Concurrent Dynamic Algebra

HITOSHI FURUSAWA, Kagoshima University, Japan
GEORG STRUTH, University of Sheffield, UK

We reconstruct Peleg's concurrent dynamic logic in the context of modal Kleene algebras. We explore the algebraic structure of its multirelational semantics and develop an axiomatization of concurrent dynamic algebras from that basis. In this context, sequential composition is not associative. It interacts with parallel composition through a weak distributivity law. The modal operators of concurrent dynamic algebra are obtained from abstract axioms for domain and antidomain operators; the Kleene star is modelled as a least fixpoint. Algebraic variants of Peleg's axioms are shown to be derivable in these algebras, and their soundness is proved relative to the multirelational model. Additional results include iteration principles for the Kleene star and a refutation of variants of Segerberg's axiom in the multirelational setting. The most important results have been verified formally with Isabelle/HOL.

Categories and Subject Descriptors: F.1.2 [**Computation by Abstract Devices**]: Modes of Computation—*Alternation and nondeterminism; Parallelism and concurrency*; F.3.1 [**Logics and Meanings of Programs**]: Specifying and Verifying and Reasoning about Programs—*Logics of programs*; F.3.2 [**Logics and Meanings of Programs**]: Semantics of Programming Languages—*Algebraic approaches to semantics*; F.4.1 [**Mathematical Logic and Formal Languages**]: Mathematical Logic—*Modal logic*; I.1.3 [**Symbolic and Algebraic Manipulation**]: Languages and Systems—*Special-purpose algebraic systems*

General Terms: Languages, Theory, Verification

Additional Key Words and Phrases: Dynamic logic, modal algebra, multirelations

ACM Reference Format:
Hitoshi Furusawa and Georg Struth. 2015. Concurrent dynamic algebra. ACM Trans. Comput. Logic 16, 4, Article 30 (August 2015), 38 pages.
DOI: http://dx.doi.org/10.1145/2785967

1. INTRODUCTION

Concurrent dynamic logic (CDL) was proposed almost three decades ago by Peleg [1987b] as an extension of propositional dynamic logic (PDL) [Harel et al. 2000] to study concurrency in "its purest form as the dual notion of nondeterminism." In this setting, a computational process is regarded as a tree with two dual kinds of branchings. According to the first one, the process may choose a transition along one of the possible branches. This is known as angelic, internal, or existential choice. According to the second one, it must progress along all possible branches in parallel, which is known as demonic, external, or universal choice. This lends itself to various interpretations.

One associates computations with games that processes play against a scheduler or environment as their opponent. A process wins if it can resolve all internal choices

Research sponsored by the Royal Society and JSPS KAKENHI grant number 25330016.
Authors' addresses: H. Furusawa, Department of Mathematics and Computer Science, Kagoshima University, Korimoto 1-21-35, Kagoshima 890-0065, Japan; email: furusawa@sci.kagoshima-u.ac.jp; G. Struth, Department of Computer Science, University of Sheffield, Regent Court, 211 Portobello, Sheffield S1 4DP, UK; email: g.struth@sheffield.ac.uk.

DOI: http://dx.doi.org/10.1145/2785967

successfully and respond to all external choices enforced by the opponent. Another one considers machines that accept inputs by nondeterministically choosing one transition along existential branches and executing all transitions in parallel among universal ones. In yet another, universal choices correspond to agents cooperating towards a collective goal while existential choices are made in competition by individual agents. Finally, in shared-variable concurrency, interferences caused by different threads accessing a global variable are observed as nondeterministic assignments by particular threads, hence as external choices imposed by the environment.

Historically, in fact, CDL has been influenced by work on alternating state machines by Chandra et al. [1981] and Parikh's game logic (GL) [1983, 1985], which is itself based on PDL. Other aspects of concurrency, such as communication or synchronization, which are at the heart of formalisms such as Petri nets or process algebras, are ignored in its basic axiomatization.

Standard PDL has a relational semantics. This captures the input/output dependencies of sequential programs. Internal choice is modelled as union, sequential composition as relational composition. External choice, however, cannot be represented by this semantics. It requires relating an individual input to a set of outputs, that is, relations of type $A \times 2^B$ instead of $A \times B$. These are known as *multirelations*.

In multirelational semantics, external choice still corresponds to union, but sequential composition must be redefined. According to Parikh's definition, a pair (a, A) is in the sequential composition of multirelation R with multirelation S if R relates element a with an intermediate set B and every element of B is related to the set A by S. With Peleg's more general definition, it suffices that S relates each element $b \in B$ with a set C_b so long as the union of all the sets C_b yields the set A. In addition, a notion of parallel composition can now be defined. If a pair (a, A) is in a multirelation R and a pair (a, B) in a multirelation S, then the parallel composition of R and S contains the pair $(a, A \cup B)$. Starting from input a, the multirelations R and S thus produce the collective output $A \cup B$ when executed in parallel. In contrast to Peleg, Parikh also imposes an up-closure condition on multirelations: $(a, A) \in R$ and $A \subseteq B$ imply $(a, B) \in R$.

In CDL, modal box and diamond operators are associated with the multirelational semantics as they are associated with a relational semantics in PDL. An expression $[\alpha]\varphi$ means that after every terminating execution of program α, property φ holds, whereas $\langle\alpha\rangle\varphi$ means that there is a terminating execution of α after which φ holds. In CDL, as in PDL, boxes and diamonds are related by De Morgan duality: $[\alpha]\varphi$ holds if and only if $\neg\langle\alpha\rangle\neg\varphi$ holds. The axioms of CDL describe how the programming constructs of internal choice, sequential and parallel composition, and (sequential) iteration interact with the modalities. CDL can as well be seen as a generalization of dual-free GL.

Wijesekera and Nerode [1990, 2005], and later Goldblatt [1992], have generalized CDL to situations in which boxes and diamonds are no longer dual. GL has been applied widely in game and social choice theory. A bridge between the two formalisms has been built by van Benthem et al. [2008] to model simultaneous games as they arise in algorithmic game theory. Peleg [1987a] has added notions of synchronization and communication to CDL. Parikh's semantics of up-closed multirelations and its duality to monotone predicate transformers has reappeared in Back and von Wright's refinement calculus [1998] and the approach to multirelational semantics of Rewitzky [2003], Rewitzky and Brink [2006], and Martin et al. [2007]. Up-closed multirelations have been studied more abstractly as a variant of Kleene algebra [Furusawa et al. 2009; Nishizawa et al. 2009].

This suggests that CDL and its variants are relevant to games and concurrency; they provide insights in games for concurrency and in concurrency for games. Despite this, beyond the up-closed case, the algebra of multirelations, as a generalization of Kleene algebras [Kozen 1994] and Tarski's relation algebra (see Maddux [2006]), has never

been studied in detail, and *concurrent dynamic algebras* as algebraic companions of CDL remain to be established. This is in contrast to PDL, in which the corresponding dynamic algebras [Pratt 1980] and test algebras [Németi 1981; Trnková and Reiterman 1987; Pratt 1991] are well studied.

