t)\circ x_r\circ z))$

$=$ ⟨ by Boolean algebra, Proposition 3.14-7, Corollary 3.21-6 and (3.2) ⟩

$\Pi(x_r)\circ\Pi(x_s)\circ\neg\Pi(x\circ y)\circ(x_r\circ z \sqcup x_s\circ y)$

$=$ ⟨ by Boolean algebra, Corollaries 3.21-4 and 3.21-3, and (3.6) ⟩

$\Pi(x_r)\circ\Pi(x_s)\circ A$

ii. Test $\Pi(x_r)\circ\neg\Pi(x_s)$.

$\Pi(x_r)\circ\neg\Pi(x_s)\circ B$

$=$ ⟨ by Boolean algebra, (3.8), Corollaries 3.21-4 and 3.21-3, and (3.6) ⟩

$\Pi(x_r)\circ\neg\Pi(x_s)\circ\neg\Pi(x\circ y)\circ\neg\Pi(x\circ z)\circ$
$(\neg\Pi(x_s)\circ x_r\circ y \sqcup (\Pi(x_r)\circ\Pi(x_t)\circ(x_r\circ z \sqcup x_t\circ z) \sqcap \neg\Pi(x_t)\circ x_r\circ z))$

$\sqsupseteq$ ⟨ by Propositions 3.14-9 and 3.14-3, (3.21), (3.20), (4.5), the definition of t and Boolean algebra,
$\Pi(\Pi(x_r)\circ\Pi(x_t)\circ(x_r\circ z \sqcup x_t\circ z))$
$= \Pi(x_r)\circ\Pi(x_t)\circ\Pi(x_r\circ z \sqcup x_t\circ z)$
$= \Pi(x_r)\circ\Pi(x_t)\circ\Pi(x_r\circ z)\circ\Pi(x_t\circ z)$
$= \Pi(x_r)\circ\Pi(x_t)\circ\Pi(x_r\circ z)\circ\Pi(x_t\circ \Pi z)$
$= \Pi(x_r)\circ\Pi(x_t)\circ\Pi(x_r\circ z)$
$= \Pi(\Pi(x_r)\circ\Pi(x_t)\circ x_r\circ z)$,
then apply (3.15) and Lemmas 3.22-3 and 3.7-1 ⟩

$\Pi(x_r)\circ\neg\Pi(x_s)\circ\neg\Pi(x\circ y)\circ(\Pi(x_r)\circ\Pi(x_t)\circ x_r\circ z \sqcap \neg\Pi(x_t)\circ x_r\circ z)$

$=$ ⟨ by Boolean algebra, Proposition 3.14-7 and Corollary 3.21-6 ⟩

$\Pi(x_r)\circ\neg\Pi(x_s)\circ\neg\Pi(x\circ y)\circ x_r\circ z$

$=$ ⟨ by Boolean algebra, Corollaries 3.21-4 and 3.21-3, and (3.6) ⟩

$$\Pi(x_r)\,\square\,\neg\Pi(x_s)\,\square\,A$$

iii. Test $\neg\Pi(x_r)\,\square\,\Pi(x_s)$.

$$\begin{array}{ll} & \neg\Pi(x_r)\,\square\,\Pi(x_s)\,\square\,B \\ = & \quad \langle \text{ by Boolean algebra, (3.8), Corollaries 3.21-4 and 3.21-3, Proposition 3.14-17 and (3.6) } \rangle \\ & \neg\Pi(x_r)\,\square\,\Pi(x_s)\,\square\,\neg\Pi(x \square y)\,\square\,\neg\Pi(x \square z)\,\square\,(\neg\Pi(x_r)\,\square\, x_s \square y \sqcup \neg\Pi(x_r)\,\square\, x_t \square z) \\ \sqsupseteq & \quad \langle \text{ by Lemma 3.7-1, (3.15) and Boolean algebra } \rangle \\ & \neg\Pi(x_r)\,\square\,\Pi(x_s)\,\square\,\neg\Pi(x \square y)\,\square\, x_s \square y \\ = & \quad \langle \text{ by Boolean algebra, Corollaries 3.21-4 and 3.21-3, and (3.6) } \rangle \\ & \neg\Pi(x_r)\,\square\,\Pi(x_s)\,\square\,A \end{array}$$

iv. Test $\neg\Pi(x_r)\,\square\,\neg\Pi(x_s)$.

$$\begin{array}{ll} & \neg\Pi(x_r)\,\square\,\neg\Pi(x_s)\,\square\,B \\ = & \quad \langle \text{ by Boolean algebra, (3.8), Corollaries 3.21-4 and 3.21-3, Proposition 3.14-17, (3.6) and (3.4) } \rangle \\ & \top \\ \sqsupseteq & \quad \langle \text{ by (3.14) } \rangle \\ & \neg\Pi(x_r)\,\square\,\neg\Pi(x_s)\,\square\,A \end{array}$$

And, finally, the main proof.

$$\begin{array}{ll} & \Pi(x_{\Pi y} \square y \sqcup x_{\Pi z} \square z)\,\square\,(x \cdot_D (y +_D z)) \\ = & \quad \langle \text{ by (3.21), (3.20), Proposition 3.14-3 and Definition 4.16 } \rangle \\ & \Pi(x_{\Pi y}\,\square\,\Pi y)\,\square\,\Pi(x_{\Pi z}\,\square\,\Pi z)\,\square\,(x \square (y +_D z) \sqcap x_{\Gamma(y +_D z)}\,\square\,(y +_D z)) \\ = & \quad \langle \text{ by (4.5) with } x, t := x, \Pi y, \text{ (4.5) with } x, t := x, \Pi z \text{ and Corollary 4.4-3 } \rangle \\ & \Pi(x_{\Pi y})\,\square\,\Pi(x_{\Pi z})\,\square\,(x \square (y +_D z) \sqcap x_{\Pi y \sqcap \Pi z}\,\square\,(y +_D z)) \\ = & \quad \langle \text{ by Corollary 3.21-4, Propositions 3.14-7 and 4.25-1, and (3.20) } \rangle \\ & \Pi(x_{\Pi y})\,\square\,\Pi(x_{\Pi z})\,\square\,\Pi(x \square \Pi(y +_D z))\,\square\, x \square (y +_D z) \sqcap \\ & \Pi(x_{\Pi y})\,\square\,\Pi(x_{\Pi z})\,\square\,\neg\Pi(x \square (\Pi y \sqcap \Pi z))\,\square\, \\ & ((x_{\Pi y} \sqcup x_{\Pi z}) \sqcap \neg\Pi(x_{\Pi y})\,\square\, x_{\Pi z} \sqcap \neg\Pi(x_{\Pi z})\,\square\, x_{\Pi y})\,\square\,(y +_D z) \\ = & \quad \langle \text{ by Corollaries 4.4-3 and 3.21-4, Proposition 3.14-11 and Boolean algebra } \rangle \\ & \Pi(x_{\Pi y})\,\square\,\Pi(x_{\Pi z})\,\square\,\Pi(x \square (\Pi y \sqcap \Pi z))\,\square\, x \square (y +_D z) \sqcap \end{array}$$

$$
\begin{array}{ll}
& \neg^{\sqcap}(x \triangleright (\sqcap y \sqcap \sqcap z)) \triangleright ((x_{\sqcap y} \sqcup x_{\sqcap z}) \sqcap \top \triangleright x_{\sqcap z} \sqcap \top \triangleright x_{\sqcap y}) \triangleright (y +_D z) \\
= & \quad \langle \text{ by Corollaries 4.26-2 and 3.21-3, and (3.6) } \rangle \\
& {}^{\sqcap}(x \triangleright (\sqcap y \sqcap \sqcap z)) \triangleright (x_{\sqcap y} \sqcup x_{\sqcap z}) \triangleright (y +_D z) \sqcap \\
& \neg^{\sqcap}(x \triangleright (\sqcap y \sqcap \sqcap z)) \triangleright (x_{\sqcap y} \sqcup x_{\sqcap z}) \triangleright (y +_D z) \\
= & \quad \langle \text{ by Corollary 3.21-6 } \rangle \\
& (x_{\sqcap y} \sqcup x_{\sqcap z}) \triangleright (y +_D z) \\
= & \quad \langle \text{ by (4.5) with } x, t := x, \sqcap y, \text{ by (4.5) with } x, t := x, \sqcap z \text{ and Corollary 4.4-1 } \rangle \\
& (x_{\sqcap y} \triangleright \sqcap y \sqcup x_{\sqcap z} \triangleright \sqcap z) \triangleright (\neg^{\sqcap} z \triangleright y \sqcap \neg^{\sqcap} y \triangleright z \sqcap (y \sqcup z)) \\
= & \quad \langle \text{ by (3.8), (3.6), Propositions 3.14-7 and 3.14-11, Corollaries 3.21-4 and 3.21-3, and Boolean algebra } \rangle \\
& x_{\sqcap y} \triangleright (\neg^{\sqcap} z \triangleright y \sqcap (y \sqcup z)) \sqcup x_{\sqcap z} \triangleright (\neg^{\sqcap} y \triangleright z \sqcap (y \sqcup z)) \\
= & \quad \langle \text{ by Propositions 3.14-7 and 3.14-20, and Corollary 3.21-15 } \rangle \\
& x_{\sqcap y} \triangleright ((\neg^{\sqcap} z \triangleright y \sqcap \sqcap z \triangleright y) \sqcup (\neg^{\sqcap} z \triangleright y \sqcap \sqcap y \triangleright z)) \sqcup \\
& x_{\sqcap z} \triangleright ((\neg^{\sqcap} y \triangleright z \sqcap \sqcap y \triangleright z) \sqcup (\neg^{\sqcap} y \triangleright z \sqcap \sqcap z \triangleright y)) \\
= & \quad \langle \text{ by Corollary 3.21-6 and (3.8) } \rangle \\
& x_{\sqcap y} \triangleright y \sqcup x_{\sqcap y} \triangleright (\neg^{\sqcap} z \triangleright y \sqcap \sqcap y \triangleright z) \sqcup x_{\sqcap z} \triangleright z \sqcup x_{\sqcap z} \triangleright (\neg^{\sqcap} y \triangleright z \sqcap \sqcap z \triangleright y) \\
= & \quad \langle \text{ by (4.43) once as is, once with } y, z := z, y, \text{ and (3.11) } \rangle \\
& x_{\sqcap y} \triangleright y \sqcup x_{\sqcap z} \triangleright z
\end{array}
$$

9.

$$
\begin{array}{ll}
& (x +_D y) \;;_D z \\
= & \quad \langle \text{ by Corollary 4.4-1 and Definition 4.16 } \rangle \\
& ((x \sqcup y) \sqcap \neg^{\sqcap} x \triangleright y \sqcap \neg^{\sqcap} y \triangleright x) \triangleright z \sqcap ((x \sqcup y) \sqcap \neg^{\sqcap} x \triangleright y \sqcap \neg^{\sqcap} y \triangleright x)_{\sqcap z} \triangleright z \\
= & \quad \langle \text{ by Corollaries 3.21-13, 4.30-1 and 3.21-4 } \rangle \\
& ((x \sqcup y) \sqcap \neg^{\sqcap} x \triangleright y \sqcap \neg^{\sqcap} y \triangleright x) \triangleright z \sqcap \\
& ((x \sqcup y)_{\sqcap z} \sqcap \neg^{\sqcap} (x \sqcup y) \triangleright (\neg^{\sqcap} x \triangleright y)_{\sqcap z} \sqcap \neg^{\sqcap} (x \sqcup y) \triangleright \neg^{\sqcap} (\neg^{\sqcap} x \triangleright y) \triangleright (\neg^{\sqcap} y \triangleright x)_{\sqcap z}) \triangleright z \\
= & \quad \langle \text{ by (3.21), Propositions 3.14-3 and 3.14-9, De Morgan and Boolean algebra } \rangle \\
& ((x \sqcup y) \sqcap \neg^{\sqcap} x \triangleright y \sqcap \neg^{\sqcap} y \triangleright x) \triangleright z \sqcap \\
& ((x \sqcup y)_{\sqcap z} \sqcap (\neg^{\sqcap} x \sqcap \neg^{\sqcap} y) \triangleright (\neg^{\sqcap} x \triangleright y)_{\sqcap z} \sqcap \neg^{\sqcap} y \triangleright (\neg^{\sqcap} y \triangleright x)_{\sqcap z}) \triangleright z \\
= & \quad \langle \text{ by Proposition 4.22-5 and Boolean algebra } \rangle \\
& ((x \sqcup y) \sqcap \neg^{\sqcap} x \triangleright y \sqcap \neg^{\sqcap} y \triangleright x) \triangleright z \sqcap ((x \sqcup y)_{\sqcap z} \sqcap \neg^{\sqcap} x \triangleright y_{\sqcap z} \sqcap \neg^{\sqcap} y \triangleright x_{\sqcap z}) \triangleright z
\end{array}
$$

$=$ ⟨ by (3.21), Propositions 3.14-3 and 3.14-9,
and Boolean algebra,
the domains of $x \sqcup y$, $\neg^{\sqcap} x \triangleright y$ and $\neg^{\sqcap} y \triangleright x$ are pairwise disjoint;
by (3.21), Propositions 3.14-3 and 3.14-9,
(4.4) with $x, t := x \sqcup y, {}^{\sqcap}z$ and Boolean algebra,
the domains of $(x \sqcup y)_{\sqcap z}$, $\neg^{\sqcap} x \triangleright y_{\sqcap z}$ and $\neg^{\sqcap} y \triangleright x_{\sqcap z}$
are pairwise disjoint;
then apply Corollary 3.21-17 ⟩

$(x \sqcup y) \triangleright z \sqcap \neg^{\sqcap} x \triangleright y \triangleright z \sqcap \neg^{\sqcap} y \triangleright x \triangleright z \sqcap (x \sqcup y)_{\sqcap z} \triangleright z \sqcap \neg^{\sqcap} x \triangleright y_{\sqcap z} \triangleright z \sqcap \neg^{\sqcap} y \triangleright x_{\sqcap z} \triangleright z$

$=$ ⟨ by Theorem 4.23 and (3.9) ⟩

$(x \triangleright z \sqcup y \triangleright z) \sqcap \neg^{\sqcap} x \triangleright y \triangleright z \sqcap \neg^{\sqcap} y \triangleright x \triangleright z \sqcap$
$({}^{\sqcap}(y \triangleright \neg^{\sqcap} z) \triangleright x \triangleright {}^{\sqcap}z \sqcap {}^{\sqcap}(y \triangleright \neg^{\sqcap} z) \triangleright x_{\sqcap z} \sqcap (x \triangleright {}^{\sqcap}z \sqcup y_{\sqcap z}) \sqcap$
${}^{\sqcap}(x \triangleright \neg^{\sqcap} z) \triangleright y \triangleright {}^{\sqcap}z \sqcap {}^{\sqcap}(x \triangleright \neg^{\sqcap} z) \triangleright y_{\sqcap z} \sqcap (x_{\sqcap z} \sqcup y \triangleright {}^{\sqcap}z) \sqcap (x_{\sqcap z} \sqcup y_{\sqcap z})) \triangleright z \sqcap$
$\neg^{\sqcap} x \triangleright y_{\sqcap z} \triangleright z \sqcap \neg^{\sqcap} y \triangleright x_{\sqcap z} \triangleright z$

$=$ ⟨ by (3.21), Propositions 3.14-3 and 3.14-9,
Remark 4.8, Lemma 3.17-4 and Boolean algebra,
the domains of ${}^{\sqcap}(y \triangleright \neg t) \triangleright x \triangleright t$, ${}^{\sqcap}(y \triangleright \neg t) \triangleright x_t$, $(x \triangleright t \sqcup y_t)$,
${}^{\sqcap}(x \triangleright \neg t) \triangleright y \triangleright t$, ${}^{\sqcap}(x \triangleright \neg t) \triangleright y_t$, $(x_t \sqcup y \triangleright t)$ and $(x_t \sqcup y_t)$
are pairwise disjoint,
then apply Corollary 3.21-17, (3.9) and Proposition 3.14-7 ⟩

$(x \triangleright z \sqcup y \triangleright z) \sqcap \neg^{\sqcap} x \triangleright y \triangleright z \sqcap \neg^{\sqcap} y \triangleright x \triangleright z \sqcap$
${}^{\sqcap}(y \triangleright \neg^{\sqcap} z) \triangleright x \triangleright z \sqcap {}^{\sqcap}(y \triangleright \neg^{\sqcap} z) \triangleright x_{\sqcap z} \triangleright z \sqcap (x \triangleright z \sqcup y_{\sqcap z} \triangleright z) \sqcap$
${}^{\sqcap}(x \triangleright \neg^{\sqcap} z) \triangleright y \triangleright z \sqcap {}^{\sqcap}(x \triangleright \neg^{\sqcap} z) \triangleright y_{\sqcap z} \triangleright z \sqcap (x_{\sqcap z} \triangleright z \sqcup y \triangleright z) \sqcap (x_{\sqcap z} \triangleright z \sqcup y_{\sqcap z} \triangleright z) \sqcap$
$\neg^{\sqcap} x \triangleright y_{\sqcap z} \triangleright z \sqcap \neg^{\sqcap} y \triangleright x_{\sqcap z} \triangleright z$

$=$ ⟨ by (3.21), (3.20), Propositions 3.14-3 and 3.14-9,
Lemmas 3.17-2 and 3.17-4, Remark 4.8, (4.5) with $x, t := x, {}^{\sqcap}z$,
(4.5) with $x, t := y, {}^{\sqcap}z$ and Boolean algebra,
the domains of the twelve operands of the eleven $\sqcap$ are
pairwise disjoint,
then apply (3.25) ⟩

$(x \triangleright z \sqcup y \triangleright z) \sqcap (x \triangleright z \sqcup y_{\sqcap z} \triangleright z) \sqcap (x_{\sqcap z} \triangleright z \sqcup y \triangleright z) \sqcap (x_{\sqcap z} \triangleright z \sqcup y_{\sqcap z} \triangleright z) \sqcap$
$\neg^{\sqcap} x \triangleright y \triangleright z \sqcap \neg^{\sqcap} x \triangleright y_{\sqcap z} \triangleright z \sqcap {}^{\sqcap}(x \triangleright \neg^{\sqcap} z) \triangleright y \triangleright z \sqcap {}^{\sqcap}(x \triangleright \neg^{\sqcap} z) \triangleright y_{\sqcap z} \triangleright z \sqcap$
$\neg^{\sqcap} y \triangleright x \triangleright z \sqcap \neg^{\sqcap} y \triangleright x_{\sqcap z} \triangleright z \sqcap {}^{\sqcap}(y \triangleright \neg^{\sqcap} z) \triangleright x \triangleright z \sqcap {}^{\sqcap}(y \triangleright \neg^{\sqcap} z) \triangleright x_{\sqcap z} \triangleright z$

$=$ ⟨ by Corollaries 3.21-14, 3.21-4 and 3.21-5, and (3.2) ⟩

$((x \triangleright z \sqcap x_{\sqcap z} \triangleright z) \sqcup (y \triangleright z \sqcap y_{\sqcap z} \triangleright z)) \sqcap (\neg^{\sqcap} x \sqcap {}^{\sqcap}(x \triangleright \neg^{\sqcap} z)) \triangleright (y \triangleright z \sqcap y_{\sqcap z} \triangleright z) \sqcap$
$(\neg^{\sqcap} y \sqcap {}^{\sqcap}(y \triangleright \neg^{\sqcap} z)) \triangleright (x \triangleright z \sqcap x_{\sqcap z} \triangleright z)$

$$
\begin{array}{ll}
= & \langle \text{ by Definition 4.16 } \rangle \\
& ((x \mathbin{\cdot_{\mathcal{D}}} z) \sqcup (y \mathbin{\cdot_{\mathcal{D}}} z)) \sqcap (\neg^{\sqcap} x \sqcap {}^{\sqcap}(x \triangleright \neg^{\sqcap} z)) \triangleleft (y \mathbin{\cdot_{\mathcal{D}}} z) \sqcap \\
& (\neg^{\sqcap} y \sqcap {}^{\sqcap}(y \triangleright \neg^{\sqcap} z)) \triangleleft (x \mathbin{\cdot_{\mathcal{D}}} z) \\
= & \langle \text{ by Proposition 4.17-5 and De Morgan } \rangle \\
& ((x \mathbin{\cdot_{\mathcal{D}}} z) \sqcup (y \mathbin{\cdot_{\mathcal{D}}} z)) \sqcap \neg^{\sqcap}(x \mathbin{\cdot_{\mathcal{D}}} z) \triangleleft (y \mathbin{\cdot_{\mathcal{D}}} z) \sqcap \neg^{\sqcap}(y \mathbin{\cdot_{\mathcal{D}}} z) \triangleleft (x \mathbin{\cdot_{\mathcal{D}}} z) \\
= & \langle \text{ by Corollary 4.4-1 } \rangle \\
& x \mathbin{\cdot_{\mathcal{D}}} z +_{\mathcal{D}} y \mathbin{\cdot_{\mathcal{D}}} z
\end{array}
$$

10. We work on $x^{*_{\mathcal{D}}} = 1 +_{\mathcal{D}} x \mathbin{\cdot_{\mathcal{D}}} x^{*_{\mathcal{D}}}$ since this is equivalent (see remark 2.2).

$$
\begin{array}{ll}
& x^{*_{\mathcal{D}}} = 1 +_{\mathcal{D}} x \mathbin{\cdot_{\mathcal{D}}} x^{*_{\mathcal{D}}} \\
\Longleftrightarrow & \langle \text{ by Definition 4.19, Lemma 4.20-1 and Proposition 4.17-4 } \rangle \\
& (x \sqcap 1)^{\times} = 1 +_{\mathcal{D}} x \triangleleft (x \sqcap 1)^{\times} \\
\Longleftrightarrow & \langle \text{ by Corollary 4.4-1 } \rangle \\
& (x \sqcap 1)^{\times} = (1 \sqcup x \triangleleft (x \sqcap 1)^{\times}) \sqcap \neg^{\sqcap} 1 \triangleleft x \triangleleft (x \sqcap 1)^{\times} \sqcap \neg^{\sqcap}(x \triangleleft (x \sqcap 1)^{\times}) \triangleleft 1 \\
\Longleftrightarrow & \langle \text{ by Proposition 3.14-1 and Boolean algebra } \rangle \\
& (x \sqcap 1)^{\times} = (1 \sqcup x \triangleleft (x \sqcap 1)^{\times}) \sqcap \top \triangleleft x \triangleleft (x \sqcap 1)^{\times} \sqcap \neg^{\sqcap}(x \triangleleft (x \sqcap 1)^{\times}) \\
\Longleftrightarrow & \langle \text{ by (3.6), Corollary 3.21-3 and (3.20) } \rangle \\
& (x \sqcap 1)^{\times} = (1 \sqcup x \triangleleft (x \sqcap 1)^{\times}) \sqcap \neg^{\sqcap}(x \triangleleft {}^{\sqcap}((x \sqcap 1)^{\times})) \\
\Longleftrightarrow & \langle \text{ by Lemma 4.20-1 and (3.7) } \rangle \\
& (x \sqcap 1)^{\times} = (1 \sqcup x \triangleleft (x \sqcap 1)^{\times}) \sqcap \neg^{\sqcap} x
\end{array}
$$

Therefore, it is sufficient to show

$$ {}^{\sqcap}x \triangleleft (x \sqcap 1)^{\times} = {}^{\sqcap}x \triangleleft ((1 \sqcup x \triangleleft (x \sqcap 1)^{\times}) \sqcap \neg^{\sqcap} x) $$

and

$$ \neg^{\sqcap} x \triangleleft (x \sqcap 1)^{\times} = \neg^{\sqcap} x \triangleleft ((1 \sqcup x \triangleleft (x \sqcap 1)^{\times}) \sqcap \neg^{\sqcap} x) $$

by Proposition 3.20-17.

Case ${}^{\sqcap}x$

$$
\begin{array}{ll}
& {}^{\sqcap}x \triangleleft (x \sqcap 1)^{\times} \\
= & \langle \text{ by (3.2) and (3.16) } \rangle \\
& {}^{\sqcap}x \triangleleft (1 \sqcup (x \sqcap 1) \triangleleft (x \sqcap 1)^{\times}) \\
= & \langle \text{ by Proposition 3.14-20 } \rangle
\end{array}
$$

$$
\begin{array}{ll}
& \Pi x \circ (1 \sqcup \Pi x \circ (x \sqcap 1) \circ (x \sqcap 1)^{\times}) \\
= & \qquad \langle \text{ by Corollary 3.21-7 and Proposition 3.14-7 } \rangle \\
& \Pi x \circ (1 \sqcup x \circ (x \sqcap 1)^{\times}) \\
= & \qquad \langle \text{ by Corollaries 3.21-4 and 3.21-3, and Boolean algebra } \rangle \\
& \Pi x \circ ((1 \sqcup x \circ (x \sqcap 1)^{\times}) \sqcap \neg \Pi x)
\end{array}
$$

Case $\neg \Pi x$

$$
\begin{array}{ll}
& \neg \Pi x \circ (x \sqcap 1)^{\times} = \neg \Pi x \circ ((1 \sqcup x \circ (x \sqcap 1)^{\times}) \sqcap \neg \Pi x) \\
\Longleftrightarrow & \qquad \langle \text{ by Lemma 4.20-2, Corollary 3.21-8 and Boolean algebra } \rangle \\
& \neg \Pi x \circ (x \sqcap 1)^{\times} = \neg \Pi x
\end{array}
$$

Since $1 \sqsubseteq (x \sqcap 1)^{\times}$ by (3.16) and (3.15), it follows that $\neg \Pi x \sqsubseteq \neg \Pi x \circ (x \sqcap 1)^{\times}$. Here is the proof of $\neg \Pi x \circ (x \sqcap 1)^{\times} \sqsubseteq \neg \Pi x$.

$$
\begin{array}{ll}
& \neg \Pi x \circ (x \sqcap 1)^{\times} \sqsubseteq \neg \Pi x \\
\Longleftarrow & \qquad \langle \text{ by (3.13) } \rangle \\
& \neg \Pi x \circ (x \sqcap 1) \sqcup \neg \Pi x \sqsubseteq \neg \Pi x \\
\Longleftrightarrow & \qquad \langle \text{ by Corollary 3.21-8 and Boolean algebra } \rangle \\
& \mathsf{true}
\end{array}
$$

11. This is direct from Corollary 4.4-2.

12. The proof of Theorem 4.31-12 is thirty pages long. Go to page 181 for the proof of Theorem 4.31-13.

    If we demonstrate

$$x \cdot_D z \leq_D z \implies x^{*_D} \cdot_D z \leq_D z \tag{4.44}$$

    then we are done as shown in the following derivation.

$$
\begin{array}{ll}
& x \cdot_D z +_D y \leq_D z \\
\Longleftrightarrow & \qquad \langle \text{ by Corollary 4.4-2 } \rangle \\
& x \cdot_D z \leq_D z \ \wedge \ y \leq_D z \\
\Longrightarrow & \qquad \langle \text{ by (4.44) } \rangle \\
& x^{*_D} \cdot_D z \leq_D z \ \wedge \ y \leq_D z
\end{array}
$$

$\Longrightarrow$ ⟨ by Theorems 4.31-11 and 4.31-8,
$y \leq_D z \Longrightarrow y +_D z = z \Longrightarrow x^{*D} \cdot_D y +_D x^{*D} \cdot_D z = x^{*D} \cdot_D z$
$\Longrightarrow x^{*D} \cdot_D y \leq_D x^{*D} \cdot_D z$,
then apply Corollary 4.4-2 ⟩
$x^{*D} \cdot_D y \leq_D z$

So here is the beginning of the proof of (4.44).

First, we show

$$x \cdot_D z \leq_D z \iff \lceil z \sqsubseteq \lceil x \circ \neg\lceil(x \circ \neg\lceil z) \wedge x \circ z \sqsubseteq \lceil(x \circ z) \circ z \wedge x_{\lceil z} \circ z \sqsubseteq \lceil(x_{\lceil z}) \circ z \ . \quad (4.45)$$

$x \cdot_D z \leq_D z$
$\iff$ ⟨ by Definition 4.1 ⟩
$\lceil z \sqsubseteq \lceil(x \cdot_D z) \ \wedge \ x \cdot_D z \sqsubseteq \lceil(x \cdot_D z) \circ z$
$\iff$ ⟨ by Proposition 4.17-5, Definition 4.16 and Corollary 3.21-16 ⟩
$\lceil z \sqsubseteq \lceil x \circ \neg\lceil(x \circ \neg\lceil z) \ \wedge \ x \circ z \barwedge x_{\lceil z} \circ z \sqsubseteq (\lceil(x \circ z) \barwedge \lceil(x_{\lceil z} \circ z)) \circ z$
$\iff$ ⟨ by Proposition 3.20-16 and Boolean algebra ⟩
$\lceil z \sqsubseteq \lceil x \circ \neg\lceil(x \circ \neg\lceil z) \ \wedge \ \lceil(x \circ z) \circ (x \circ z \barwedge x_{\lceil z} \circ z) \sqsubseteq \lceil(x \circ z) \circ z \ \wedge$
$\neg\lceil(x \circ z) \circ (x \circ z \barwedge x_{\lceil z} \circ z) \sqsubseteq \neg\lceil(x \circ z) \circ \lceil(x_{\lceil z} \circ z) \circ z$
$\iff$ ⟨ by Corollaries 3.21-7 and 3.21-8, Propositions 3.14-7 and 3.14-9, (4.5) with $x, t := x, \lceil z$ and Boolean algebra ⟩
$\lceil z \sqsubseteq \lceil x \circ \neg\lceil(x \circ \neg\lceil z) \ \wedge \ x \circ z \sqsubseteq \lceil(x \circ z) \circ z \ \wedge \ x_{\lceil z} \circ z \sqsubseteq \lceil(x_{\lceil z}) \circ z$

Suppose $x \cdot_D z \leq_D z$. By (4.45),

$$\lceil z \ \sqsubseteq \ \lceil x \circ \neg\lceil(x \circ \neg\lceil z) \quad (4.46)$$
$$x \circ z \ \sqsubseteq \ \lceil(x \circ z) \circ z \quad (4.47)$$
$$x_{\lceil z} \circ z \ \sqsubseteq \ \lceil(x_{\lceil z}) \circ z \quad (4.48)$$

all hold.

We have to show $x^{*D} \cdot_D z \leq_D z$. By (4.45) with $x := x^{*D}$ and Definition 4.19, this means that we have to prove the following equations.

$$\lceil z \ \sqsubseteq \ \lceil(x \barwedge 1)^{\times} \circ \neg\lceil((x \barwedge 1)^{\times} \circ \neg\lceil z) \quad (4.49)$$
$$(x \barwedge 1)^{\times} \circ z \ \sqsubseteq \ \lceil((x \barwedge 1)^{\times} \circ z) \circ z \quad (4.50)$$
$$((x \barwedge 1)^{\times})_{\lceil z} \circ z \ \sqsubseteq \ \lceil(((x \barwedge 1)^{\times})_{\lceil z}) \circ z \quad (4.51)$$

Before embarking in these proofs, we need the following intermediate results. Note that the proofs of all the subsequent identities depend directly or indirectly on

(4.46). Therefore, the following results depend on the context and this is why they are not stated in an independent proposition.

$$x = {}^{\sqcap}z \sqsupset x \sqsupset \neg {}^{\sqcap}z \sqsupset x \sqsupset \neg {}^{\sqcap}z \tag{4.52}$$

$$x \sqsupset {}^{\sqcap}z = {}^{\sqcap}z \sqsupset x \sqsupset {}^{\sqcap}z \tag{4.53}$$

$$\neg {}^{\sqcap}z \sqsupset x = \neg {}^{\sqcap}z \sqsupset x \sqsupset \neg {}^{\sqcap}z \tag{4.54}$$

$$\neg {}^{\sqcap}z \sqsupset (x \sqsupset 1) = \neg {}^{\sqcap}z \sqsupset (x \sqsupset 1) \sqsupset \neg {}^{\sqcap}z \tag{4.55}$$

$$x_{{}^{\sqcap}z} = {}^{\sqcap}z \sqsupset x_{{}^{\sqcap}z} \text{ and } x_{\neg {}^{\sqcap}z} = {}^{\sqcap}z \sqsupset x_{\neg {}^{\sqcap}z} \tag{4.56}$$

$${}^{\sqcap}((x \sqsupset 1)^{\times} \sqsupset \neg {}^{\sqcap}z) = \neg {}^{\sqcap}z \tag{4.57}$$

$$\neg {}^{\sqcap}((x \sqsupset 1)^{\times} \sqsupset \neg {}^{\sqcap}z) = {}^{\sqcap}z \tag{4.58}$$

$$\neg {}^{\sqcap}z \sqsupset (x \sqsupset 1)^{\times} = (x \sqsupset 1)^{\times} \sqsupset \neg {}^{\sqcap}z \tag{4.59}$$

$$\neg {}^{\sqcap}x \sqsupset (x \sqsupset 1)^{\times} = \neg {}^{\sqcap}x \tag{4.60}$$

$$\neg {}^{\sqcap}z \sqsupset ((x \sqsupset 1)^{\times})_{\neg {}^{\sqcap}z} = \top \tag{4.61}$$

$$\neg {}^{\sqcap}x \sqsupset ((x \sqsupset 1)^{\times})_{\neg {}^{\sqcap}z} = \top \tag{4.62}$$

$${}^{\sqcap}(((x \sqsupset 1)^{\times})_{\neg {}^{\sqcap}z}) = \neg {}^{\sqcap}((x \sqsupset 1)^{\times} \sqsupset {}^{\sqcap}z) \sqsupset {}^{\sqcap}z \tag{4.63}$$

$$((x \sqsupset 1)^{\times})_{\neg {}^{\sqcap}z} = {}^{\sqcap}z \sqsupset ((x \sqsupset 1)^{\times})_{\neg {}^{\sqcap}z} \tag{4.64}$$

$$(x \sqsupset (x \sqsupset 1)^{\times})_{\neg {}^{\sqcap}z} = {}^{\sqcap}z \sqsupset (x \sqsupset (x \sqsupset 1)^{\times})_{\neg {}^{\sqcap}z} \tag{4.65}$$

$$((x \sqsupset 1)^{\times})_{\neg {}^{\sqcap}z} = {}^{\sqcap}x \sqsupset ((x \sqsupset 1)^{\times})_{\neg {}^{\sqcap}z} \tag{4.66}$$

(a) Proof of (4.52).

$$\begin{array}{ll} & x \\ = & \quad \langle \text{ by (4.46) and Boolean algebra,} \\ & \quad {}^{\sqcap}z \sqsupset {}^{\sqcap}(x \sqsupset \neg {}^{\sqcap}z) \sqsubseteq {}^{\sqcap}x, \\ & \quad \text{then apply Proposition 3.14-7 and Boolean algebra } \rangle \\ & ({}^{\sqcap}z \sqsupset {}^{\sqcap}(x \sqsupset \neg {}^{\sqcap}z)) \sqsupset x \\ = & \quad \langle \text{ by Boolean algebra } \rangle \\ & ({}^{\sqcap}z \sqsupset \neg {}^{\sqcap}z \sqsupset {}^{\sqcap}(x \sqsupset \neg {}^{\sqcap}z)) \sqsupset x \\ = & \quad \langle \text{ Corollary 3.21-5 } \rangle \\ & {}^{\sqcap}z \sqsupset x \sqsupset \neg {}^{\sqcap}z \sqsupset {}^{\sqcap}(x \sqsupset \neg {}^{\sqcap}z) \sqsupset x \\ = & \quad \langle \text{ by (3.19) } \rangle \\ & {}^{\sqcap}z \sqsupset x \sqsupset \neg {}^{\sqcap}z \sqsupset x \sqsupset \neg {}^{\sqcap}z \end{array}$$

(b) Proof of (4.53).

$$\begin{array}{ll} & \mathsf{true} \\ \Longleftrightarrow & \quad \langle \text{ by (4.52) } \rangle \end{array}$$

$$
\begin{array}{ll}
& x = {}^{\Gamma}z \mathbin{\square} x \mathbin{\boxplus} \neg {}^{\Gamma}z \mathbin{\square} x \mathbin{\square} \neg {}^{\Gamma}z \\
\Longrightarrow & \quad \langle \text{ by Proposition 3.14-9 and Boolean algebra,} \\
& \quad {}^{\Gamma}({}^{\Gamma}z \mathbin{\square} x) \mathbin{\square} {}^{\Gamma}(\neg {}^{\Gamma}z \mathbin{\square} x \mathbin{\square} \neg {}^{\Gamma}z) = {}^{\Gamma}z \mathbin{\square} {}^{\Gamma}x \mathbin{\square} \neg {}^{\Gamma}z \mathbin{\square} {}^{\Gamma}(x \mathbin{\square} \neg {}^{\Gamma}z) = \top, \\
& \quad \text{then apply Corollary 3.21-17 } \rangle \\
& x \mathbin{\square} {}^{\Gamma}z = {}^{\Gamma}z \mathbin{\square} x \mathbin{\square} {}^{\Gamma}z \mathbin{\boxplus} \neg {}^{\Gamma}z \mathbin{\square} x \mathbin{\square} \neg {}^{\Gamma}z \mathbin{\square} {}^{\Gamma}z \\
\Longleftrightarrow & \quad \langle \text{ by Boolean algebra, (3.6) and Corollary 3.21-3 } \rangle \\
& x \mathbin{\square} {}^{\Gamma}z = {}^{\Gamma}z \mathbin{\square} x \mathbin{\square} {}^{\Gamma}z
\end{array}
$$

(c) Proof of (4.54). This follows from (4.52), Corollaries 3.21-4 and 3.21-3, Boolean algebra and (3.6).

(d) Proof of (4.55).

$$
\begin{array}{ll}
& \neg {}^{\Gamma}z \mathbin{\square} (x \mathbin{\boxplus} 1) \\
= & \quad \langle \text{ by Corollary 3.21-4 and Boolean algebra } \rangle \\
& \neg {}^{\Gamma}z \mathbin{\square} x \mathbin{\boxplus} \neg {}^{\Gamma}z \\
= & \quad \langle \text{ by (4.54), Corollary 3.21-2, Proposition 3.14-9, De} \\
& \quad \text{Morgan and Boolean algebra } \rangle \\
& \neg {}^{\Gamma}z \mathbin{\square} x \mathbin{\square} \neg {}^{\Gamma}z \mathbin{\boxplus} \neg {}^{\Gamma}z \mathbin{\square} \neg {}^{\Gamma}x \mathbin{\square} \neg {}^{\Gamma}z \\
= & \quad \langle \text{ by Propositions 3.14-9 and 3.14-1, and Boolean algebra,} \\
& \quad {}^{\Gamma}(\neg {}^{\Gamma}z \mathbin{\square} x) \mathbin{\square} {}^{\Gamma}(\neg {}^{\Gamma}z \mathbin{\square} \neg {}^{\Gamma}x) = \neg {}^{\Gamma}z \mathbin{\square} {}^{\Gamma}x \mathbin{\square} \neg {}^{\Gamma}z \mathbin{\square} \neg {}^{\Gamma}x = \top, \\
& \quad \text{then apply Corollary 3.21-17 } \rangle \\
& (\neg {}^{\Gamma}z \mathbin{\square} x \mathbin{\boxplus} \neg {}^{\Gamma}z \mathbin{\square} \neg {}^{\Gamma}x) \mathbin{\square} \neg {}^{\Gamma}z \\
= & \quad \langle \text{ by Corollaries 3.21-4 and 3.21-2, and Boolean algebra } \rangle \\
& \neg {}^{\Gamma}z \mathbin{\square} (x \mathbin{\boxplus} 1) \mathbin{\square} \neg {}^{\Gamma}z
\end{array}
$$

(e) Proof of (4.56).

$$
\begin{array}{ll}
& x_{\Gamma z} \\
= & \quad \langle \text{ by (4.52) } \rangle \\
& ({}^{\Gamma}z \mathbin{\square} x \mathbin{\boxplus} \neg {}^{\Gamma}z \mathbin{\square} x \mathbin{\square} \neg {}^{\Gamma}z)_{\Gamma z} \\
= & \quad \langle \text{ by Corollary 4.30-1 } \rangle \\
& ({}^{\Gamma}z \mathbin{\square} x)_{\Gamma z} \mathbin{\boxplus} \neg {}^{\Gamma}({}^{\Gamma}z \mathbin{\square} x) \mathbin{\square} (\neg {}^{\Gamma}z \mathbin{\square} x \mathbin{\square} \neg {}^{\Gamma}z)_{\Gamma z} \\
= & \quad \langle \text{ by Proposition 4.22-5, Corollaries 4.26-1 and 3.21-3, and} \\
& \quad (3.6) \rangle \\
& {}^{\Gamma}z \mathbin{\square} x_{\Gamma z}
\end{array}
$$

The proof of $x_{\neg \Gamma z} = {}^{\Gamma}z \mathbin{\square} x_{\neg \Gamma z}$ is similar.

(f) Proof of (4.57). By Lemma 4.20-3 and Proposition 3.14-1, $\neg^{\sqcap} z \sqsubseteq \sqcap((x \pitchfork 1)^{\times} \natural \neg^{\sqcap} z)$. The proof of the other refinement follows.

$$
\begin{array}{ll}
& \sqcap((x \pitchfork 1)^{\times} \natural \neg^{\sqcap} z) \sqsubseteq \neg^{\sqcap} z \\
\Longleftarrow & \quad \langle \text{ by (3.22) } \rangle \\
& \sqcap((x \pitchfork 1) \natural \neg^{\sqcap} z) \sqsubseteq \neg^{\sqcap} z \\
\Longleftrightarrow & \quad \langle \text{ by Corollaries 3.21-2 and 3.21-17 } \rangle \\
& \sqcap(x \natural \neg^{\sqcap} z \pitchfork \neg^{\sqcap} x \natural \neg^{\sqcap} z) \sqsubseteq \neg^{\sqcap} z \\
\Longleftrightarrow & \quad \langle \text{ by Corollary 3.21-16 and Proposition 3.14-1 } \rangle \\
& \sqcap(x \natural \neg^{\sqcap} z) \pitchfork \neg^{\sqcap} x \natural \neg^{\sqcap} z \sqsubseteq \neg^{\sqcap} z \\
\Longleftrightarrow & \quad \langle \text{ by De Morgan and Boolean algebra } \rangle \\
& \sqcap(x \natural \neg^{\sqcap} z) \sqsubseteq \neg^{\sqcap} z \natural (^{\sqcap} x \pitchfork {}^{\sqcap} z) \\
\Longleftrightarrow & \quad \langle \text{ by Boolean algebra } \rangle \\
& {}^{\sqcap} z \sqsubseteq {}^{\sqcap} x \natural \neg^{\sqcap}(x \natural \neg^{\sqcap} z) \\
\Longleftrightarrow & \quad \langle \text{ by (4.46) } \rangle \\
& \mathsf{true}
\end{array}
$$

(g) Proof of (4.58). This is direct from (4.57) by Boolean algebra.

(h) Proof of (4.59). By (4.57) and Proposition 3.14-7, $\neg^{\sqcap} z \natural (x \pitchfork 1)^{\times} = (x \pitchfork 1)^{\times} \natural \neg^{\sqcap} z$ is equivalent to $\neg^{\sqcap} z \natural (x \pitchfork 1)^{\times} = \neg^{\sqcap} z \natural (x \pitchfork 1)^{\times} \natural \neg^{\sqcap} z$. We prove the latter. The refinement $\neg^{\sqcap} z \natural (x \pitchfork 1)^{\times} \sqsubseteq \neg^{\sqcap} z \natural (x \pitchfork 1)^{\times} \natural \neg^{\sqcap} z$ follows from Lemma 3.7-1. The other refinement is proved as follows.

$$
\begin{array}{ll}
& \neg^{\sqcap} z \natural (x \pitchfork 1)^{\times} \natural \neg^{\sqcap} z \sqsubseteq \neg^{\sqcap} z \natural (x \pitchfork 1)^{\times} \\
\Longleftrightarrow & \quad \langle \text{ by Proposition 3.14-6 } \rangle \\
& (x \pitchfork 1)^{\times} \natural \neg^{\sqcap} z \sqsubseteq \neg^{\sqcap} z \natural (x \pitchfork 1)^{\times} \\
\Longleftarrow & \quad \langle \text{ by (3.12) } \rangle \\
& (x \pitchfork 1) \natural \neg^{\sqcap} z \natural (x \pitchfork 1)^{\times} \sqcup \neg^{\sqcap} z \sqsubseteq \neg^{\sqcap} z \natural (x \pitchfork 1)^{\times} \\
\Longleftarrow & \quad \langle \text{ by Proposition 3.3-1 } \rangle \\
& (x \pitchfork 1) \natural \neg^{\sqcap} z \natural (x \pitchfork 1)^{\times} \sqsubseteq \neg^{\sqcap} z \natural (x \pitchfork 1) \natural (x \pitchfork 1)^{\times} \\
\Longleftrightarrow & \quad \langle \text{ by (4.55) and Proposition 3.14-6 } \rangle \\
& \mathsf{true}
\end{array}
$$

(i) Proof of (4.60). We prove $\neg^{\sqcap} x \natural (x \pitchfork 1)^{\times} \sqsubseteq \neg^{\sqcap} x$ first.

$$
\begin{array}{ll}
& \neg^{\sqcap} x \,\square\, (x \pitchfork 1)^{\times} \sqsubseteq \neg^{\sqcap} x \\
\Longleftarrow & \quad \langle \text{ by (3.18) } \rangle \\
& \neg^{\sqcap} x \,\square\, (x \pitchfork 1) \sqsubseteq \neg^{\sqcap} x \\
\Longleftrightarrow & \quad \langle \text{ by Corollary 3.21-4 and (3.7) } \rangle \\
& \neg^{\sqcap} x \,\square\, x \pitchfork \neg^{\sqcap} x \sqsubseteq \neg^{\sqcap} x \\
\Longleftrightarrow & \quad \langle \text{ by Proposition 3.14-17 and Corollary 3.21-3 } \rangle \\
& \mathsf{true}
\end{array}
$$

The refinement $\sqsupseteq$ follows from Lemma 3.7-6.

(j) Proof of (4.61).

$$
\begin{array}{ll}
& \neg^{\sqcap} z \,\square\, ((x \pitchfork 1)^{\times})_{\neg^{\sqcap} z} \\
= & \quad \langle \text{ by Proposition 4.22-5 } \rangle \\
& (\neg^{\sqcap} z \,\square\, (x \pitchfork 1)^{\times})_{\neg^{\sqcap} z} \\
= & \quad \langle \text{ by (4.59) } \rangle \\
& ((x \pitchfork 1)^{\times} \,\square\, \neg^{\sqcap} z)_{\neg^{\sqcap} z} \\
= & \quad \langle \text{ by Corollary 4.26-1 } \rangle \\
& \top
\end{array}
$$

(k) Proof of (4.62).

$$
\begin{array}{ll}
& \neg^{\sqcap} x \,\square\, ((x \pitchfork 1)^{\times})_{\neg^{\sqcap} z} \\
= & \quad \langle \text{ by Proposition 4.22-5 } \rangle \\
& (\neg^{\sqcap} x \,\square\, (x \pitchfork 1)^{\times})_{\neg^{\sqcap} z} \\
= & \quad \langle \text{ by (4.60) } \rangle \\
& (\neg^{\sqcap} x)_{\neg^{\sqcap} z} \\
= & \quad \langle \text{ by (4.11) } \rangle \\
& \top
\end{array}
$$

(l) Proof of (4.63).

$$
\begin{array}{ll}
& {}^{\sqcap}(((x \pitchfork 1)^{\times})_{\neg^{\sqcap} z}) \\
= & \quad \langle \text{ by (4.4) with } x, t := (x \pitchfork 1)^{\times}, {}^{\sqcap} z \rangle \\
& \neg^{\sqcap}((x \pitchfork 1)^{\times} \,\square\, {}^{\sqcap} z) \,\square\, \neg^{\sqcap}((x \pitchfork 1)^{\times} \,\square\, \neg^{\sqcap} z) \,\square\, {}^{\sqcap}(x \pitchfork 1)^{\times} \\
= & \quad \langle \text{ by (4.58) and Lemma 4.20-1 } \rangle \\
& \neg^{\sqcap}((x \pitchfork 1)^{\times} \,\square\, {}^{\sqcap} z) \,\square\, {}^{\sqcap} z
\end{array}
$$

(m) Proof of (4.64).

$$
\begin{array}{ll}
 & ((x \pitchfork 1)^{\times})_{\neg \Pi z} \\
= & \quad \langle \text{ by (3.7) and Boolean algebra } \rangle \\
 & (\Pi z \pitchfork \neg \Pi z) \triangleright ((x \pitchfork 1)^{\times})_{\neg \Pi z} \\
= & \quad \langle \text{ by Corollaries 3.21-17 and 3.21-3, and (4.61) } \rangle \\
 & \Pi z \triangleright ((x \pitchfork 1)^{\times})_{\neg \Pi z}
\end{array}
$$

(n) Proof of (4.65). First, one has $\neg \Pi z \triangleright x \triangleright (x \pitchfork 1)^{\times} = \neg \Pi z \triangleright x \triangleright (x \pitchfork 1)^{\times} \triangleright \neg \Pi z$ by (4.54) and (4.59). Then $\neg \Pi z \triangleright (x \triangleright (x \pitchfork 1)^{\times})_{\neg \Pi z} = \top$ is shown like for (4.61). Finally, the desired result is shown like (4.64).

(o) Proof of (4.66). This proof is similar to the one of (4.64).

And now back to the proof of (4.49), (4.50) and (4.51).

Proof of (4.49).

$$
\begin{array}{ll}
 & \Pi (x \pitchfork 1)^{\times} \triangleright \neg \Pi ((x \pitchfork 1)^{\times} \triangleright \neg \Pi z) \\
= & \quad \langle \text{ by (4.58) } \rangle \\
 & \Pi (x \pitchfork 1)^{\times} \triangleright \Pi z \\
= & \quad \langle \text{ by Lemma 4.20-1 and Boolean algebra } \rangle \\
 & \Pi z
\end{array}
$$

Proof of (4.50).

$$
\begin{array}{ll}
 & (x \pitchfork 1)^{\times} \triangleright z \sqsubseteq \Pi ((x \pitchfork 1)^{\times} \triangleright z) \triangleright z \\
\Longleftarrow & \quad \langle \text{ by (3.12) } \rangle \\
 & (x \pitchfork 1) \triangleright \Pi ((x \pitchfork 1)^{\times} \triangleright z) \triangleright z \sqcup z \sqsubseteq \Pi ((x \pitchfork 1)^{\times} \triangleright z) \triangleright z \\
\Longleftrightarrow & \quad \langle \text{ by Propositions 3.14-7, 3.3-1 and 3.14-8, and (3.7),} \\
 & \qquad z = \Pi z \triangleright z = \Pi (1 \triangleright z) \triangleright z \sqsubseteq \Pi ((x \pitchfork 1)^{\times} \triangleright z) \triangleright z \ \rangle \\
 & (x \pitchfork 1) \triangleright \Pi ((x \pitchfork 1)^{\times} \triangleright z) \triangleright z \sqsubseteq \Pi ((x \pitchfork 1)^{\times} \triangleright z) \triangleright z \\
\Longleftrightarrow & \quad \langle \text{ by (3.19) } \rangle \\
 & \Pi ((x \pitchfork 1) \triangleright \Pi ((x \pitchfork 1)^{\times} \triangleright z)) \triangleright (x \pitchfork 1) \triangleright z \sqsubseteq \Pi ((x \pitchfork 1)^{\times} \triangleright z) \triangleright z \\
\Longleftrightarrow & \quad \langle \text{ by (3.20) } \rangle \\
 & \Pi ((x \pitchfork 1) \triangleright (x \pitchfork 1)^{\times} \triangleright z) \triangleright (x \pitchfork 1) \triangleright z \sqsubseteq \Pi ((x \pitchfork 1)^{\times} \triangleright z) \triangleright z \\
\Longleftarrow & \quad \langle \text{ by Proposition 3.3-1 } \rangle
\end{array}
$$

$$
\begin{array}{ll}
& \Cap((x \pitchfork 1)^{\times} \cdot z) \cdot (x \pitchfork 1) \cdot z \sqsubseteq \Cap((x \pitchfork 1)^{\times} \cdot z) \cdot z \\
\iff & \quad \langle \text{ by Proposition 3.14-6 } \rangle \\
& (x \pitchfork 1) \cdot z \sqsubseteq \Cap((x \pitchfork 1)^{\times} \cdot z) \cdot z \\
\impliedby & \quad \langle \text{ by Proposition 3.3-2 } \rangle \\
& (x \pitchfork 1) \cdot z \sqsubseteq \Cap((x \pitchfork 1) \cdot z) \cdot z \\
\iff & \quad \langle \text{ by Corollary 3.21-2, Boolean algebra and (4.52) } \rangle \\
& (\Cap z \cdot x \pitchfork \neg \Cap z \cdot x \cdot \neg \Cap z \pitchfork \neg \Cap x) \cdot z \sqsubseteq \Cap((\Cap z \cdot x \pitchfork \neg \Cap z \cdot x \cdot \neg \Cap z \pitchfork \neg \Cap x) \cdot z) \cdot z \\
\iff & \quad \langle \text{ by Propositions 3.14-9 and 3.14-1, Boolean algebra} \\
& \quad \text{and Lemma 3.17-2,} \\
& \quad \Cap(\Cap z \cdot x) \cdot \Cap(\neg \Cap z \cdot x \cdot \neg \Cap z) = \Cap z \cdot \Cap x \cdot \neg \Cap z \cdot \Cap(x \cdot \neg \Cap z) = \top, \\
& \quad \Cap(\Cap z \cdot x) \cdot \neg \Cap x = \Cap z \cdot \Cap x \cdot \neg \Cap x = \top \\
& \quad \text{and } \Cap(\neg \Cap z \cdot x \cdot \neg \Cap z) \cdot \neg \Cap x = \neg \Cap z \cdot \Cap(x \cdot \neg \Cap z) \cdot \neg \Cap x = \top, \\
& \quad \text{then apply Corollaries 3.21-17 and 3.21-3, Proposition 3.14-17} \\
& \quad \text{and (3.6) } \rangle \\
& \Cap z \cdot x \cdot z \pitchfork \neg \Cap x \cdot z \sqsubseteq \Cap(\Cap z \cdot x \cdot z \pitchfork \neg \Cap x \cdot z) \cdot z \\
\iff & \quad \langle \text{ by Corollary 3.21-16 and Proposition 3.14-9 } \rangle \\
& \Cap z \cdot x \cdot z \pitchfork \neg \Cap x \cdot z \sqsubseteq (\Cap z \cdot \Cap(x \cdot z) \pitchfork \neg \Cap x \cdot \Cap z) \cdot z \\
\iff & \quad \langle \text{ by Propositions 3.20-16, 3.14-7 and 3.14-9, Corollaries 3.21-4} \\
& \quad \text{and 3.21-3, Boolean algebra and (3.6) } \rangle \\
& \Cap z \cdot x \cdot z \sqsubseteq \Cap z \cdot \Cap(x \cdot z) \cdot z \ \wedge \ \neg \Cap x \cdot z \sqsubseteq \neg \Cap x \cdot \Cap z \cdot z \\
\iff & \quad \langle \text{ by Propositions 3.14-6 and 3.14-7, and Boolean algebra } \rangle \\
& x \cdot z \sqsubseteq \Cap(x \cdot z) \cdot z \\
\iff & \quad \langle \text{ by (4.47) } \rangle \\
& \mathsf{true}
\end{array}
$$

Proof of (4.51). Let

$$
\begin{aligned}
B &= x \cdot \Cap z \pitchfork x_{\Cap z} \pitchfork \Cap(x \cdot \neg \Cap z) \pitchfork \neg \Cap x, && (4.67) \\
A &= \Cap(((x \pitchfork 1)^{\times})_{\Cap z}) \cdot B^{\times} \quad \text{and} && (4.68) \\
C &= (x \pitchfork 1)^{\times} \cdot \Cap z. && (4.69)
\end{aligned}
$$

By (4.4) with $x, t := (x \pitchfork 1)^{\times}, \Cap z$, (4.69), (4.58) and Lemma 4.20-1,

$$A = \neg \Cap C \cdot \Cap z \cdot B^{\times}. \tag{4.70}$$

Before proving (4.51), we will prove that the following properties hold for all x, z, t.

$$B \cdot \Cap z = \Cap z \cdot B \tag{4.71}$$

$$
\begin{array}{rcll}
{}^{\sqcap}B & = & 1 & (4.72)\\
{}^{\sqcap}A & = & {}^{\sqcap}(((x \pitchfork 1)^{\times})_{\sqcap z}) & (4.73)\\
\neg{}^{\sqcap}x \triangleright B = \neg{}^{\sqcap}x \triangleright B^{\times} & = & \neg{}^{\sqcap}x \triangleright (x \pitchfork 1) = \neg{}^{\sqcap}x \triangleright (x \pitchfork 1)^{\times} = \neg{}^{\sqcap}x & (4.74)\\
{}^{\sqcap}(x \triangleright t) \triangleright B & = & {}^{\sqcap}(x \triangleright t) \triangleright (x \triangleright {}^{\sqcap}z \triangleright t \pitchfork x_{\sqcap z} \triangleright t \pitchfork {}^{\sqcap}(x \triangleright \neg{}^{\sqcap}z)) & (4.75)\\
A & = & A \triangleright {}^{\sqcap}z & (4.76)\\
{}^{\sqcap}(x \triangleright {}^{\sqcap}C) \triangleright A & = & \top & (4.77)\\
C & \sqsubseteq & {}^{\sqcap}C \triangleright B^{\times} & (4.78)\\
((x \pitchfork 1)^{\times})_{\neg \sqcap z} & = & {}^{\sqcap}z \triangleright x \triangleright (x \pitchfork 1)^{\times} \triangleright \neg{}^{\sqcap}z \pitchfork (x \triangleright (x \pitchfork 1)^{\times})_{\neg \sqcap z} & (4.79)\\
{}^{\sqcap}x \triangleright \neg{}^{\sqcap}(x \triangleright \neg{}^{\sqcap}z) \triangleright B & = & x \triangleright {}^{\sqcap}z \pitchfork x_{\sqcap z} & (4.80)\\
{}^{\sqcap}x \triangleright \neg{}^{\sqcap}(x \triangleright \neg{}^{\sqcap}z) \triangleright A & \sqsupseteq & (x \triangleright {}^{\sqcap}z \pitchfork x_{\sqcap z}) \triangleright B^{\times} & (4.81)\\
{}^{\sqcap}(A \sqcup ((x \pitchfork 1)^{\times})_{\neg \sqcap z}) & = & {}^{\sqcap}(((x \pitchfork 1)^{\times})_{\sqcap z}) & (4.82)\\
{}^{\sqcap}(((x \pitchfork 1)^{\times})_{\sqcap z}) \triangleright (x \pitchfork 1)^{\times} & \sqsubseteq & A \sqcup ((x \pitchfork 1)^{\times})_{\neg \sqcap z} & (4.83)\\
((x \pitchfork 1)^{\times})_{\sqcap z} & \sqsubseteq & A & (4.84)
\end{array}
$$

(a) Proof of (4.71).

$$
\begin{array}{ll}
 & B \triangleright {}^{\sqcap}z\\
= & \quad \langle \text{ by (4.67) } \rangle\\
 & (x \triangleright {}^{\sqcap}z \pitchfork x_{\sqcap z} \pitchfork {}^{\sqcap}(x \triangleright \neg{}^{\sqcap}z) \pitchfork \neg{}^{\sqcap}x) \triangleright {}^{\sqcap}z\\
= & \quad \langle \text{ by Remark 4.8, Boolean algebra and Corollary 3.21-17 } \rangle\\
 & x \triangleright {}^{\sqcap}z \pitchfork x_{\sqcap z} \triangleright {}^{\sqcap}z \pitchfork {}^{\sqcap}(x \triangleright \neg{}^{\sqcap}z) \triangleright {}^{\sqcap}z \pitchfork \neg{}^{\sqcap}x \triangleright {}^{\sqcap}z\\
= & \quad \langle \text{ by Boolean algebra, (4.53), (4.5) with } x, t := x, {}^{\sqcap}z \text{ and (4.56) } \rangle\\
 & {}^{\sqcap}z \triangleright x \triangleright {}^{\sqcap}z \pitchfork {}^{\sqcap}z \triangleright x_{\sqcap z} \pitchfork {}^{\sqcap}z \triangleright {}^{\sqcap}(x \triangleright \neg{}^{\sqcap}z) \pitchfork {}^{\sqcap}z \triangleright \neg{}^{\sqcap}x\\
= & \quad \langle \text{ by Corollary 3.21-4 and (4.67) } \rangle\\
 & {}^{\sqcap}z \triangleright B
\end{array}
$$

(b) Proof of (4.72).

$$
\begin{array}{ll}
 & {}^{\sqcap}B\\
= & \quad \langle \text{ by (4.67) } \rangle\\
 & {}^{\sqcap}(x \triangleright {}^{\sqcap}z \pitchfork x_{\sqcap z} \pitchfork {}^{\sqcap}(x \triangleright \neg{}^{\sqcap}z) \pitchfork \neg{}^{\sqcap}x)\\
= & \quad \langle \text{ by Corollary 3.21-16 and Proposition 3.14-1 } \rangle\\
 & {}^{\sqcap}(x \triangleright {}^{\sqcap}z) \pitchfork {}^{\sqcap}(x_{\sqcap z}) \pitchfork {}^{\sqcap}(x \triangleright \neg{}^{\sqcap}z) \pitchfork \neg{}^{\sqcap}x\\
= & \quad \langle \text{ by Remark 4.8 and Boolean algebra } \rangle
\end{array}
$$

$$
\begin{array}{ll}
& \Gamma x \pitchfork \neg \Gamma x \\
= & \qquad \langle \text{ by Boolean algebra } \rangle \\
& 1
\end{array}
$$

(c) Proof of (4.73).

$$
\begin{array}{ll}
& \Gamma A \\
= & \qquad \langle \text{ by (4.68) and Proposition 3.14-9 } \rangle \\
& \Gamma(((x \pitchfork 1)^{\times})_{\Gamma z}) \triangleleft \Gamma(B^{\times}) \\
= & \qquad \langle \text{ by (4.72) and Proposition 3.14-22,} \\
& \quad \mathsf{true} \Longleftrightarrow \Gamma B = 1 \Longrightarrow \Gamma(B^{\times}) = 1, \\
& \quad \text{then apply (3.7) } \rangle \\
& \Gamma(((x \pitchfork 1)^{\times})_{\Gamma z})
\end{array}
$$

(d) Proof of (4.74). The equalities $\neg \Gamma x \triangleleft (x \pitchfork 1) = \neg \Gamma x \triangleleft (x \pitchfork 1)^{\times} = \neg \Gamma x$ follow from Corollaries 3.21-4 and 3.21-3, Proposition 3.14-17, Boolean algebra and (4.60).

Here is the derivation for $\neg \Gamma x \triangleleft B = \neg \Gamma x$.

$$
\begin{array}{ll}
& \neg \Gamma x \triangleleft B \\
= & \qquad \langle \text{ by (4.67) } \rangle \\
& \neg \Gamma x \triangleleft (x \triangleleft \Gamma z \pitchfork x_{\Gamma z} \pitchfork \Gamma(x \triangleleft \neg \Gamma z) \pitchfork \neg \Gamma x) \\
= & \qquad \langle \text{ by Corollaries 3.21-4 and 3.21-3, Proposition 3.14-17 and} \\
& \quad \text{Boolean algebra } \rangle \\
& \neg \Gamma x \triangleleft x_{\Gamma z} \pitchfork \neg \Gamma x \triangleleft \Gamma(x \triangleleft \neg \Gamma z) \pitchfork \neg \Gamma x \\
= & \qquad \langle \text{ by (4.10), Lemma 3.17-2 and Corollary 3.21-3 } \rangle \\
& \neg \Gamma x
\end{array}
$$

The refinement $\neg \Gamma x \sqsubseteq \neg \Gamma x \triangleleft B^{\times}$ follows from Lemma 3.7-6 and here is the derivation for $\neg \Gamma x \triangleleft B^{\times} \sqsubseteq \neg \Gamma x$.

$$
\begin{array}{ll}
& \neg \Gamma x \triangleleft B^{\times} \sqsubseteq \neg \Gamma x \\
\Longleftarrow & \qquad \langle \text{ by (3.13) } \rangle \\
& \neg \Gamma x \triangleleft B \sqcup \neg \Gamma x \sqsubseteq \neg \Gamma x \\
\Longleftrightarrow & \qquad \langle \text{ see the previous derivation } \rangle \\
& \mathsf{true}
\end{array}
$$

(e) Proof of (4.75).

$$
\begin{array}{ll}
& \Pi(x \triangleright t) \triangleright B \\
= & \qquad \langle \text{ by (4.67) } \rangle \\
& \Pi(x \triangleright t) \triangleright (x \triangleright \Pi z \between x_{\Pi z} \between \Pi(x \triangleright \neg \Pi z) \between \neg \Pi x) \\
= & \qquad \langle \text{ by Boolean algebra and Corollary 3.21-4 } \rangle \\
& \Pi(x \triangleright t) \triangleright (\Pi(x \triangleright t) \triangleright x \triangleright \Pi z \between \Pi(x \triangleright t) \triangleright x_{\Pi z} \between \Pi(x \triangleright t) \triangleright \Pi(x \triangleright \neg \Pi z) \between \Pi(x \triangleright t) \triangleright \neg \Pi x) \\
= & \qquad \langle \text{ by (3.19), Proposition 4.22-6, Lemma 3.17-2 and Boolean algebra } \rangle \\
& \Pi(x \triangleright t) \triangleright (x \triangleright \Pi z \triangleright t \between \Pi(x \triangleright t) \triangleright x_{\Pi z} \triangleright t \between \Pi(x \triangleright t) \triangleright \Pi(x \triangleright \neg \Pi z) \between \top) \\
= & \qquad \langle \text{ by Corollaries 3.21-3 and 3.21-4 } \rangle \\
& \Pi(x \triangleright t) \triangleright (x \triangleright \Pi z \triangleright t \between x_{\Pi z} \triangleright t \between \Pi(x \triangleright \neg \Pi z))
\end{array}
$$

(f) Proof of (4.76). We only need to show $A \triangleright \Pi z \sqsubseteq A$, since the other refinement follows from Lemma 3.7-1.

$$
\begin{array}{ll}
& A \triangleright \Pi z \sqsubseteq A \\
\Longleftarrow & \qquad \langle \text{ by (4.70) } \rangle \\
& \Pi z \triangleright B^{\times} \triangleright \Pi z \sqsubseteq \Pi z \triangleright B^{\times} \\
\Longleftrightarrow & \qquad \langle \text{ by Proposition 3.14-6 } \rangle \\
& B^{\times} \triangleright \Pi z \sqsubseteq \Pi z \triangleright B^{\times} \\
\Longleftarrow & \qquad \langle \text{ by Proposition 3.3-3 } \rangle \\
& B \triangleright \Pi z \sqsubseteq \Pi z \triangleright B \\
\Longleftrightarrow & \qquad \langle \text{ by (4.71) } \rangle \\
& \mathsf{true}
\end{array}
$$

(g) Proof of (4.77).

$$
\begin{array}{ll}
& \Pi(x \triangleright \Pi C) \triangleright A \\
= & \qquad \langle \text{ by (4.70), (4.69) and (3.20) } \rangle \\
& \Pi(x \triangleright C) \triangleright \neg \Pi((x \between 1)^{\times} \triangleright \Pi z) \triangleright \Pi z \triangleright B^{\times} \\
= & \qquad \langle \text{ by (3.16), (3.9), (3.21) and Proposition 3.14-1 } \rangle \\
& \Pi(x \triangleright C) \triangleright \neg(\Pi((x \between 1) \triangleright (x \between 1)^{\times} \triangleright \Pi z) \sqcup \Pi z) \triangleright \Pi z \triangleright B^{\times} \\
= & \qquad \langle \text{ by Boolean algebra } \rangle \\
& \Pi(x \triangleright C) \triangleright \neg \Pi((x \between 1) \triangleright (x \between 1)^{\times} \triangleright \Pi z) \triangleright \Pi z \triangleright B^{\times} \\
\sqsupseteq & \qquad \langle \text{ by (4.69) and Corollary 3.21-12 } \rangle \\
& \Pi(x \triangleright C) \triangleright \neg \Pi(x \triangleright C) \triangleright \Pi z \triangleright B^{\times}
\end{array}
$$

$$
\begin{array}{ll}
= & \langle \text{ by Boolean algebra and (3.6) } \rangle \\
\top &
\end{array}
$$

(h) Proof of (4.78).

$$
\begin{array}{ll}
& C \sqsubseteq \lceil C \rceil \mathbin{\triangleright} B^{\times} \\
\Longleftarrow & \langle \text{ by (4.69) and (3.12) } \rangle \\
& (x \barwedge 1) \mathbin{\triangleright} \lceil C \rceil \mathbin{\triangleright} B^{\times} \sqcup \lceil z \rceil \sqsubseteq \lceil C \rceil \mathbin{\triangleright} B^{\times} \\
\Longleftrightarrow & \langle \text{ by (3.7), Propositions 3.14-1 and 3.3-1, and (4.69),} \\
& \quad \lceil z \rceil = \lceil (1 \mathbin{\triangleright} \lceil z \rceil) \mathbin{\triangleright} 1 \sqsubseteq \lceil (x \barwedge 1)^{\times} \mathbin{\triangleright} \lceil z \rceil \rceil \mathbin{\triangleright} B^{\times} = \lceil C \rceil \mathbin{\triangleright} B^{\times} \text{ } \rangle \\
& (x \barwedge 1) \mathbin{\triangleright} \lceil C \rceil \mathbin{\triangleright} B^{\times} \sqsubseteq \lceil C \rceil \mathbin{\triangleright} B^{\times} \\
\Longleftrightarrow & \langle \text{ by (3.7), Proposition 3.3-1, (3.20) and (4.69),} \\
& \quad \lceil z \rceil = \lceil 1 \mathbin{\triangleright} z \rceil \sqsubseteq \lceil (x \barwedge 1)^{\times} \mathbin{\triangleright} z \rceil = \lceil (x \barwedge 1)^{\times} \mathbin{\triangleright} \lceil z \rceil \rceil = \lceil C \rceil, \\
& \quad \text{then apply Boolean algebra } \rangle \\
& (x \barwedge 1) \mathbin{\triangleright} \lceil C \rceil \mathbin{\triangleright} \lceil z \rceil \mathbin{\triangleright} B^{\times} \sqsubseteq \lceil C \rceil \mathbin{\triangleright} B^{\times} \\
\Longleftarrow & \langle \text{ by Proposition 3.3-2, (3.20) and (4.69),} \\
& \quad \lceil (x \barwedge 1) \mathbin{\triangleright} z \rceil \sqsubseteq \lceil (x \barwedge 1)^{\times} \mathbin{\triangleright} z \rceil = \lceil C \rceil, \\
& \quad \text{then apply (3.19), (3.20), Proposition 3.3-1 and Boolean} \\
& \quad \text{algebra } \rangle \\
& \lceil (x \barwedge 1) \mathbin{\triangleright} C \rceil \mathbin{\triangleright} (x \barwedge 1) \mathbin{\triangleright} \lceil z \rceil \mathbin{\triangleright} B^{\times} \sqsubseteq \lceil C \rceil \mathbin{\triangleright} \lceil (x \barwedge 1) \mathbin{\triangleright} \lceil z \rceil \rceil \mathbin{\triangleright} B \mathbin{\triangleright} B^{\times} \\
\Longleftrightarrow & \langle \text{ by Proposition 3.14-6 } \rangle \\
& \lceil C \rceil \mathbin{\triangleright} \lceil (x \barwedge 1) \mathbin{\triangleright} C \rceil \mathbin{\triangleright} (x \barwedge 1) \mathbin{\triangleright} \lceil z \rceil \mathbin{\triangleright} B^{\times} \sqsubseteq \lceil C \rceil \mathbin{\triangleright} \lceil (x \barwedge 1) \mathbin{\triangleright} \lceil z \rceil \rceil \mathbin{\triangleright} B \mathbin{\triangleright} B^{\times} \\
\Longleftrightarrow & \langle \text{ by (4.69) and Proposition 3.3-1,} \\
& \quad \lceil (x \barwedge 1) \mathbin{\triangleright} C \rceil = \lceil (x \barwedge 1) \mathbin{\triangleright} (x \barwedge 1)^{\times} \mathbin{\triangleright} \lceil z \rceil \rceil \\
& \quad \sqsubseteq \lceil (x \barwedge 1)^{\times} \mathbin{\triangleright} \lceil z \rceil \rceil = \lceil C \rceil, \\
& \quad \text{then apply Boolean algebra } \rangle \\
& \lceil C \rceil \mathbin{\triangleright} (x \barwedge 1) \mathbin{\triangleright} \lceil z \rceil \mathbin{\triangleright} B^{\times} \sqsubseteq \lceil C \rceil \mathbin{\triangleright} \lceil (x \barwedge 1) \mathbin{\triangleright} \lceil z \rceil \rceil \mathbin{\triangleright} B \mathbin{\triangleright} B^{\times} \\
\Longleftarrow & \langle \text{ } \rangle \\
& (x \barwedge 1) \mathbin{\triangleright} \lceil z \rceil \sqsubseteq \lceil (x \barwedge 1) \mathbin{\triangleright} \lceil z \rceil \rceil \mathbin{\triangleright} B \\
\Longleftrightarrow & \langle \text{ by Corollaries 3.21-2, 3.21-17 and 3.21-16, and Boolean} \\
& \quad \text{algebra } \rangle \\
& x \mathbin{\triangleright} \lceil z \rceil \barwedge \neg \lceil x \mathbin{\triangleright} \lceil z \rceil \sqsubseteq (\lceil x \mathbin{\triangleright} \lceil z \rceil \rceil \barwedge \neg \lceil x \mathbin{\triangleright} \lceil z \rceil \rceil) \mathbin{\triangleright} B \\
\Longleftrightarrow & \langle \text{ by (4.67) and Corollary 3.21-4 } \rangle \\
& x \mathbin{\triangleright} \lceil z \rceil \barwedge \neg \lceil x \mathbin{\triangleright} \lceil z \rceil \sqsubseteq (\lceil x \mathbin{\triangleright} \lceil z \rceil \rceil \barwedge \neg \lceil x \mathbin{\triangleright} \lceil z \rceil \rceil) \mathbin{\triangleright} x \mathbin{\triangleright} \lceil z \rceil \barwedge \\
& \qquad\qquad (\lceil x \mathbin{\triangleright} \lceil z \rceil \rceil \barwedge \neg \lceil x \mathbin{\triangleright} \lceil z \rceil \rceil) \mathbin{\triangleright} x_{\lceil z \rceil} \barwedge \\
& \qquad\qquad (\lceil x \mathbin{\triangleright} \lceil z \rceil \rceil \barwedge \neg \lceil x \mathbin{\triangleright} \lceil z \rceil \rceil) \mathbin{\triangleright} \lceil x \mathbin{\triangleright} \neg \lceil z \rceil \rceil
\end{array}
$$

$$
\begin{array}{ll}
 & (\Gamma(x \triangleright \Gamma z) \between \neg\Gamma x \triangleright \Gamma z) \triangleright \neg\Gamma x \\
\iff & \quad \langle \text{ by Proposition 3.14-7, Boolean algebra, Lemmas 3.17-2 and 3.17-4, and Corollary 3.21-3 } \rangle \\
 & x \triangleright \Gamma z \between \neg\Gamma x \triangleright \Gamma z \sqsubseteq x \triangleright \Gamma z \between (\Gamma(x \triangleright \Gamma z) \between \neg\Gamma x \triangleright \Gamma z) \triangleright x_{\Gamma z} \between \neg\Gamma x \triangleright \Gamma z \\
\iff & \quad \langle \text{ by Proposition 3.14-7, Boolean algebra, Remark 4.8, (3.6) and Corollary 3.21-3 } \rangle \\
 & \mathsf{true}
\end{array}
$$