An algebraic reconstruction of CDL complements the logical one in important ways. Algebras of multirelations yield abstract, yet fine-grained, views on the structure of simultaneous games; they might also serve as intermediate semantics for shared-variable concurrency, where interferences have been resolved. The study of dynamic and test algebras shows how modal algebras arise from Kleene and relation algebras in simple direct ways. Powerful tools from universal algebra and category theory support their analysis. Reasoning with modal algebras is essentially first-order equational, therefore highly suitable for mechanization and automation. In the context of CDL, this could make the design of tools for analyzing games or concurrent programs simple and flexible. In contrast, the set theory of multirelations is essentially second-order.

Our main contribution is a minimalist axiomatization of concurrent dynamic algebras. It is obtained from axioms for the algebra of multirelations that generalize modal Kleene algebras [Desharnais et al. 2006; Desharnais and Struth 2008, 2011]. In more detail, our main contributions are as follows.

—We investigate the basic properties of the multirelational semantics of CDL. Those of sequential composition are rather weak—the operation is not even associative—while parallel composition and union form a commutative idempotent semiring. We find a new interaction law for sequential and parallel composition. We investigate special properties of subidentities, which yield propositions and tests in CDL, and of multirelational domain and antidomain (domain-complement) operations.
—We axiomatize variants of semirings (called *proto-dioids* and *proto-trioids*) that capture the basic algebra of multirelations without and with parallel composition. We expand these structures by axioms for domain and antidomain operations, explore the algebraic laws governing these operations, and characterize the subalgebras of domain elements, which serve as state or proposition spaces in this setting. We also prove soundness with respect to the underlying multirelational model.
—We define algebraic diamond and box operators from the domain and antidomain ones as abstract preimage operators and their De Morgan duals. We show that algebraic counterparts of the axioms of star-free CDL can be derived in this setting. The diamond axioms of CDL are obtained over a state space that forms a distributive lattice; the additional box axioms are derivable over a Boolean algebra.
—We investigate the Kleene star (or reflexive transitive closure operation) in the multirelational model and turn the resulting laws into axioms of *proto-Kleene algebras with domain* and *antidomain* as well as *proto-bi-Kleene algebras with domain* and *antidomain*. The latter two allow us to derive the full set of CDL axioms; they are therefore informally called *concurrent dynamic algebras*. Once more, we prove soundness with respect to the underlying multirelational model.
—Finally, we study notions of finite iteration for the Kleene star in the multirelational setting and refute the validity of a variant of Segerberg's axiom of PDL.

A complete list of concurrent dynamic algebra axioms can be found in Appendix 1.

Our analysis of the multirelational model and our axiomatizations are minimalistic in that we have aimed at the most general algebraic conditions for deriving the CDL axioms. Many interesting properties of multirelations have therefore been ignored. Due to the absence of associativity of sequential composition and of left distributivity of sequential composition over union, many proofs seem rather fragile and depend on stronger algebraic properties of special elements. Sequential composition, for instance, is associative if one of the participating multirelations is a domain or antidomain

element. This requires a significant generalization of previous approaches to Kleene algebras with domain and antidomain [Desharnais and Struth 2008, 2011].

Moreover, proofs about multirelations are rather tedious due to the complexity and second-order nature of sequential composition. We have therefore formalized and verified the most important proofs with the Isabelle proof assistant [Nipkow et al. 2002] (see Appendix 3 for a list). This makes our work an exercise in formalized mathematics. The complete code can be found online[1]. Nevertheless, we present all proofs to make this article self-contained; the less interesting ones have been delegated to Appendix 2.

2. MULTIRELATIONS

A *multirelation* R over a set X is a subset of $X \times 2^X$. Inputs $a \in X$ are related by R to outputs $A \subseteq X$; each single input a may be related to many subsets of X. The set of all multirelations over X is denoted $\mathscr{M}(X)$.

An intuitive interpretation is the accessibility or reachability in a (directed) graph: (a, A) means that the set A of vertices is reachable from vertex a in the graph. $(a, \emptyset)$ means that no set of vertices is reachable from a, which makes a a terminal node. This is different from (a, A) not being an element of a multirelation for all $A \subseteq X$. Similarly, an element (a, A) of a program R indicates that starting from state a, program R terminates in each state in A in a parallel execution, whereas all intermediate states have been forgotten [Peleg 1987b].

By definition, (a, A) and $(a, \emptyset)$ can be elements of the same multirelation. This can be interpreted as a system, program, or player making an "internal," existential, or angelic choice to access either A or $\emptyset$. The elements of A can therefore be seen as "external," universal, or demonic choices made by an environment, scheduler or adversary player.

This ability to capture internal and external choices makes multirelations relevant to games and game logics [Parikh 1985], demonic/angelic semantics of programs [Back and von Wright 1998; Martin et al. 2007], alternating automata and concurrency [Peleg 1987b]. Different applications, however, require different definitions of operations on multirelations. The application used in the concurrent setting by Peleg [1987b] and Goldblatt [1992] is the most general one and we follow it in this article.

Example 2.1. Let $X = \{a, b, c, d\}$. Then

$$R = \{(a, \emptyset), (a, \{d\}), (b, \{a\}), (b, \{b\}), (b, \{a, b\})(c, \{a\}), (c, \{d\})\}$$

is a multirelation over X. Vertex a can alternatively reach no vertex at all—the empty set—or the singleton set $\{d\}$. Vertex b can either reach set $\{a\}$, set $\{b\}$, or their union $\{a, b\}$. Vertex c can either reach set $\{a\}$ or set $\{d\}$, but not their union. Vertex d cannot even reach the empty set; no execution from it is enabled. This is in contrast to the situation $(a, \emptyset)$, in which execution is enabled from a, but no state can be reached.

Peleg defines the following operations of sequential and concurrent composition of multirelations. Let R and S be multirelations over X. The *sequential composition* of R and S is the multirelation

$$R \cdot S = \left\{(a, A) \mid \exists B.\ (a, B) \in R \wedge \exists f.\ (\forall b \in B.\ (b,\ f(b)) \in S) \wedge A = \bigcup f(B)\right\}.$$

The *unit of sequential composition* is the multirelation

$$1_\sigma = \{(a, \{a\}) \mid a \in X\}.$$

The *parallel composition* of R and S is the multirelation

$$R \| S = \{(a, A \cup B) \mid (a, A) \in R \wedge (a, B) \in S\}.$$

[1] http://www.dcs.shef.ac.uk/~georg/isa/cda.

The *unit of parallel composition* is the multirelation

$$1_\pi = \{(a, \emptyset) \mid a \in X\}.$$

The *universal multirelation* over X is

$$U = \{(a, A) \mid a \in X \wedge A \subseteq X\}.$$

In the definition of sequential composition, $f(B) = \{f(b) \mid b \in B\}$ is the image of B under f. The intended meaning of $(a, A) \in R \cdot S$ is as follows: the set A is reachable from vertex a by $R \cdot S$ if some intermediate set B is reachable from a by R, and from each vertex $b \in B$ a set A_b is reachable (represented by $f(b)$) such that

$$A = \bigcup_{b \in B} A_b = \bigcup_{b \in B} f(b) = \bigcup f(B).$$

Thus, from each vertex $b \in B$, the locally reachable set $f(b)$ contributes to the global reachability of A. In Peleg's intended interpretation, a pair (a, A) is in the sequential composition $R \cdot S$ of two concurrent programs R and S if, starting from a, the program R reaches all the elements of an intermediate concurrent state B and from each state $b \in B$, the program S reaches all the states in a local set A_b such that, by all these parallel executions, the global concurrent state $A = \bigcup_{b \in B} A_b$ is reached.