(i) Proof of (4.79).

$$
\begin{array}{ll}
 & ((x \between 1)^{\times})_{\neg\Gamma z} \\
= & \quad \langle \text{ by (4.64), (4.66) and (3.16) } \rangle \\
 & \Gamma x \triangleright \Gamma z \triangleright ((x \between 1) \triangleright (x \between 1)^{\times} \sqcup 1)_{\neg\Gamma z} \\
= & \quad \langle \text{ by Theorem 4.23, Boolean algebra and Proposition 3.14-1 } \rangle \\
 & \Gamma x \triangleright \Gamma z \triangleright \Big(\Gamma z \triangleright (x \between 1) \triangleright (x \between 1)^{\times} \triangleright \neg\Gamma z \between \Gamma z \triangleright ((x \between 1) \triangleright (x \between 1)^{\times})_{\neg\Gamma z} \between \\
 & \qquad ((x \between 1) \triangleright (x \between 1)^{\times} \triangleright \neg\Gamma z \sqcup 1_{\neg\Gamma z}) \between \\
 & \qquad \Gamma((x \between 1) \triangleright (x \between 1)^{\times} \triangleright \Gamma z) \triangleright \neg\Gamma z \between \\
 & \qquad \Gamma((x \between 1) \triangleright (x \between 1)^{\times} \triangleright \Gamma z) \triangleright 1_{\neg\Gamma z} \between \\
 & \qquad (((x \between 1) \triangleright (x \between 1)^{\times})_{\neg\Gamma z} \sqcup \neg\Gamma z) \between \\
 & \qquad (((x \between 1) \triangleright (x \between 1)^{\times})_{\neg\Gamma z} \sqcup 1_{\neg\Gamma z}) \Big) \\
= & \quad \langle \text{ by (4.11), Corollaries 3.21-4 and 3.21-3, (3.8), Boolean algebra and (3.4) } \rangle \\
 & \Gamma x \triangleright (\Gamma z \triangleright (x \between 1) \triangleright (x \between 1)^{\times} \triangleright \neg\Gamma z \between \Gamma z \triangleright ((x \between 1) \triangleright (x \between 1)^{\times})_{\neg\Gamma z}) \\
= & \quad \langle \text{ by Corollaries 3.21-4 and 3.21-7, Boolean algebra, Propositions 4.22-5 and 3.14-7, and (4.65) } \rangle \\
 & \Gamma z \triangleright x \triangleright (x \between 1)^{\times} \triangleright \neg\Gamma z \between (x \triangleright (x \between 1)^{\times})_{\neg\Gamma z}
\end{array}
$$

(j) Proof of (4.80).

$$
\begin{array}{ll}
 & \Gamma x \triangleright \neg\Gamma(x \triangleright \neg\Gamma z) \triangleright B \\
= & \quad \langle \text{ by (4.8), Boolean algebra, Corollary 3.21-16 and (4.67) } \rangle \\
 & (\Gamma(x \triangleright \Gamma z) \between \Gamma(x_{\Gamma z})) \triangleright (x \triangleright \Gamma z \between x_{\Gamma z} \between \Gamma(x \triangleright \neg\Gamma z) \between \neg\Gamma x) \\
= & \quad \langle \text{ by Remark 4.8 and Corollary 3.21-17 and (3.25) } \rangle \\
 & \Gamma(x \triangleright \Gamma z) \triangleright (x \triangleright \Gamma z \between x_{\Gamma z} \between \Gamma(x \triangleright \neg\Gamma z) \between \neg\Gamma x) \between \\
 & \Gamma(x_{\Gamma z}) \triangleright (x_{\Gamma z} \between x \triangleright \Gamma z \between \Gamma(x \triangleright \neg\Gamma z) \between \neg\Gamma x)
\end{array}
$$

$$
\begin{array}{ll}
= & \langle \text{ by Corollary 3.21-7 and Proposition 3.14-7 } \rangle \\
& x \rhd \top z \pitchfork x_{\top z}
\end{array}
$$

(k) Proof of (4.81).

$$
\begin{array}{ll}
& (x \rhd \top z \pitchfork x_{\top z}) \rhd B^{\times} \\
= & \langle \text{ by (4.80) } \rangle \\
& \top x \rhd \neg \top (x \rhd \neg \top z) \rhd B \rhd B^{\times} \\
\sqsubseteq & \langle \text{ by Proposition 3.3-1, Lemma 3.7-1 and (4.68) } \rangle \\
& \top x \rhd \neg \top (x \rhd \neg \top z) \rhd A
\end{array}
$$

(l) Proof of (4.82).

$$
\begin{array}{ll}
& \top (A \sqcup ((x \pitchfork 1)^{\times})_{\neg \top z}) \\
= & \langle \text{ by (3.21) and (4.73) } \rangle \\
& \top (((x \pitchfork 1)^{\times})_{\top z}) \sqcup \top (((x \pitchfork 1)^{\times})_{\neg \top z}) \\
= & \langle \text{ by (4.4) with } x, t := (x \pitchfork 1)^{\times}, \top z \text{ and Boolean algebra } \rangle \\
& \top (((x \pitchfork 1)^{\times})_{\top z})
\end{array}
$$

(m) Proof of (4.83).

$$
\begin{array}{ll}
& \top (((x \pitchfork 1)^{\times})_{\top z}) \rhd (x \pitchfork 1)^{\times} \sqsubseteq A \sqcup ((x \pitchfork 1)^{\times})_{\neg \top z} \\
\Longleftarrow & \langle \text{ by (3.13) } \rangle \\
& (A \sqcup ((x \pitchfork 1)^{\times})_{\neg \top z}) \rhd (x \pitchfork 1) \sqcup \top (((x \pitchfork 1)^{\times})_{\top z}) \sqsubseteq A \sqcup ((x \pitchfork 1)^{\times})_{\neg \top z} \\
\Longleftrightarrow & \langle \text{ by (3.7), Proposition 3.3-1 and (4.68),} \\
& \quad \top (((x \pitchfork 1)^{\times})_{\top z}) = \top (((x \pitchfork 1)^{\times})_{\top z}) \rhd 1 \\
& \quad \sqsubseteq \top (((x \pitchfork 1)^{\times})_{\top z}) \rhd B^{\times} = A \rangle \\
& (A \sqcup ((x \pitchfork 1)^{\times})_{\neg \top z}) \rhd (x \pitchfork 1) \sqsubseteq A \sqcup ((x \pitchfork 1)^{\times})_{\neg \top z} \\
\Longleftarrow & \langle \text{ by (3.9), (3.15) and (3.3) } \rangle \\
& A \rhd (x \pitchfork 1) \sqsubseteq A \sqcup ((x \pitchfork 1)^{\times})_{\neg \top z} \ \wedge \\
& ((x \pitchfork 1)^{\times})_{\neg \top z} \rhd (x \pitchfork 1) \sqsubseteq ((x \pitchfork 1)^{\times})_{\neg \top z} \\
\Longleftrightarrow & \langle \text{ by (4.6) with } x, t := (x \pitchfork 1)^{\times}, \top z \text{ and (4.55) } \rangle \\
& A \rhd (x \pitchfork 1) \sqsubseteq A \sqcup ((x \pitchfork 1)^{\times})_{\neg \top z} \ \wedge \\
& ((x \pitchfork 1)^{\times})_{\neg \top z} \rhd (x \pitchfork 1) \rhd \neg \top z \sqsubseteq ((x \pitchfork 1)^{\times})_{\neg \top z} \\
\Longleftrightarrow & \langle \text{ by (4.5) with } x, t := (x \pitchfork 1)^{\times}, \top z, \text{ (4.6) with} \\
& \quad x, t := (x \pitchfork 1)^{\times}, \top z, \text{ (4.4) with } x, t := (x \pitchfork 1)^{\times}, \top z, \\
& \quad \text{Propositions 4.22-2 and 3.14-7, and Corollary 4.26-10 } \rangle
\end{array}
$$

$$
\begin{array}{ll}
& A \triangleright (x \pitchfork 1) \sqsubseteq A \sqcup ((x \pitchfork 1)^\times)_{\neg\lceil z} \ \wedge \\
& ((x \pitchfork 1)^\times)_{\neg\lceil z} \triangleright (x \pitchfork 1) \triangleright \neg\lceil z \sqsubseteq \lceil((x \pitchfork 1)^\times)_{\lceil z} \triangleright (x \pitchfork 1)^\times \\
\Longleftarrow & \quad \langle \text{ by (4.6) with } x, t := (x \pitchfork 1)^\times, \lceil z, \text{ (4.55) and Proposition 3.3-1 } \rangle \\
& A \triangleright (x \pitchfork 1) \sqsubseteq A \sqcup ((x \pitchfork 1)^\times)_{\neg\lceil z} \ \wedge \\
& ((x \pitchfork 1)^\times)_{\neg\lceil z} \triangleright (x \pitchfork 1) \sqsubseteq \lceil((x \pitchfork 1)^\times)_{\lceil z} \triangleright (x \pitchfork 1)^\times \triangleright (x \pitchfork 1) \\
\Longleftarrow & \quad \langle \text{ by (4.68), (4.82) and Proposition 3.14-7 } \rangle \\
& \lceil(((x \pitchfork 1)^\times)_{\lceil z}) \triangleright B^\times \triangleright (x \pitchfork 1) \sqsubseteq \lceil(((x \pitchfork 1)^\times)_{\lceil z}) \triangleright (A \sqcup ((x \pitchfork 1)^\times)_{\neg\lceil z}) \ \wedge \\
& ((x \pitchfork 1)^\times)_{\neg\lceil z} \sqsubseteq \lceil(((x \pitchfork 1)^\times)_{\lceil z}) \triangleright (x \pitchfork 1)^\times \\
\Longleftrightarrow & \quad \langle \text{ by Propositions 3.14-6, 3.14-7 and 4.22-2, (3.15) and (4.82) } \rangle \\
& B^\times \triangleright (x \pitchfork 1) \sqsubseteq A \sqcup ((x \pitchfork 1)^\times)_{\neg\lceil z} \\
\Longleftarrow & \quad \langle \text{ by Corollary 3.21-12 } \rangle \\
& B^\times \triangleright (x \pitchfork 1) \sqsubseteq (A \sqcup ((x \pitchfork 1)^\times)_{\neg\lceil z}) \pitchfork C \\
\Longleftarrow & \quad \langle \text{ by (3.12) } \rangle \\
& B \triangleright ((A \sqcup ((x \pitchfork 1)^\times)_{\neg\lceil z}) \pitchfork C) \sqcup (x \pitchfork 1) \sqsubseteq (A \sqcup ((x \pitchfork 1)^\times)_{\neg\lceil z}) \pitchfork C \\
\Longleftrightarrow & \quad \langle \text{ By (4.69), (4.82), Remark 4.8 and Boolean algebra,} \\
& \quad \text{the domains of } A \sqcup ((x \pitchfork 1)^\times)_{\neg\lceil z} \text{ and } C \text{ are disjoint} \\
& \quad \text{and thus, by Proposition 3.14-7 and Boolean Algebra,} \\
& \quad \neg\lceil(A \sqcup ((x \pitchfork 1)^\times)_{\neg\lceil z}) \triangleright C = C, \\
& \quad \text{then apply Lemma 3.22-6 } \rangle \\
& B \triangleright ((A \sqcup ((x \pitchfork 1)^\times)_{\neg\lceil z}) \pitchfork C) \sqcup (x \pitchfork 1) \sqsubseteq A \sqcup ((x \pitchfork 1)^\times)_{\neg\lceil z} \ \wedge \\
& B \triangleright ((A \sqcup ((x \pitchfork 1)^\times)_{\neg\lceil z}) \pitchfork C) \sqcup (x \pitchfork 1) \sqsubseteq C \\
\Longleftarrow & \quad \langle \text{ By (4.69), (4.82), Remark 4.8 and Boolean algebra,} \\
& \quad \text{the domains of } A \sqcup ((x \pitchfork 1)^\times)_{\neg\lceil z} \text{ and } C \text{ are disjoint,} \\
& \quad \text{then apply (3.25), Corollaries 3.21-15 and 3.21-12, (3.8)} \\
& \quad \text{and (3.3) } \rangle \\
& B \triangleright (C \pitchfork A) \sqsubseteq A \ \wedge \\
& B \triangleright (C \pitchfork ((x \pitchfork 1)^\times)_{\neg\lceil z}) \sqsubseteq A \sqcup ((x \pitchfork 1)^\times)_{\neg\lceil z} \ \wedge \\
& x \pitchfork 1 \sqsubseteq A \sqcup ((x \pitchfork 1)^\times)_{\neg\lceil z} \ \wedge \\
& B \triangleright C \sqsubseteq C \ \wedge \\
& x \pitchfork 1 \sqsubseteq C \\
\Longleftrightarrow & \quad \langle \text{ by (4.73), (4.69) and Remark 4.8,} \\
& \quad \text{the domains of } A \text{ and } C \text{ are disjoint} \\
& \quad \text{and the domains of } ((x \pitchfork 1)^\times)_{\neg\lceil z} \text{ and } C \text{ are disjoint,} \\
& \quad \text{then apply (3.25) } \rangle
\end{array}
$$

$$
\begin{array}{l}
B \triangleleft (A \barwedge C) \sqsubseteq A \ \wedge \\
B \triangleleft (((x \barwedge 1)^{\times})_{\neg \Pi z} \barwedge C) \sqsubseteq A \sqcup ((x \barwedge 1)^{\times})_{\neg \Pi z} \ \wedge \\
x \barwedge 1 \sqsubseteq A \sqcup ((x \barwedge 1)^{\times})_{\neg \Pi z} \ \wedge \\
B \triangleleft C \sqsubseteq C \ \wedge \\
x \barwedge 1 \sqsubseteq C
\end{array}
$$

Thus, we have to prove the five following properties in order to terminate the demonstration of (4.83).

$$B \triangleleft (A \barwedge C) \sqsubseteq A \tag{4.85}$$

$$B \triangleleft (((x \barwedge 1)^{\times})_{\neg \Pi z} \barwedge C) \sqsubseteq A \sqcup ((x \barwedge 1)^{\times})_{\neg \Pi z} \tag{4.86}$$

$$x \barwedge 1 \sqsubseteq A \sqcup ((x \barwedge 1)^{\times})_{\neg \Pi z} \tag{4.87}$$

$$B \triangleleft C \sqsubseteq C \tag{4.88}$$

$$x \barwedge 1 \sqsubseteq C \tag{4.89}$$

These proofs frequently use case analysis (Corollary 3.21-19) based on appropriate tests. To be appropriate will mean that the tests must be disjoint and cover Πx, i.e., their meet must refine Πx. Indeed, the test $\neg \Pi x$ can be ignored, since all five properties hold for this case. This is easily seen by the following.

Firstly,

$$
\begin{array}{ll}
 & \neg \Pi x \triangleleft A \\
= & \quad \langle \text{ by (4.68) } \rangle \\
 & \neg \Pi x \triangleleft \Pi (((x \barwedge 1)^{\times})_{\neg \Pi z}) \triangleleft B^{\times} \\
= & \quad \langle \text{ by Propositions 3.14-9 and 3.14-19, (4.62) and (3.6) } \rangle \\
 & \top
\end{array}
$$

so the right part of (4.85), (4.86) and (4.87) is $\top$ in the presence of $\neg \Pi x$, making them true when restricted to the test $\neg \Pi x$.

Secondly, $\neg \Pi x \triangleleft B \triangleleft C = \neg \Pi x \triangleleft C$ by (4.74), so (4.88) is true when restricted to the test $\neg \Pi x$.

Finally,

$$
\begin{array}{ll}
 & \neg \Pi x \triangleleft (x \barwedge 1) \\
= & \quad \langle \text{ by Corollary 3.21-8 and Boolean algebra } \rangle \\
 & \neg \Pi x \\
\sqsubseteq & \quad \langle \text{ by Boolean algebra } \rangle
\end{array}
$$

$$
\begin{array}{ll}
& \neg\Gamma x \sqcap \Gamma z \\
= & \qquad \langle \text{ by (4.60) and (4.69) } \rangle \\
& \neg\Gamma x \sqcap C
\end{array}
$$

so (4.89) is true when restricted to the test $\neg\Gamma x$.

Here we go with the proof of the five aforementioned properties.

i. Proof of (4.85).

$$
\begin{array}{ll}
& B \sqcap (A \sqcap C) \\
\sqsubseteq & \qquad \langle \text{ by (4.78) and Lemma 3.22-1 } \rangle \\
& B \sqcap (A \sqcap \Gamma C \sqcap B^\times) \\
= & \qquad \langle \text{ by (4.69), Lemma 3.7-6 and Propositions 3.14-8} \\
& \quad \text{and 3.14-1,} \\
& \quad \mathsf{true} \iff \Gamma z \sqsubseteq C \implies \Gamma z \sqsubseteq \Gamma C, \\
& \quad \text{then apply (4.70) and Boolean algebra } \rangle \\
& B \sqcap (\neg\Gamma C \sqcap \Gamma z \sqcap B^\times \sqcap \Gamma C \sqcap \Gamma z \sqcap B^\times) \\
= & \qquad \langle \text{ by Corollary 3.21-6 } \rangle \\
& B \sqcap \Gamma z \sqcap B^\times \\
= & \qquad \langle \text{ by (4.71) } \rangle \\
& \Gamma z \sqcap B \sqcap B^\times \\
\sqsubseteq & \qquad \langle \text{ by Proposition 3.3-1, Lemma 3.7-1 and (4.70) } \rangle \\
& A
\end{array}
$$

ii. Proof of (4.86). We use case analysis with the following tests

$$\Gamma(x \sqcap \neg\Gamma z), \Gamma(x \sqcap \Gamma C), \Gamma(x \sqcap \neg\Gamma C) \sqcap \neg\Gamma(x \sqcap \neg\Gamma z), \Gamma(x_{\Gamma C}) \sqcap \neg\Gamma(x \sqcap \neg\Gamma z) \ .$$

They are disjoint by (4.69), (4.59), Boolean algebra, Lemma 3.17-4 and Remark 4.8. They cover Γx by Remark 4.8 and Boolean algebra.

A. Test $\Gamma(x \sqcap \neg\Gamma z)$.

$$
\begin{array}{ll}
& \Gamma(x \sqcap \neg\Gamma z) \sqcap B \sqcap (((x \sqcap 1)^\times)_{\neg\Gamma z} \sqcap C) \\
\sqsubseteq & \qquad \langle \text{ by Corollary 3.21-12 } \rangle \\
& \Gamma(x \sqcap \neg\Gamma z) \sqcap B \sqcap ((x \sqcap 1)^\times)_{\neg\Gamma z} \\
= & \qquad \langle \text{ by (4.67) and Corollary 3.21-4 } \rangle \\
& (\Gamma(x \sqcap \neg\Gamma z) \sqcap x \sqcap \Gamma z \sqcap \Gamma(x \sqcap \neg\Gamma z) \sqcap x_{\Gamma z} \sqcap \\
& \ \Gamma(x \sqcap \neg\Gamma z) \sqcap \Gamma(x \sqcap \neg\Gamma z) \sqcap \Gamma(x \sqcap \neg\Gamma z) \sqcap \neg\Gamma x) \sqcap ((x \sqcap 1)^\times)_{\neg\Gamma z} \\
= & \qquad \langle \text{ by Propositions 3.14-7 and 3.14-9, Remark 4.8,} \\
& \quad \text{Boolean algebra, (3.6) and Corollary 3.21-3 } \rangle
\end{array}
$$

$$
\begin{array}{ll}
& \Cap(x \sqcap \neg \Cap z) \sqcap ((x \boxplus 1)^{\times})_{\neg \Cap z} \\
\sqsubseteq & \quad \langle \text{ by (3.15) } \rangle \\
& \Cap(x \sqcap \neg \Cap z) \sqcap (A \sqcup ((x \boxplus 1)^{\times})_{\neg \Cap z})
\end{array}
$$

B. Test $\Cap(x \sqcap \Cap C)$.

$$
\begin{array}{ll}
& \Cap(x \sqcap \Cap C) \sqcap B \sqcap (((x \boxplus 1)^{\times})_{\neg \Cap z} \boxplus C) \\
\sqsubseteq & \quad \langle \text{ by (3.14) } \rangle \\
& \top \\
= & \quad \langle \text{ by (4.77) } \rangle \\
& \Cap(x \sqcap \Cap C) \sqcap A \\
\sqsubseteq & \quad \langle \text{ by (3.15) } \rangle \\
& \Cap(x \sqcap \Cap C) \sqcap (A \sqcup ((x \boxplus 1)^{\times})_{\neg \Cap z})
\end{array}
$$

C. Test $\Cap(x \sqcap \neg \Cap C) \sqcap \neg \Cap(x \sqcap \neg \Cap z)$.

$$
\begin{array}{ll}
& \Cap(x \sqcap \neg \Cap C) \sqcap \neg \Cap(x \sqcap \neg \Cap z) \sqcap (A \sqcup ((x \boxplus 1)^{\times})_{\neg \Cap z}) \\
\sqsupseteq & \quad \langle \text{ by (3.15) } \rangle \\
& \Cap(x \sqcap \neg \Cap C) \sqcap \neg \Cap(x \sqcap \neg \Cap z) \sqcap ((x \boxplus 1)^{\times})_{\neg \Cap z} \\
= & \quad \langle \text{ by (4.79) } \rangle \\
& \Cap(x \sqcap \neg \Cap C) \sqcap \neg \Cap(x \sqcap \neg \Cap z) \sqcap (\Cap z \sqcap x \sqcap (x \boxplus 1)^{\times} \sqcap \neg \Cap z \boxplus \\
& \qquad\qquad (x \sqcap (x \boxplus 1)^{\times})_{\neg \Cap z}) \\
= & \quad \langle \text{ by Corollary 3.21-4, Boolean algebra, (4.59) and Proposition 4.22-5 } \rangle \\
& \Cap(x \sqcap \neg \Cap C) \sqcap (\Cap z \sqcap \neg \Cap(x \sqcap \neg \Cap z) \sqcap x \sqcap \neg \Cap z \sqcap (x \boxplus 1)^{\times} \boxplus \\
& \qquad (\neg \Cap(x \sqcap \neg \Cap z) \sqcap x \sqcap (x \boxplus 1)^{\times})_{\neg \Cap z}) \\
= & \quad \langle \text{ by Propositions 3.14-17 and 4.22-5, (3.6) and Corollary 3.21-3 } \rangle \\
& (\Cap(x \sqcap \neg \Cap C) \sqcap \neg \Cap(x \sqcap \neg \Cap z) \sqcap x \sqcap (x \boxplus 1)^{\times})_{\neg \Cap z} \\
= & \quad \langle \text{ by Boolean algebra and (3.19) } \rangle \\
& (\neg \Cap(x \sqcap \neg \Cap z) \sqcap x \sqcap \neg \Cap C \sqcap (x \boxplus 1)^{\times})_{\neg \Cap z} \\
= & \quad \langle \text{ by (4.3) with } x, t := x, \Cap z, \text{ Proposition 3.14-7, Corollaries 3.21-4 and 3.21-3, Lemma 3.17-5 and Remark 4.8 } \rangle \\
& ((x \sqcap \Cap z \boxplus (x_{\Cap z} \sqcup x_{\neg \Cap z})) \sqcap \neg \Cap C \sqcap (x \boxplus 1)^{\times})_{\neg \Cap z}
\end{array}
$$

$$
\begin{array}{ll}
= & \langle \text{ by Remark 4.8, (3.21), Proposition 3.14-3} \\
& \quad \text{and Boolean algebra,} \\
& \quad \text{the domains of } x \mathbin{\triangleright} {}^{\Gamma}z \text{ and } x_{\Gamma z} \sqcup x_{\neg \Gamma z} \text{ are disjoint,} \\
& \quad \text{then apply Corollary 3.21-17 and Propositions} \\
& \quad 3.14\text{-}7 \text{ and } 3.14\text{-}20 \ \rangle \\
& (x \mathbin{\triangleright} {}^{\Gamma}z \mathbin{\triangleright} \neg {}^{\Gamma}C \mathbin{\triangleright} (x \mathbin{\barwedge} 1)^{\times} \mathbin{\barwedge} {}^{\Gamma}(x_{\Gamma z}) \mathbin{\triangleright} (x_{\Gamma z} \sqcup x_{\neg \Gamma z}) \mathbin{\triangleright} \neg {}^{\Gamma}C \mathbin{\triangleright} (x \mathbin{\barwedge} 1)^{\times})_{\neg \Gamma z} \\
= & \langle \text{ by Proposition 3.14-18, Boolean algebra,} \\
& \quad \text{Lemma 4.20-1, (3.20) and (4.4) with } x, t := x, {}^{\Gamma}z, \\
& \quad \mathsf{true} \iff {}^{\Gamma}(x \mathbin{\triangleright} {}^{\Gamma}z) \sqsubseteq {}^{\Gamma}(x \mathbin{\triangleright} {}^{\Gamma}z \mathbin{\triangleright} \neg {}^{\Gamma}C) \\
& \quad \iff \neg {}^{\Gamma}(x \mathbin{\triangleright} {}^{\Gamma}z \mathbin{\triangleright} \neg {}^{\Gamma}C) \sqsubseteq \neg {}^{\Gamma}(x \mathbin{\triangleright} {}^{\Gamma}z) \\
& \quad \iff \neg {}^{\Gamma}(x \mathbin{\triangleright} {}^{\Gamma}z \mathbin{\triangleright} \neg {}^{\Gamma}C \mathbin{\triangleright} (x \mathbin{\barwedge} 1)^{\times}) \sqsubseteq {}^{\Gamma}(x_{\Gamma z}) \\
& \quad \iff \neg {}^{\Gamma}(x \mathbin{\triangleright} {}^{\Gamma}z \mathbin{\triangleright} \neg {}^{\Gamma}C \mathbin{\triangleright} (x \mathbin{\barwedge} 1)^{\times}) \mathbin{\triangleright} {}^{\Gamma}(x_{\Gamma z}) = {}^{\Gamma}(x_{\Gamma z}), \\
& \quad \text{then apply Corollary 4.30-1 and Propositions} \\
& \quad 4.22\text{-}5, 3.14\text{-}7 \text{ and } 3.14\text{-}20 \ \rangle \\
& (x \mathbin{\triangleright} {}^{\Gamma}z \mathbin{\triangleright} \neg {}^{\Gamma}C \mathbin{\triangleright} (x \mathbin{\barwedge} 1)^{\times})_{\neg \Gamma z} \mathbin{\barwedge} ((x_{\Gamma z} \sqcup x_{\neg \Gamma z}) \mathbin{\triangleright} \neg {}^{\Gamma}C \mathbin{\triangleright} (x \mathbin{\barwedge} 1)^{\times})_{\neg \Gamma z} \\
= & \langle \text{ by (4.69), Lemma 3.7-6 and Propositions 3.14-8} \\
& \quad \text{and } 3.14\text{-}1, \\
& \quad {}^{\Gamma}z \sqsubseteq {}^{\Gamma}C, \\
& \quad \text{then apply (3.9), (4.5) with } x, t := x, {}^{\Gamma}z, \text{ (4.6)} \\
& \quad \text{with } x, t := x, {}^{\Gamma}z \text{ and Boolean algebra} \ \rangle \\
& (x \mathbin{\triangleright} {}^{\Gamma}z \mathbin{\triangleright} \neg {}^{\Gamma}C \mathbin{\triangleright} (x \mathbin{\barwedge} 1)^{\times})_{\neg \Gamma z} \mathbin{\barwedge} \\
& (x_{\Gamma z} \mathbin{\triangleright} {}^{\Gamma}z \mathbin{\triangleright} \neg {}^{\Gamma}C \mathbin{\triangleright} (x \mathbin{\barwedge} 1)^{\times} \sqcup x_{\neg \Gamma z} \mathbin{\triangleright} \neg {}^{\Gamma}z \mathbin{\triangleright} (x \mathbin{\barwedge} 1)^{\times})_{\neg \Gamma z} \\
= & \langle \text{ by (4.69), (4.63), Proposition 4.22-2, (3.8),} \\
& \quad \text{Boolean algebra and (4.59)} \ \rangle \\
& (x \mathbin{\triangleright} ((x \mathbin{\barwedge} 1)^{\times})_{\Gamma z} \sqcup x \mathbin{\triangleright} ((x \mathbin{\barwedge} 1)^{\times})_{\neg \Gamma z})_{\neg \Gamma z} \mathbin{\barwedge} \\
& (x_{\Gamma z} \mathbin{\triangleright} ((x \mathbin{\barwedge} 1)^{\times})_{\Gamma z} \sqcup x_{\Gamma z} \mathbin{\triangleright} ((x \mathbin{\barwedge} 1)^{\times})_{\neg \Gamma z} \sqcup x_{\neg \Gamma z} \mathbin{\triangleright} (x \mathbin{\barwedge} 1)^{\times} \mathbin{\triangleright} \neg {}^{\Gamma}z)_{\neg \Gamma z} \\
= & \langle \text{ by (3.2), (4.5) with } x, t := (x \barwedge 1)^{\times}, {}^{\Gamma}z, \text{ (4.6) with} \\
& \quad x, t := (x \barwedge 1)^{\times}, {}^{\Gamma}z, \text{ Boolean algebra and Corollary} \\
& \quad 4.26\text{-}9 \ \rangle \\
& {}^{\Gamma}(x \mathbin{\triangleright} ((x \mathbin{\barwedge} 1)^{\times})_{\Gamma z}) \mathbin{\triangleright} x \mathbin{\triangleright} ((x \mathbin{\barwedge} 1)^{\times})_{\neg \Gamma z} \mathbin{\barwedge} \\
& {}^{\Gamma}(x_{\Gamma z} \mathbin{\triangleright} ((x \mathbin{\barwedge} 1)^{\times})_{\Gamma z}) \mathbin{\triangleright} (x_{\Gamma z} \mathbin{\triangleright} ((x \mathbin{\barwedge} 1)^{\times})_{\neg \Gamma z} \sqcup x_{\neg \Gamma z} \mathbin{\triangleright} (x \mathbin{\barwedge} 1)^{\times} \mathbin{\triangleright} \neg {}^{\Gamma}z) \\
= & \langle \text{ by Propositions 3.14-20 and 3.14-7, (3.20), (3.19)} \\
& \quad \text{and (4.4) with } x, t := (x \barwedge 1)^{\times}, {}^{\Gamma}z \ \rangle \\
& x \mathbin{\triangleright} ((x \mathbin{\barwedge} 1)^{\times})_{\neg \Gamma z} \mathbin{\barwedge} (x_{\Gamma z} \mathbin{\triangleright} ((x \mathbin{\barwedge} 1)^{\times})_{\neg \Gamma z} \sqcup x_{\neg \Gamma z} \mathbin{\triangleright} (x \mathbin{\barwedge} 1)^{\times} \mathbin{\triangleright} \neg {}^{\Gamma}z) \\
\sqsupseteq & \langle \text{ by Lemma 3.22-1} \ \rangle \\
& x \mathbin{\triangleright} ((x \mathbin{\barwedge} 1)^{\times})_{\neg \Gamma z} \mathbin{\barwedge} x_{\Gamma z} \mathbin{\triangleright} ((x \mathbin{\barwedge} 1)^{\times})_{\neg \Gamma z} \\
= & \langle \text{ by (4.64), Remark 4.8 and Corollary 3.21-17} \ \rangle
\end{array}
$$

$$(x \Box \ulcorner z \sqcap x_{\ulcorner z}) \Box ((x \sqcap 1)^{\times})_{\neg \ulcorner z}$$

$\sqsupseteq$ $\langle$ by (4.80) and Corollary 3.21-12 $\rangle$

$$\ulcorner x \Box \neg \ulcorner (x \Box \neg \ulcorner z) \Box B \Box (((x \sqcap 1)^{\times})_{\neg \ulcorner z} \sqcap C)$$

We have shown

$$\ulcorner x \Box \neg \ulcorner (x \Box \neg \ulcorner z) \Box B \Box (((x \sqcap 1)^{\times})_{\neg \ulcorner z} \sqcap C)$$
$$\sqsubseteq \ulcorner (x \Box \neg \ulcorner C) \Box \neg \ulcorner (x \Box \neg \ulcorner z) \Box (A \sqcup ((x \sqcap 1)^{\times})_{\neg \ulcorner z}) \ .$$

By Proposition 3.14-6 and Lemma 3.17-1, this is equivalent to

$$\ulcorner (x \Box \neg \ulcorner C) \Box \neg \ulcorner (x \Box \neg \ulcorner z) \Box B \Box (((x \sqcap 1)^{\times})_{\neg \ulcorner z} \sqcap C)$$
$$\sqsubseteq \ulcorner (x \Box \neg \ulcorner C) \Box \neg \ulcorner (x \Box \neg \ulcorner z) \Box (A \sqcup ((x \sqcap 1)^{\times})_{\neg \ulcorner z})$$

which corresponds to (4.86) restricted to the test

$$\ulcorner (x \Box \neg \ulcorner C) \Box \neg \ulcorner (x \Box \neg \ulcorner z) \ .$$