We write $G_f(b) = (b, f(b))$ for the graph of f at point b, and $G_f(B) = \{G_f(b) \mid b \in B\}$ for the graph of f on the set B. We can then write somewhat more compactly

$$(a, A) \in R \cdot S \Leftrightarrow \exists B.\ (a, B) \in R \wedge \exists f.\ G_f(B) \subseteq S \wedge A = \bigcup f(B).$$

This definition of sequential composition is subtly different from the one used by Parikh [1985] in game logics, which appears also in articles on multirelational semantics and monotone predicate transformers. In addition, Parikh considers up-closed multirelations. This leads not only to much simpler proofs, but also to structural differences. Peleg has argued that up-closure is not desirable for concurrency since it makes all programs—even tests—and assertions automatically nondeterministic. In addition, it can be shown that, in the up-closed case, parallel composition reduces to intersection: it is easy to see that a multirelation R is up-closed if $R = R\|U$; thus it remains to check that $(R\|U)\|(S\|U) = (R\|U) \cap (S\|U)$ for all multirelations R and S, which is straightforward with Isabelle.

The sequential identity 1_σ is defined similarly to the identity relation or identity function. It is given by (the graph of) the embedding $\lambda x.\{x\}$ into singleton sets.

In a parallel composition, $(a, A) \in R\|S$ if A is reachable from a by R or S in collaboration, that is, each of R and S must contribute part of the reachability to A.

The parallel identity 1_π is the function $\lambda x.\ \emptyset$ that does not reach any set from any vertex. Several interpretations of a pair $(a, \emptyset)$ suggest themselves: it might be the case that nothing is reachable from a due to an error or success, or due to nontermination.

Example 2.2. Consider the multirelations

$$R = \{(a, \{b, c\})\}, \qquad S = \{(b, \{b\})\}, \qquad T = \{(b, \{b\}), (c, \emptyset)\}.$$

Then $R \cdot S = \emptyset$ because S cannot contribute from c. Moreover, $R \cdot T = \{(a, \{b\})\}$. Finally, $T \cdot S = T$, since, from c, the empty set is the only intermediate set that satisfies the conditions for S and A above.

Example 2.3. Consider the multirelations

$$R = \{(a, \{a, b\})\}, \qquad S = \{(a, \{b, c\}), (b, \{b\})\}, \qquad T = \{(b, \emptyset)\}.$$

Then $R\|S = \{(a, \{a, b, c\})\}$ and $S\|T = \{(b, \{b\})\}$.

Example 2.4. Parallel composition, which can be associated with *universal*, *external,* or *demonic choice*, is captured within individual pairs of multirelations. For (a, A) and (b, B) in $X \times 2^X$, we can define the partial operation of external choice

$$(a, A) \| (b, B) = \begin{cases} (a, A \cup B), & \text{if } a = b, \\ \bot, & \text{otherwise,} \end{cases}$$

of type $(X \times 2^X) \to (X \times 2^X) \to (X \times 2^X)$ directly on pairs. It lifts to a total operation of parallel composition on powersets—hence multirelations—in the obvious way. Starting from externally deterministic pairs such as $(a, \{b\})$ and $(a, \{c\})$, which are isomorphic to pairs in binary relations, one can form externally nondeterministic pairs such as $(a, \{b, c\})$ with pair-level external choices and observe the effect of this construction in parallel compositions of multirelations. In Peleg's intended interpretation, each $(a, \{b\})$ corresponds to a deterministic program execution, while pairs $(a, \{b, c\})$ model the parallel or externally nondeterministic executions of a program, or of several ones.

Finally, we sketch the relationship of Peleg's notion of sequential composition with runs of alternating automata [Brzozowski and Leiss 1980; Chandra et al. 1981; Kozen 1976], where it arises in a natural way.

Example 2.5. An *alternating automaton* over finite alphabet Σ is usually modelled as a tuple (X, a_0, δ, F), where X is a finite set of states, $a_0 \in X$ the initial state, $F \subseteq X$ the set of accepting states, and $\delta : X \times \Sigma \to B^+(X)$ the transition function that maps states and letters into positive Boolean formulas over states in X. The Boolean formulas **true** and **false** are included. Without loss of generality, positive Boolean formulas are assumed to be in disjunctive normal form and encoded as sets of subsets of X, hence as dual-clause sets. The set $\{\{a, b\}, \{c\}\}$, for instance, represents $(a \wedge b) \vee c$, the empty set represents **true**, and no set can represent **false**. We write $C(\varphi)$ for the dual-clause set associated with a positive Boolean formula φ.

A set $A \subseteq X$ satisfies $\varphi \in B^+(X)$, written $A \models \varphi$, if assigning true to the elements in A and false to those in $X - A$ evaluates φ to true. Thus $\emptyset \models$ **true**, whereas **false** has no model. In particular, the sets in $C(\varphi)$ form minimal models of φ.

A run of an alternating automaton on a word w is an X-labelled tree because transitions into conjuncts must be executed in parallel in order to resolve universal choices, whereas transitions into disjuncts generate different runs and therefore different (sub)trees. The root of a run is labelled with a_0 and the nodes at the first level are labelled with the elements of a set in $C(\delta(a_0, \sigma))$ where σ is the head of w. More generally, if a is a label at level i and the $i + 1$-th letter in w is σ, then the elements of a set in $C(\delta(a, \sigma))$ label part of the $i + 1$-th level of the tree, and the remaining part of that level is obtained accordingly with transitions from the other nodes at the i-th level. This construction encapsulates the idea of Peleg's sequential composition.

To make this more precise, we associate a transition relation $R_\delta : X \times \Sigma \to 2^X$ with the function δ such that $(a, \sigma, B) \in R_\delta$ if and only if $B \in C(\delta(a, \sigma))$. We lift R_δ to a transition relation $\hat{R}_\delta : X \times \Sigma^* \to 2^X$ by recursion on words. First, if $\sigma \in \Sigma$, then $(a, \sigma, B) \in \hat{R}_\delta \Leftrightarrow (a, \sigma, B) \in R_\delta$. Second, $(a, w\sigma, B) \in \hat{R}_\delta$ if and only if there exists a $C \subseteq X$ with $(a, w, C) \in \hat{R}_\delta$ and a family $\{D_c \mid c \in C\}$ with $(c, \sigma, D_c) \in R_\delta$ for all $c \in C$ such that $B = \bigcup\{D_c \mid c \in C\}$. Replacing $\hat{R}_\delta$ by R and R_δ by S, forgetting the alphabet and rewriting the family of D_c as a function $f : X \to 2^X$ yields Peleg's definition of sequential composition $R \cdot S$ of multirelations.