D. Test $\ulcorner (x_{\ulcorner C}) \Box \neg \ulcorner (x \Box \neg \ulcorner z)$.
Firstly, we show

$$x_{\ulcorner C} \Box C \sqsubseteq \ulcorner (x_{\ulcorner C}) \Box \neg \ulcorner (x \Box \neg \ulcorner z) \Box A \ . \qquad (4.90)$$

$$\ulcorner (x_{\ulcorner C}) \Box \neg \ulcorner (x \Box \neg \ulcorner z) \Box A$$

$=$ $\langle$ by (4.4) with $x, t := x, \ulcorner C$ and Boolean algebra $\rangle$

$$\ulcorner (x_{\ulcorner C}) \Box \ulcorner x \Box \neg \ulcorner (x \Box \neg \ulcorner z) \Box A$$

$\sqsupseteq$ $\langle$ by (4.81) $\rangle$

$$\ulcorner (x_{\ulcorner C}) \Box (x \Box \ulcorner z \sqcap x_{\ulcorner z}) \Box B^{\times}$$

$=$ $\langle$ by Corollary 3.21-9, (4.4) with $x, t := x, \ulcorner z$, Proposition 3.14-7 and Boolean algebra $\rangle$

$$\ulcorner (x_{\ulcorner C}) \Box (x \Box \ulcorner z \sqcap_{\ulcorner (x \Box \ulcorner z)} x_{\ulcorner z}) \Box B^{\times}$$

$=$ $\langle$ by Propositions 3.20-8 and 4.22-5 $\rangle$

$$(\ulcorner (x_{\ulcorner C}) \Box x \Box \ulcorner z \sqcap_{\ulcorner (x \Box \ulcorner z)} (\ulcorner (x_{\ulcorner C}) \Box x)_{\ulcorner z}) \Box B^{\times}$$

$\sqsupseteq$ $\langle$ by Propositions 4.22-2 and 3.20-14, and (3.15) $\rangle$

$$(x_{\ulcorner C} \Box \ulcorner z \sqcap_{\ulcorner (x \Box \ulcorner z)} (x_{\ulcorner C} \sqcup x_{\neg \ulcorner C})_{\ulcorner z}) \Box B^{\times}$$

$=$ $\langle$ by Lemma 3.7-6 and (4.69),
$\ulcorner z \sqsubseteq (x \sqcap 1)^{\times} \Box \ulcorner z = \ulcorner C$,
then apply (4.5) with $x, t := x, \ulcorner z$, (4.6) with $x, t := x, \ulcorner z$, Corollary 4.26-5 and Boolean algebra $\rangle$

$$
\begin{array}{ll}
 & \Big(x_{\Cap C} \between_{\Cap(x \cup \Cap z)} (\Cap(x_{\neg \Cap C} \cup \neg \Cap z) \cup x_{\Cap C} \between (x_{\Cap C} \sqcup (x_{\neg \Cap C})_{\Cap z}))\Big) \cup B^{\times} \\
= & \quad \langle \text{ by (4.4) with } x, t := x_{\neg \Cap C}, \Cap z \\
 & \quad \text{and Boolean algebra,} \\
 & \quad \neg \Cap(x_{\neg \Cap C} \cup \neg \Cap z) \cup \Cap(x_{\neg \Cap C})_{\Cap z} = \Cap(x_{\neg \Cap C})_{\Cap z}, \\
 & \quad \text{then apply Propositions 3.14-7 and 3.14-20, and} \\
 & \quad \text{Corollary 3.21-9 } \rangle \\
 & \Big(x_{\Cap C} \between_{\Cap(x \cup \Cap z)} (x_{\Cap C} \between_{\Cap(x_{\neg \Cap C} \cup \neg \Cap z)} (x_{\Cap C} \sqcup (x_{\neg \Cap C})_{\Cap z}))\Big) \cup B^{\times} \\
\sqsupseteq & \quad \langle \text{ by (3.15) and Proposition 3.20-15 } \rangle \\
 & (x_{\Cap C} \between_{\Cap(x \cup \Cap z)} (x_{\Cap C} \between_{\Cap(x_{\neg \Cap C} \cup \neg \Cap z)} x_{\Cap C})) \cup B^{\times} \\
= & \quad \langle \text{ by Proposition 3.20-13 } \rangle \\
 & x_{\Cap C} \cup B^{\times} \\
\sqsupseteq & \quad \langle \text{ by (4.5) with } x, t := x, \Cap C \text{ and (4.78) } \rangle \\
 & x_{\Cap C} \cup C
\end{array}
$$

Secondly, we prove

$$
\begin{array}{l}
\Cap(x_{\neg \Cap C} \cup \Cap z \cup ((x \between 1)^{\times})_{\neg \Cap z}) \cup \\
\Cap(x_{\neg \Cap C} \cup \neg \Cap z \cup (x \between 1)^{\times} \between (x_{\neg \Cap C})_{\Cap z} \cup ((x \between 1)^{\times})_{\neg \Cap z}) = \top \ . \qquad (4.91)
\end{array}
$$

$$
\begin{array}{ll}
 & \Cap(x_{\neg \Cap C} \cup \Cap z \cup ((x \between 1)^{\times})_{\neg \Cap z}) \cup \\
 & \Cap(x_{\neg \Cap C} \cup \neg \Cap z \cup (x \between 1)^{\times} \between (x_{\neg \Cap C})_{\Cap z} \cup ((x \between 1)^{\times})_{\neg \Cap z}) \\
\sqsupseteq & \quad \langle \text{ by Proposition 3.14-18 and Corollary 3.21-16 } \rangle \\
 & \Cap(x_{\neg \Cap C} \cup \Cap z) \cup (\Cap(x_{\neg \Cap C} \cup \neg \Cap z \cup (x \between 1)^{\times}) \between \Cap((x_{\neg \Cap C})_{\Cap z} \cup ((x \between 1)^{\times})_{\neg \Cap z})) \\
\sqsupseteq & \quad \langle \text{ by Proposition 3.14-18 } \rangle \\
 & \Cap(x_{\neg \Cap C} \cup \Cap z) \cup (\Cap(x_{\neg \Cap C} \cup \neg \Cap z) \between \Cap((x_{\neg \Cap C})_{\Cap z})) \\
= & \quad \langle \text{ by Remark 4.8 and Boolean algebra } \rangle \\
 & \top
\end{array}
$$

Thirdly, we prove

$$
\begin{array}{ll}
 & x_{\neg \Cap C} \cup \Cap z \cup ((x \between 1)^{\times})_{\neg \Cap z} \between (x_{\neg \Cap C})_{\Cap z} \cup ((x \between 1)^{\times})_{\neg \Cap z} \between \\
 & x_{\neg \Cap C} \cup \neg \Cap z \cup (x \between 1)^{\times} \qquad (4.92) \\
\sqsubseteq & \Cap(x_{\Cap C}) \cup \neg \Cap(x \cup \neg \Cap z) \cup ((x \between 1)^{\times})_{\neg \Cap z}
\end{array}
$$

using (4.91).

$$
\begin{array}{ll}
 & \Cap(x_{\Cap C}) \cup \neg \Cap(x \cup \neg \Cap z) \cup ((x \between 1)^{\times})_{\neg \Cap z} \\
= & \quad \langle \text{ by (4.79) and (4.59) } \rangle
\end{array}
$$

$$
\begin{array}{ll}
& {}^{\Gamma\!\!\Gamma}(x_{\Gamma\!\!\Gamma C}) \circ \neg {}^{\Gamma\!\!\Gamma}(x \circ \neg {}^{\Gamma\!\!\Gamma} z) \circ ({}^{\Gamma\!\!\Gamma} z \circ x \circ \neg {}^{\Gamma\!\!\Gamma} z \circ (x \pitchfork 1)^{\times} \pitchfork (x \circ (x \pitchfork 1)^{\times})_{\neg \Gamma\!\!\Gamma z}) \\
= & \quad \langle \text{ by Corollary 3.21-4 and Proposition 4.22-5 } \rangle \\
& {}^{\Gamma\!\!\Gamma}(x_{\Gamma\!\!\Gamma C}) \circ \neg {}^{\Gamma\!\!\Gamma}(x \circ \neg {}^{\Gamma\!\!\Gamma} z) \circ {}^{\Gamma\!\!\Gamma} z \circ x \circ \neg {}^{\Gamma\!\!\Gamma} z \circ (x \pitchfork 1)^{\times} \pitchfork \\
& ({}^{\Gamma\!\!\Gamma}(x_{\Gamma\!\!\Gamma C}) \circ \neg {}^{\Gamma\!\!\Gamma}(x \circ \neg {}^{\Gamma\!\!\Gamma} z) \circ x \circ (x \pitchfork 1)^{\times})_{\neg \Gamma\!\!\Gamma z} \\
= & \quad \langle \text{ by Boolean algebra, Proposition 3.14-17, (3.6) and} \\
& \quad \text{Corollary 3.21-3 } \rangle \\
& ({}^{\Gamma\!\!\Gamma}(x_{\Gamma\!\!\Gamma C}) \circ \neg {}^{\Gamma\!\!\Gamma}(x \circ \neg {}^{\Gamma\!\!\Gamma} z) \circ x \circ (x \pitchfork 1)^{\times})_{\neg \Gamma\!\!\Gamma z} \\
= & \quad \langle \text{ by (4.3) with } x, t := x, {}^{\Gamma\!\!\Gamma} z, \text{ Propositions 3.14-7,} \\
& \quad \text{3.14-17 and 3.14-20, Corollaries 3.21-4 and 3.21-3,} \\
& \quad \text{Lemma 3.17-5, (4.4) with } x, t := x, {}^{\Gamma\!\!\Gamma} z \text{ and Boolean} \\
& \quad \text{algebra } \rangle \\
& ({}^{\Gamma\!\!\Gamma}(x_{\Gamma\!\!\Gamma C}) \circ (x \circ {}^{\Gamma\!\!\Gamma} z \pitchfork (x_{\Gamma\!\!\Gamma z} \sqcup x_{\neg \Gamma\!\!\Gamma z})) \circ (x \pitchfork 1)^{\times})_{\neg \Gamma\!\!\Gamma z} \\
= & \quad \langle \text{ by Remark 4.8,} \\
& \quad \text{the domains of } x \circ {}^{\Gamma\!\!\Gamma} z \text{ and } x_{\Gamma\!\!\Gamma z} \sqcup x_{\neg \Gamma\!\!\Gamma z} \text{ are disjoint,} \\
& \quad \text{then apply Corollaries 3.21-4, 3.21-17 and 4.30-2 } \rangle \\
& ({}^{\Gamma\!\!\Gamma}(x_{\Gamma\!\!\Gamma C}) \circ x \circ {}^{\Gamma\!\!\Gamma} z \circ (x \pitchfork 1)^{\times})_{\neg \Gamma\!\!\Gamma z} \pitchfork ({}^{\Gamma\!\!\Gamma}(x_{\Gamma\!\!\Gamma C}) \circ (x_{\Gamma\!\!\Gamma z} \sqcup x_{\neg \Gamma\!\!\Gamma z}) \circ (x \pitchfork 1)^{\times})_{\neg \Gamma\!\!\Gamma z} \\
= & \quad \langle \text{ by (3.8) and Propositions 4.22-5 and 4.22-2 } \rangle \\
& ((x_{\Gamma\!\!\Gamma C} \sqcup x_{\neg \Gamma\!\!\Gamma C}) \circ {}^{\Gamma\!\!\Gamma} z \circ (x \pitchfork 1)^{\times})_{\neg \Gamma\!\!\Gamma z} \pitchfork \\
& \Big(((x_{\Gamma\!\!\Gamma C} \sqcup x_{\neg \Gamma\!\!\Gamma C})_{\Gamma\!\!\Gamma z} \sqcup (x_{\Gamma\!\!\Gamma C} \sqcup x_{\neg \Gamma\!\!\Gamma C})_{\neg \Gamma\!\!\Gamma z}) \circ (x \pitchfork 1)^{\times}\Big)_{\neg \Gamma\!\!\Gamma z} \\
= & \quad \langle \text{ by Lemma 3.7-6 and (4.69),} \\
& \quad {}^{\Gamma\!\!\Gamma} z \sqsubseteq (x \pitchfork 1)^{\times} \circ {}^{\Gamma\!\!\Gamma} z = {}^{\Gamma\!\!\Gamma} C, \\
& \quad \text{then apply (3.9), (3.2), (4.5) with } x, t := x, {}^{\Gamma\!\!\Gamma} C, \\
& \quad \text{Boolean algebra and Corollaries 4.26-6 and 4.26-8 } \rangle \\
& (x_{\Gamma\!\!\Gamma C} \circ (x \pitchfork 1)^{\times} \sqcup x_{\neg \Gamma\!\!\Gamma C} \circ {}^{\Gamma\!\!\Gamma} z \circ (x \pitchfork 1)^{\times})_{\neg \Gamma\!\!\Gamma z} \pitchfork \\
& \Big(\Big(({}^{\Gamma\!\!\Gamma}(x_{\neg \Gamma\!\!\Gamma C} \circ \neg {}^{\Gamma\!\!\Gamma} z) \circ x_{\Gamma\!\!\Gamma C} \pitchfork (x_{\Gamma\!\!\Gamma C} \sqcup (x_{\neg \Gamma\!\!\Gamma C})_{\Gamma\!\!\Gamma z})) \sqcup \\
& \quad (x_{\neg \Gamma\!\!\Gamma C} \circ \neg {}^{\Gamma\!\!\Gamma} z \pitchfork (x_{\neg \Gamma\!\!\Gamma C})_{\neg \Gamma\!\!\Gamma z})\Big) \circ (x \pitchfork 1)^{\times}\Big)_{\neg \Gamma\!\!\Gamma z} \\
= & \quad \langle \text{ by (3.21), Remark 4.8 and Boolean algebra,} \\
& \quad \text{the domains of } x_{\Gamma\!\!\Gamma C} \sqcup (x_{\neg \Gamma\!\!\Gamma C})_{\Gamma\!\!\Gamma z} \text{ and } x_{\neg \Gamma\!\!\Gamma C} \circ \neg {}^{\Gamma\!\!\Gamma} z \\
& \quad \text{are disjoint} \\
& \quad \text{and the domains of } {}^{\Gamma\!\!\Gamma}(x_{\neg \Gamma\!\!\Gamma C} \circ \neg {}^{\Gamma\!\!\Gamma} z) \circ x_{\Gamma\!\!\Gamma C} \text{ and } (x_{\neg \Gamma\!\!\Gamma C})_{\neg \Gamma\!\!\Gamma z} \\
& \quad \text{are disjoint,} \\
& \quad \text{then apply Lemma 3.22-7 } \rangle \\
& (x_{\Gamma\!\!\Gamma C} \circ (x \pitchfork 1)^{\times} \sqcup x_{\neg \Gamma\!\!\Gamma C} \circ {}^{\Gamma\!\!\Gamma} z \circ (x \pitchfork 1)^{\times})_{\neg \Gamma\!\!\Gamma z} \pitchfork \\
& \Big(\Big(({}^{\Gamma\!\!\Gamma}(x_{\neg \Gamma\!\!\Gamma C} \circ \neg {}^{\Gamma\!\!\Gamma} z) \circ x_{\Gamma\!\!\Gamma C} \sqcup x_{\neg \Gamma\!\!\Gamma C} \circ \neg {}^{\Gamma\!\!\Gamma} z) \pitchfork \\
& \quad (x_{\Gamma\!\!\Gamma C} \sqcup (x_{\neg \Gamma\!\!\Gamma C})_{\Gamma\!\!\Gamma z} \sqcup (x_{\neg \Gamma\!\!\Gamma C})_{\neg \Gamma\!\!\Gamma z})\Big) \circ (x \pitchfork 1)^{\times}\Big)_{\neg \Gamma\!\!\Gamma z}
\end{array}
$$

$$
\begin{array}{ll}
= & \langle \text{ by (3.21), Proposition 3.14-9 and Remark 4.8,} \\
& \quad \text{the domains of } {}^{\sqcap}(x_{\neg\sqcap C} \triangleright \neg {}^{\sqcap} z) \triangleright x_{\sqcap C} \sqcup x_{\neg\sqcap C} \triangleright \neg {}^{\sqcap} z \\
& \quad \text{and } x_{\sqcap C} \sqcup (x_{\neg\sqcap C})_{\sqcap z} \sqcup (x_{\neg\sqcap C})_{\neg\sqcap z} \\
& \quad \text{are disjoint,} \\
& \quad \text{then apply Corollary 3.21-17 and (3.9) } \rangle \\
& (x_{\sqcap C} \triangleright (x \boxplus 1)^{\times} \sqcup x_{\neg\sqcap C} \triangleright {}^{\sqcap} z \triangleright (x \boxplus 1)^{\times})_{\neg\sqcap z} \boxplus \\
& \Big(({}^{\sqcap}(x_{\neg\sqcap C} \triangleright \neg {}^{\sqcap} z) \triangleright x_{\sqcap C} \triangleright (x \boxplus 1)^{\times} \sqcup x_{\neg\sqcap C} \triangleright \neg {}^{\sqcap} z \triangleright (x \boxplus 1)^{\times}) \boxplus \\
& \quad (x_{\sqcap C} \triangleright (x \boxplus 1)^{\times} \sqcup (x_{\neg\sqcap C})_{\sqcap z} \triangleright (x \boxplus 1)^{\times} \sqcup (x_{\neg\sqcap C})_{\neg\sqcap z} \triangleright (x \boxplus 1)^{\times}) \Big)_{\neg\sqcap z} \\
= & \quad \langle \text{ by Propositions 3.14-20, 3.14-9 and 3.14-7,} \\
& \quad (4.4) \text{ with } x, t := x_{\neg\sqcap C}, {}^{\sqcap} z \text{ and Boolean algebra,} \\
& \quad \text{the domains of} \\
& \quad {}^{\sqcap}(x_{\neg\sqcap C} \triangleright \neg {}^{\sqcap} z) \triangleright x_{\sqcap C} \triangleright (x \boxplus 1)^{\times} \sqcup x_{\neg\sqcap C} \triangleright \neg {}^{\sqcap} z \triangleright (x \boxplus 1)^{\times} \\
& \quad \text{and} \\
& \quad x_{\sqcap C} \triangleright (x \boxplus 1)^{\times} \sqcup (x_{\neg\sqcap C})_{\sqcap z} \triangleright (x \boxplus 1)^{\times} \sqcup (x_{\neg\sqcap C})_{\neg\sqcap z} \triangleright (x \boxplus 1)^{\times} \\
& \quad \text{are disjoint,} \\
& \quad \text{then apply Corollary 4.30-2 } \rangle \\
& (x_{\sqcap C} \triangleright (x \boxplus 1)^{\times} \sqcup x_{\neg\sqcap C} \triangleright {}^{\sqcap} z \triangleright (x \boxplus 1)^{\times})_{\neg\sqcap z} \boxplus \\
& ({}^{\sqcap}(x_{\neg\sqcap C} \triangleright \neg {}^{\sqcap} z) \triangleright x_{\sqcap C} \triangleright (x \boxplus 1)^{\times} \sqcup x_{\neg\sqcap C} \triangleright \neg {}^{\sqcap} z \triangleright (x \boxplus 1)^{\times})_{\neg\sqcap z} \boxplus \\
& (x_{\sqcap C} \triangleright (x \boxplus 1)^{\times} \sqcup (x_{\neg\sqcap C})_{\sqcap z} \triangleright (x \boxplus 1)^{\times} \sqcup (x_{\neg\sqcap C})_{\neg\sqcap z} \triangleright (x \boxplus 1)^{\times})_{\neg\sqcap z} \\
= & \quad \langle \text{ by (4.5) with } x, t := x, {}^{\sqcap} C, (4.6) \text{ with } x, t := x, {}^{\sqcap} C \\
& \quad \text{and Proposition 4.22-7 } \rangle \\
& (x_{\sqcap C} \triangleright {}^{\sqcap} C \triangleright (x \boxplus 1)^{\times} \sqcup x_{\neg\sqcap C} \triangleright \neg {}^{\sqcap} C \triangleright {}^{\sqcap} z \triangleright (x \boxplus 1)^{\times})_{\neg\sqcap z} \boxplus \\
& ({}^{\sqcap}(x_{\neg\sqcap C} \triangleright \neg {}^{\sqcap} z) \triangleright x_{\sqcap C} \triangleright {}^{\sqcap} C \triangleright (x \boxplus 1)^{\times} \sqcup x_{\neg\sqcap C} \triangleright \neg {}^{\sqcap} z \triangleright (x \boxplus 1)^{\times})_{\neg\sqcap z} \boxplus \\
& (x_{\sqcap C} \triangleright {}^{\sqcap} C \triangleright (x \boxplus 1)^{\times} \sqcup (x_{\neg\sqcap C})_{\sqcap z} \triangleright \neg {}^{\sqcap} C \triangleright {}^{\sqcap} z \triangleright (x \boxplus 1)^{\times} \sqcup \\
& \quad (x_{\neg\sqcap C})_{\neg\sqcap z} \triangleright \neg {}^{\sqcap} z \triangleright (x \boxplus 1)^{\times})_{\neg\sqcap z} \\
= & \quad \langle \text{ by (4.69), (3.19), (4.63), (4.59) and (4.4) with} \\
& \quad x, t := (x \boxplus 1)^{\times}, {}^{\sqcap} z \rangle \\
& (x_{\sqcap C} \triangleright (x \boxplus 1)^{\times} \triangleright {}^{\sqcap} z \sqcup x_{\neg\sqcap C} \triangleright {}^{\sqcap}(((x \boxplus 1)^{\times})_{\sqcap z}) \triangleright (x \boxplus 1)^{\times})_{\neg\sqcap z} \boxplus \\
& ({}^{\sqcap}(x_{\neg\sqcap C} \triangleright \neg {}^{\sqcap} z) \triangleright x_{\sqcap C} \triangleright (x \boxplus 1)^{\times} \triangleright {}^{\sqcap} z \sqcup x_{\neg\sqcap C} \triangleright (x \boxplus 1)^{\times} \triangleright \neg {}^{\sqcap} z)_{\neg\sqcap z} \boxplus \\
& (x_{\sqcap C} \triangleright (x \boxplus 1)^{\times} \triangleright {}^{\sqcap} z \sqcup (x_{\neg\sqcap C})_{\sqcap z} \triangleright {}^{\sqcap}(((x \boxplus 1)^{\times})_{\sqcap z}) \triangleright (x \boxplus 1)^{\times} \sqcup \\
& \quad (x_{\neg\sqcap C})_{\neg\sqcap z} \triangleright (x \boxplus 1)^{\times} \triangleright \neg {}^{\sqcap} z)_{\neg\sqcap z} \\
= & \quad \langle \text{ by Proposition 4.22-2 and (3.8) } \rangle \\
& (x_{\sqcap C} \triangleright (x \boxplus 1)^{\times} \triangleright {}^{\sqcap} z \sqcup x_{\neg\sqcap C} \triangleright ((x \boxplus 1)^{\times})_{\sqcap z} \sqcup x_{\neg\sqcap C} \triangleright ((x \boxplus 1)^{\times})_{\neg\sqcap z})_{\neg\sqcap z} \boxplus \\
& ({}^{\sqcap}(x_{\neg\sqcap C} \triangleright \neg {}^{\sqcap} z) \triangleright x_{\sqcap C} \triangleright (x \boxplus 1)^{\times} \triangleright {}^{\sqcap} z \sqcup x_{\neg\sqcap C} \triangleright (x \boxplus 1)^{\times} \triangleright \neg {}^{\sqcap} z)_{\neg\sqcap z} \boxplus \\
& (x_{\sqcap C} \triangleright (x \boxplus 1)^{\times} \triangleright {}^{\sqcap} z \sqcup (x_{\neg\sqcap C})_{\sqcap z} \triangleright ((x \boxplus 1)^{\times})_{\sqcap z} \sqcup \\
& \quad (x_{\neg\sqcap C})_{\sqcap z} \triangleright ((x \boxplus 1)^{\times})_{\neg\sqcap z} \sqcup (x_{\neg\sqcap C})_{\neg\sqcap z} \triangleright (x \boxplus 1)^{\times} \triangleright \neg {}^{\sqcap} z)_{\neg\sqcap z}
\end{array}
$$

$$
\begin{array}{ll}
= & \quad \langle \text{ by (3.2), (4.5) with } x,t := (x \pitchfork 1)^{\times}, {}^{\sqcap}z, \text{ (4.6) with} \\
& \quad\ x,t := (x \pitchfork 1)^{\times}, {}^{\sqcap}z, \text{ (3.9) and Corollary 4.26-9 } \rangle \\
& {}^{\sqcap}(x_{\sqcap C} \triangleleft (x \pitchfork 1)^{\times} \triangleleft {}^{\sqcap}z \sqcup x_{\neg\sqcap C} \triangleleft ((x \pitchfork 1)^{\times})_{\sqcap z}) \triangleleft x_{\neg\sqcap C} \triangleleft ((x \pitchfork 1)^{\times})_{\neg\sqcap z} \pitchfork \\
& {}^{\sqcap}({}^{\sqcap}(x_{\neg\sqcap C} \triangleleft \neg{}^{\sqcap}z) \triangleleft x_{\sqcap C} \triangleleft (x \pitchfork 1)^{\times} \triangleleft {}^{\sqcap}z) \triangleleft x_{\neg\sqcap C} \triangleleft (x \pitchfork 1)^{\times} \triangleleft \neg{}^{\sqcap}z \pitchfork \\
& {}^{\sqcap}(x_{\sqcap C} \triangleleft (x \pitchfork 1)^{\times} \triangleleft {}^{\sqcap}z \sqcup (x_{\neg\sqcap C})_{\sqcap z} \triangleleft ((x \pitchfork 1)^{\times})_{\sqcap z}) \triangleleft \\
& \quad ((x_{\neg\sqcap C})_{\sqcap z} \triangleleft ((x \pitchfork 1)^{\times})_{\neg\sqcap z} \sqcup (x_{\neg\sqcap C})_{\neg\sqcap z} \triangleleft (x \pitchfork 1)^{\times} \triangleleft \neg{}^{\sqcap}z) \\
\sqsupseteq & \quad \langle \text{ by (4.59), (4.64), (3.15) and Lemmas 3.7-1 and 3.22-1} \\
& \quad\ \rangle \\
& {}^{\sqcap}(x_{\sqcap C} \triangleleft (x \pitchfork 1)^{\times} \triangleleft {}^{\sqcap}z \sqcup x_{\neg\sqcap C} \triangleleft ((x \pitchfork 1)^{\times})_{\sqcap z}) \triangleleft x_{\neg\sqcap C} \triangleleft {}^{\sqcap}z \triangleleft ((x \pitchfork 1)^{\times})_{\neg\sqcap z} \pitchfork \\
& {}^{\sqcap}({}^{\sqcap}(x_{\neg\sqcap C} \triangleleft \neg{}^{\sqcap}z) \triangleleft x_{\sqcap C} \triangleleft (x \pitchfork 1)^{\times} \triangleleft {}^{\sqcap}z) \triangleleft x_{\neg\sqcap C} \triangleleft \neg{}^{\sqcap}z \triangleleft (x \pitchfork 1)^{\times} \pitchfork \\
& (x_{\neg\sqcap C})_{\sqcap z} \triangleleft ((x \pitchfork 1)^{\times})_{\neg\sqcap z} \\
\sqsupseteq & \quad \langle \text{ by Lemma 3.7-1,} \\
& \quad\ x_{\neg\sqcap C} \triangleleft \neg{}^{\sqcap}z \triangleleft (x \pitchfork 1)^{\times} \\
& \quad\ \sqsubseteq {}^{\sqcap}({}^{\sqcap}(x_{\neg\sqcap C} \triangleleft \neg{}^{\sqcap}z) \triangleleft x_{\sqcap C} \triangleleft (x \pitchfork 1)^{\times} \triangleleft {}^{\sqcap}z) \triangleleft x_{\neg\sqcap C} \triangleleft \neg{}^{\sqcap}z \triangleleft (x \pitchfork 1)^{\times}, \\
& \quad\ \text{then apply Lemma 3.22-1 } \rangle \\
& {}^{\sqcap}(x_{\sqcap C} \triangleleft (x \pitchfork 1)^{\times} \triangleleft {}^{\sqcap}z \sqcup x_{\neg\sqcap C} \triangleleft ((x \pitchfork 1)^{\times})_{\sqcap z}) \triangleleft x_{\neg\sqcap C} \triangleleft {}^{\sqcap}z \triangleleft ((x \pitchfork 1)^{\times})_{\neg\sqcap z} \pitchfork \\
& x_{\neg\sqcap C} \triangleleft \neg{}^{\sqcap}z \triangleleft (x \pitchfork 1)^{\times} \pitchfork (x_{\neg\sqcap C})_{\sqcap z} \triangleleft ((x \pitchfork 1)^{\times})_{\neg\sqcap z} \\
\sqsupseteq & \quad \langle \text{ by Lemma 3.7-1,} \\
& \quad\ x_{\neg\sqcap C} \triangleleft {}^{\sqcap}z \triangleleft ((x \pitchfork 1)^{\times})_{\neg\sqcap z} \\
& \quad\ \sqsubseteq {}^{\sqcap}(x_{\sqcap C} \triangleleft (x \pitchfork 1)^{\times} \triangleleft {}^{\sqcap}z \sqcup x_{\neg\sqcap C} \triangleleft ((x \pitchfork 1)^{\times})_{\sqcap z}) \triangleleft \\
& \quad\quad x_{\neg\sqcap C} \triangleleft {}^{\sqcap}z \triangleleft ((x \pitchfork 1)^{\times})_{\neg\sqcap z}; \\
& \quad\ \text{by Proposition 3.14-9, (4.91) and Boolean algebra,} \\
& \quad\ \text{the domains of} \\
& \quad\ {}^{\sqcap}(x_{\sqcap C} \triangleleft (x \pitchfork 1)^{\times} \triangleleft {}^{\sqcap}z \sqcup x_{\neg\sqcap C} \triangleleft ((x \pitchfork 1)^{\times})_{\sqcap z}) \triangleleft \\
& \quad\ x_{\neg\sqcap C} \triangleleft {}^{\sqcap}z \triangleleft ((x \pitchfork 1)^{\times})_{\neg\sqcap z} \\
& \quad\ \text{and} \\
& \quad\ x_{\neg\sqcap C} \triangleleft \neg{}^{\sqcap}z \triangleleft (x \pitchfork 1)^{\times} \pitchfork (x_{\neg\sqcap C})_{\sqcap z} \triangleleft ((x \pitchfork 1)^{\times})_{\neg\sqcap z} \\
& \quad\ \text{are disjoint;} \\
& \quad\ \text{then apply and Lemma 3.22-4 } \rangle \\
& x_{\neg\sqcap C} \triangleleft {}^{\sqcap}z \triangleleft ((x \pitchfork 1)^{\times})_{\neg\sqcap z} \pitchfork x_{\neg\sqcap C} \triangleleft \neg{}^{\sqcap}z \triangleleft (x \pitchfork 1)^{\times} \pitchfork \\
& (x_{\neg\sqcap C})_{\sqcap z} \triangleleft ((x \pitchfork 1)^{\times})_{\neg\sqcap z} \\
= & \quad \langle \text{ by Propositions 3.14-7 and 3.14-9, Boolean algebra} \\
& \quad\ \text{and Remark 4.8,} \\
& \quad\ \text{the domains of } x_{\neg\sqcap C} \triangleleft \neg{}^{\sqcap}z \triangleleft (x \pitchfork 1)^{\times} \\
& \quad\ \text{and } (x_{\neg\sqcap C})_{\sqcap z} \triangleleft ((x \pitchfork 1)^{\times})_{\neg\sqcap z} \\
& \quad\ \text{are disjoint,} \\
& \quad\ \text{then apply (3.25) } \rangle
\end{array}
$$

$$x_{\neg\Cap C}{\sqcap}{}^{\Cap}z{\sqcap}((x \barwedge 1)^{\times})_{\neg\Cap z} \barwedge (x_{\neg\Cap C})_{\Cap z}{\sqcap}((x \barwedge 1)^{\times})_{\neg\Cap z} \barwedge$$
$$x_{\neg\Cap C}{\sqcap}\neg{}^{\Cap}z{\sqcap}(x \barwedge 1)^{\times}$$

Finally, we use (4.90) and (4.92) in the proof of (4.86) restricted to the test

$$^{\Cap}(x_{\Cap C}){\sqcap}\neg{}^{\Cap}(x{\sqcap}\neg{}^{\Cap}z) \ .$$

$$\begin{array}{ll}
& {}^{\Cap}(x_{\Cap C}){\sqcap}\neg{}^{\Cap}(x{\sqcap}\neg{}^{\Cap}z){\sqcap}(A \sqcup ((x \barwedge 1)^{\times})_{\neg\Cap z}) \\
\sqsupseteq & \quad \langle \text{ by (3.8), (4.90) and (4.92) } \rangle \\
& x_{\Cap C}{\sqcap}C \sqcup (x_{\neg\Cap C}{\sqcap}{}^{\Cap}z{\sqcap}((x \barwedge 1)^{\times})_{\neg\Cap z} \barwedge \\
& (x_{\neg\Cap C})_{\Cap z}{\sqcap}((x \barwedge 1)^{\times})_{\neg\Cap z} \barwedge x_{\neg\Cap C}{\sqcap}\neg{}^{\Cap}z{\sqcap}(x \barwedge 1)^{\times}) \\
= & \quad \langle \text{ by Corollary 3.21-14 } \rangle \\
& (x_{\Cap C}{\sqcap}C \sqcup x_{\neg\Cap C}{\sqcap}{}^{\Cap}z{\sqcap}((x \barwedge 1)^{\times})_{\neg\Cap z}) \barwedge \\
& (x_{\Cap C}{\sqcap}C \sqcup (x_{\neg\Cap C})_{\Cap z}{\sqcap}((x \barwedge 1)^{\times})_{\neg\Cap z}) \barwedge \\
& (x_{\Cap C}{\sqcap}C \sqcup x_{\neg\Cap C}{\sqcap}\neg{}^{\Cap}z{\sqcap}(x \barwedge 1)^{\times}) \\
\sqsupseteq & \quad \langle \text{ by Propositions 3.14-7 and 3.14-20, (3.15) and} \\
& \quad \text{Lemma 3.22-1 } \rangle \\
& (x_{\Cap C}{\sqcap}C \sqcup x_{\neg\Cap C}{\sqcap}{}^{\Cap}z{\sqcap}((x \barwedge 1)^{\times})_{\neg\Cap z}) \barwedge \\
& (x_{\Cap C}{\sqcap}C \sqcup (x_{\neg\Cap C})_{\Cap z}{\sqcap}((x \barwedge 1)^{\times})_{\neg\Cap z}) \barwedge {}^{\Cap}(x_{\neg\Cap C}{\sqcap}\neg{}^{\Cap}z){\sqcap}x_{\Cap C}{\sqcap}C \\
= & \quad \langle \text{ by (4.69), (4.63) and Boolean algebra,} \\
& \quad {}^{\Cap}C{\sqcap}{}^{\Cap}(((x \barwedge 1)^{\times})_{\neg\Cap z}) = \top, \\
& \quad \text{then apply (4.5) with } x, t := x, {}^{\Cap}C, \text{ (3.9),} \\
& \quad \text{Corollaries 3.21-4 and 3.21-3, Propositions 3.14-7} \\
& \quad \text{and 4.22-7, Boolean algebra and (3.6) } \rangle \\
& (x_{\Cap C} \sqcup x_{\neg\Cap C}{\sqcap}{}^{\Cap}z){\sqcap}(C \barwedge ((x \barwedge 1)^{\times})_{\neg\Cap z}) \barwedge \\
& (x_{\Cap C} \sqcup (x_{\neg\Cap C})_{\Cap z}){\sqcap}(C \barwedge ((x \barwedge 1)^{\times})_{\neg\Cap z}) \barwedge \\
& {}^{\Cap}(x_{\neg\Cap C}{\sqcap}\neg{}^{\Cap}z){\sqcap}x_{\Cap C}{\sqcap}(C \barwedge ((x \barwedge 1)^{\times})_{\neg\Cap z}) \\
= & \quad \langle \text{ by Proposition 3.14-11, Remark 4.8 and Corollary} \\
& \quad \text{3.21-17 } \rangle \\
& ((x_{\Cap C} \sqcup x_{\neg\Cap C}{\sqcap}{}^{\Cap}z) \barwedge (x_{\Cap C} \sqcup (x_{\neg\Cap C})_{\Cap z}) \barwedge {}^{\Cap}(x_{\neg\Cap C}{\sqcap}\neg{}^{\Cap}z){\sqcap}x_{\Cap C}){\sqcap} \\
& (C \barwedge ((x \barwedge 1)^{\times})_{\neg\Cap z}) \\
= & \quad \langle \text{ by (3.21), Propositions 3.14-3 and 3.14-9,} \\
& \quad \text{and Remark 4.8,} \\
& \quad {}^{\Cap}(x_{\Cap C} \sqcup (x_{\neg\Cap C})_{\Cap z}){\sqcap}{}^{\Cap}({}^{\Cap}(x_{\neg\Cap C}{\sqcap}\neg{}^{\Cap}z){\sqcap}x_{\Cap C}) = \top \\
& \quad \text{and } {}^{\Cap}C{\sqcap}{}^{\Cap}(((x \barwedge 1)^{\times})_{\neg\Cap z}) = \top, \\
& \quad \text{then apply (3.25) } \rangle \\
& ((x_{\Cap C} \sqcup x_{\neg\Cap C}{\sqcap}{}^{\Cap}z) \barwedge {}^{\Cap}(x_{\neg\Cap C}{\sqcap}\neg{}^{\Cap}z){\sqcap}x_{\Cap C} \barwedge (x_{\Cap C} \sqcup (x_{\neg\Cap C})_{\Cap z})){\sqcap}
\end{array}$$

$$
\begin{array}{ll}
& (((x \pitchfork 1)^{\times})_{\neg \Cap z} \pitchfork C) \\
= & \quad \langle \text{ by Lemma 3.7-6 and (4.69),} \\
& \quad \Cap z \sqsubseteq (x \pitchfork 1)^{\times} \fatsemi \Cap z = \Cap C, \\
& \quad \text{then apply (4.5) with } x, t := x, \Cap C, \text{ Boolean algebra} \\
& \quad \text{and Corollary 4.26-6 } \rangle \\
& ((x_{\Cap C} \fatsemi \Cap z \sqcup x_{\neg \Cap C} \fatsemi \Cap z) \pitchfork (x_{\Cap C} \sqcup x_{\neg \Cap C})_{\Cap z}) \fatsemi (((x \pitchfork 1)^{\times})_{\neg \Cap z} \pitchfork C) \\
= & \quad \langle \text{ by (3.9), Propositions 4.22-2 and 4.22-5, and} \\
& \quad \text{Corollary 3.21-4 } \rangle \\
& \Cap(x_{\Cap C}) \fatsemi (x \fatsemi \Cap z \pitchfork x_{\Cap z}) \fatsemi (((x \pitchfork 1)^{\times})_{\neg \Cap z} \pitchfork C) \\
= & \quad \langle \text{ by (4.4) with } x, t := x, \Cap C \text{ and Boolean algebra,} \\
& \quad \Cap x \sqsubseteq \Cap(x_{\Cap C}), \\
& \quad \text{then apply (4.80) and Boolean algebra } \rangle \\
& \Cap(x_{\Cap C}) \fatsemi \neg \Cap(x \fatsemi \neg \Cap z) \fatsemi B \fatsemi (((x \pitchfork 1)^{\times})_{\neg \Cap z} \pitchfork C)
\end{array}
$$

iii. Proof of (4.87). We use case analysis with the following tests

$$\Cap(x \fatsemi \Cap z), \Cap(x \fatsemi \neg \Cap z), \Cap(x_{\Cap z}) \ .$$

They are disjoint by Remark 4.8. They cover $\Cap x$ by Remark 4.8 and Boolean algebra.