By the definition of δ, some branches of a run may lead to **true**. Such transitions produce empty sets of states, from which no further transitions are possible; they are ignored when computing transitions to the next level. Transitions into **true** are therefore considered successful, and alternating automata can accept words without

scanning them completely. Accordingly, Peleg's multirelational composition considers pairs $(a, \emptyset)$—they persist in sequential compositions. The composition $1_\pi \cdot S = 1_\pi$ shows an extreme case. Such pairs can denote completion of a concurrent component, depending on the intended semantics.

In the light of Example 2.4, one can reconstruct a transition relation of an alternating automaton from deterministic pairs $(a, \{b\})$, using parallel composition for the universal choices and union for the existential choices required.

3. BASIC LAWS FOR MULTIRELATIONS

The definition of sequential composition is second-order; many proofs depend on second-order Skolemization, which is an instance of the Axiom of Choice:

$$(\forall a \in A.\exists b.\ P(a,b)) \Leftrightarrow (\exists f.\forall a \in A.\ P(a,\ f(a))).$$

First, we derive some basic laws of sequential composition.

LEMMA 3.1. *Let R, S, and T be multirelations.*

(1) $R \cdot 1_\sigma = R$ *and* $1_\sigma \cdot R = R$,
(2) $\emptyset \cdot R = \emptyset$,
(3) $(R \cdot S) \cdot T \subseteq R \cdot (S \cdot T)$,
(4) $(R \cup S) \cdot T = R \cdot T \cup S \cdot T$,
(5) $R \cdot S \cup R \cdot T \subseteq R \cdot (S \cup T)$.

See Appendix 2 for proofs. Property (1) confirms that 1_σ is indeed an identity of sequential composition. Property (2) shows that $\emptyset$ is a left annihilator. It is, however, not a right annihilator by Lemma 3.4, to follow. Similarly, Property (3) is a weak associativity law, which, again by Lemma 3.4, cannot be strengthened to an identity. In fact, Property (3) is not needed for the algebraic development in this article; it is listed for the sake of completeness. Property (5) is a left subdistributivity law for sequential composition, which, again by Lemma 3.4, cannot be strengthened to an identity. Left subdistributivity and right distributivity imply that sequential composition is left and right isotone:

$$R \subseteq S \Rightarrow T \cdot R \subseteq T \cdot S, \qquad R \subseteq S \Rightarrow R \cdot T \subseteq S \cdot T.$$

Next, we verify some basic laws of parallel composition. These reveal more pleasant algebraic structure.

LEMMA 3.2. *Let R, S, and T be multirelations.*

(1) $(R\|S)\|T = R\|(S\|T)$,
(2) $R\|S = S\|R$,
(3) $R\|1_\pi = R$,
(4) $R\|\emptyset = \emptyset$,
(5) $R\|(S \cup T) = R\|S \cup R\|T$.

See Appendix 2 for proofs. This shows that multirelations under union and parallel composition form a commutative dioid, as introduced in Section 6. It follows that parallel composition is left and right isotone:

$$R \subseteq S \Rightarrow T\|R \subseteq T\|S, \qquad R \subseteq S \Rightarrow R\|T \subseteq S\|T.$$

Next, we establish an important interaction law between sequential and parallel composition; a right subdistributivity law of sequential over parallel composition.

LEMMA 3.3. *Let R, S, and T be multirelations. Then*

$$(R\|S) \cdot T \subseteq (R \cdot T)\|(S \cdot T).$$

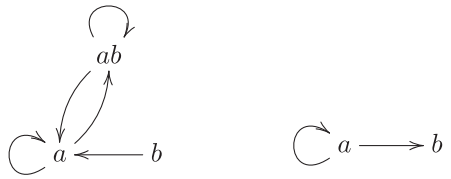

Fig. 1. Diagrams for R and S in the proof of Lemma 3.4(2).

See Appendix 2 for a proof. Once more, this general law is not needed for our algebraic development. We use a full right distributivity law that holds in particular cases.

Finally, counterexamples show that the algebraic properties studied so far are sharp.

LEMMA 3.4.

(1) $R \cdot \emptyset \neq \emptyset$*, for some* $R \in \mathscr{M}(X)$*,*
(2) $R \cdot (S \cdot T) \not\subseteq (R \cdot S) \cdot T$*, for some* $R, S, T \in \mathscr{M}(X)$*,*
(3) $R \cdot (S \cup T) \not\subseteq R \cdot S \cup R \cdot T$*, for some* $R, S, T \in \mathscr{M}(X)$*,*
(4) $(R \cdot T) \| (S \cdot T) \not\subseteq (R \| S) \cdot T$*, for some* $R, S, T \in \mathscr{M}(X)$*.*

PROOF.

(1) Let $R = \{(a, \emptyset)\}$. Then $(a, A) \in R \cdot S \Leftrightarrow \exists f.\ G_f(B) \in S \wedge A = \bigcup f(\emptyset) \Leftrightarrow A = \emptyset$. Hence, in this particular case, $R \cdot \emptyset = \{(a, \emptyset)\} \neq \emptyset$.
(2) Let $R = \{(a, \{a, b\}), (a, \{a\}), (b, \{a\})\}$ and $S = \{(a, \{a\}), (a, \{b\})\}$. Then

$$\begin{aligned}(R \cdot R) \cdot S &= \{(a, \{a\}), (a, \{b\}), (b, \{a\}), (b, \{b\})\} \\ &\subset \{(a, \{a, b\}), (a, \{a\}), (a, \{b\}), (b, \{a\}), (b, \{b\})\} \\ &= R \cdot (R \cdot S).\end{aligned}$$

(3) Consider that $R = \{(a, \{a, b\})\}$, $S = \{(a, \{a\})\}$, and $T = \{(b, \{b\})\}$. It follows that $S \cup T = \{(a, \{a\}), (b, \{b\})\}$ and $R \cdot (S \cup T) = R$, but $R \cdot S = R \cdot T = \emptyset$, whence $R \cdot S \cup R \cdot T = \emptyset$.
(4) Let $R = \{(a, \{a\})\}$ and $S = \{(a, \{a\}), (a, \{b\})\}$. Then

$$(R \| R) \cdot T = T \subset \{(a, \{a\}), (a, \{b\}), (a, \{a, b\})\} = (R \cdot T) \| (R \cdot T). \quad \square$$

The following Hasse diagrams are useful for visualizing multirelations and finding counterexamples. We depict the multirelations R and S from Case (2) in the Hasse diagram of the carrier set in Figure 1. We write ab as shorthand for the set $\{a, b\}$. The arrows $a \to a$, $a \to ab$ and $b \to a$ correspond to the pairs in R. The "virtual" arrows $ab \to ab$ and $ab \to a$ have been added to indicate which states are reachable from the set ab by R. We have omitted the empty set because it is not reachable.