A. Test $\Cap(x \fatsemi \Cap z)$.

$$
\begin{array}{ll}
& \Cap(x \fatsemi \Cap z) \fatsemi (x \pitchfork 1) \\
= & \quad \langle \text{ by Proposition 3.14-18, Corollary 3.21-7 and} \\
& \quad (3.19) \ \rangle \\
& x \fatsemi \Cap z \\
= & \quad \langle \text{ by (4.67), Corollaries 3.21-4 and 3.21-3,} \\
& \quad \text{Proposition 3.14-7, Boolean algebra, Remark 4.8,} \\
& \quad \text{Lemma 3.17-2 and (3.6) } \rangle \\
& \Cap(x \fatsemi \Cap z) \fatsemi B \\
\sqsubseteq & \quad \langle \text{ by Boolean algebra and Proposition 3.3-2 } \rangle \\
& \Cap(x \fatsemi \Cap z) \fatsemi \neg \Cap C \fatsemi \Cap z \fatsemi B^{\times} \\
= & \quad \langle \text{ by (4.70) } \rangle \\
& \Cap(x \fatsemi \Cap z) \fatsemi A \\
\sqsubseteq & \quad \langle \text{ by (3.15) } \rangle \\
& \Cap(x \fatsemi \Cap z) \fatsemi (A \sqcup ((x \pitchfork 1)^{\times})_{\neg \Cap z})
\end{array}
$$

B. Test $\Cap(x \fatsemi \neg \Cap z)$.

$$
\begin{array}{ll}
& \Cap(x \fatsemi \neg \Cap z) \fatsemi (A \sqcup ((x \pitchfork 1)^{\times})_{\neg \Cap z}) \\
\sqsupseteq & \quad \langle \text{ by (3.15) } \rangle
\end{array}
$$

$$
\begin{array}{ll}
& \Pi(x \rhd \neg \Pi z) \rhd ((x \pitchfork 1)^{\times})_{\neg \Pi z} \\
= & \quad \langle \text{ by (4.79) } \rangle \\
& \Pi(x \rhd \neg \Pi z) \rhd (\Pi z \rhd x \rhd (x \pitchfork 1)^{\times} \rhd \neg \Pi z \pitchfork (x \rhd (x \pitchfork 1)^{\times})_{\neg \Pi z}) \\
= & \quad \langle \text{ by Corollary 3.21-4, Boolean algebra and Proposition 4.22-5 } \rangle \\
& \Pi z \rhd \Pi(x \rhd \neg \Pi z) \rhd x \rhd (x \pitchfork 1)^{\times} \rhd \neg \Pi z \pitchfork (\Pi(x \rhd \neg \Pi z) \rhd x \rhd (x \pitchfork 1)^{\times})_{\neg \Pi z} \\
= & \quad \langle \text{ by (3.19) } \rangle \\
& \Pi z \rhd x \rhd \neg \Pi z \rhd (x \pitchfork 1)^{\times} \rhd \neg \Pi z \pitchfork (x \rhd \neg \Pi z \rhd (x \pitchfork 1)^{\times})_{\neg \Pi z} \\
= & \quad \langle \text{ by (4.59) and Boolean algebra } \rangle \\
& \Pi z \rhd x \rhd \neg \Pi z \rhd (x \pitchfork 1)^{\times} \pitchfork (x \rhd (x \pitchfork 1)^{\times} \rhd \neg \Pi z)_{\neg \Pi z} \\
= & \quad \langle \text{ by Corollaries 4.26-1 and 3.21-3 } \rangle \\
& \Pi z \rhd x \rhd \neg \Pi z \rhd (x \pitchfork 1)^{\times} \\
\sqsupseteq & \quad \langle \text{ by Lemmas 3.7-1 and 3.7-6 } \rangle \\
& x \rhd \neg \Pi z \\
= & \quad \langle \text{ by Proposition 3.14-18, Corollary 3.21-7 and (3.19) } \rangle \\
& \Pi(x \rhd \neg \Pi z) \rhd (x \pitchfork 1)
\end{array}
$$

C. Test $\Pi(x_{\Pi z})$.

$$
\begin{array}{ll}
& \Pi(x_{\Pi z}) \rhd (x \pitchfork 1) \sqsubseteq \Pi(x_{\Pi z}) \rhd (A \sqcup ((x \pitchfork 1)^{\times})_{\neg \Pi z}) \\
\Longleftrightarrow & \quad \langle \text{ by (4.4) with } x, t := x, \Pi z \text{, Boolean algebra and Corollary 3.21-7 } \rangle \\
& \Pi(x_{\Pi z}) \rhd x \sqsubseteq \Pi(x_{\Pi z}) \rhd (A \sqcup ((x \pitchfork 1)^{\times})_{\neg \Pi z}) \\
\Longleftrightarrow & \quad \langle \text{ by Proposition 4.22-2 and (3.8) } \rangle \\
& x_{\Pi z} \sqcup x_{\neg \Pi z} \sqsubseteq \Pi(x_{\Pi z}) \rhd A \sqcup \Pi(x_{\Pi z}) \rhd ((x \pitchfork 1)^{\times})_{\neg \Pi z}) \\
\Longleftarrow & \quad \langle \ \rangle \\
& x_{\Pi z} \sqsubseteq \Pi(x_{\Pi z}) \rhd A \ \wedge \ x_{\neg \Pi z} \sqsubseteq \Pi(x_{\Pi z}) \rhd ((x \pitchfork 1)^{\times})_{\neg \Pi z}
\end{array}
$$

We show the two conditions of the last formula separately. The proof of $x_{\Pi z} \sqsubseteq \Pi(x_{\Pi z}) \rhd A$ goes as follows.

$$
\begin{array}{ll}
& x_{\Pi z} \\
= & \quad \langle \text{ by (4.67), Corollaries 3.21-4 and 3.21-3, Proposition 3.14-7, Remark 4.8, Boolean algebra and (3.6) } \rangle \\
& \Pi(x_{\Pi z}) \rhd B \\
\sqsubseteq & \quad \langle \text{ by Proposition 3.3-2 } \rangle
\end{array}
$$

$$
\begin{array}{ll}
& \Cap(x_{\Cup z})\odot B^{\times} \\
\sqsubseteq & \quad \langle \text{ by (4.68) and Lemma 3.7-1 } \rangle \\
& \Cap(x_{\Cup z})\odot A
\end{array}
$$

And here is the proof of $x_{\neg\Cup z} \sqsubseteq \Cap(x_{\Cup z})\odot((x \between 1)^{\times})_{\neg\Cup z}$.

$$
\begin{array}{ll}
& \Cap(x_{\Cup z})\odot((x \between 1)^{\times})_{\neg\Cup z} \\
= & \quad \langle \text{ by (4.79), Corollary 3.21-4 and Proposition 4.22-5 } \rangle \\
& \Cap(x_{\Cup z})\odot\Cap z\odot x\odot(x \between 1)^{\times}\odot\neg\Cap z \between (\Cap(x_{\Cup z})\odot x\odot(x \between 1)^{\times})_{\neg\Cup z} \\
= & \quad \langle \text{ by Boolean algebra, (4.59) and Proposition 4.22-2 } \rangle \\
& \Cap z\odot(x_{\Cup z} \sqcup x_{\neg\Cup z})\odot\neg\Cap z\odot(x \between 1)^{\times} \between ((x_{\Cup z} \sqcup x_{\neg\Cup z})\odot(x \between 1)^{\times})_{\neg\Cup z} \\
= & \quad \langle \text{ by (3.9), (4.5) with } x, t := x, \Cap z, \text{ Boolean algebra and (3.6) } \rangle \\
& \Cap z\odot(\top \sqcup x_{\neg\Cup z}\odot\neg\Cap z)\odot(x \between 1)^{\times} \between ((x_{\Cup z} \sqcup x_{\neg\Cup z})\odot(x \between 1)^{\times})_{\neg\Cup z} \\
= & \quad \langle \text{ by (3.4), (3.6), Corollary 3.21-3 and (3.9) } \rangle \\
& (x_{\Cup z}\odot(x \between 1)^{\times} \sqcup x_{\neg\Cup z}\odot(x \between 1)^{\times})_{\neg\Cup z} \\
= & \quad \langle \text{ by (4.6) with } x, t := x, \Cap z \text{ and (4.59) } \rangle \\
& (x_{\Cup z}\odot(x \between 1)^{\times} \sqcup x_{\neg\Cup z}\odot(x \between 1)^{\times}\odot\neg\Cap z)_{\neg\Cup z} \\
= & \quad \langle \text{ by Theorem 4.23 and Boolean algebra } \rangle \\
& \Cap(x_{\neg\Cup z}\odot(x \between 1)^{\times}\odot\neg\Cap z\odot\Cap z)\odot x_{\Cup z}\odot(x \between 1)^{\times}\odot\neg\Cap z \between \\
& \Cap(x_{\neg\Cup z}\odot(x \between 1)^{\times}\odot\neg\Cap z\odot\Cap z)\odot(x_{\Cup z}\odot(x \between 1)^{\times})_{\neg\Cup z} \between \\
& (x_{\Cup z}\odot(x \between 1)^{\times}\odot\neg\Cap z \sqcup (x_{\neg\Cup z}\odot(x \between 1)^{\times}\odot\neg\Cap z)_{\neg\Cup z}) \between \\
& \Cap(x_{\Cup z}\odot(x \between 1)^{\times}\odot\Cap z)\odot x_{\neg\Cup z}\odot(x \between 1)^{\times}\odot\neg\Cap z \between \\
& \Cap(x_{\Cup z}\odot(x \between 1)^{\times}\odot\Cap z)\odot(x_{\neg\Cup z}\odot(x \between 1)^{\times}\odot\neg\Cap z)_{\neg\Cup z} \between \\
& ((x_{\Cup z}\odot(x \between 1)^{\times})_{\neg\Cup z} \sqcup x_{\neg\Cup z}\odot(x \between 1)^{\times}\odot\neg\Cap z) \between \\
& ((x_{\Cup z}\odot(x \between 1)^{\times})_{\neg\Cup z} \sqcup (x_{\neg\Cup z}\odot(x \between 1)^{\times}\odot\neg\Cap z)_{\neg\Cup z}) \\
= & \quad \langle \text{ by Boolean algebra, (3.6), Proposition 3.14-19, Corollary 4.26-1 and (3.4) } \rangle \\
& \top \between \top \between \top \between \Cap(x_{\Cup z}\odot(x \between 1)^{\times}\odot\Cap z)\odot x_{\neg\Cup z}\odot(x \between 1)^{\times}\odot\neg\Cap z \between \\
& \top \between ((x_{\Cup z}\odot(x \between 1)^{\times})_{\neg\Cup z} \sqcup x_{\neg\Cup z}\odot(x \between 1)^{\times}\odot\neg\Cap z) \between \top \\
\sqsupseteq & \quad \langle \text{ by Corollary 3.21-3, (3.15) and Lemma 3.22-1 } \rangle \\
& \Cap(x_{\Cup z}\odot(x \between 1)^{\times}\odot\Cap z)\odot x_{\neg\Cup z}\odot(x \between 1)^{\times}\odot\neg\Cap z \between x_{\neg\Cup z}\odot(x \between 1)^{\times}\odot\neg\Cap z
\end{array}
$$

$\sqsupseteq$ ⟨ by Lemma 3.7-1,
$x_{\neg\ulcorner z} \square (x \sqcap 1)^{\times} \sqsubseteq x_{\neg\ulcorner z} \square (x \sqcap 1)^{\times} \square \neg \ulcorner z$,
then apply Lemma 3.22-2, (4.59) and (4.6) with
$x, t := x, \ulcorner z$ ⟩

$x_{\neg\ulcorner z} \square (x \sqcap 1)^{\times}$

$=$ ⟨ by Proposition 3.3-1 and (3.7) ⟩

$x_{\neg\ulcorner z}$

iv. Proof of (4.88). We use case analysis with the following tests

$$\ulcorner(x \square \ulcorner z), \ulcorner(x \square \neg \ulcorner z), \ulcorner(x_{\ulcorner z}) \ .$$

They are disjoint by Remark 4.8. They cover $\ulcorner x$ by Remark 4.8.

A. Test $\ulcorner(x \square \ulcorner z)$.

$\ulcorner(x \square \ulcorner z) \square B \square C$

$=$ ⟨ by (4.67), Corollaries 3.21-4 and 3.21-3,
Proposition 3.14-7, Boolean algebra, Remark 4.8,
Lemma 3.17-2 and (3.6) ⟩

$x \square \ulcorner z \square C$

$=$ ⟨ by Proposition 3.14-18, Corollary 3.21-7, (3.19)
and (4.69) ⟩

$\ulcorner(x \square \ulcorner z) \square (x \sqcap 1) \square (x \sqcap 1)^{\times} \square \ulcorner z$

$\sqsubseteq$ ⟨ by Proposition 3.3-1 ⟩

$\ulcorner(x \square \ulcorner z) \square (x \sqcap 1)^{\times} \square \ulcorner z$

$=$ ⟨ by (4.69) ⟩

$\ulcorner(x \square \ulcorner z) \square C$

B. Test $\ulcorner(x \square \neg \ulcorner z)$. Using (4.67), Corollaries 3.21-4 and 3.21-3, Proposition 3.14-7, Boolean algebra, Remark 4.8, Lemma 3.17-2 and (3.6) yields

$$\ulcorner(x \square \neg \ulcorner z) \square B = \ulcorner(x \square \neg \ulcorner z) \ ,$$

so that $\ulcorner(x \square \neg \ulcorner z) \square B \square C = \ulcorner(x \square \neg \ulcorner z) \square C$.

C. Test $\ulcorner(x_{\ulcorner z})$.

$\ulcorner(x_{\ulcorner z}) \square B \square C$

$=$ ⟨ by (4.67), Corollaries 3.21-4 and 3.21-3,
Proposition 3.14-7, Boolean algebra, Remark 4.8,
Lemma 3.17-2 and (3.6) ⟩

$x_{\ulcorner z} \square C$

$$
\begin{array}{ll}
\sqsubseteq & \langle \text{ by (3.15) } \rangle \\
(x_{\lceil z} \sqcup x_{\neg\lceil z}) \circ C & \\
= & \langle \text{ by (4.4) with } x,t := x, \lceil z, \text{ Boolean algebra,} \\
 & \quad \text{Proposition 4.22-2, Corollary 3.21-7 and (4.69) } \rangle \\
\lceil (x_{\lceil z}) \circ (x \pitchfork 1) \circ (x \pitchfork 1)^{\times} \circ \lceil z & \\
\sqsubseteq & \langle \text{ by Proposition 3.3-1 } \rangle \\
\lceil (x_{\lceil z}) \circ (x \pitchfork 1)^{\times} \circ \lceil z & \\
= & \langle \text{ by (4.69) } \rangle \\
\lceil (x_{\lceil z}) \circ C &
\end{array}
$$

v. Proof of (4.89). By Proposition 3.3-2, Boolean algebra and (4.69),

$$x \pitchfork 1 = (x \pitchfork 1) \circ 1 \sqsubseteq (x \pitchfork 1)^{\times} \circ \lceil z = C \ .$$

(n) Proof of (4.84).

$$
\begin{array}{ll}
 & \mathsf{true} \\
\Longleftrightarrow & \langle \text{ by (4.83) } \rangle \\
 & \lceil ((x \pitchfork 1)^{\times})_{\lceil z} \circ (x \pitchfork 1)^{\times} \sqsubseteq A \sqcup ((x \pitchfork 1)^{\times})_{\neg\lceil z} \\
\Longrightarrow & \langle \text{ by Proposition 4.22-2 and (3.15) } \rangle \\
 & ((x \pitchfork 1)^{\times})_{\lceil z} \sqsubseteq A \sqcup ((x \pitchfork 1)^{\times})_{\neg\lceil z} \\
\Longleftrightarrow & \langle \text{ by (4.5) with } x,t := (x \pitchfork 1)^{\times}, \lceil z, \text{ (4.6) with} \\
 & \quad x,t := (x \pitchfork 1)^{\times}, \lceil z \text{ and (4.76) } \rangle \\
 & ((x \pitchfork 1)^{\times})_{\lceil z} \circ \lceil z \sqsubseteq A \circ \lceil z \sqcup ((x \pitchfork 1)^{\times})_{\neg\lceil z} \circ \neg\lceil z \\
\Longleftrightarrow & \langle \text{ by Corollary 4.26-10 } \rangle \\
 & ((x \pitchfork 1)^{\times})_{\lceil z} \circ \lceil z \sqsubseteq \lceil (((x \pitchfork 1)^{\times})_{\neg\lceil z} \circ \neg\lceil z) \circ A \circ \lceil z \\
\Longleftrightarrow & \langle \text{ by (4.5) with } x,t := (x \pitchfork 1)^{\times}, \lceil z, \text{ (4.6) with} \\
 & \quad x,t := (x \pitchfork 1)^{\times}, \lceil z \text{ and (4.76) } \rangle \\
 & ((x \pitchfork 1)^{\times})_{\lceil z} \sqsubseteq \lceil ((x \pitchfork 1)^{\times})_{\lceil z} \circ A \\
\Longleftrightarrow & \langle \text{ by (4.68) and Boolean algebra } \rangle \\
 & ((x \pitchfork 1)^{\times})_{\lceil z} \sqsubseteq A
\end{array}
$$

And, finally, back to the proof of (4.51).

$$
\begin{array}{ll}
 & ((x \pitchfork 1)^{\times})_{\lceil z} \circ z \sqsubseteq \lceil (((x \pitchfork 1)^{\times})_{\lceil z}) \circ z \\
\Longleftarrow & \langle \text{ by (4.84) } \rangle \\
 & A \circ z \sqsubseteq \lceil (((x \pitchfork 1)^{\times})_{\lceil z}) \circ z
\end{array}
$$

$\Longleftrightarrow$ $\langle$ by (4.68) $\rangle$

$\ulcorner((x \barwedge 1)^{\times})_{\ulcorner z} \circ B^{\times} \circ z \sqsubseteq \ulcorner(((x \barwedge 1)^{\times})_{\ulcorner z}) \circ z$

$\Longleftarrow$ $\langle\ \rangle$

$B^{\times} \circ z \sqsubseteq z$

$\Longleftarrow$ $\langle$ by (3.12) $\rangle$

$B \circ z \sqcup z \sqsubseteq z$

$\Longleftrightarrow$ $\langle$ by (4.67) $\rangle$

$(x \circ \ulcorner z \barwedge x_{\ulcorner z} \barwedge \ulcorner(x \circ \neg \ulcorner z) \barwedge \neg \ulcorner x) \circ z \sqsubseteq z$

$\Longleftrightarrow$ $\langle$ by Remark 4.8 and Proposition 3.14-1,
the domains of $x \circ \ulcorner z$, $x_{\ulcorner z}$, $\ulcorner(x \circ \neg \ulcorner z)$ and $\neg \ulcorner x$
are pairwise disjoint,
then apply Corollary 3.21-17 and Proposition 3.14-7 $\rangle$

$x \circ z \barwedge x_{\ulcorner z} \circ z \barwedge \ulcorner(x \circ \neg \ulcorner z) \circ z \barwedge \neg \ulcorner x \circ z \sqsubseteq z$

$\Longleftrightarrow$ $\langle$ by Remark 4.8,
the tests $\ulcorner(x \circ z)$, $\ulcorner(x_{\ulcorner z})$, $\ulcorner(x \circ \neg \ulcorner z)$ and $\neg \ulcorner x$
are pairwise disjoint;
by Remark 4.8 and Boolean algebra,
$\ulcorner(x \circ z) \barwedge \ulcorner(x_{\ulcorner z}) \barwedge \ulcorner(x \circ \neg \ulcorner z) \barwedge \neg \ulcorner x = 1$;
then apply Corollaries 3.21-19, 3.21-4 and 3.21-3, Proposition 3.14-7, Remark 4.8, Boolean algebra and (3.6) $\rangle$

$x \circ z \sqsubseteq \ulcorner(x \circ z) \circ z \ \wedge\ x_{\ulcorner z} \circ z \sqsubseteq \ulcorner(x_{\ulcorner z}) \circ z \ \wedge$
$\ulcorner(x \circ \neg \ulcorner z) \circ z \sqsubseteq \ulcorner(x \circ \neg \ulcorner z) \circ z \ \wedge\ \neg \ulcorner x \circ z \sqsubseteq \neg \ulcorner x \circ z$

$\Longleftrightarrow$ $\langle$ by (4.47) and (4.48) $\rangle$

true

13. According to Definition 4.1, we need to obtain

$$z \cdot_D x +_D y \leq_D z \Longrightarrow \ulcorner z \sqsubseteq \ulcorner(y \cdot_D x^{*_D}) \tag{4.93}$$

and

$$z \cdot_D x +_D y \leq_D z \Longrightarrow y \cdot_D x^{*_D} \sqsubseteq \ulcorner(y \cdot_D x^{*_D}) \circ z \tag{4.94}$$

in order to show $y \cdot_D x^{*_D} \leq_D z$ from $z \cdot_D x +_D y \leq_D z$.

We begin with the proof of (4.93).

$z \cdot_D x +_D y \leq_D z$

$\Longleftrightarrow$ ⟨ by Remark 4.5 ⟩

$\Cap z \sqsubseteq \Cap(z \mathbin{\cdot_D} x +_D y)$

$\Longleftrightarrow$ ⟨ by Corollary 4.4-3 ⟩

$\Cap z \sqsubseteq \Cap(z \mathbin{\cdot_D} x) \sqcap \Cap y$

$\Longrightarrow$ ⟨ by Boolean algebra ⟩

$\Cap z \sqsubseteq \Cap y$

$\Longleftrightarrow$ ⟨ by (3.20), Lemma 4.20-1 and (3.7) ⟩

$\Cap z \sqsubseteq \Cap(y \mathbin{\triangledown} (x \sqcap 1)^\times)$

$\Longleftrightarrow$ ⟨ by Lemma 4.20-1 and Proposition 4.17-4 ⟩

$\Cap z \sqsubseteq \Cap(y \mathbin{\cdot_D} (x \sqcap 1)^\times)$

$\Longleftrightarrow$ ⟨ by Definition 4.19 ⟩

$\Cap z \sqsubseteq \Cap(y \mathbin{\cdot_D} x^{*_D})$

And now we work on (4.94). The following two derivations will be helpful.

$z \mathbin{\cdot_D} x +_D y \leq_D z$

$\Longrightarrow$ ⟨ by Definition 4.1 ⟩

$z \mathbin{\cdot_D} x +_D y \sqsubseteq \Cap(z \mathbin{\cdot_D} x +_D y) \mathbin{\triangledown} z$

$\Longleftrightarrow$ ⟨ by Corollary 4.4-3 and Proposition 4.17-5 ⟩

$z \mathbin{\cdot_D} x +_D y \sqsubseteq (\Cap z \mathbin{\triangledown} \neg\Cap(z \mathbin{\triangledown} \neg\Cap x) \sqcap \Cap y) \mathbin{\triangledown} z$

$\Longleftrightarrow$ ⟨ by Boolean algebra ⟩

$z \mathbin{\cdot_D} x +_D y \sqsubseteq \Cap y \mathbin{\triangledown} z$

$\Longleftrightarrow$ ⟨ by Corollary 4.4-1 ⟩

$((z \mathbin{\cdot_D} x) \sqcup y) \sqcap \neg\Cap(z \mathbin{\cdot_D} x) \mathbin{\triangledown} y \sqcap \neg\Cap y \mathbin{\triangledown} (z \mathbin{\cdot_D} x) \sqsubseteq \Cap y \mathbin{\triangledown} z$

$\Longleftrightarrow$ ⟨ by Definition 4.16, Proposition 4.17-5 and De Morgan ⟩

$((z \mathbin{\triangledown} x \sqcap z_{\Cap x} \mathbin{\triangledown} x) \sqcup y) \sqcap (\neg\Cap z \sqcap \Cap(z \mathbin{\triangledown} \neg\Cap x)) \mathbin{\triangledown} y \sqcap \neg\Cap y \mathbin{\triangledown} (z \mathbin{\triangledown} x \sqcap z_{\Cap x} \mathbin{\triangledown} x) \sqsubseteq \Cap y \mathbin{\triangledown} z$

$\Longleftrightarrow$ ⟨ by Propositions 3.14-9, 3.14-6 and 3.14-7 ⟩

$\Cap y \mathbin{\triangledown} \Cap z \mathbin{\triangledown} (((z \mathbin{\triangledown} x \sqcap z_{\Cap x} \mathbin{\triangledown} x) \sqcup y) \sqcap (\neg\Cap z \sqcap \Cap(z \mathbin{\triangledown} \neg\Cap x)) \mathbin{\triangledown} y \sqcap \neg\Cap y \mathbin{\triangledown} (z \mathbin{\triangledown} x \sqcap z_{\Cap x} \mathbin{\triangledown} x))$
$\sqsubseteq \Cap y \mathbin{\triangledown} z$

$\Longleftrightarrow$ ⟨ by Corollaries 3.21-4 and 3.21-3, Propositions 3.14-20 and 3.14-7, (4.4) with $x, t := z, \Cap x$, Boolean algebra, Lemma 3.17-1 and (3.6) ⟩

$((z \mathbin{\triangledown} x \sqcap z_{\Cap x} \mathbin{\triangledown} x) \sqcup y) \sqcap \Cap(z \mathbin{\triangledown} \neg\Cap x) \mathbin{\triangledown} y \sqsubseteq \Cap y \mathbin{\triangledown} z$

$$
\begin{array}{ll}
& y \mathbin{\cdot_{\mathcal{D}}} x^{*_{\mathcal{D}}} \sqsubseteq \Pi(y \mathbin{\cdot_{\mathcal{D}}} x^{*_{\mathcal{D}}}) \mathbin{;} z \\
\iff & \quad \langle \text{ by Definition 4.19, Lemma 4.20-1 and Proposition 4.17-4 } \rangle \\
& y \mathbin{;} (x \sqcap 1)^{\times} \sqsubseteq \Pi(y \mathbin{;} (x \sqcap 1)^{\times}) \mathbin{;} z \\
\iff & \quad \langle \text{ by (3.20), Lemma 4.20-1 and (3.7) } \rangle \\
& y \mathbin{;} (x \sqcap 1)^{\times} \sqsubseteq \Pi y \mathbin{;} z \\
\impliedby & \quad \langle \text{ by (3.13) } \rangle \\
& \Pi y \mathbin{;} z \mathbin{;} (x \sqcap 1) \sqcup y \sqsubseteq \Pi y \mathbin{;} z \\
\iff & \quad \langle \text{ by Propositions 3.14-7 and 3.14-20 } \rangle \\
& z \mathbin{;} (x \sqcap 1) \sqcup y \sqsubseteq \Pi y \mathbin{;} z
\end{array}
$$

The previous two derivations teach us that it is sufficient to work on

$$((z \mathbin{;} x \sqcap z_{\Pi_x} \mathbin{;} x) \sqcup y) \sqcap \Pi(z \mathbin{;} \neg \Pi x) \mathbin{;} y \sqsubseteq \Pi y \mathbin{;} z \implies z \mathbin{;} (x \sqcap 1) \sqcup y \sqsubseteq \Pi y \mathbin{;} z \ . \quad (4.95)$$

It will be shown by using case analysis (Corollary 3.21-19) with the tests $\neg \Pi z$, $\Pi(z \mathbin{;} \Pi x)$, $\Pi(z \mathbin{;} \neg \Pi x)$ and $\Pi(z_{\Pi_x})$. By Remark 4.8 and Boolean algebra, these tests are disjoint and they satisfy

$$\neg \Pi z \sqcap \Pi(z \mathbin{;} \Pi x) \sqcap \Pi(z \mathbin{;} \neg \Pi x) \sqcap \Pi(z_{\Pi_x}) = 1 \ .$$

Case $\neg \Pi z$

$$
\begin{array}{ll}
& \neg \Pi z \mathbin{;} (z \mathbin{;} (x \sqcap 1) \sqcup y) \sqsubseteq \neg \Pi z \mathbin{;} \Pi y \mathbin{;} z \\
\iff & \quad \langle \text{ Boolean algebra and Proposition 3.14-17 } \rangle \\
& \neg \Pi z \mathbin{;} (z \mathbin{;} (x \sqcap 1) \sqcup y) \sqsubseteq \top \\
\iff & \quad \langle \text{ by (3.14) } \rangle \\
& \mathsf{true} \\
\impliedby & \quad \langle \ \rangle \\
& ((z \mathbin{;} x \sqcap z_{\Pi_x} \mathbin{;} x) \sqcup y) \sqcap \Pi(z \mathbin{;} \neg \Pi x) \mathbin{;} y \sqsubseteq \Pi y \mathbin{;} z
\end{array}
$$

Case $\Pi(z \mathbin{;} \Pi x)$

$$
\begin{array}{ll}
& \Pi(z \mathbin{;} \Pi x) \mathbin{;} (z \mathbin{;} (x \sqcap 1) \sqcup y) \sqsubseteq \Pi(z \mathbin{;} \Pi x) \mathbin{;} \Pi y \mathbin{;} z \\
\iff & \quad \langle \text{ by Proposition 3.14-20 and (3.19) } \rangle \\
& z \mathbin{;} \Pi x \mathbin{;} (x \sqcap 1) \sqcup y \sqsubseteq \Pi(z \mathbin{;} \Pi x) \mathbin{;} \Pi y \mathbin{;} z \\
\iff & \quad \langle \text{ by Corollary 3.21-7 and Proposition 3.14-7 } \rangle
\end{array}
$$

$$
\begin{array}{ll}
& z \sqcap x \sqcup y \sqsubseteq \lceil (z \sqcap \lceil x) \sqcap \lceil y \sqcap z \\
\iff & \quad \langle \text{ by Proposition 3.14-7, Remark 4.8, Boolean algebra, (3.6) and Corollary 3.21-3 } \rangle \\
& ((z \sqcap x \sqcap \lceil (z \sqcap \lceil x) \sqcap z_{\lceil x} \sqcap x) \sqcup y) \sqcap \lceil (z \sqcap \lceil x) \sqcap \lceil (z \sqcap \neg \lceil x) \sqcap y \sqsubseteq \lceil (z \sqcap \lceil x) \sqcap \lceil y \sqcap z \\
\iff & \quad \langle \text{ by Propositions 3.14-7 and 3.14-20, (3.20) and Corollary 3.21-4 } \rangle \\
& \lceil (z \sqcap \lceil x) \sqcap (((z \sqcap x \sqcap z_{\lceil x} \sqcap x) \sqcup y) \sqcap \lceil (z \sqcap \neg \lceil x) \sqcap y) \sqsubseteq \lceil (z \sqcap \lceil x) \sqcap \lceil y \sqcap z \\
\impliedby & \quad \langle \ \rangle \\
& ((z \sqcap x \sqcap z_{\lceil x} \sqcap x) \sqcup y) \sqcap \lceil (z \sqcap \neg \lceil x) \sqcap y \sqsubseteq \lceil y \sqcap z
\end{array}
$$

Case $\lceil (z \sqcap \neg \lceil x)$

$$
\begin{array}{ll}
& \lceil (z \sqcap \neg \lceil x) \sqcap (z \sqcap (x \sqcap 1) \sqcup y) \sqsubseteq \lceil (z \sqcap \neg \lceil x) \sqcap \lceil y \sqcap z \\
\iff & \quad \langle \text{ by (3.8), (3.19) and Boolean algebra } \rangle \\
& z \sqcap \neg \lceil x \sqcap (x \sqcap 1) \sqcup \lceil (z \sqcap \neg \lceil x) \sqcap y \sqsubseteq \lceil y \sqcap z \sqcap \neg \lceil x \\
\iff & \quad \langle \text{ by Corollary 3.21-8 and Boolean algebra } \rangle \\
& \lceil y \sqcap z \sqcap \neg \lceil x \sqcup \lceil (z \sqcap \neg \lceil x) \sqcap y \sqsubseteq \lceil y \sqcap z \sqcap \neg \lceil x \\
\iff & \quad \langle \text{ by (3.15), (3.3), (3.19) and Boolean algebra } \rangle \\
& \lceil (z \sqcap \neg \lceil x) \sqcap y \sqsubseteq \lceil (z \sqcap \neg \lceil x) \sqcap \lceil y \sqcap z \\
\iff & \quad \langle \text{ by Proposition 3.14-7, Remark 4.8, Boolean algebra, (3.6), Corollary 3.21-3 and (3.4) } \rangle \\
& ((\lceil (z \sqcap \neg \lceil x) \sqcap z \sqcap x \sqcap \lceil (z \sqcap \neg \lceil x) \sqcap z_{\lceil x} \sqcap x) \sqcup y) \sqcap \lceil (z \sqcap \neg \lceil x) \sqcap y \sqsubseteq \lceil (z \sqcap \neg \lceil x) \sqcap \lceil y \sqcap z \\
\iff & \quad \langle \text{ by Corollary 3.21-4, Proposition 3.14-20 and Boolean algebra } \rangle \\
& \lceil (z \sqcap \neg \lceil x) \sqcap (((z \sqcap x \sqcap z_{\lceil x} \sqcap x) \sqcup y) \sqcap \lceil (z \sqcap \neg \lceil x) \sqcap y) \sqsubseteq \lceil (z \sqcap \neg \lceil x) \sqcap \lceil y \sqcap z \\
\impliedby & \quad \langle \ \rangle \\
& ((z \sqcap x \sqcap z_{\lceil x} \sqcap x) \sqcup y) \sqcap \lceil (z \sqcap \neg \lceil x) \sqcap y \sqsubseteq \lceil y \sqcap z
\end{array}
$$

Case $\lceil (z_{\lceil x})$

$$
\begin{array}{ll}
& \lceil (z_{\lceil x}) \sqcap (z \sqcap (x \sqcap 1) \sqcup y) \sqsubseteq \lceil (z_{\lceil x}) \sqcap \lceil y \sqcap z \\
\iff & \quad \langle \text{ by Propositions 3.14-20 and 4.22-2, and Boolean algebra } \rangle \\
& (z_{\lceil x} \sqcup z_{\neg \lceil x}) \sqcap (x \sqcap 1) \sqcup y \sqsubseteq \lceil y \sqcap (z_{\lceil x} \sqcup z_{\neg \lceil x}) \\
\iff & \quad \langle \text{ by (3.9), Propositions 3.14-7 and 3.14-20, and (3.8) } \rangle \\
& z_{\lceil x} \sqcap (x \sqcap 1) \sqcup \lceil y \sqcap z_{\neg \lceil x} \sqcap (x \sqcap 1) \sqcup y \sqsubseteq \lceil y \sqcap z_{\lceil x} \sqcup \lceil y \sqcap z_{\neg \lceil x}
\end{array}
$$

$\iff$ ⟨ by (4.5) with $x,t := z, \Cap x$, (4.6) with $x,t := z, \Cap x$, Corollaries 3.21-7 and 3.21-8, Proposition 3.14-7 and Boolean algebra ⟩

$z_{\Cap x} \rhd x \sqcup \Cap y \rhd z_{\neg \Cap x} \sqcup y \sqsubseteq \Cap y \rhd z_{\Cap x} \sqcup \Cap y \rhd z_{\neg \Cap x}$

$\iff$ ⟨ by (3.3), (3.2) and (3.15) ⟩

$z_{\Cap x} \rhd x \sqcup y \sqsubseteq \Cap y \rhd z_{\Cap x} \sqcup \Cap y \rhd z_{\neg \Cap x}$

$\iff$ ⟨ by (3.8), Proposition 4.22-2 and Boolean algebra ⟩

$z_{\Cap x} \rhd x \sqcup y \sqsubseteq \Cap(z_{\Cap x}) \rhd \Cap y \rhd z$

$\iff$ ⟨ by Proposition 3.14-7, (3.20), Remark 4.8, Boolean algebra, (3.6) and Corollary 3.21-3 ⟩

$((\Cap(z_{\Cap x}) \rhd z \rhd x \sqcap \Cap(z_{\Cap x}) \rhd z_{\Cap x} \rhd x) \sqcup y) \sqcap \Cap(z_{\Cap x}) \rhd \Cap(z \rhd \neg \Cap x) \rhd y \sqsubseteq \Cap(z_{\Cap x}) \rhd \Cap y \rhd z$

$\iff$ ⟨ by Corollary 3.21-4 and Proposition 3.14-20 ⟩

$\Cap(z_{\Cap x}) \rhd (((z \rhd x \sqcap z_{\Cap x} \rhd x) \sqcup y) \sqcap \Cap(z \rhd \neg \Cap x) \rhd y) \sqsubseteq \Cap(z_{\Cap x}) \rhd \Cap y \rhd z$

$\impliedby$ ⟨ ⟩

$((z \rhd x \sqcap z_{\Cap x} \rhd x) \sqcup y) \sqcap \Cap(z \rhd \neg \Cap x) \rhd y \sqsubseteq \Cap y \rhd z$

□

Theorem 4.32. *Suppose $\mathcal{A}$ is an algebra of decomposable elements. Then* $(\mathsf{test}(A), +_D, \cdot_D, \neg, \top, 1)$ *is a Boolean algebra, hence* $(A, \mathsf{test}(A), +_D, \cdot_D, {}^{*_D}, \top, 1, \neg)$ *is a KAT.*

Proof : We show that for all $s, t \in \mathsf{test}(A)$,

$$s \sqsubseteq t \iff t \leq_D s \tag{4.96}$$

$$s \sqcup t = s \cdot_D t \tag{4.97}$$

$$s \sqcap t = s +_D t \ . \tag{4.98}$$

Therefore, since $(\mathsf{test}(A), \sqcup, \sqcap, \neg, 1, \top)$ is a Boolean algebra, then so is $(\mathsf{test}(A), +_D, \cdot_D, \neg, \top, 1)$ by Corollary 4.4.

(4.96) is true by Remark 4.5.

Proof of (4.97)

$s \sqcup t$

$=$ ⟨ by Proposition 3.14-3 ⟩

$s \rhd t$

$$
\begin{array}{ll}
= & \langle \text{ by Proposition 4.17-3 } \rangle \\
s \cdot_D t &
\end{array}
$$

Proof of (4.98)

$$
\begin{array}{ll}
& s \sqcap t \\
= & \langle \text{ by Boolean algebra } \rangle \\
& (s \sqcup t) \sqcap \neg t \circ s \sqcap \neg s \circ t \\
= & \langle \text{ by Corollary 4.4-1 } \rangle \\
& s +_D t
\end{array}
$$

□

Theorem 4.33. *Suppose $\mathcal{A}$ is an algebra of decomposable elements. The following inequalities are valid for all $x, y \in A$ and all $t \in \mathsf{test}(A)$, hence $(A, \mathsf{test}(A), +_D, \cdot_D, ^{*_D}, \top, 1, \neg, \pi)$ is KAD.*

1. $x \leq_D \pi x \cdot_D x$
2. $\pi(t \cdot_D x) \leq_D t$
3. $\pi(x \cdot_D \pi y) \leq_D \pi(x \cdot_D y)$

Proof :

1.
$$
\begin{array}{ll}
& x \\
\leq_D & \langle \text{ by Corollary 4.4-2 } \rangle \\
& x \\
= & \langle \text{ by Proposition 3.14-7 } \rangle \\
& \pi x \circ x \\
= & \langle \text{ by Proposition 4.17-3 } \rangle \\
& \pi x \cdot_D x
\end{array}
$$

2.
$$
\begin{array}{ll}
 & \Pi(t \cdot_D x) \\
= & \quad \langle \text{ by Proposition 4.17-3 } \rangle \\
 & \Pi(t \sqcap x) \\
= & \quad \langle \text{ by Proposition 3.14-9 } \rangle \\
 & t \sqcap \Pi x \\
\leq_D & \quad \langle \text{ by Boolean Algebra and Theorem 4.32 } \rangle \\
 & t
\end{array}
$$

3. Since $\leq_D$ is a partial order (see Corollary 4.4-2), it is sufficient to prove equality instead of $\leq_D$.

$$
\begin{array}{ll}
 & \Pi(x \cdot_D y) \\
= & \quad \langle \text{ by Proposition 4.17-5 } \rangle \\
 & \Pi x \sqcap \neg \Pi(x \sqcap \neg \Pi y) \\
= & \quad \langle \text{ by Propositions 3.14-1 and 4.17-5 } \rangle \\
 & \Pi(x \cdot_D \Pi y)
\end{array}
$$

□

Chapter 5

A Duality Between KADs and Algebras of Decomposable Elements

We are now ready for the ultimate goal of this text (refer to item 8 of Section 1.3). We will establish an algebraic connection between the bottom part and the upper part of the lattice of Figure 1.4 for any model of KAD.

In Section 5.1, having Figure 1.5 in mind, we are going to define a function $\mathcal{F}$ from the set of all KADs to the set of all algebras of decomposable elements. Symmetrically, we are going to define a function $\mathcal{G}$ from the set of all algebras of decomposable elements to the set of all KADs. Then, we will demonstrate that $\mathcal{F}(\mathcal{K})$ is an algebra of decomposable elements for each KAD $\mathcal{K}$. Also, we will demonstrate that $\mathcal{G} \circ \mathcal{F}$ is the identity on $\mathcal{K}$.

In Section 5.2, we will demonstrate that $\mathcal{G}(\mathcal{A})$ is a KAD for each algebra of decomposable elements $\mathcal{A}$. Also, we will demonstrate that $\mathcal{F} \circ \mathcal{G}$ is the identity on $\mathcal{A}$.

This chapter is the third and last step toward the desired duality (refer to Section 1.3).

5.1 From KAD to DAD-⊓, and Back

In this section, we introduce two transformations between the angelic and demonic worlds that will be studied all along this chapter. Then, we present a few useful lemmas

and we finish with the main theorem of this section.

Definition 5.1. *Let $\mathcal{F}$ denote the transformation that sends any KAD $\mathcal{K} = (K, \mathsf{test}(K), +, \cdot, ^*, 0, 1, \neg, ^\lceil)$ to*

$$(K, \mathsf{test}(K), \sqcup_A, \sqsubset_A, ^{\times_A}, 0, 1, \neg, \sqcap_A, ^\lceil, \sqcap_{A\bullet}) \ ,$$

where $\sqcup_A$, $\sqsubset_A$, $^{\times_A}$, $\sqcap_A$ and $\sqcap_{A\bullet}$ are the operators defined in Proposition 2.10 and Definitions 2.12, 2.14, 2.17 and 2.18 respectively.

Similarly, let $\mathcal{G}$ denote the transformation that sends any algebra of decomposable elements $\mathcal{A} = (A, \mathsf{test}(A), \sqcup, \sqsubset, ^\times, \top, 1, \neg_D, \sqcap, ^\Gamma, \sqcap_\bullet)$ to

$$(A, \mathsf{test}(A), +_D, \cdot_D, ^{*_D}, \top, 1, \neg_D, ^\Gamma) \ ,$$

where $+_D$, $\cdot_D$, ^{*_D} and $\neg_D$ are the operators defined in Corollary 4.4-1, and Definitions 4.16, 4.19 and 3.4 respectively (since no special notation was introduced in Definition 3.4 to distinguish DAT's negation from KAT's negation, we have added a subscript D to $\neg$ in order to avoid confusion in Theorem 5.5).

By this definition, the transformations $\mathcal{F}$ and $\mathcal{G}$ transport the domain operator and the negation operator unchanged between the angelic and demonic worlds. Indeed, it turns out that $^\lceil x = {}^\Gamma x$ and $\neg t = \neg_D t$ are the right transformations.

Having defined $\mathcal{F}$ and $\mathcal{G}$, we can now state a crucial theorem. But before doing that, we need to introduce the following three lemmas.

Lemma 5.2. *Let $\mathcal{K}$ be a KAD. For all $x \in K$ and all $t \in \mathsf{test}(K)$,*

$$x = x \sqsubset_A t \iff x = x \cdot t \ .$$

Proof :

$$\begin{array}{ll}
& x \sqsubset_A t = x \\
\iff & \quad \langle \text{ by Definition 2.12 } \rangle \\
& (x \rightarrow t) \cdot x \cdot t = x \\
\iff & \quad \langle \text{ by Proposition 2.7-4 } \rangle \\
& (x \rightarrow t) \cdot x \cdot t \cdot t = x \cdot t \ \wedge \ (x \rightarrow t) \cdot x \cdot t \cdot \neg t = x \cdot \neg t \\
\iff & \quad \langle \text{ by Definition 2.8, Proposition 2.7-10, Boolean algebra and (2.6) } \rangle
\end{array}$$

$$
\begin{aligned}
& \neg\ulcorner(x \cdot \neg t) \cdot x \cdot t \cdot t = x \cdot t \ \wedge\ 0 = x \cdot \neg t \\
\iff & \qquad \langle \text{ substituting } 0 \text{ for } x \cdot \neg t \text{ in } \neg\ulcorner(x \cdot \neg t), \text{ by Proposition 2.7-10, (2.6)} \\
& \qquad \text{and Boolean algebra } \rangle \\
& x \cdot t \cdot t = x \cdot t \ \wedge\ x \cdot t \cdot \neg t = x \cdot \neg t \\
\iff & \qquad \langle \text{ by Proposition 2.7-4 } \rangle \\
& x \cdot t = x
\end{aligned}
$$

□

Lemma 5.3. *Let $\mathcal{A}, \mathcal{A}'$ be algebras of decomposable elements. Let $\phi : \mathcal{A} \to \mathcal{A}'$ be a homomorphism. Then*

$$\phi(x \sqcap y) = \phi(x) \sqcap \phi(y)$$

for all $x, y \in A$.

Proof :

$$
\begin{aligned}
& \phi(x \sqcap y) \\
= & \qquad \langle \text{ by (3.24) } \rangle \\
& \phi(x \sqcap_{\ulcorner x} y) \\
= & \qquad \langle \text{ since } \phi \text{ is a homomorphism } \rangle \\
& \phi(x) \sqcap_{\ulcorner \phi(x))} \phi(y) \\
= & \qquad \langle \text{ by (3.24) } \rangle \\
& \phi(x) \sqcap \phi(y)
\end{aligned}
$$

□

Lemma 5.4. *Let $\mathcal{A}, \mathcal{A}'$ be algebras of decomposable elements. Let $\phi : \mathcal{A} \to \mathcal{A}'$ be a homomorphism. Then*

$$\phi(x_t) = \phi(x)_{\phi(t)}$$

for all $x \in A$ and all $t \in \mathsf{test}(A)$.

Proof : We have to show that $\phi(x_t)$ and $\phi\,(x_{\neg t})$ satisfy (4.3), (4.4), (4.5) and (4.6) with $x, t := \phi(x), \phi(t)$.

Proof of (4.3)

$$
\begin{aligned}
& \phi(x)\cdot\phi(t) \sqcap \phi(x)\cdot\neg\phi(t) \sqcap (\phi(x_t) \sqcup \phi(x_{\neg t})) \\
= & \qquad \langle \text{ since } \phi \text{ is a homomorphism and by Lemma 5.3 } \rangle \\
& \phi(x\cdot t \sqcap x\cdot\neg t \sqcap (x_t \sqcup x_{\neg t})) \\
= & \qquad \langle \text{ by (4.3) } \rangle \\
& \phi(x)
\end{aligned}
$$

Proof of (4.4)

$$
\begin{aligned}
& \pi(\phi(x_t)) \\
= & \qquad \langle \text{ since } \phi \text{ is a homomorphism } \rangle \\
& \phi(\pi(x_t)) \\
= & \qquad \langle \text{ by (4.4) } \rangle \\
& \phi(\neg\pi(x\cdot t))\cdot\neg\pi(x\cdot\neg t)\cdot\pi x) \\
= & \qquad \langle \text{ since } \phi \text{ is a homomorphism } \rangle \\
& \neg\pi(\phi(x)\cdot\phi(t))\cdot\neg\pi(\phi(x)\cdot\neg\phi(t))\cdot\pi(\phi(x))
\end{aligned}
$$

The derivation is similar for $\pi(\phi(x_{\neg t})) = \neg\pi(\phi(x)\cdot\phi(t))\cdot\neg\pi(\phi(x)\cdot\neg\phi(t))\cdot\pi(\phi(x))$.

Proof of (4.5).

$$
\begin{aligned}
& \phi(x_t)\cdot\phi(t) \\
= & \qquad \langle \text{ since } \phi \text{ is a homomorphism } \rangle \\
& \phi(x_t\cdot t) \\
= & \qquad \langle \text{ by (4.5) } \rangle \\
& \phi(x_t)
\end{aligned}
$$

The derivation is similar for (4.6). □

Theorem 5.5. *Let $\mathcal{K}$ be a KAD and let $\mathcal{F}$ and $\mathcal{G}$ be the transformations introduced in Definition 5.1.*

1. *$\mathcal{F}(\mathcal{K})$ is a DAD-$\sqcap$.*

2. *All elements of $\mathcal{F}(\mathcal{K})$ are decomposable and, for all $x \in K$ and all $t \in \mathsf{test}(K)$,*

$$\begin{aligned} x_t &= \ulcorner(x \cdot \neg t) \cdot x \cdot t \ , \\ x_{\neg t} &= \ulcorner(x \cdot t) \cdot x \cdot \neg t \ . \end{aligned}$$

Hence, $\mathcal{F}(\mathcal{K})$ is an algebra of decomposable elements.

3. *$\mathcal{G} \circ \mathcal{F}$ is the identity on $\mathcal{K}$. In other words, the algebra $(K, \mathsf{test}(K), +_D, \cdot_D, ^{*_D}, 0, 1, \neg, \ulcorner)$ derived from the algebra of decomposable elements $\mathcal{F}(\mathcal{K})$ is equal to $\mathcal{K}$ (only the symbols denoting the operators differ).*

4. *Let $\mathcal{K}'$ be a KAD. If $\psi : \mathcal{K} \to \mathcal{K}'$ is a homomorphism, then ψ is also a homomorphism from $\mathcal{F}(\mathcal{K})$ to $\mathcal{F}(\mathcal{K}')$. Thus, if $\mathcal{K} \preccurlyeq \mathcal{K}'$, then $\mathcal{F}(\mathcal{K}) \preccurlyeq \mathcal{F}(\mathcal{K}')$ (where $\preccurlyeq$ denotes substructure).*

Proof :

1. This is direct from Theorem 2.23.

2. Let x be any element of K and t be any test. We have to show

$$x = x \barwedge_A t \barvee_A x \barwedge_A \neg t \barvee_A (x_t \barcup_A x_{\neg t}) \ ,$$

where x_t and $x_{\neg t}$ have the unique solution given in the statement. Also we have to verify that these solutions satisfy (4.4), (4.5) and (4.6). Remark 4.8 shows that $\ulcorner x$ can be split in three disjoint parts, namely $\ulcorner(x \barwedge_A t)$, $\ulcorner(x \barwedge_A \neg t)$ and $\ulcorner(x_t)$. Thus, by Proposition 3.20-17, the above equality holds if and only if the following four equalities also do.

$$\begin{aligned} \neg\ulcorner x \barwedge_A x &= \neg\ulcorner x \barwedge_A (x \barwedge_A t \barvee_A x \barwedge_A \neg t \barvee_A (x_t \barcup_A x_{\neg t})) \\ \ulcorner(x \barwedge_A t) \barwedge_A x &= \ulcorner(x \barwedge_A t) \barwedge_A (x \barwedge_A t \barvee_A x \barwedge_A \neg t \barvee_A (x_t \barcup_A x_{\neg t})) \\ \ulcorner(x \barwedge_A \neg t) \barwedge_A x &= \ulcorner(x \barwedge_A \neg t) \barwedge_A (x \barwedge_A t \barvee_A x \barwedge_A \neg t \barvee_A (x_t \barcup_A x_{\neg t})) \\ \ulcorner(x_t) \barwedge_A x &= \ulcorner(x_t) \barwedge_A (x \barwedge_A t \barvee_A x \barwedge_A \neg t \barvee_A (x_t \barcup_A x_{\neg t})) \end{aligned}$$

Using Propositions 3.14-17 and 3.14-11, Corollary 3.21-4, (4.4), Boolean algebra and (3.6), the first equality reduces to $\top = \top$. The second one follows from Corollary 3.21-7, Proposition 3.14-7 and (3.19), and the third one from Remark 4.8, (3.25), Corollary 3.21-7, Proposition 3.14-7 and (3.19). The following derivation is about the fourth equality and constructs the unique expressions for x_t and $x_{\neg t}$, assuming that x_t and $x_{\neg t}$ satisfy (4.4), (4.5) and (4.6). Uniqueness is due to the sequence of equivalences.

$$
\begin{aligned}
& \ulcorner(x_t) \boxdot_A x = \ulcorner(x_t) \boxdot_A (x \boxdot_A t \boxplus_A x \boxdot_A \neg t \boxplus_A (x_t \sqcup_A x_{\neg t})) \\
\iff & \quad \langle \text{ by Corollary 3.21-8, (4.4) and Boolean algebra } \rangle \\
& \ulcorner(x_t) \boxdot_A x = \ulcorner(x_t) \boxdot_A (x \boxdot_A \neg t \boxplus_A (x_t \sqcup_A x_{\neg t})) \\
\iff & \quad \langle \text{ by Corollary 3.21-8, (4.4) and Boolean algebra } \rangle \\
& \ulcorner(x_t) \boxdot_A x = \ulcorner(x_t) \boxdot_A (x_t \sqcup_A x_{\neg t}) \\
\iff & \quad \langle \text{ by Proposition 2.13-2 } \rangle \\
& \ulcorner(x_t) \cdot x = \ulcorner(x_t) \cdot (x_t \sqcup_A x_{\neg t}) \\
\iff & \quad \langle \text{ by Proposition 2.10, (4.4) and Boolean algebra } \rangle \\
& \ulcorner(x_t) \cdot x = \ulcorner(x_t) \cdot (x_t + x_{\neg t}) \\
\iff & \quad \langle \text{ by (2.8), Proposition 2.7-6 and (4.4) } \rangle \\
& \ulcorner(x_t) \cdot x = x_t + x_{\neg t} \\
\iff & \quad \langle \text{ by Proposition 2.7-4 } \rangle \\
& \ulcorner(x_t) \cdot x \cdot t = (x_t + x_{\neg t}) \cdot t \ \wedge \ \ulcorner(x_t) \cdot x \cdot \neg t = (x_t + x_{\neg t}) \cdot \neg t \\
\iff & \quad \langle \text{ by (4.5), (4.6) and Lemma 5.2 } \rangle \\
& \ulcorner(x_t) \cdot x \cdot t = (x_t \cdot t + x_{\neg t} \cdot \neg t) \cdot t \ \wedge \ \ulcorner(x_t) \cdot x \cdot \neg t = (x_t \cdot t + x_{\neg t} \cdot \neg t) \cdot \neg t \\
\iff & \quad \langle \text{ by (2.9), Boolean algebra, (2.6) and (2.4) } \rangle \\
& \ulcorner(x_t) \cdot x \cdot t = x_t \cdot t \ \wedge \ \ulcorner(x_t) \cdot x \cdot \neg t = x_{\neg t} \cdot \neg t \\
\iff & \quad \langle \text{ by (4.5), (4.6) and Lemma 5.2 } \rangle \\
& \ulcorner(x_t) \cdot x \cdot t = x_t \ \wedge \ \ulcorner(x_t) \cdot x \cdot \neg t = x_{\neg t} \\
\iff & \quad \langle \text{ by (4.4), Propositions 2.13-4 and 2.7-6, and De Morgan } \rangle \\
& (\neg(x \to t) + \neg\ulcorner x) \cdot (\neg(x \to \neg t) + \neg\ulcorner x) \cdot x \cdot t = x_t \ \wedge \\
& (\neg(x \to t) + \neg\ulcorner x) \cdot (\neg(x \to \neg t) + \neg\ulcorner x) \cdot x \cdot \neg t = x_{\neg t} \\
\iff & \quad \langle \text{ by Boolean algebra, (2.9), Proposition 2.7-9 and (2.4) } \rangle \\
& x_t = \neg(x \to t) \cdot \neg(x \to \neg t) \cdot x \cdot t \ \wedge \\
& x_{\neg t} = \neg(x \to t) \cdot \neg(x \to \neg t) \cdot x \cdot \neg t \\
\iff & \quad \langle \text{ by Definition 2.8, Boolean algebra and Propositions 2.7-6 and 2.7-10 } \rangle \\
& x_t = \ulcorner(x \cdot \neg t) \cdot x \cdot t \ \wedge \ x_{\neg t} = \ulcorner(x \cdot t) \cdot x \cdot \neg t
\end{aligned}
$$

By Theorem 5.5-1 and since all elements of $\mathcal{F}(\mathcal{K})$ are decomposable, then $\mathcal{F}(\mathcal{K})$ is an algebra of decomposable elements.

3. To show the third part of the theorem, it suffices to prove $x+y = x+_D y$, $x \cdot y = x \cdot_D y$ and $x^* = x^{*_D}$ for $x, y \in K$, since $\neg$ and $\ulcorner$ are unchanged either by $\mathcal{F}$ or $\mathcal{G}$.

(a) Firstly, we show that $x \leq y \iff x \leq_D y$.

$$
\begin{aligned}
& x \leq_D y \\
\iff & \quad \langle \text{ by Definition 4.1 } \rangle \\
& \ulcorner y \sqsubseteq_A \ulcorner x \ \wedge \ x \sqsubseteq_A \ulcorner x \boxdot_A y \\
\iff & \quad \langle \text{ by Remark 2.11 and Definition 2.9 } \rangle \\
& \ulcorner x \leq \ulcorner y \ \wedge \ \ulcorner(\ulcorner x \boxdot_A y) \leq \ulcorner x \ \wedge \ \ulcorner(\ulcorner x \boxdot_A y) \cdot x \leq \ulcorner x \boxdot_A y \\
\iff & \quad \langle \text{ by Proposition 2.13-2 } \rangle \\
& \ulcorner x \leq \ulcorner y \ \wedge \ \ulcorner(\ulcorner x \cdot y) \leq \ulcorner x \ \wedge \ \ulcorner(\ulcorner x \cdot y) \cdot x \leq \ulcorner x \cdot y \\
\iff & \quad \langle \text{ by Proposition 2.7-11 and Boolean algebra } \rangle \\
& \ulcorner x \leq \ulcorner y \ \wedge \ \ulcorner x \cdot \ulcorner y \cdot x \leq \ulcorner x \cdot y \\
\iff & \quad \langle \text{ since } \ulcorner x \leq \ulcorner y \text{ and by Boolean algebra } \rangle \\
& \ulcorner x \leq \ulcorner y \ \wedge \ \ulcorner x \cdot x \leq \ulcorner x \cdot y \\
\iff & \quad \langle \text{ by Proposition 2.7-14 for } \Longleftarrow, \\
& \qquad \text{and by Proposition 2.7-6 for } \Longrightarrow \text{ since } \ulcorner x \cdot x \leq \ulcorner x \cdot y \leq y \\
& \quad \rangle \\
& x \leq y
\end{aligned}
$$

So $x + y = x +_D y$ by (2.11) and Corollary 4.4-2.

(b)

$$
\begin{aligned}
& x \between_D y \\
= & \quad \langle \text{ by Proposition 4.17-7 } \rangle \\
& (x \boxdot_A \ulcorner y \boxminus_A x_{\ulcorner y}) \boxdot_A y \\
= & \quad \langle \text{ by (3.24), Definition 2.18 and Proposition 2.13-2 } \rangle \\
& (\ulcorner(x \boxdot_A \ulcorner y) \boxdot_A x \boxdot_A \ulcorner y + \neg\ulcorner(x \boxdot_A \ulcorner y) \boxdot_A x_{\ulcorner y}) \boxdot_A y \\
= & \quad \langle \text{ by Propositions 3.14-7 and 3.14-1, (4.4) with } x, t := x, \ulcorner y \\
& \qquad \text{and Boolean algebra } \rangle \\
& (x \boxdot_A \ulcorner y + x_{\ulcorner y}) \boxdot_A y \\
= & \quad \langle \text{ by Definition 2.12, Proposition 2.7-10 and Theorem 5.5-2 } \rangle \\
& ((x \rightarrow \ulcorner y) \cdot x \cdot \ulcorner y + \ulcorner(x \cdot \neg\ulcorner y) \cdot x \cdot \ulcorner y) \boxdot_A y \\
= & \quad \langle \text{ by Definition 2.8, Proposition 2.7-10, (2.9), Boolean} \\
& \qquad \text{algebra and (2.7) } \rangle \\
& (x \cdot \ulcorner y) \boxdot_A y \\
= & \quad \langle \text{ by Definition 2.12 and Proposition 2.7-6 } \rangle \\
& (x \cdot \ulcorner y \rightarrow y) \cdot x \cdot y
\end{aligned}
$$

$=$ ⟨ by Definition 2.8, Boolean algebra, (2.6), Proposition 2.7-10 and (2.7) ⟩

$x \cdot y$

(c) x^{*_D}

$=$ ⟨ by Theorem 4.31 and Remark 2.2 ⟩

$\mu_{\leq_D}(y :: y \cdot_D x +_D 1)$

$=$ ⟨ by the previous two derivations ⟩

$\mu_{\leq}(y :: y \cdot x + 1)$

$=$ ⟨ by Remark 2.2 ⟩

x^*

4. If $\psi : \mathcal{K} \to \mathcal{K}'$ is a homomorphism, then

$$\begin{aligned}
\psi(x + y) &= \psi(x) + \psi(y) \ , && (5.1)\\
\psi(x \cdot y) &= \psi(x) \cdot \psi(y) \ , && (5.2)\\
\psi(x^*) &= (\psi(x))^* \ , && (5.3)\\
\psi(0) &= 0' \ , && (5.4)\\
\psi(1) &= 1' \ , && (5.5)\\
\psi(\neg t) &= \neg(\psi(t)) \ , && (5.6)\\
\psi(\ulcorner x) &= \ulcorner(\psi(x)) \ . && (5.7)
\end{aligned}$$

We need to derive

$$\begin{aligned}
\psi(x \sqcup_A y) &= \psi(x) \sqcup_A \psi(y) \ , && (5.8)\\
\psi(x \sqcap_A y) &= \psi(x) \sqcap_A \psi(y) \ , && (5.9)\\
\psi(x^{\times_A}) &= (\psi(x))^{\times_A} \ , && (5.10)\\
\psi(0) &= 0' \ , && (5.11)\\
\psi(1) &= 1' \ , && (5.12)\\
\psi(\neg t) &= \neg(\psi(t)) \ , && (5.13)\\
\psi(\ulcorner x) &= \ulcorner(\psi(x)) \ , && (5.14)\\
\psi(x \sqcap\!\!\!\sqcap_{A_t} y) &= \psi(x) \sqcap\!\!\!\sqcap_{A_{\psi(t)}} \psi(y) \ . && (5.15)
\end{aligned}$$

(a) Proof of (5.8).

$\psi(x \sqcup_A y)$

$=$ ⟨ by Proposition 2.10 ⟩

$\psi(\ulcorner x \cdot \ulcorner y \cdot (x + y))$

$$
\begin{aligned}
&= && \langle \text{ by (5.2), (5.1) and (5.7) } \rangle \\
&\quad \ulcorner(\psi(x)) \cdot \ulcorner(\psi(y)) \cdot (\psi(x) + \psi(y)) \\
&= && \langle \text{ by Proposition 2.10 } \rangle \\
&\quad \psi(x) \sqcup_A \psi(y)
\end{aligned}
$$

(b) Proof of (5.9).

$$
\begin{aligned}
&\quad \psi(x \mathbin{\square_A} y) \\
&= && \langle \text{ by Definitions 2.12 and 2.8 } \rangle \\
&\quad \psi(\neg\ulcorner(x \cdot \neg\ulcorner y) \cdot x \cdot y) \\
&= && \langle \text{ by (5.2), (5.6) and (5.7) } \rangle \\
&\quad \neg\ulcorner(\psi(x) \cdot \neg\ulcorner(\psi(y))) \cdot \psi(x) \cdot \psi(y) \\
&= && \langle \text{ by Definitions 2.8 and 2.12 } \rangle \\
&\quad \psi(x) \mathbin{\square_A} \psi(y)
\end{aligned}
$$

(c) Proof of (5.10).

$$
\begin{aligned}
&\quad \psi(x^{\times_A}) \\
&= && \langle \text{ by Definition 2.14 } \rangle \\
&\quad \psi(x^* \mathbin{\square_A} \ulcorner x) \\
&= && \langle \text{ by the previous derivation, (5.3) and (5.7) } \rangle \\
&\quad (\psi(x))^* \mathbin{\square_A} \ulcorner(\psi(x))) \\
&= && \langle \text{ by Definition 2.14 } \rangle \\
&\quad \psi(x)^{\times_A}
\end{aligned}
$$

(d) Proof of (5.11). This is direct from (5.4).

(e) Proof of (5.12). This is direct from (5.5).

(f) Proof of (5.13). This is direct from (5.6).

(g) Proof of (5.14). This is direct from (5.7).

(h) Proof of (5.15).

$$
\begin{aligned}
&\quad \psi(x \mathbin{\sqcap_{A_t}} y) \\
&= && \langle \text{ by Definition 2.18 } \rangle \\
&\quad \psi(t \cdot x + \neg t \cdot y) \\
&= && \langle \text{ by (5.1), (5.2) and (5.6) } \rangle
\end{aligned}
$$

$$\begin{aligned} & \psi(t) \cdot \psi(x) + \neg(\psi(t)) \cdot \psi(y) \\ = & \qquad \langle \text{ by Definition 2.18 } \rangle \\ & \psi(x) \pitchfork_{A\psi(t)} \psi(y) \end{aligned}$$

□

5.2 From DAD-$\pitchfork$ to KAD and Back

This section is the dual version of Section 5.1. Essentially, we derive similar results but starting with algebra of decomposable elements instead of KAD. Its main content is the following theorem.

Theorem 5.6. *Let $\mathcal{A}$ be an algebra of decomposable elements and let $\mathcal{F}$ and $\mathcal{G}$ be the transformations introduced in Definition 5.1.*

1. *$\mathcal{G}(\mathcal{A})$ is a KAD.*
2. *$\mathcal{F} \circ \mathcal{G}$ is the identity on $\mathcal{A}$. In other words, the algebra $(A, \mathsf{test}(A), \sqcup_A, \cdot_A, {}^{\times_A}, \top, 1, \neg_D, \pitchfork_A, {}^{\top})$ derived from the KAD $\mathcal{G}(\mathcal{A})$ is equal to $\mathcal{A}$ (only the symbols denoting the operators differ).*
3. *Let $\mathcal{A}'$ be an algebra of decomposable elements. If $\phi : \mathcal{A} \to \mathcal{A}'$ is a homomorphism, then ϕ is also a homomorphism from $\mathcal{G}(\mathcal{A})$ to $\mathcal{G}(\mathcal{A}')$. Thus, if $\mathcal{A} \preccurlyeq \mathcal{A}'$, then $\mathcal{G}(\mathcal{A}) \preccurlyeq \mathcal{G}(\mathcal{A}')$ (where $\preccurlyeq$ denotes substructure).*

Proof :

1. This is direct from Theorem 4.33.
2. To show the second part of the theorem, it suffices to prove $x \sqcup y = x \sqcup_A y$, $x \cdot y = x \cdot_A y$, $x^{\times} = x^{\times_A}$ and $x \pitchfork_t y = x \pitchfork_{At} y$ since $\neg_D$ and ${}^{\top}$ are unchanged either by $\mathcal{G}$ or $\mathcal{F}$.
   (a) Firstly, we show that $x \sqsubseteq y \iff x \sqsubseteq_A y$.

$$\begin{aligned} & x \sqsubseteq_A y \\ \iff & \qquad \langle \text{ by Definition 2.9 } \rangle \\ & {}^{\top}y \leq_D {}^{\top}x \ \wedge \ {}^{\top}y \cdot_D x \leq_D y \end{aligned}$$

$$
\begin{aligned}
&\iff && \langle \text{ by Remark 4.5 and Definition 4.1 } \rangle \\
&\quad {}^{\sqcap}x \sqsubseteq {}^{\sqcap}y \ \wedge\ {}^{\sqcap}y \sqsubseteq {}^{\sqcap}({}^{\sqcap}y \mathbin{\cdot_D} x) \ \wedge\ {}^{\sqcap}y \mathbin{\cdot_D} x \sqsubseteq {}^{\sqcap}({}^{\sqcap}y \mathbin{\cdot_D} x) \mathbin{\square} y \\
&\iff && \langle \text{ by Proposition 4.17-3 } \rangle \\
&\quad {}^{\sqcap}x \sqsubseteq {}^{\sqcap}y \ \wedge\ {}^{\sqcap}y \sqsubseteq {}^{\sqcap}({}^{\sqcap}y \mathbin{\square} x) \ \wedge\ {}^{\sqcap}y \mathbin{\square} x \sqsubseteq {}^{\sqcap}({}^{\sqcap}y \mathbin{\square} x) \mathbin{\square} y \\
&\iff && \langle \text{ by Proposition 3.14-9 and Boolean algebra } \rangle \\
&\quad {}^{\sqcap}x \sqsubseteq {}^{\sqcap}y \ \wedge\ {}^{\sqcap}y \mathbin{\square} x \sqsubseteq {}^{\sqcap}y \mathbin{\square} {}^{\sqcap}x \mathbin{\square} y \\
&\iff && \langle \text{ since } {}^{\sqcap}x \sqsubseteq {}^{\sqcap}y \text{ and by Boolean algebra } \rangle \\
&\quad {}^{\sqcap}x \sqsubseteq {}^{\sqcap}y \ \wedge\ {}^{\sqcap}y \mathbin{\square} x \sqsubseteq {}^{\sqcap}y \mathbin{\square} y \\
&\iff && \langle \text{ by Proposition 3.14-8 for } \Longleftarrow, \\
&&& \quad \text{and by Proposition 3.14-7 for } \Longrightarrow \text{ since, by Lemma 3.7-1,} \\
&&& \quad x \sqsubseteq {}^{\sqcap}y \mathbin{\square} x \sqsubseteq {}^{\sqcap}y \mathbin{\square} y \ \rangle \\
&\quad x \sqsubseteq y
\end{aligned}
$$

So $x \sqcup y = x \sqcup_A y$ by (3.11) and Proposition 2.10.