The resulting lifting of the multirelation of type $X \to 2^X$ to a relation $2^X \times 2^X$ allows us to compute powers of R and products such as $R \cdot S$ by using relational composition, that is, by chasing reachability arrows directly in the diagram. It is reminiscent of Rabin and Scott's construction of deterministic finite automata from nondeterministic ones. In the context of alternating automata, a lifting of transition functions of type $Q \times \Sigma \to B^+(Q)$ to functions of type $B^+(Q) \times \Sigma \to B^+(Q)$ is related [Brzozowski and Leiss 1980]. For concurrent programs, it corresponds to a lifting to global concurrent system states. A systematic study of this lifting is postponed to future work.

Accordingly, we compute $R \cdot R$, $R \cdot S$, $(R \cdot R) \cdot S$, and $R \cdot (R \cdot S)$ as depicted in Figure 2.

The failure of associativity arises as follows: Executing S after any other transition allows accessing a or b, but not both states in parallel, because S can only execute from a. Executing S after R allows any transition between a and b (ignoring brackets),

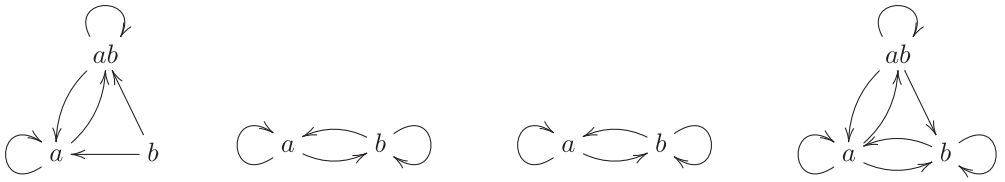

Fig. 2. Diagrams for $R \cdot R$, $R \cdot S$, $(R \cdot R) \cdot S$, and $R \cdot (R \cdot S)$ with R and S from the proof of Lemma 3.4(2).

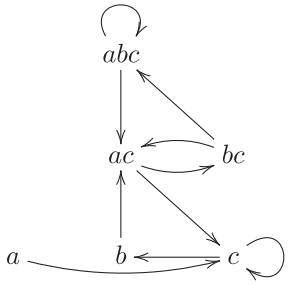

Fig. 3. Diagram for R from the refutation of $R \cdot (R \cdot R) = (R \cdot R) \cdot R$.

because R can access a from b and loop on a. Executing R before $R \cdot S$ therefore allows accessing a and b in parallel from a with R and then looping with $R \cdot S$ on that pair.

We even have a counterexample to $R \cdot (R \cdot R) \subseteq (R \cdot R) \cdot R$. Consider the multirelation $R = \{(a, \{c\}), (b, \{a, c\}), (c, \{b\}), (c, \{c\})\}$ with the Hasse diagram shown in Figure 3. Then

$$R \cdot R = \{(a, \{b\}), (a, \{c\}), (b, \{c\}), (b, \{b, c\}), (c, \{b\}), (c, \{c\}), (c, \{a, c\})\}$$

can be obtained by chasing arrows in the diagram. It is clear that there is no path of length three from b to bc in the diagram, hence $(b, \{b, c\}) \notin (R \cdot R) \cdot R$. Nevertheless, there are paths of length two from a to c and from c to b (as indicated in the set for $R \cdot R$). These allow extending the path from b to ac in R to the set bc in $R \cdot (R \cdot R)$. This fact is captured by the following set-theoretic relationship.

$$\begin{aligned} R \cdot (R \cdot R) = {} & \{(a, \{b\}), (a, \{c\}), (a, \{a, c\}), (b, \{b\}), (b, \{c\}), (b, \{a, c\}), (b, \{b, c\}), (b, \{a, b, c\}), \\ & (c, \{b\}), (c, \{c\}), (c, \{a, c\}), (c, \{b, c\})\} \\ \supset {} & \{(a, \{b\}), (a, \{c\}), (a, \{a, c\}), (b, \{b\}), (b, \{c\}), (b, \{a, c\}), (b, \{a, b, c\}), \\ & (c, \{b\}), (c, \{c\}), (c, \{b, c\})\} \\ = {} & (R \cdot R) \cdot R. \end{aligned}$$

Multirelation R corresponds to an alternating automaton with states $X = \{a, b, c\}$, alphabet $\Sigma = \{\sigma\}$, and transition function δ given by

$$\delta(a, \sigma) = c, \qquad \delta(b, \sigma) = a \wedge c, \qquad \delta(c, \sigma) = b \vee c.$$

It can be checked easily that there is no run on word $\sigma\sigma\sigma$ from state b into states b and c, meaning that $b \wedge c$ becomes true. However, there are parallel runs on $\sigma\sigma$ from state a to state c and from state c to state b; there is also a run on σ from state b to states a and c, which could be executed prior to the two parallel ones. This reverse construction, of course, does not yield a well-formed run of an alternating automaton. It contains the intermediate state c, which allows a parallel transition with R into bc, but not a sequential one. Alternating automata unfold their transition relations according to $R \cdot (R \cdot (R \cdot \ldots))$ when constructing runs. The lack of associativity in this construction reflects the lack of symmetry in computation trees as opposed to sequences

or traces. The sequential composition of multirelations constructs computation trees as well. The internal tree structure is forgotten in this composition, but reflected in its lack of associativity.

Finally, the nonassociativity of R hints at complications in the definition of the finite iteration of multirelations, which is considered in Section 13.

4. STRONGER LAWS FOR SEQUENTIAL SUBIDENTITIES

A multirelation P is a *(sequential) subidentity* if $P \subseteq 1_\sigma$. As mentioned in Section 2, $1_\sigma = \lambda x.\{x\}$ embeds X into 2^X. Every sequential subidentity is therefore a partial embedding. We usually write P or Q for subidentities. We write $\iota = \lambda x.\{x\}$ for the embedding of X into 2^X. One can see $G_\iota(a)$ as well as a lifting of a point $a \in X$ to a multirelational "point" $(a, \{a\})$ and $G_\iota(A)$ as a lifting of a set A to a subidentity.

More generally, this yields an isomorphism between points and multirelational points as well as sets and subidentities.

The next lemma shows that multiplying a multirelation with a subidentity from the left or right amounts to an input or output restriction.

LEMMA 4.1. *Let R be a multirelation and P a subidentity.*

(1) $(a, A) \in R \cdot P \Leftrightarrow (a, A) \in R \wedge G_\iota(A) \subseteq P$,
(2) $(a, A) \in P \cdot R \Leftrightarrow G_\iota(a) \in P \wedge (a, A) \in R$.

See Appendix 2 for proofs. These properties help us to verify that subidentities satisfy equational associativity and interaction laws and a left distributivity law.

LEMMA 4.2. *Let R, S, and T be multirelations.*

(1) $(R \cdot S) \cdot T = R \cdot (S \cdot T)$ *if R, S, or T is a subidentity,*
(2) $(R \| S) \cdot T = (R \cdot T) \| (S \cdot T)$ *if T is a subidentity,*
(3) $R \cdot (S \cup T) = R \cdot S \cup R \cdot T$ *if R is a subidentity.*

See Appendix 2 for proofs. Lemma 4.2 is essential for deriving the axioms of concurrent dynamic algebra.