(b)
$$
\begin{aligned}
& x \mathbin{\square_A} y \\
=\ & && \langle \text{ by Definitions 2.12 and 2.8 } \rangle \\
& \neg_D {}^{\sqcap}(x \mathbin{\cdot_D} \neg_D {}^{\sqcap}y) \mathbin{\cdot_D} x \mathbin{\cdot_D} y \\
=\ & && \langle \text{ by Propositions 4.17-5 and 4.17-3, Boolean algebra, De} \\
&&& \quad \text{Morgan and Definition 4.16 } \rangle \\
& (\neg_D {}^{\sqcap}x \sqcap {}^{\sqcap}(x \mathbin{\square} {}^{\sqcap}y)) \mathbin{\square} (x \mathbin{\square} y \sqcap x_{{}^{\sqcap}y} \mathbin{\square} y) \\
=\ & && \langle \text{ by Corollary 3.21-5 and (3.20) } \rangle \\
& \neg_D {}^{\sqcap}x \mathbin{\square} (x \mathbin{\square} y \sqcap x_{{}^{\sqcap}y} \mathbin{\square} y) \sqcap {}^{\sqcap}(x \mathbin{\square} y) \mathbin{\square} (x \mathbin{\square} y \sqcap x_{{}^{\sqcap}y} \mathbin{\square} y) \\
=\ & && \langle \text{ by Corollary 3.21-4, Proposition 3.14-7, Boolean algebra,} \\
&&& \quad (3.20) \text{ and Remark 4.8 } \rangle \\
& (\top \mathbin{\square} x \mathbin{\square} y \sqcap \top \mathbin{\square} x_{{}^{\sqcap}y} \mathbin{\square} y) \sqcap (x \mathbin{\square} y \sqcap \top \mathbin{\square} x_{{}^{\sqcap}y} \mathbin{\square} y) \\
=\ & && \langle \text{ by (3.6) and Corollary 3.21-3 } \rangle \\
& x \mathbin{\square} y
\end{aligned}
$$

(c)
$$
\begin{aligned}
& x^{\times_A} \\
=\ & && \langle \text{ by Theorem 2.20 and Remark 3.2 } \rangle \\
& \mu_{\sqsubseteq_A}(y :: y \mathbin{\square_A} x \sqcup_A 1) \\
=\ & && \langle \text{ by the previous two derivations } \rangle \\
& \mu_{\sqsubseteq}(y :: y \mathbin{\square} x \sqcup 1) \\
=\ & && \langle \text{ by Remark 3.2 } \rangle
\end{aligned}
$$

(d)
$$
\begin{aligned}
& x^{\times} \\
& x \pitchfork_{At} y \\
= \quad & \langle \text{ by Definition 2.18 } \rangle \\
& t \cdot_D x +_D \neg_D t \cdot_D y \\
= \quad & \langle \text{ by Proposition 4.17-3 } \rangle \\
& t \circ x +_D \neg_D t \circ y \\
= \quad & \langle \text{ by Corollary 4.4-1 } \rangle \\
& (t \circ x \sqcup \neg_D t \circ y) \pitchfork \neg_D{}^{\sqcap}(t \circ x) \circ \neg_D t \circ y \pitchfork \neg_D{}^{\sqcap}(\neg_D t \circ y) \circ t \circ x \\
= \quad & \langle \text{ by Boolean algebra, Propositions 3.14-11 and 3.14-9, and De Morgan } \rangle \\
& \top \circ (t \circ x \sqcup \neg_D t \circ y) \pitchfork (\neg_D t \pitchfork \neg_D{}^{\sqcap} x) \circ \neg_D t \circ y \pitchfork (t \pitchfork \neg_D{}^{\sqcap} y) \circ t \circ x \\
= \quad & \langle \text{ by (3.6), Corollary 3.21-3 and Boolean algebra } \rangle \\
& \neg_D t \circ y \pitchfork t \circ x \\
= \quad & \langle \text{ by Boolean algebra, Corollary 3.21-9 and Proposition 3.20-2 } \rangle \\
& x \pitchfork_t y
\end{aligned}
$$

3. If $\phi : \mathcal{A} \to \mathcal{A}'$ is a homomorphism, then

$$
\begin{aligned}
\phi(x \sqcup y) &= \phi(x) \sqcup \phi(y) \ , && (5.16)\\
\phi(x \circ y) &= \phi(x) \circ \phi(y) \ , && (5.17)\\
\phi(x^{\times}) &= (\phi(x))^{\times} \ , && (5.18)\\
\phi(\top) &= \top' \ , && (5.19)\\
\phi(1) &= 1' \ , && (5.20)\\
\phi(\neg_D t) &= \neg_D(\phi(t)) \ , && (5.21)\\
\phi({}^{\sqcap} x) &= {}^{\sqcap}(\phi(x)) \ , && (5.22)\\
\phi(x \pitchfork_t y) &= \phi(x) \pitchfork_{\phi(t)} \phi(y) \ . && (5.23)
\end{aligned}
$$

We need to derive

$$
\begin{aligned}
\phi(x +_D y) &= \phi(x) +_D \phi(y) \ , && (5.24)\\
\phi(x \cdot_D y) &= \phi(x) \cdot_D \phi(y) \ , && (5.25)\\
\phi(x^{*_D}) &= (\phi(x))^{*_D} \ , && (5.26)\\
\phi(\top) &= \top' \ , && (5.27)\\
\phi(1) &= 1' \ , && (5.28)\\
\phi(\neg_D t) &= \neg_D(\phi(t)) \ , && (5.29)\\
\phi({}^{\sqcap} x) &= {}^{\sqcap}(\phi(x)) \ . && (5.30)
\end{aligned}
$$

(a) Proof of (5.24).

$$\begin{aligned}
&\phi(x +_D y)\\
=\quad &\langle \text{ by Corollary 4.4-1 } \rangle\\
&\phi((x \sqcup y) \pitchfork \neg_D{}^{\pi}\overline{y}\triangleright x \pitchfork \neg_D{}^{\pi}\overline{x}\triangleright y)\\
=\quad &\langle \text{ by Lemma 5.3, (5.16), (5.17), (5.21) and (5.22) } \rangle\\
&(\phi(x) \sqcup \phi(y)) \pitchfork \neg_D{}^{\pi}\overline{(\phi(y))}\triangleright\phi(x) \pitchfork \neg_D{}^{\pi}\overline{(\phi(x))}\triangleright\phi(y)\\
=\quad &\langle \text{ by Corollary 4.4-1 } \rangle\\
&\phi(x) +_D \phi(y)
\end{aligned}$$

(b) Proof of (5.25).

$$\begin{aligned}
&\phi(x \cdot_D y)\\
=\quad &\langle \text{ by Definition 4.16 } \rangle\\
&\phi(x\triangleright y \pitchfork x_{\pi_{\overline{y}}}\triangleright y)\\
=\quad &\langle \text{ by Lemmas 5.3 and 5.4, (5.17) and (5.22) } \rangle\\
&\phi(x)\triangleright\phi(y) \pitchfork \phi(x)_{\pi_{\overline{(\phi(y))}}}\triangleright\phi(y)\\
=\quad &\langle \text{ by Definition 4.16 } \rangle\\
&\phi(x) \cdot_D \phi(y)
\end{aligned}$$

(c) Proof of (5.26).

$$\begin{aligned}
&\phi(x^{*_D})\\
=\quad &\langle \text{ by Definition 4.19 } \rangle\\
&\phi((x \pitchfork 1)^{\times})\\
=\quad &\langle \text{ by (5.18), Lemma 5.3 and (5.20) } \rangle\\
&(\phi(x) \pitchfork 1')^{\times}\\
=\quad &\langle \text{ by Definition 4.19 } \rangle\\
&\phi(x)^{*_D}
\end{aligned}$$

(d) Proof of (5.27). This is direct from (5.19).

(e) Proof of (5.28). This is direct from (5.20).

(f) Proof of (5.29). This is direct from (5.21).

(g) Proof of (5.30). This is direct from (5.22). □

We easily deduce the following Galois connection from Theorems 5.5 and 5.6.

Corollary 5.7. *Let $\mathcal{K}$ be a KAD, $\mathcal{A}$ be an algebra of decomposable elements and let $\mathcal{F}$ and $\mathcal{G}$ be the transformations introduced in Definition 5.1. Then*

$$\mathcal{F}(\mathcal{K}) \preccurlyeq \mathcal{A} \iff \mathcal{K} \preccurlyeq \mathcal{G}(\mathcal{A}) \ .$$

Theorem 5.5, Theorem 5.6 and Corollary 5.7 together with their proof show why it is necessary and sufficient to work with algebras of decomposable elements in order to establish the desired duality.

Chapter 6

Algebras of Ordered Pairs

Thanks to Theorems 2.20, 2.21, 2.22 and 2.23, one can use Lemma 4.11 to construct models of DAD-$\mathbb{F}_\bullet$ from models of KAD-based DAD-$\mathbb{F}_\bullet$. Lemma 4.11 can also be used to construct models of DAD-$\mathbb{F}_\bullet$ from other models of DAD-$\mathbb{F}_\bullet$. These models are algebras of ordered pairs. It turns out that pair-based representations have been used numerous times in program semantics, such as in [BZ86, Doo94, HMS06, MS05, Par83], to cite just a few. In this chapter, we deal with algebras of ordered pairs related to our problems of algebraic connections between the different parts of the lattice of Figure 1.4.

In Section 6.1, thanks to Lemma 4.11, we present a semantics of programs that might help understand DAD-$\mathbb{F}_\bullet$. In Section 6.2, we present a result from [DD06c, DD08b] that establishes an algebraic connection between the bottom part of the lattice and the whole lattice of Figure 1.4.

These two sections talk about algebras of ordered pairs in two different contexts that are close to our subject. One is related to semantics and the other to transformation. This is a short chapter that displays several informations that are relevant to this thesis but that did not fit the exact goals of the previous chapters.

6.1 DAD-$\mathbb{F}_\bullet$ and Program Semantics

The main results of Section 2.5, Section 4.5 and Chapter 5 are about algebras of decomposable elements. Any algebra of decomposable elements is isomorphic to a KAD-based DAD-$\mathbb{F}_\bullet$ and vice versa. A legitimate question would be: what about nondecomposable

Figure 6.1: Hasse diagram of Example 6.1.

elements? According to Definition 4.7, there are two ways for an element not to be decomposable. It can either admit multiple decompositions or it can admit no decomposition at all. How can we deal with all those elements in the realm of programs?

There is the beginning of an answer in Lemma 4.11. As we explained in Example 4.12, this lemma enables to construct models of DAD-⊓ containing elements with multiple decompositions.

Actually, it can also give birth to algebras of decomposable elements. Indeed, look at the following example.

Example 6.1. Take $A = \mathsf{test}(A) = \{\top, 1\}$. The operators defined by the following tables, omitting ⊓, make $(A, \mathsf{test}(A), \sqcup, \circ, \times, \top, 1, \neg, \sqcap, \overline{\top}, \sqcap)$ a DAD-⊓.

$\sqcup$	$\top$	1
$\top$	$\top$	$\top$
1	$\top$	1

$\circ$	$\top$	1
$\top$	$\top$	$\top$
1	$\top$	1

	$\times$
$\top$	$\top$
1	1

	$\neg$
$\top$	1
1	$\top$

	$\overline{\top}$
$\top$	$\top$
1	1

The refinement ordering corresponding to $\sqcup$ is represented in the lattice of Figure 6.1. Then, using Lemma 4.11, one gets a DAD-⊓ with $E = \{(1,1),(1,\top),(\top,\top)\}$ and $T = \{(1,1),(\top,\top)\}$. Since the only tests are $\mathsf{1} = (1,1)$ and $\overline{\top} = (\top,\top)$, and since all elements of a DAD-⊓ are $\mathsf{1}$-decomposable and $\overline{\top}$-decomposable by Remark 4.9, then we have an algebra of decomposable elements.

We do not know whether there is a way to construct models of DAD-⊓ containing elements that admit no decomposition using Lemma 4.11. However, we propose the following interpretation for these algebras of ordered pairs. Let $\mathcal{A}$ be a DAD-⊓ and take $x \in A$ and $s \in \mathsf{test}(A)$. An ordered pair (x, s) (with $\overline{\top}x \sqsubseteq s$) in such an algebra created by Lemma 4.11 may be thought of as a program via the following semantics.

- For those states in s, we know that the program terminates successfully and it behaves like $s \circ x$.
- For those states in $\overline{\top}x$ but not in s (read $\neg s \circ \overline{\top}x$), we do not know how the program behaves with respect to termination. If ever the program terminates successfully, it behaves like $\neg s \circ x$.

- For those states outside $\urcorner x$ (read $\neg\urcorner x$), there is at least one possibility of unsuccessful termination for the program x. The program may also terminate, but the semantics is demonic and considers that the program has no output.

Therefore, for a test (s, s),

- for those states in s, we know that the program s terminates successfully and it behaves like s.
- There are no such states that are in s but not in s.
- For those states outside s, there is at least one possibility of unsuccessful termination for the program s.

The elements having the form $(x, \urcorner x)$ and the tests are the only elements for which there is no doubt.

This semantics agrees perfectly with the definitions of the operators $\oplus$, $\odot$, $^{\circledast}$, $\overline{}$, $\Cap$, $\ulcorner$ and $\Cap_{\bullet}$ of Lemma 4.11. Further investigation needs to be done about Lemma 4.11, Examples 4.10, 4.12 and 6.1, and this semantics (see Section 7.1).

At first sight, the semantics we just presented is not that far from the relational semantics studied by Parnas [Par83]. However, they are different. In his paper, he studies an algebra of ordered pairs (R, C), where R is a relation and $C \subseteq \ulcorner R$. C is called a *competence set* and it does not have the same interpretation as the tests in the ordered pairs of Lemma 4.11. Indeed, look at Table 6.1 (taken from [Par83]) that gives a summary of the semantics of an ordered pair (R, C) representing a program P in Parnas' algebra. Note that in this table, x and y do not stand for relations, but rather for states.

Let us point out two differences between the algebra of ordered pairs of Lemma 4.11 and Parnas' algebra. Those differences can be understood without explaining in detail the work of Parnas. Firstly, Parnas supposes a complete knowledge of the programs represented by the ordered pairs. The semantics proposed with the algebra of Lemma 4.11 only supposes partial information (when the program is in those states in $\neg s \triangleright \urcorner x$). Secondly, Parnas' point of view is both angelic and demonic, while ours is exclusively demonic. Indeed, look at the definition of composition of ordered pairs. According to Parnas' algebra,

$$(R_1, C_1) \circ (R_2, C_2) = (R_1 \cdot R_2, \ulcorner(C_1 \triangleright R_1 \triangleright C_2)) \ ,$$

Behavior of program P	Competence set C	$\ulcorner R$	R
P terminates when started in x	Includes x	Includes x	Includes (x, y) if P might terminate in y when started in x
P sometimes terminates when started in x	Does not include x	Includes x	Includes (x, y) if P might terminate in y when started in x
P never terminates when started in x	Does not include x	Does not include x	No pairs of the form (x, y)
P never terminates	Empty	Empty	Empty
P is never guaranteed to terminate but may	Empty	Nonempty	Includes (x, y) if P might terminate in y when started in x

Table 6.1: Semantics of the algebra of ordered pairs of Parnas [Par83].

where $\cdot$ is the usual (angelic) composition of relations and $\boxdot$ is the standard demonic composition of relations. But, according to Lemma 4.11,

$$(x, s) \odot (y, t) = (x \boxdot y, \sqcap(s \boxdot x \boxdot t)) \ .$$

6.2 Another Algebraic Connection

In this section, we cite an important result from [DD06c, DD08b] stating that, under suitable hypotheses, there is an algebraic connection between the bottom part of the lattice and the whole lattice of Figure 1.4 (Theorem 6.7). It is a quick presentation but it is so closely related to this thesis that it cannot be eluded. See [DD06c, DD08b] for demonstrations.

The suitable hypotheses mentioned above are related to the following operator.

Definition 6.2 (Divergence operator)**.** *Let $\mathcal{K}$ be a KAD and take $x \in K$. The* divergence of x *[DMS06a], noted ∇x, is axiomatised by*

$$\begin{array}{rcl} \nabla x & \leq & \ulcorner(x \cdot \nabla x) \\ t \leq \ulcorner(x \cdot t) & \Longrightarrow & t \leq \nabla x \end{array}$$

for all $t \in \mathsf{test}(K)$.

The divergence of x is a test that characterizes those states from which x might iterate indefinitely. One can demonstrate that $\nabla x = \nu(t : \mathsf{test}(K) : \ulcorner(x \cdot t))$. In order to illustrate this new operator, let us calculate the divergence operator for some relations defined over $S_3 = \{1, 2, 3\}$. Take $x = \{(1, 2), (2, 1), (2, 2), (3, 3)\}$, $y = \{(1, 2)\}$ and $z = \{(1, 1)\}$. Then $\nabla x = \{(1, 1), (2, 2), (3, 3)\}$, $\nabla y = \{\}$ and $\nabla z = \{(1, 1)\}$. Given a KAD, we do not know whether ∇x exists for all elements x. However, when needed, we will suppose its existence.

We mentioned in the introduction (Chapter 1) that *demonic refinement algebra with enabledness* (DRAe) [Sol07, SvW06] is an algebraic structure that has the positively conjunctive predicate transformers as its intended model. Moreover, it is an algebraic description of the whole lattice of Figure 1.4 [DD06c, DD08b]. The following definitions are going to lead to DRAe (Definition 6.4). We skip many details, but what the reader ought to keep in mind is that DRAe is an algebraic foundation for the whole lattice of Figure 1.4.

Definition 6.3 (Demonic refinement algebra)**.** *A* demonic refinement algebra *(DRA) is a structure* $\mathcal{D} = (D, +, \cdot, ^*, ^\omega, 0, 1)$ *such that the following properties are satisfied for all* $x, y, z \in D$*.*

$$\begin{aligned}
x + (y + z) &= (x + y) + z && (6.1)\\
x + y &= y + x && (6.2)\\
x + x &= x && (6.3)\\
0 + x &= x && (6.4)\\
x \cdot (y \cdot z) &= (x \cdot y) \cdot z && (6.5)\\
0 \cdot x &= 0 && (6.6)\\
1 \cdot x &= x \cdot 1 = x && (6.7)\\
x \cdot (y + z) &= x \cdot y + x \cdot z && (6.8)\\
(x + y) \cdot z &= x \cdot z + y \cdot z && (6.9)\\
x^* &= x^* \cdot x + 1 && (6.10)\\
x^\omega &= x^\omega \cdot x + 1 && (6.11)\\
x^\omega &= x^* + x^\omega \cdot 0 && (6.12)
\end{aligned}$$

There is a partial order $\leq$ *induced by* $+$ *such that for all* $x, y \in D$*,*

$$x \leq y \iff x + y = y \ . \qquad (6.13)$$

The next two properties are also satisfied for all $x, y, z \in D$*.*

$$\begin{aligned}
x \cdot z + y \leq z &\implies x^* \cdot y \leq z && (6.14)\\
z \cdot x + y \leq z &\implies y \cdot x^* \leq z && (6.15)\\
z \leq x \cdot z + y &\implies z \leq x^\omega \cdot y && (6.16)
\end{aligned}$$

As in KA or in DA, it is easy to verify that $\leq$ is a partial order. However, there are two major differences between DRA and KA. Firstly, there is an additional operator in DRA, namely $^\omega$. Secondly, the laws of DRA do not ask for $x \cdot 0 = 0$. If we compare DRA to DA, again there is this extra operator $^\omega$ in DRA. Also, DA does not contain any 0 element. However, as for DA, DRA admits a top element. Indeed, the top element is

$$\top = 1^\omega \ .$$

One can show that in DRA, $\top \cdot x = \top$ for all $x \in D$, but that there exists $x \in D$ such that $x \cdot \top \neq \top$ (unlike in DA). Indeed, $0 \cdot \top = 0 \neq \top$.

We now define a concept close to that of tests. Let $\mathcal{D}$ be a DRA. An element $t \in D$ that has a complement $\neg t$ satisfying

$$t \cdot \neg t = \neg t \cdot t = 0 \qquad \text{and} \qquad t + \neg t = 1$$

is called a *guard*. Let $\mathsf{guard}(D)$ be the set of guards of $\mathcal{D}$. Then $(\mathsf{guard}(D), +, \cdot, \neg, 0, 1)$ is a Boolean algebra.

Then we are ready to define DRAe. It includes the *enabledness operator* that reminds of the domain operator of KAD and DAD.

Definition 6.4 (Demonic refinement algebra with enabledness)**.** *A* demonic refinement algebra with enabledness *(DRAe) is a structure* $\mathcal{D} = (D, \mathsf{guard}(D), +, \cdot, {}^*, {}^\omega, 0, 1, \neg, {}^\ulcorner)$ *such that* $(D, +, \cdot, {}^*, {}^\omega, 0, 1)$ *is a DRA,* $\mathsf{guard}(D)$ *is the set of guards and the* enabledness operator ${}^\ulcorner : D \to \mathsf{guard}(D)$ *satisfies the following axioms for all* $x \in D$ *and all* $t \in \mathsf{guard}(D)$*.*

$$\begin{aligned} {}^\ulcorner x \cdot x &= x \ , \\ {}^\ulcorner(t \cdot x) &\leq t \ , \\ {}^\ulcorner(x \cdot y) &= {}^\ulcorner(x \cdot {}^\ulcorner y) \ , \\ {}^\ulcorner x \cdot \top &= x \cdot \top \ . \end{aligned}$$

The following proposition explains how one can always find a KAD at the bottom of a DRAe, like in the lattice of Figure 1.4. Moreover, this KAD has two important properties.

Proposition 6.5. *Let* $\mathcal{D}$ *be a DRAe and consider* $K_D = \{x : D \mid x \cdot 0 = 0\}$*. Then* $(K_D, \mathsf{guard}(D), +, \cdot, {}^*, 0, 1, \neg, {}^\ulcorner)$ *is a KAD where* $\triangledown x$ *exists for all* $x \in K_D$*. Also, for all* $x, y, z \in K_D$*,*

$$\triangledown x = {}^\ulcorner(x^\omega \cdot 0) \qquad \textit{and} \qquad \triangledown x = 0 \wedge z \leq x \cdot z + y \implies z \leq x^* \cdot y \ .$$

So the structure of Figure 1.4 is not a coincidence.

Lastly, here is the algebra of ordered pairs that is behind the promised algebraic connection.

Lemma 6.6. *Let* $\mathcal{K}$ *be a KAD such that*

$$\triangledown x \textit{ exists for all } x \in K \qquad \textit{and} \qquad \triangledown x = 0 \wedge z \leq x \cdot z + y \implies z \leq x^* \cdot y \ . \tag{6.17}$$

Consider $E = \{(x, t) : K \times \mathsf{test}(K) \mid t \cdot x = 0\}$ *and* $T = \{(t, 0) : \mathsf{test}(K) \times \mathsf{test}(K)\}$ *and define the following operations for elements of* E*, where* $x, y \in K$ *and* $s, t \in \mathsf{test}(K)$*.*

$$\begin{aligned} (x, s) \oplus (y, t) &= (\neg(s + t) \cdot (x + y), s + t) \\ (x, s) \odot (y, t) &= (\neg{}^\ulcorner(x \cdot t) \cdot x \cdot y, s + {}^\ulcorner(x \cdot t)) \end{aligned}$$

$$\begin{aligned}
(x,s)^{\circledast} &= (\neg\ulcorner(x^*\cdot t)\cdot x^*, \ulcorner(x^*\cdot t))\\
(x,s)^{\tilde{\omega}} &= (\neg\ulcorner(x^*\cdot t)\cdot\neg\triangledown x\cdot x^*, \ulcorner(x^*\cdot t)+\triangledown x)\\
\neg(t,0) &= (\neg t,0)\\
\ulcorner(x,s) &= (\ulcorner x+t,0)
\end{aligned}$$

Then $(E,T,\oplus,\odot,^{\circledast},^{\tilde{\omega}},(0,0),(1,0),\neg,\ulcorner)$ *is a DRAe and the partial order* $\sqsubseteq$ *related to* $\oplus$ *satisfies*

$$(x,s)\sqsubseteq(y,t) \iff s\leq t\wedge\neg t\cdot x\leq y \ .$$

And here is the algebraic connection.

Theorem 6.7.

1. *Every DRAe is isomorphic to an algebra of ordered pairs as in Lemma 6.6. The isomorphism is given by*

$$\phi(x)=(\neg\ulcorner(x\cdot 0)\cdot x, \ulcorner(x\cdot 0)) \ ,$$

   with inverse

$$\psi((x,s))=x+s\cdot\top \ .$$

2. *Every KAD* $\mathcal{K}$ *satisfying (6.17) can be embedded in a DRAe* $\mathcal{D}$ *in such a way that* D_K *(see Proposition 6.5) is the image of* K *by the embedding.*

In conclusion, thanks to Theorems 5.5 and 5.6, one can freely travel between KADs and DAD-⊓s, as long as the DAD-⊓s are algebras of decomposable elements. Also, thanks to Theorem 6.7, one can freely travel between KADs and DRAes, as long as the KADs satisfy (6.17). We summarize these transformations in the lattice of Figure 6.2 which is a more complete version of the lattice of Figure 1.4. In this lattice, we use the following notations.

$$\mathsf{0}=\begin{pmatrix}0&0\\0&0\end{pmatrix}\quad \mathsf{s}=\begin{pmatrix}1&0\\0&0\end{pmatrix}\quad \mathsf{t}=\begin{pmatrix}0&0\\0&1\end{pmatrix}\quad \mathsf{1}=\begin{pmatrix}1&0\\0&1\end{pmatrix}$$

$$\mathsf{a}=\begin{pmatrix}1&0\\1&1\end{pmatrix}\quad \mathsf{b}=\begin{pmatrix}1&1\\0&1\end{pmatrix}\quad \mathsf{c}=\begin{pmatrix}1&1\\1&1\end{pmatrix}\quad \mathsf{d}=\begin{pmatrix}1&1\\0&0\end{pmatrix}$$

$$\mathsf{e}=\begin{pmatrix}0&0\\1&1\end{pmatrix}\quad \mathsf{f}=\begin{pmatrix}1&0\\1&0\end{pmatrix}\quad \mathsf{g}=\begin{pmatrix}0&1\\0&1\end{pmatrix}\quad \mathsf{h}=\begin{pmatrix}0&1\\0&0\end{pmatrix}$$

$$\mathsf{i}=\begin{pmatrix}0&0\\1&0\end{pmatrix}\quad \mathsf{j}=\begin{pmatrix}0&1\\1&0\end{pmatrix}\quad \mathsf{k}=\begin{pmatrix}0&1\\1&1\end{pmatrix}\quad \mathsf{l}=\begin{pmatrix}1&1\\1&0\end{pmatrix}$$

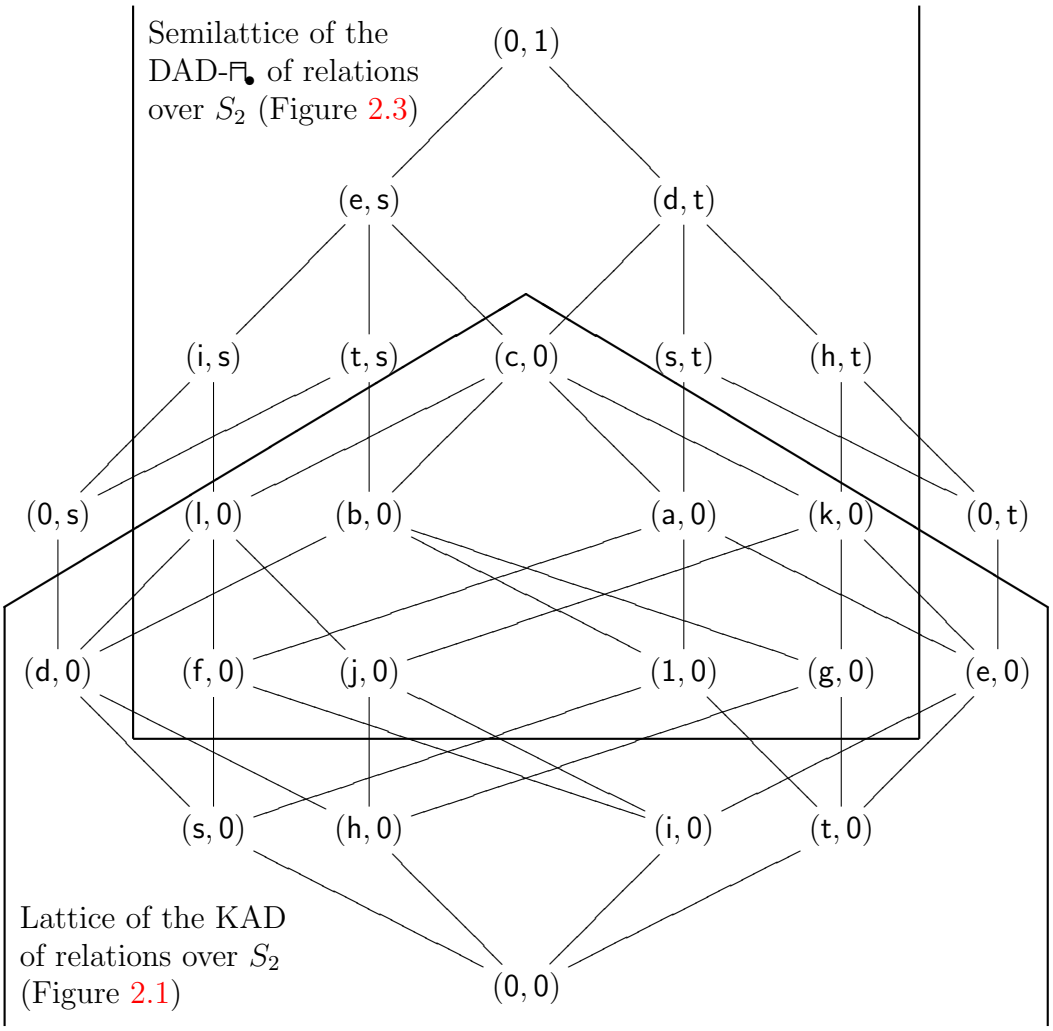


Figure 6.2: Lattice of the DRAe of positively conjunctive predicate transformers over S_2, a synthesis of the semilattices of Figures 2.1 and 2.3.

The conjunctive predicate transformer f corresponding to a pair (x, t) is given by $f(s) = \neg t \cdot \neg^{\lceil}(x \cdot \neg s)$. 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 ($\neg^{\lceil}(x \cdot \neg s)$).

The predicate transformers for all pairs follow. The entry for line $(\mathsf{k}, \mathsf{0})$ and column t, for instance, is s because $f(\mathsf{t}) = \neg\mathsf{0} \cdot \neg^{\lceil}(\mathsf{k} \cdot \neg\mathsf{t}) = \mathsf{s}$.

	0	s	t	1
$(0,1)$	0	0	0	0
(e,s)	0	0	0	t
(d,t)	0	0	0	s
(i,s)	0	t	0	t
(t,s)	0	0	t	t
$(c, 0)$	0	0	0	1
(s,t)	0	s	0	s
(h,t)	0	0	s	s
$(0,\mathsf{s})$	t	t	t	t

	0	s	t	1
$(\mathsf{l},0)$	0	t	0	1
$(\mathsf{b},0)$	0	0	t	1
$(\mathsf{a},0)$	0	s	0	1
$(\mathsf{k},0)$	0	0	s	1
$(0,\mathsf{t})$	s	s	s	s
$(\mathsf{d},0)$	t	t	t	1
$(\mathsf{f},0)$	0	1	0	1
$(\mathsf{j},0)$	0	t	s	1

	0	s	t	1
$(1,0)$	0	s	t	1
$(\mathsf{g},0)$	0	0	1	1
$(\mathsf{e},0)$	s	s	s	1
$(\mathsf{s},0)$	t	1	t	1
$(\mathsf{h},0)$	t	t	1	1
$(\mathsf{i},0)$	s	1	s	1
$(\mathsf{t},0)$	s	s	1	1
$(0,0)$	1	1	1	1

Chapter 7

Conclusion

At the very beginning of this research, when we first got aware of Figure 1.4, we were trying to answer two questions.

1. If we define demonic operators from the (angelic) operators of KAD and then forget the angelic ones, what kind of algebraic structure do we get?
2. We can define demonic operators from the angelic ones. Is it possible to do the opposite?

The goal of the first question was to get a better understanding of some of the algebraic structures that exist in the landscape of the semantics of programs. The goal of the second question (that is, somehow, also related to the first one) was to compare in an algebraic way angelic semantics and demonic semantics. Our work led us to a new algebraic structure that we call "demonic algebra with domain and t-conditional".

Why did we have to define a new algebraic structure in order to understand other algebraic structures that already exist? The lattice of Figure 1.4 (see also Figure 6.2) that has been cited so many times hides a strong algebraic activity. There was an algebraic foundation for the lower part (KAD) and for the whole lattice (DRAe), but there was no algebraic foundation for the upper part. Once this upper part has been given structure, then we were able to look for algebraic connections. Those connections are described in Theorems 5.5, 5.6 and 6.7.

What we get if we define demonic operators from the (angelic) operators of KAD and then forget the angelic ones turned out to be way more complicated than expected.

What we first planned to be a gentle algebraic structure that we would have called[1] "Demonic Kleene Algebra" turned out to be a deep algebraic object that is an algebra of what we call decomposable elements. If one thinks about some complicated proofs like the one of Theorem 4.31-12 that is thirty pages long, one might ask whether algebra of decomposable elements is manageable enough to work with. What makes algebra of decomposable elements powerful is not how easy it is to prove some of its properties. It is rather its duality with KAD. Now that we have established an algebraic connection, we can easily go from one world to the other. Let us say a demonic problem is easier to solve in the angelic world. Then use $\mathcal{G}$ (from Definition 5.1) to get in a better context for the resolution of the problem and translate back the answer with $\mathcal{F}$ (also from Definition 5.1). In other words, we get the best of both worlds.

7.1 Open Questions

The passage between the lower part and the upper part of the lattice of Figure 1.4 is not the only one that exists. Theorem 6.7 tells us that there is a connection with the whole lattice too. Now, relations, predicate transformers, KAs, DRAes and DAD-$⊓_•$ are intimately related. However, this work does not only reveal the beauties of that now-famous lattice, it also raises many questions. We have gathered some open problems related to this field of research in this final section.

Firstly, we know that the canonical models (i.e. the free algebras) of algebras of decomposable elements are the same as for KAD-based DAD-$⊓_•$. Indeed, these two structures are isomorphic by Theorems 5.5 and 5.6. Once the problem is solved for KAD, it is solved for the algebra of decomposable elements. Indeed, note $\mathcal{M}$ a canonical model of KAD. Then $\mathcal{F}(\mathcal{M})$ is a canonical model of the algebra of decomposable elements.

Now, think about it as a decidability problem. Suppose we have an algorithm for deciding equalities in KAD. Let $\mathcal{A}$ be an algebra of decomposable elements. Let us say we want to know if $x = y$ is true ($x = y$ being an equality in $\mathcal{A}$). Then here is an algorithm giving the answer.

1. In $x = y$, replace respectively the operators $⊔$, $▫$, $^\times$, $\neg$, $⌜$ and $⊓_•$ by $⊔_A$, $▫_A$, $^{\times_A}$, $\neg$, $⌜$ and $⊓_{A•}$. The equality is now an expression in $\mathcal{G}(\mathcal{A})$.

2. In the equality obtained at the previous step, translate every operators using

[1] We kept the name "Demonic Kleene Algebra" for the title of this thesis because it says in three words what we did in two hundred and twenty-nine pages.