In addition, it is straightforward to verify that the sequential subidentities form a Boolean subalgebra of the algebra of multirelations over X. The empty set is the least element of this algebra and 1_σ its greatest element. Join is union and meet coincides with sequential composition, which is equal to parallel composition in this special case. The Boolean complement of a subidentity $\bigcup_{a \in A}\{G_\iota(a)\}$, for some set $A \subseteq X$, is the subidentity $\bigcup_{b \in X - A}\{G_\iota(b)\}$.

Subidentities play an important role in providing the state spaces of modal operators in concurrent dynamic algebras. In our axiomatization, however, they arise only indirectly through definitions of domain and antidomain elements. In the concrete case of multirelations, these are described in the next section.

5. DOMAIN AND ANTIDOMAIN OF MULTIRELATIONS

This section presents the second important step towards concurrent dynamic algebra within the multirelational model: the definitions of domain and antidomain operations and the verification of some of their basic properties. These are then abstracted into algebraic domain and antidomain axioms, which, in turn, allow us to define the modal box and diamond operations of concurrent dynamic algebra.

The *domain* of a multirelation R is the multirelation

$$d(R) = \{G_\iota(a) \mid \exists A.\ (a, A) \in R\}.$$

The *antidomain* of a multirelation R is the multirelation

$$a(R) = \{G_\iota(a)\} \mid \neg\exists A.\ (a, A) \in R\}.$$

Domain and antidomain elements are therefore Boolean complements.

The next lemmas collect basic properties justifying the algebraic axioms in Section 6.

LEMMA 5.1. *Let R and S be multirelations.*

(1) $d(R) \subseteq 1_\sigma$,
(2) $d(R) \cdot R = R$,
(3) $d(R \cup S) = d(R) \cup d(S)$,
(4) $d(\emptyset) = \emptyset$,
(5) $d(R \cdot S) = d(R \cdot d(S))$,
(6) $d(R \| S) = d(R) \cap d(S)$,
(7) $d(R) \| d(S) = d(R) \cdot d(S)$.

See Appendix 2 for proofs. Most of these laws are similar to those of relational domain, but Properties (6) and (7) are particular to multirelations. Property (1) shows that domain elements are subidentities. According to Property (2), a multirelation is preserved by multiplying it from the left with its domain element. According to Properties (3) and (4), domain is strict and additive: the domain of the union of two multirelations is the union of their domains and the domain of the empty set is the empty set. The locality Property (5) states that it suffices to know the domain of the second multirelation when computing the domain of the sequential composition of two multirelations. By Property (6), the domain of a parallel composition of two multirelations is the intersection of their domains. Finally, by Property (7), the parallel composition of two domain elements equals their intersection. More generally, parallel composition of sequential subidentities is meet.

An intuitive explanation of domain is that it yields the set of all states from which a multirelation is enabled. Accordingly, by Property (3), the union of two multirelations is enabled if one is enabled, whereas, by Property (6), their parallel composition is enabled if both are enabled. It follows immediately from the definition that $d(\{(a, \emptyset)\}) = \{(a, \{a\})\}$. Hence, the multirelation $\{(a, \emptyset)\}$ is enabled, but does not yield an output set.

The next lemma, proved in Appendix 2, links domain and antidomain. It shows, in particular, that domain and antidomain elements are complemented.

LEMMA 5.2. *Let R be a multirelation.*

(1) $a(R) = 1_\sigma \cap -d(R)$,
(2) $d(R) = a(a(R))$,
(3) $d(a(R)) = a(R)$.

Many essential properties of antidomain can now be derived by De Morgan duality.

LEMMA 5.3. *Let R and S be multirelations.*

(1) $a(R) \cdot R = \emptyset$,
(2) $a(R \cdot S) = a(R \cdot d(S))$,
(3) $a(R) \cup d(R) = 1_\sigma$,
(4) $a(R \cup S) = a(R) \cdot a(S)$,
(5) $a(R \| S) = a(R) \cup a(S)$,
(6) $a(R) \| a(S) = a(R) \cdot a(S)$.

See Appendix 2 for proofs. If $d(R)$ describes those states from which multirelation R is enabled, then $a(R)$ models those in which R is not enabled. Property (1) says that antidomain elements are left annihilators: R cannot be executed from states in which

it is not enabled. Property (2) is a locality property similar to that in Lemma 5.1(5). Property (3) is a complementation law between domain and antidomain elements. It implies that antidomain elements are sequential subidentities. Properties (4) through (6) are the obvious De Morgan duals of domain properties.

Finally, and crucially for our purposes, domain and antidomain elements support stronger associativity and distributivity properties.

COROLLARY 5.4. *Let R, S, and T be multirelations.*

(1) $(R \cdot S) \cdot T = R \cdot (S \cdot T)$ *if R, S, or T is a domain or antidomain element,*
(2) $(R \| S) \cdot T = (R \cdot T) \| (S \cdot T)$ *if T is a domain or antidomain element,*
(3) $R \cdot (S \cup T) = R \cdot S \cup R \cdot T$ *if R is a domain or antidomain element.*

PROOF. By Lemma 5.1(1) and 5.1(3), domain and antidomain elements are subidentities. The results then follow by Lemma 4.2. □

Domain and antidomain satisfy, of course, additional properties. We have only presented those needed to justify the abstract domain and antidomain axioms in the following section. Further properties can then be derived by simple equational reasoning at the abstract level from those axioms, a considerable simplification.

6. AXIOMS FOR MULTIRELATIONS WITH DOMAIN AND ANTIDOMAIN

We have now collected sufficiently many facts about multirelations to abstract the domain and antidomain laws from the previous section into algebraic axioms. The approach is inspired by the axiomatization of domain semirings [Desharnais and Struth 2011] in the relational setting and the weakening of these axioms to families of near-semirings [Desharnais and Struth 2008]. In those approaches, however, sequential composition is associative, which considerably simplifies proofs and leads to simpler axiomatizations. Here, we can only assume associativity, interaction, and left distributivity in the presence of domain and antidomain elements, which holds in the multirelational model according to Corollary 5.4 and yields just the right assumptions for reconstructing concurrent dynamic logic.

We keep the development modular so that it also captures multirelational semirings and Kleene algebras without concurrent composition. We expect that the axioms of Parikh's game logic can be derived from that basis.

A *proto-dioid* is a structure $(S, +, \cdot, 0, 1)$ such that $(S, +, 0)$ is a semilattice with least element 0, and the following additional axioms hold:

$$1 \cdot x = x, \qquad x \cdot 1 = x,$$

$$x \cdot y + x \cdot z \leq x \cdot (y + z), \qquad (x + y) \cdot z = x \cdot z + y \cdot z, \qquad 0 \cdot x = 0.$$

Here, $\leq$ is the semilattice order defined, as usual, by $x \leq y \Leftrightarrow x + y = y$.

We do not include the weak associativity law $(x \cdot y) \cdot z \leq x \cdot (y \cdot z)$, although it is present in multirelations (Lemma 3.1(3)). It is independent from our axioms.

A *dioid* is a proto-dioid in which multiplication is associative for all elements and the left distributivity law $x \cdot (y + z) = x \cdot y + x \cdot z$ and the right annihilation law $x \cdot 0 = 0$ hold. A dioid is *commutative* if multiplication is commutative: $x \cdot y = y \cdot x$.

A *proto-trioid* is a structure $(S, +, \cdot, \|, 0, 1_\sigma, 1_\pi)$ such that $(S, +, \cdot, 0, 1_\sigma)$ is a proto-dioid and $(S, +, \|, 0, 1_\pi)$ is a commutative dioid.

In every proto-dioid, multiplication is left-isotone, $x \leq y \Rightarrow z \cdot x \leq z \cdot y$.

A *domain proto-dioid* (*dp-dioid*) is a proto-dioid expanded by a domain operation that satisfies the *domain associativity* axiom

$$x \cdot (y \cdot z) = (x \cdot y) \cdot z,$$

if one of x, y, or z is equal to $d(w)$ for some w, and the domain axioms

$$x \leq d(x) \cdot x, \qquad d(x \cdot y) = d(x \cdot d(y)), \qquad d(x + y) = d(x) + d(y),$$
$$d(x) \leq 1_\sigma, \qquad d(0) = 0.$$

The first domain axiom is called the *left preservation* axiom, the second is called the *locality* axiom, the third is called the *additivity* axiom, the fourth is called the *subidentity* axiom, and the fifth is called the *strictness* axiom.

A *domain proto-trioid* (*dp-triod*) is a dp-dioid that is also a proto-trioid and satisfies the *domain interaction* axiom and the *domain concurrency* axioms

$$(x \| y) \cdot d(z) = (x \cdot d(z)) \| (y \cdot d(z)), \qquad d(x \| y) = d(x) \cdot d(y), \qquad d(x) \| d(y) = d(x) \cdot d(y).$$

In the presence of antidomain, the axioms can be simplified further. An *antidomain proto-dioid* (*ap-dioid*) is a proto-dioid expanded by an antidomain operation that satisfies the *antidomain associativity* axiom

$$x \cdot (y \cdot z) = (x \cdot y) \cdot z,$$

where x, y, or z is equal to $a(w)$ for some w, and satisfies the antidomain axioms

$$a(x) \cdot x = 0, \qquad a(x \cdot y) = a(x \cdot a(a(y))), \qquad a(x) + a(a(x)) = 1_\sigma,$$
$$a(x) \cdot (y + z) = a(x) \cdot y + a(x) \cdot z.$$

The first antidomain axiom is called the *left annihilation* axiom, the second is called the *locality* axiom, the third is called the *complementation* axiom, and the fourth is called the *antidomain left distributivity* axiom.

An *antidomain proto-trioid* (*ap-trioid*) is an ap-dioid that is also a proto-trioid and satisfies the *antidomain interaction* and *antidomain concurrency* axioms

$$(x \| y) \cdot a(z) = (x \cdot a(z)) \| (y \cdot a(z)), \qquad a(x \| y) = a(x) + a(y), \qquad a(x) \| a(y) = a(x) \cdot a(y).$$

We have verified irredundancy of all domain and antidomain axioms with Isabelle. The full set of axioms of dp-trioids and ap-trioids (with additional axioms for the Kleene star) is listed in Appendix 1.

We can now relate the multirelational model set up in Sections 3 through 5 with the abstract algebraic definitions. The theorem is stated only for the smallest axiomatic class; it then holds automatically in all superclasses.

THEOREM 6.1. *Let X be a set.*

(*1*) *The structure* $(\mathscr{M}(X), \cup, \cdot, \|, \emptyset, 1_\sigma, 1_\pi, d)$ *forms a dp-trioid.*
(*2*) *The structure* $(\mathscr{M}(X), \cup, \cdot, \|, \emptyset, 1_\sigma, 1_\pi, a)$ *forms an ap-trioid.*

PROOF. The union axioms follow from set theory. The remaining proto-dioid axioms of sequential composition have been verified in Lemma 3.1; the commutative dioid axioms of concurrent composition in Lemma 3.2; and the domain and antidomain axioms in Lemma 5.1, Lemma 5.3, and Corollary 5.4. □

We call the structure $(\mathscr{M}(X), \cup, \cdot, \|, \emptyset, 1_\sigma, 1_\pi, d)$ the *full multirelational dp-trioid* and the structure $(\mathscr{M}(X), \cup, \cdot, \|, \emptyset, 1_\sigma, 1_\pi, a)$ the *full multirelational ap-trioid* over X. Since dp-trioids and ap-trioids are equational classes, they are closed under subalgebras, products, and homomorphic images. Hence, in particular, any subalgebra of a full dp-trioid is a dp-trioid and any subalgebra of a full ap-trioid is an ap-trioid.

7. MODAL OPERATORS

Following Desharnais and Struth [2011], we define modal box and diamond operators from domain and antidomain. In every dp-dioid, we define

$$\langle x\rangle y = d(x \cdot y).$$

This captures the intuition behind the Kripke-style semantics of modal logics. As explained in Section 4, sequential multiplication of a multirelation by a sequential subidentity from the left and right forms an input or output restriction of that multirelation. Therefore, $d(x \cdot y) = d(x \cdot d(y))$ abstractly represents a generalized multirelational preimage of the subidentity $d(y)$ under the element x. In other words, $\langle x\rangle y = \langle x\rangle d(y)$ yields the set of all elements from which, with x, one may reach a set that is a subset of $d(y)$. This can be checked readily in the multirelational model: if $P \subseteq X \times 2^X$ is a sequential subidentity and $R \subseteq X \times 2^X$ a multirelation, then

$$\langle R\rangle P = \{G_\iota(a) \mid \exists B.\ (a, B) \in R \wedge G_\iota(B) \subseteq P\}.$$

This abstractly represents the set of all states $A \subseteq X$ from which R may reach the set B, which is a subset of the set represented by the multirelation P. Identifying sets of states with predicates or assertions and R with the execution of a concurrent program, $\langle R\rangle P$ means that R enables P in the sense that there exists a parallel execution of program R such that P holds upon termination in all output states of that execution. In particular, if all output sets of the multirelation are singletons, the case of a relational preimage is recovered. The definition of multirelational diamonds thus generalizes the relational Kripke semantics in a natural way.