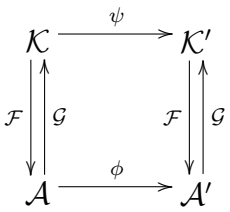


Figure 7.1: Commutative diagram for Theorems 5.5 and 5.6.

Proposition 2.10 and Definitions 2.12, 2.14 and 2.18. The equality is now an expression in $\mathcal{G}(\mathcal{A})$ written exclusively with angelic operators.

3. Apply the algorithm for KAD.

We now ask what are the canonical models for DA, DAT, DAD and DAD-⊓• (without the restriction to decomposable elements)? And what about decidability?

We algebraically linked KADs, DRAes and DAD-⊓•. Would it be possible to establish links with other structures? Since we want to put together angelic and demonic semantics, it would be interesting to find a link with multirelations [MCR04, MCR07, Rew03] that basically mix those semantics. Moreover, links between predicate transformers and multirelations have already been pointed out [RB06]. Thinking about other algebraic structures, why would not there be a link with probabilistic algebraic structures for semantics of programs? Among other aspects, the resemblance between the *probabilistic choice operator* ${}_p\oplus$ from [MH08, MS08a, MS08b] and the operator ⊓• needs to be studied.

There is also the category theory point of view. We can rewrite Theorems 5.5 and 5.6 with the commutative diagram of Figure 7.1. What more can we learn from category theory?

Finally, the discussion of Section 6.1 must be completed. On the one hand, what is the difference between elements that admit no decomposition and elements that admit multiple decompositions? On the other hand, we need to clarify how the semantics suggested can be used in practice.

Bibliography

[Bro89] J. G. Brookshear. *Theory of Computation: Formal Language, Automata, and complexity*. The Benjamin/Cummings Publishing Company, Inc., 1989.

[BvdW93] Roland Carl Backhouse and Jaap van der Woude. Demonic operators and monotype factors. *Mathematical Structures in Computer Science*, 3(4):417–433, 1993.

[BvW92] R. J. R. Back and J. von Wright. Combining angels, demons and miracles in program specifications. *Theoretical Computer Science*, 100:365–383, 1992.

[BZ86] R. Berghammer and H. Zierer. Relational algebraic semantics of deterministic and nondeterministic programs. *Theoretical Computer Science*, 43:123–147, 1986.

[Con71] J.H. Conway. *Regular Algebra and Finite Machines*. Chapman and Hall, London, 1971.

[DBS+95] J. Desharnais, N. Belkhiter, S.B.M. Sghaier, F. Tchier, A. Jaoua, A. Mili, and N. Zaguia. Embedding a demonic semilattice in a relation algebra. *Theoretical Computer Science*, 149:333–360, 1995.

[DD06a] Jean-Lou De Carufel and Jules 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.

[DD06b] Jean-Lou De Carufel and Jules Desharnais. Demonic algebra with domain. In R. A. Schmidt, editor, *9th International Conference on Relational Methods in Computer Science and 4th International Workshop on Applications of Kleene Algebra*, volume 4136 of *Lecture Notes in Computer Science*, pages 120–134, 2006.

[DD06c] Jean-Lou De Carufel and Jules Desharnais. On the structure of demonic refinement algebras. Research report DIUL-RR-0802, Département d'informatique et de génie logiciel, Université Laval, Canada, 2006.

[DD08a] Jean-Lou De Carufel and Jules Desharnais. Latest news about demonic algebra with domain. In *10th International Conference on Relational Methods in Computer Science and 5th International Workshop on Applications of Kleene Algebra*, volume 4988 of *Lecture Notes in Computer Science*, pages 54–68, 2008.

[DD08b] Jean-Lou De Carufel and Jules Desharnais. On the structure of demonic refinement algebras with enabledness and termination. In *10th International Conference on Relational Methods in Computer Science and 5th International Workshop on Applications of Kleene Algebra*, volume 4988 of *Lecture Notes in Computer Science*, pages 69–83, 2008.

[Dij76] E.W. Dijkstra. *A Discipline of Programming*. Prentice Hall, 1976.

[DM01] Jules Desharnais and Bernhard Möller. Characterizing determinacy in Kleene algebras. *Information Sciences*, 139(3–4):253–273, December 2001.

[DMN97] J. Desharnais, A. Mili, and T.T. Nguyen. Refinement and demonic semantics. In C. Brink, W. Kahl, and G. Schmidt, editors, *Relational Methods in Computer Science*, pages 166–183. Springer, 1997.

[DMS04] Jules Desharnais, Bernhard Möller, and Georg Struth. Modal Kleene algebra and applications — a survey. *JoRMiCS — Journal on Relational Methods in Computer Science*, 1:93–131, 2004.

[DMS06a] Jules Desharnais, Bernhard Möller, and Georg Struth. Algebraic notions of termination. Technical Report 2006-23, Institut für Informatik, Augsburg, Germany, October 2006.

[DMS06b] Jules Desharnais, Bernhard Möller, and Georg Struth. Kleene algebra with domain. *ACM Transactions on Computational Logic*, 7(4):798–833, 2006.

[DMT00] J. Desharnais, B. Möller, and F. Tchier. Kleene under a demonic star. In *AMAST 2000*, volume 1816 of *Lecture Notes in Computer Science*, pages 355–370. Springer, May 2000.

[DMT06] Jules Desharnais, Bernhard Möller, and Fairouz Tchier. Kleene under a modal demonic star. *Journal of Logic and Algebraic Programming, Special issue on Relation Algebra and Kleene Algebra*, 66(2):127–160, February-March 2006.

[Doo94] Henk Doornbos. A relational model of programs without the restriction to Egli-Milner-monotone constructs. In *Proceedings of the IFIP TC2/WG2.1/WG2.2/WG2.3 Working Conference on Programming Concepts, Methods and Calculi*, pages 363–382, Amsterdam, The Netherlands, The Netherlands, 1994. North-Holland Publishing Co.

[HHJ+87] C. A. R. Hoare, I. J. Hayes, He Jifeng, C. C. Morgan, A. W. Roscoe, J. W. Sanders, I. H. Sorensen, J. M. Spivey, and B. A. Sufrin. Laws of programming. *Communications of the ACM*, 30(8):672–686, 1987.

[HJ98] C. A. R. Hoare and He Jifeng. *Unifying Theories of Programming*. International Series in Computer Science. Prentice Hall, 1998.

[HMS06] Peter Höfner, Bernhard Möller, and Kim Solin. Omega algebra, demonic refinement algebra and commands. In Renate A. Schmidt, editor, *9th International Conference on Relational Methods in Computer Science and 4th International Workshop on Applications of Kleene Algebra*, volume 4136 of *Lecture Notes in Computer Science*, pages 222–234, 2006.

[Hol96] Marco Hollenberg. Equational axioms of test algebra, 1996. Logic Group Preprint Series 172, Department of Philosophy, Utrecht University. Available at http://citeseer.ifi.unizh.ch/hollenberg96equational.html.

[Jec73] T. Jech. *The Axiom of Choice*. Elsevier Science, 1973.

[Kah01] Wolfram Kahl. Parallel composition and decomposition of specifications. *Information Sciences*, 139(3–4):197–220, 2001.

[Koz90] Dexter Kozen. On Kleene algebras and closed semirings. In B. Rovan, editor, *Mathematical Foundations of Computer Science 1990*, volume 452 of *Lecture Notes In Computer Science*, pages 26–47. Springer, 1990.

[Koz94] D. Kozen. A completeness theorem for Kleene algebras and the algebra of regular events. *Information and Computation*, 110(2):366–390, May 1994.

[Koz97] D. Kozen. Kleene algebra with tests. *ACM Transactions on Programming Languages and Systems*, 19(3):427–443, 1997.

[Mac] Mace4. http://www.cs.unm.edu/~mccune/mace4/.

[Mad96] R.D. Maddux. Relation-algebraic semantics. *Theoretical Computer Science*, 160:1–85, 1996.

[McC63] John McCarthy. A basis for a mathematical theory of computation. In P. Braffort and D. Hirschberg, editors, *Computer Programming and Formal*

Systems, pages 33–70. North-Holland, Amsterdam, 1963. Available at http://www-formal.stanford.edu/jmc/basis/basis.html.

[MCR04] C.E. Martin, S.A. Curtis, and I. Rewitzky. Modelling nondeterminism. In *Mathematics of Program Construction*, volume 3125, pages 228–251. Springer, 2004.

[MCR07] C. E. Martin, S. A. Curtis, and I. Rewitzky. Modelling angelic and demonic nondeterminism with multirelations. *Science of Computer programming*, 65:140–158, 2007.

[MH08] L. Meinicke and I.J. Hayes. Probabilistic choice in refinement algebra. In *Mathematics of Program Construction*, volume 5133 of *Lecture Notes in Computer Science*, pages 243–267, 2008.

[MS05] Bernhard Möller and Georg Struth. wp. In Wendy MacCaull, Michael Winter, and Ivo Düntsch, editors, *8th International Conference on Relational Methods in Computer Science and 3rd International Workshop on Applications of Kleene Algebra*, volume 3929 of *Lecture Notes in Computer Science*, pages 200–211, 2005.

[MS08a] L.A. Meinicke and K. Solin. Reactive probabilistic programs and refinement algebra. In *10th International Conference on Relational Methods in Computer Science and 5th International Workshop on Applications of Kleene Algebra*, volume 4988 of *Lecture Notes in Computer Science*, pages 304–319, 2008.

[MS08b] L.A. Meinicke and K. Solin. Refinement algebra for probabilistic programs. *Electronic Notes in Theoretical Computer Science*, 201:177–195, 2008.

[Par83] D.L. Parnas. A generalized control structure and its formal definition. *Communications of the ACM*, 26(8):572–581, 1983.

[RB06] Ingrid Rewitzky and Chris Brink. Monotone predicate transformers as up-closed multirelations. In R. A. Schmidt, editor, *9th International Conference on Relational Methods in Computer Science and 4th International Workshop on Applications of Kleene Algebra*, volume 4136 of *Lecture Notes in Computer Science*, pages 311–327. Springer, August 2006.

[Rew03] I. Rewitzky. Binary multirelations. In *Theory and Applications of Relational Structures as Knowledge Instruments*, volume 2929 of *Lecture Note in Computer Science*, pages 256–271. Springer, 2003.

[Sol07] K. Solin. *Abstract Algebra of Program Refinement*. PhD thesis, Turku Center for Computer Science, University of Turku, Finland, 2007.

[Som06] I. Sommerville. *Software engineering*. Pearson Education, 8th edition, 2006.

[SS93] G. Schmidt and T. Ströhlein. *Relations and Graphs - Discrete Mathematics for Computer Scientists*. EATCS Monographs on Theoretical Computer Science. Springer, 1993.

[SvW06] Kim Solin and Joakim 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.

[Tar41] A. Tarski. On the calculus of relations. *Journal of Symbolic Logic*, 6(3):73–89, 1941.

[TD99] F. Tchier and J. Desharnais. Applying a generalization of a theorem of Mills to generalized looping structures. In *Colloquium on Science and Engineering for Software Development, organised in the memory of Dr. Harlan D. Mills, and affiliated to the 21st International Conference on Software Engineering*, pages 31–38, Los Angeles, May 1999.

[vW04] J. von Wright. Towards a refinement algebra. *Science of Computer Programming*, 51:23–45, 2004.

Appendix A

Demonstration of Lemma 4.11

In this appendix, we demonstrate Lemma 4.11. We first recall its terms.

Lemma 4.11. *Let* $(A, \mathsf{test}(A), \sqcup, \circ, ^{\times}, \top, 1, \neg, \pitchfork, {}^{\sqcap}, \pitchfork_\bullet)$ *be a DAD-*$\pitchfork_\bullet$*. Consider* $E = \{(x,t) : A \times \mathsf{test}(A) \mid {}^{\sqcap}x \sqsubseteq t\}$ *and* $T = \{(t,t) : \mathsf{test}(A) \times \mathsf{test}(A)\}$ *and define the following operations for elements of* E*, where* $x, y \in A$ *and* $s, t, u \in \mathsf{test}(A)$*.*

$$\begin{aligned}
(x,s) \oplus (y,t) &= (x \sqcup y, s \sqcup t) \\
(x,s) \odot (y,t) &= (x \circ y, {}^{\sqcap}(s \circ x \circ t)) \\
(x,s)^{\circledast} &= (x^{\times}, {}^{\sqcap}(x^{\times} \circ s)) \\
\overline{(s,s)} &= (\neg s, \neg s) \\
(s,s) \mathbin{\Cap} (t,t) &= (s \pitchfork t, s \pitchfork t) \\
{}^{\sqcap}(x,s) &= ({}^{\sqcap}x, {}^{\sqcap}x) \\
(x,s) \mathbin{\Cap_{(u,u)}} (y,t) &= (x \pitchfork_u y, s \pitchfork_u t)
\end{aligned}$$

Then $(E, T, \oplus, \odot, ^{\circledast}, (\top,\top), (1,1), \overline{}, \Cap, {}^{\sqcap}, \Cap_\bullet)$ *is a DAD-*$\Cap_\bullet$ *and the partial order related to* $\oplus$ *satisfies*

$$(x,s) \sqsubseteq (y,t) \iff x \sqsubseteq y \wedge s \sqsubseteq t \ . \tag{A.1}$$

Proof : We first show that E is closed under $\oplus$, $\odot$, $^{\circledast}$ and $\Cap_\bullet$ and that T is closed under $\oplus$, $\odot$ and $\Cap$ (T is trivially closed under $\overline{}$ and it is clear that the type of ${}^{\sqcap}$ is ${}^{\sqcap} : E \to T$.)

- E is closed under $\oplus$.

We have to show that $\sqcap(x \sqcup y) \sqsubseteq s \sqcup t$. This follows directly from (3.21) and Boolean algebra, since $(x, s), (y, t) \in E$.

- E is closed under $\odot$.

  We have to show that $\sqcap(x \boxdot y) \sqsubseteq \sqcap(s \boxdot x \boxdot t)$.

  $$\begin{array}{ll} & \mathsf{true} \\ \Longrightarrow & \quad \langle \text{ by the hypothesis } \rangle \\ & \sqcap y \sqsubseteq t \\ \Longrightarrow & \quad \langle \text{ by Proposition 3.14-8 and (3.20) } \rangle \\ & \sqcap(x \boxdot y) \sqsubseteq \sqcap(x \boxdot t) \\ \Longrightarrow & \quad \langle \text{ by Boolean algebra and Proposition 3.14-9 } \rangle \\ & \sqcap(x \boxdot y) \sqsubseteq \sqcap(s \boxdot x \boxdot t) \end{array}$$

- E is closed under $^{\circledast}$.

  We have to show that $\sqcap(x^{\times}) \sqsubseteq \sqcap(x^{\times} \boxdot s)$. This follows directly from Proposition 3.14-18.

- T is closed under $\oplus$.

  Since $(s, s) \oplus (t, t) = (s \sqcup t, s \sqcup t)$ by definition of $\oplus$, then $(s, s) \oplus (t, t) \in T$.

- T is closed under $\odot$.

  $$\begin{array}{ll} & (s, s) \odot (t, t) \\ = & \quad \langle \text{ by definition of } \odot \rangle \\ & (s \boxdot t, \sqcap(s \boxdot s \boxdot t)) \\ = & \quad \langle \text{ by Boolean algebra and Proposition 3.14-1 } \rangle \\ & (s \boxdot t, s \boxdot t) \end{array}$$

  So $(s, s) \odot (t, t) \in T$

- T is closed under $\Cap$.

  Since $(s, s) \Cap (t, t) = (s \sqcap t, s \sqcap t)$ by definition of $\Cap$, then $(s, s) \Cap (t, t) \in T$.

- E is closed under $\Cap_{\bullet}$.

  We have to show that $\sqcap(x \sqcap_u y) \sqsubseteq s \sqcap_u t$. This follows directly from Proposition 3.20-20, since $(x, s), (y, t) \in E$.

So we know that the operators $\oplus$, $\odot$, $^{\circledast}$, $\overline{}$, $\Cap$, $\sqcap$ and $\Cap_{\bullet}$ are well defined.

We immediately derive (A.1). It will be used later on. The proof uses (3.11), which holds for $\oplus$ only if (3.1), (3.2) and (3.3) also hold for $\oplus$. It is shown below that they do hold, and the proof does not use (A.1).

$$
\begin{array}{ll}
 & (x,s) \sqsubseteq (y,t) \\
\iff & \quad \langle \text{ by (3.11) } \rangle \\
 & (x,s) \oplus (y,t) = (y,t) \\
\iff & \quad \langle \text{ by definition of } \oplus \rangle \\
 & (x \sqcup y, s \sqcup t) = (y,t) \\
\iff & \quad \langle \ \rangle \\
 & x \sqcup y = y \ \wedge \ s \sqcup t = t \\
\iff & \quad \langle \text{ by (3.11) } \rangle \\
 & x \sqsubseteq y \ \wedge \ s \sqsubseteq t
\end{array}
$$

Then we show that $\oplus$, $\odot$ and $^{\circledast}$ satisfy the axioms of a DA. Take $(x,s),(y,t),(z,u) \in E$.

- Axiom (3.1)

  By definition of $\oplus$, it follows directly from (3.1).

- Axiom (3.2)

  By definition of $\oplus$, it follows directly from (3.2).

- Axiom (3.3)

  By definition of $\oplus$, it follows directly from (3.3).

- Axiom (3.4)

  By definition of $\oplus$, it follows directly from (3.4)

- Axiom (3.5)

$$
\begin{array}{ll}
 & (x,s) \odot ((y,t) \odot (z,u)) \\
= & \quad \langle \text{ by definition of } \odot \rangle
\end{array}
$$

$$
\begin{array}{ll}
 & (x,s) \odot (y \circ z, \sqcap(t \circ y \circ u)) \\
= & \quad \langle \text{ by definition of } \odot \ \rangle \\
 & (x \circ (y \circ z), \sqcap(s \circ x \circ \sqcap(t \circ y \circ u))) \\
= & \quad \langle \text{ by (3.20) } \rangle \\
 & (x \circ y \circ z, \sqcap(s \circ x \circ t \circ y \circ u)) \\
= & \quad \langle \text{ by (3.19) and Proposition 3.14-9 } \rangle \\
 & (x \circ y \circ z, \sqcap(\sqcap(s \circ x \circ t) \circ x \circ y \circ u)) \\
= & \quad \langle \text{ by definition of } \odot \ \rangle \\
 & (x \circ y, \sqcap(s \circ x \circ t)) \odot (z,u) \\
= & \quad \langle \text{ by definition of } \odot \ \rangle \\
 & ((x,s) \odot (y,t)) \odot (z,u)
\end{array}
$$

- Axiom (3.6)

$$
\begin{array}{ll}
 & (\top,\top) \odot (x,s) \\
= & \quad \langle \text{ by definition of } \odot \ \rangle \\
 & (\top \circ x, \sqcap(\top \circ \top \circ s)) \\
= & \quad \langle \text{ by (3.6) and Proposition 3.14-1 } \rangle \\
 & (\top,\top) \\
= & \quad \langle \text{ by (3.6) and Proposition 3.14-1 } \rangle \\
 & (x \circ \top, \sqcap(s \circ x \circ \top)) \\
= & \quad \langle \text{ by definition of } \odot \ \rangle \\
 & (x,s) \odot (\top,\top)
\end{array}
$$

- Axiom (3.7)

$$
\begin{array}{ll}
 & (1,1) \odot (x,s) \\
= & \quad \langle \text{ by definition of } \odot \ \rangle \\
 & (1 \circ x, \sqcap(1 \circ 1 \circ s)) \\
= & \quad \langle \text{ by (3.7) and Proposition 3.14-1 } \rangle \\
 & (x,s) \\
= & \quad \langle \text{ by (3.7) } \rangle \\
 & (x \circ 1, \sqcap(s \circ x \circ 1))
\end{array}
$$

$$
\begin{aligned}
&= && \langle \text{ by definition of } \odot \rangle \\
&(x,s) \odot (1,1)
\end{aligned}
$$

- Axiom (3.8)

$$
\begin{aligned}
&(x,s) \odot ((y,t) \oplus (z,u)) \\
&= && \langle \text{ by definition of } \oplus \rangle \\
&(x,s) \odot (y \sqcup z, t \sqcup u) \\
&= && \langle \text{ by definition of } \odot \rangle \\
&(x \barwedge (y \sqcup z), \barpi(s \barwedge x \barwedge (t \sqcup u))) \\
&= && \langle \text{ by (3.8) and (3.21) } \rangle \\
&(x \barwedge y \sqcup x \barwedge z, \barpi(s \barwedge x \barwedge t) \sqcup \barpi(s \barwedge x \barwedge u)) \\
&= && \langle \text{ by definition of } \oplus \rangle \\
&(x \barwedge y, \barpi(s \barwedge x \barwedge t)) \oplus (x \barwedge z, \barpi(s \barwedge x \barwedge u)) \\
&= && \langle \text{ by definition of } \odot \rangle \\
&(x,s) \odot (y,t) \oplus (x,s) \odot (z,u)
\end{aligned}
$$

- Axiom (3.9)

$$
\begin{aligned}
&((x,s) \oplus (y,t)) \odot (z,u) \\
&= && \langle \text{ by definition of } \oplus \rangle \\
&(x \sqcup y, s \sqcup t) \odot (z,u) \\
&= && \langle \text{ by definition of } \odot \rangle \\
&((x \sqcup y) \barwedge z, \barpi((s \sqcup t) \barwedge (x \sqcup y) \barwedge u)) \\
&= && \langle \text{ by (3.9), Proposition 3.14-3, (3.8) and (3.21) } \rangle \\
&(x \barwedge z \sqcup y \barwedge z, \barpi(s \barwedge t \barwedge x \barwedge u) \sqcup \barpi(s \barwedge t \barwedge y \barwedge u)) \\
&= && \langle \text{ by Proposition 3.14-9 and Boolean algebra } \rangle \\
&(x \barwedge z \sqcup y \barwedge z, \barpi(s \barwedge x \barwedge u) \sqcup \barpi(t \barwedge y \barwedge u)) \\
&= && \langle \text{ by definition of } \oplus \rangle \\
&(x \barwedge z, \barpi(s \barwedge x \barwedge u)) \oplus (y \barwedge z, \barpi(t \barwedge y \barwedge u)) \\
&= && \langle \text{ by definition of } \odot \rangle \\
&(x,s) \odot (z,u) \oplus (y,t) \odot (z,u)
\end{aligned}
$$

- Axiom (3.10)

$$
\begin{array}{ll}
& (x,s)^{\circledast} \odot (x,s) \oplus (1,1) \\
= & \qquad \langle \text{ by definition of } {}^{\circledast} \rangle \\
& (x^{\times}, \sqcap(x^{\times} \square s)) \odot (x,s) \oplus (1,1) \\
= & \qquad \langle \text{ by definition of } \odot \rangle \\
& (x^{\times} \square x, \sqcap(\sqcap(x^{\times} \square s) \square x^{\times} \square s)) \oplus (1,1) \\
= & \qquad \langle \text{ by definition of } \oplus \rangle \\
& (x^{\times} \square x \sqcup 1, \sqcap(\sqcap(x^{\times} \square s) \square x^{\times} \square s) \sqcup 1) \\
= & \qquad \langle \text{ by (3.10), Proposition 3.14-7 and Boolean algebra } \rangle \\
& (x^{\times}, \sqcap(x^{\times} \square s)) \\
= & \qquad \langle \text{ by definition of } {}^{\circledast} \rangle \\
& (x,s)^{\circledast}
\end{array}
$$

Rather than demonstrate (3.12) and (3.13), we work on Laws (3.17) and (3.18) which are equivalent (see Remark 3.2).

- Law (3.17)

$$
\begin{array}{ll}
& (x,s) \odot (z,u) \sqsubseteq (z,u) \\
\iff & \qquad \langle \text{ by definition of } \odot \rangle \\
& (x \square z, \sqcap(s \square x \square u)) \sqsubseteq (z,u) \\
\iff & \qquad \langle \text{ by (A.1) } \rangle \\
& x \square z \sqsubseteq z \ \wedge \ \sqcap(s \square x \square u) \sqsubseteq u \\
\iff & \qquad \langle \text{ by Proposition 3.14-9 and Boolean algebra } \rangle \\
& x \square z \sqsubseteq z \ \wedge \ s \sqsubseteq u \ \wedge \ \sqcap(x \square u) \sqsubseteq u \\
\implies & \qquad \langle \text{ by (3.17) and (3.22) } \rangle \\
& x^{\times} \square z \sqsubseteq z \ \wedge \ s \sqsubseteq u \ \wedge \ \sqcap(x^{\times} \square u) \sqsubseteq u \\
\implies & \qquad \langle \text{ by Proposition 3.14-8 } \rangle \\
& x^{\times} \square z \sqsubseteq z \ \wedge \ \sqcap(x^{\times} \square s) \sqsubseteq \sqcap(x^{\times} \square u) \ \wedge \ \sqcap(x^{\times} \square u) \sqsubseteq u \\
\implies & \qquad \langle \text{ by Boolean algebra and Proposition 3.14-9 } \rangle \\
& x^{\times} \square z \sqsubseteq z \ \wedge \ \sqcap(\sqcap(x^{\times} \square s) \square x^{\times} \square u) \sqsubseteq u
\end{array}
$$

$$
\begin{array}{ll}
\iff & \langle \text{ by (A.1) } \rangle \\
& (x^{\times} \mathbin{\square} z, \sqcap(\sqcap(x^{\times} \mathbin{\square} s) \mathbin{\square} x^{\times} \mathbin{\square} u)) \sqsubseteq (z, u) \\
\iff & \langle \text{ by definition of } \odot \rangle \\
& (x^{\times}, \sqcap(x^{\times} \mathbin{\square} s)) \odot (z, u) \sqsubseteq (z, u) \\
\iff & \langle \text{ by definition of } {}^{\circledast} \rangle \\
& (x, s)^{\circledast} \odot (z, u) \sqsubseteq (z, u)
\end{array}
$$

- Law (3.18)

$$
\begin{array}{ll}
& (z, u) \odot (x, s) \sqsubseteq (z, u) \\
\iff & \langle \text{ by definition of } \odot \rangle \\
& (z \mathbin{\square} x, \sqcap(u \mathbin{\square} z \mathbin{\square} s)) \sqsubseteq (z, u) \\
\iff & \langle \text{ by (A.1) } \rangle \\
& z \mathbin{\square} x \sqsubseteq z \ \wedge \ \sqcap(u \mathbin{\square} z \mathbin{\square} s) \sqsubseteq u \\
\iff & \langle \text{ by Proposition 3.14-9 and Boolean algebra } \rangle \\
& z \mathbin{\square} x \sqsubseteq z \ \wedge \ \sqcap(z \mathbin{\square} s) \sqsubseteq u \\
\implies & \langle \text{ by (3.18) } \rangle \\
& z \mathbin{\square} x^{\times} \sqsubseteq z \ \wedge \ \sqcap(z \mathbin{\square} s) \sqsubseteq u \\
\iff & \langle \text{ by Proposition 3.14-8 } \rangle \\
& z \mathbin{\square} x^{\times} \sqsubseteq z \ \wedge \ \sqcap(z \mathbin{\square} x^{\times} \mathbin{\square} s) \sqsubseteq \sqcap(z \mathbin{\square} s) \ \wedge \ \sqcap(z \mathbin{\square} s) \sqsubseteq u \\
\implies & \langle \text{ by (3.20) } \rangle \\
& z \mathbin{\square} x^{\times} \sqsubseteq z \ \wedge \ \sqcap(z \mathbin{\square} \sqcap(x^{\times} \mathbin{\square} s)) \sqsubseteq u \\
\iff & \langle \text{ by Boolean algebra and Proposition 3.14-9 } \rangle \\
& z \mathbin{\square} x^{\times} \sqsubseteq z \ \wedge \ \sqcap(u \mathbin{\square} z \mathbin{\square} \sqcap(x^{\times} \mathbin{\square} s)) \sqsubseteq u \\
\iff & \langle \text{ by (A.1) } \rangle \\
& (z \mathbin{\square} x^{\times}, \sqcap(u \mathbin{\square} z \mathbin{\square} \sqcap(x^{\times} \mathbin{\square} s))) \sqsubseteq (z, u) \\
\iff & \langle \text{ by definition of } \odot \rangle \\
& (z, u) \odot (x^{\times}, \sqcap(x^{\times} \mathbin{\square} s)) \sqsubseteq (z, u) \\
\iff & \langle \text{ by definition of } {}^{\circledast} \rangle \\
& (z, u) \odot (x, s)^{\circledast} \sqsubseteq (z, u)
\end{array}
$$

The fact that $(T, \oplus, \Cap, \overline{}, (1, 1), (\top, \top))$ is a Boolean algebra directly follows from

the fact that $(\mathsf{test}(A), \sqcup, \sqcap, \neg, 1, \top)$ is a Boolean algebra. So $(E, T, \oplus, \odot, (\top, \top), (1,1), \overline{}, \Cap)$ is a DAT.

Then we show that $\Cap$ satisfies all the axioms of a DAD. Take $(x,s),(y,t) \in E$ and $(u,u) \in T$.

- Axiom (3.19)

$$
\begin{aligned}
& \Cap((x,s) \odot (u,u)) \odot (x,s) \\
= & \quad \langle \text{ by definition of } \odot \ \rangle \\
& \Cap(x \fatsemi u, \Cap(s \fatsemi x \fatsemi u)) \odot (x,s) \\
= & \quad \langle \text{ by definition of } \Cap \ \rangle \\
& (\Cap(x \fatsemi u), \Cap(x \fatsemi u)) \odot (x,s) \\
= & \quad \langle \text{ by definition of } \odot \ \rangle \\
& (\Cap(x \fatsemi u) \fatsemi x, \Cap(\Cap(x \fatsemi u) \fatsemi \Cap(x \fatsemi u) \fatsemi s)) \\
= & \quad \langle \text{ by (3.19), Boolean algebra and (3.20) } \rangle \\
& (x \fatsemi u, \Cap(s \fatsemi x \fatsemi u)) \\
= & \quad \langle \text{ by definition of } \odot \ \rangle \\
& (x,s) \odot (u,u)
\end{aligned}
$$

- Axiom (3.20)

$$
\begin{aligned}
& \Cap((x,s) \odot (y,t)) \\
= & \quad \langle \text{ by definition of } \odot \ \rangle \\
& \Cap(x \fatsemi y, \Cap(s \fatsemi x \fatsemi t)) \\
= & \quad \langle \text{ by definition of } \Cap \ \rangle \\
& (\Cap(x \fatsemi y), \Cap(x \fatsemi y)) \\
= & \quad \langle \text{ by (3.20) } \rangle \\
& (\Cap(x \fatsemi \overline{\Cap y}), \Cap(x \fatsemi \overline{\Cap y})) \\
= & \quad \langle \text{ by definition of } \Cap \ \rangle \\
& \Cap(x \fatsemi \overline{\Cap y}, \Cap(s \fatsemi x \fatsemi \overline{\Cap y})) \\
= & \quad \langle \text{ by definition of } \odot \ \rangle \\
& \Cap((x,s) \odot (\overline{\Cap y}, \Cap y))
\end{aligned}
$$

$$
\begin{array}{ll}
= & \langle \text{ by definition of } \sqcap \rangle \\
& \sqcap((x,s) \odot \sqcap(y,t))
\end{array}
$$

- Axiom (3.21)

$$
\begin{array}{ll}
& \sqcap((x,s) \oplus (y,t)) \\
= & \langle \text{ by definition of } \oplus \rangle \\
& \sqcap(x \sqcup y, s \sqcup t) \\
= & \langle \text{ by definition of } \sqcap \rangle \\
& (\sqcap(x \sqcup y), \sqcap(x \sqcup y)) \\
= & \langle \text{ by (3.21) } \rangle \\
& (\sqcap x \sqcup \sqcap y, \sqcap x \sqcup \sqcap y) \\
= & \langle \text{ by definition of } \oplus \rangle \\
& (\sqcap x, \sqcap x) \oplus (\sqcap y, \sqcap y) \\
= & \langle \text{ by definition of } \sqcap \rangle \\
& \sqcap(x,s) \oplus \sqcap(y,t)
\end{array}
$$

- Axiom (3.22)

$$
\begin{array}{ll}
& \sqcap((x,s) \odot (u,u)) \sqsubseteq (u,u) \\
\iff & \langle \text{ by definition of } \odot \rangle \\
& \sqcap(x \circ u, \sqcap(s \circ x \circ u)) \sqsubseteq (u,u) \\
\iff & \langle \text{ by definition of } \sqcap \rangle \\
& (\sqcap(x \circ u), \sqcap(x \circ u)) \sqsubseteq (u,u) \\
\iff & \langle \text{ by (A.1) } \rangle \\
& \sqcap(x \circ u) \sqsubseteq u \\
\implies & \langle \text{ by (3.22) } \rangle \\
& \sqcap(x^{\times} \circ u) \sqsubseteq u \\
\iff & \langle \text{ by (A.1) } \rangle \\
& (\sqcap(x^{\times} \circ u), \sqcap(x^{\times} \circ u)) \sqsubseteq (u,u) \\
\iff & \langle \text{ by definition of } \sqcap \rangle \\
& \sqcap(x^{\times} \circ u, \sqcap(\sqcap(x^{\times} \circ s) \circ x^{\times} \circ u)) \sqsubseteq (u,u) \\
\iff & \langle \text{ by definition of } \odot \rangle
\end{array}
$$

$$
\begin{array}{ll}
& \Pi((x^{\times}, \Pi(x^{\times} \boxdot s)) \odot (u,u)) \sqsubseteq (u,u) \\
\iff & \quad \langle \text{ by definition of } {}^{\circledast} \rangle \\
& \Pi((x,s)^{\circledast} \odot (u,u)) \sqsubseteq (u,u)
\end{array}
$$

Then we show that $\Cap_{\bullet}$ satisfies (3.23) so $(E, T, \oplus, \odot, {}^{\circledast}, (\top,\top), (1,1), \overline{}, \Cap, {}^{\Pi}, \Cap_{\bullet})$ is a DAD-$\Cap_{\bullet}$. Take $(x,s),(y,t),(z,u) \in E$ and $(v,v) \in T$.

$$
\begin{array}{ll}
& (x,s) \mathbin{\Cap_{(v,v)}} (y,t) = (z,u) \\
\iff & \quad \langle \text{ by definition of } \Cap_{\bullet} \rangle \\
& (x \mathbin{\Pi_v} y, s \mathbin{\Pi_v} t) = (z,u) \\
\iff & \quad \langle \ \rangle \\
& x \mathbin{\Pi_v} y = z \ \wedge \ s \mathbin{\Pi_v} t = u \\
\iff & \quad \langle \text{ by (3.23) } \rangle \\
& v \boxdot x = v \boxdot z \ \wedge \ \neg v \boxdot y = \neg v \boxdot z \ \wedge \ v \boxdot s = v \boxdot u \ \wedge \ \neg v \boxdot t = \neg v \boxdot u \\
\iff & \quad \langle \text{ by Boolean algebra and Proposition 3.14-1 } \rangle \\
& v \boxdot x = v \boxdot z \ \wedge \ \neg v \boxdot y = \neg v \boxdot z \ \wedge \ \Pi(v \boxdot v \boxdot s) = \Pi(v \boxdot v \boxdot u) \ \wedge \\
& \Pi(\neg v \boxdot \neg v \boxdot t) = \Pi(\neg v \boxdot \neg v \boxdot u) \\
\iff & \quad \langle \ \rangle \\
& (v \boxdot x, \Pi(v \boxdot v \boxdot s)) = (v \boxdot z, \Pi(v \boxdot v \boxdot u)) \ \wedge \\
& (\neg v \boxdot y, \Pi(\neg v \boxdot \neg v \boxdot t)) = (\neg v \boxdot z, \Pi(\neg v \boxdot \neg v \boxdot u)) \\
\iff & \quad \langle \text{ by definition of } \odot \rangle \\
& (v,v) \odot (x,s) = (v,v) \odot (z,u) \ \wedge \ (\neg v, \neg v) \odot (y,t) = (\neg v, \neg v) \odot (z,u) \\
\iff & \quad \langle \text{ by definition of } \overline{} \rangle \\
& (v,v) \odot (x,s) = (v,v) \odot (z,u) \ \wedge \ \overline{(v,v)} \odot (y,t) = \overline{(v,v)} \odot (z,u)
\end{array}
$$

□

Index