In ap-dioids, the situation is similar. Boxes can now be defined by De Morgan duality as well. In accordance with the multirelational model (Lemma 5.2(2)) we show in Section 11 that $d = a \circ a$. Then

$$\langle x\rangle y = d(x \cdot y) = a(a(x \cdot y)), \qquad [x]y = a(x \cdot a(y)).$$

Intuitively, one might expect that $[R]P = [R]d(P)$ models the set of all states from which, with R, one must reach sets of elements that are all in $d(P)$, that is, the assertion P holds in all states after every terminating execution of concurrent program R. An analysis in the multirelational model, however, shows a subtly different behavior:

$$\begin{aligned}
[R]P &= \{G_\iota(a) \mid \neg\exists B.\ (a, B) \in R \cdot a(P)\} \\
&= \{G_\iota(a) \mid \neg\exists B.\ (a, B) \in R \wedge G_\iota(B) \subseteq a(P)\} \\
&= \{G_\iota(a) \mid \neg\exists B.\ (a, B) \in R \wedge G_\iota(B) \cap P = \emptyset\} \\
&= \{G_\iota(a) \mid \forall B.\ (a, B) \in R \Rightarrow G_\iota(B) \cap P \neq \emptyset\}.
\end{aligned}$$

The condition $(a, B) \in R \Rightarrow G_\iota(B) \cap P \neq \emptyset$, which is enforced by De Morgan duality, is weaker than the one described earlier. It does not force *all* states in all terminating executions of R to satisfy P, but only *some* states in all terminating executions. At least the standard relational case is contained in this definition.

Goldblatt [1992], following Nerode and Wijesekera [1990], has therefore argued for replacing this condition by the more intuitive condition $(a, B) \in R \Rightarrow G_\iota(B) \subseteq P$, which breaks De Morgan duality. Here, we follow Peleg's De Morgan dual definition (without attributing much conceptual significance to it) and leave the algebraization of its more appealing alternative for future work.

8. THE STRUCTURE OF DP-TRIOIDS

This section presents the basic laws of dp-dioids and dp-trioids. Section 9 shows that algebraic variants of the axioms of concurrent dynamic logic, except the star axiom, can be derived in this setting. The star is then treated in Section 10.

We write $d(S)$ for the image of the carrier set S under the domain operation d and call this set the set of all *domain elements*. We often write $p, q, r, \ldots$ for domain elements.

The following identity is immediate from locality and properties of 1_σ.

LEMMA 8.1. *In every dp-dioid, operation d is a retraction:* $d \circ d = d$.

The next fact is a general property of retractions. Here, it gives a syntactic characterisation of domain elements as fixpoints of d (see Desharnais and Struth [2011]).

PROPOSITION 8.2. *If S is a dp-dioid, then* $x \in d(S) \Leftrightarrow d(x) = x$.

This characterization helps in checking closure properties of domain elements. We first prove some auxiliary properties (see Appendix 2).

LEMMA 8.3. *In every dp-dioid,*

(1) $x \leq y \Rightarrow d(x) \leq d(y)$,
(2) $d(x) \cdot x = x$,
(3) $d(x \cdot y) \leq d(x)$,
(4) $x \leq 1_\sigma \Rightarrow x \leq d(x)$,
(5) $d(d(x) \cdot y) = d(x) \cdot d(y)$.

The *domain export* law (5) is instrumental in proving further domain laws.

PROPOSITION 8.4. *Let S be a dp-dioid. Then* $d(S)$ *is a subalgebra of S that forms a bounded distributive lattice.*

PROOF. First, we check that $d(S)$ is closed under the operations, using the fixpoint property $d(x) = x$ from Proposition 8.2.

—$d(0) = 0$ is an axiom.
—$d(1_\sigma) = 1_\sigma$ follows from Lemma 8.3(1).
—$d(d(x) + d(y)) = d(x) + d(y)$ follows from additivity and idempotency of domain.
—$d(d(x) \cdot d(y)) = d(x) \cdot d(y)$ follows from domain export (Lemma 8.3(5)) and locality.

Next, we verify that the subalgebra forms a distributive lattice with least element 0 and greatest element 1_σ.

—It is obvious that 1_σ is the greatest and 0 the least element of $d(S)$.
—Associativity of domain elements follows from the dp-dioid axioms.
—$d(x) \cdot d(y) = d(y) \cdot d(x)$. We show that $d(x) \cdot d(y) \leq d(y) \cdot d(x)$, the converse direction being symmetric.

$$d(x) \cdot d(y) = d(d(x) \cdot d(y)) \cdot d(x) \cdot d(y) = d(x) \cdot d(y) \cdot d(y) \cdot d(x) \leq d(y) \cdot d(x),$$

using Lemma 8.3(2), domain export, associativity of domain elements, and the fact that domain elements are subidentities.
—$d(x) \cdot d(x) = d(x)$ holds since $d(x) = d(d(x) \cdot x) = d(x) \cdot d(x)$ by Lemma 8.3(2) and domain export.

It follows that $(d(S), \cdot, 0, 1)$ is a bounded meet semilattice with meet operation $\cdot$. It is also clear that $(d(S), +, 0, 1)$ is a bounded join semilattice. Hence, it remains to verify the absorption and distributivity laws.

—For $d(x) \cdot (d(x) + d(y)) = d(x)$, we calculate

$$d(x) \cdot (d(y) + d(z)) = (d(y) + d(x)) \cdot d(x) = d(y) \cdot d(x) + d(x) \cdot d(x) = d(y) \cdot d(x) + d(x) = d(x)$$

by commutativity and idempotency of meet as well as distributivity.
—$d(x) + d(x) \cdot d(y) = d(x)$. This is the last step of the previous proof.

—$d(x) \cdot (d(y) + d(z)) = d(x) \cdot d(y) + d(x) \cdot d(z)$ is obvious from commutativity of meet and right distributivity.
—The distributivity law $d(x) + d(y) \cdot d(z) = (d(x) + d(y)) \cdot (d(x) + d(z))$ holds by lattice duality. □

The next lemma presents additional domain laws; it is proved in Appendix 2.

LEMMA 8.5. *In every dp-dioid,*

(1) $x \leq d(y) \cdot x \Leftrightarrow d(x) \leq d(y)$,
(2) $d(x) \cdot 0 = 0$,
(3) $d(x) = 0 \Leftrightarrow x = 0$,
(4) $d(x) \leq d(x + y)$.

The *least left preservation* law (1) is a characteristic property of domain operations. It states that $d(x)$ is the least domain element that satisfies the inequality $x \leq p \cdot x$. Law (2) shows that 0 is a right annihilator in the subalgebra of domain elements.

Next, we study the interaction between domain, parallel composition, and its unit.

LEMMA 8.6. *In every dp-trioid,*

(1) $d(1_\pi) = 1_\sigma$,
(2) $d(x \| y) = d(x) \| d(y)$,
(3) $d(d(x) \| d(y)) = d(x) \| d(y)$,
(4) $d(x) \| d(x) = d(x)$.

See Appendix 2 for proofs. By (3), the subalgebra of domain elements is also closed with respect to parallel products, which are mapped to meets. Property (4) follows from the fact that parallel products of domain elements, hence of subidentities, are meets.

At the end of this section, we characterize domain elements in terms of a weak notion of complementation, following Desharnais and Struth [2011]. This further describes the structure of domain elements within the subalgebra of subidentities.

PROPOSITION 8.7. *Let S be a dp-dioid. Then $x \in d(S)$ if $x + y = 1_\sigma$ and $y \cdot x = 0$ hold for some $y \in S$.*

PROOF. Fix x and let p be an element that satisfies $x + p = 1_\sigma$ and $p \cdot x = 0$. We must show that $d(x) = x$.

—$x \cdot d(x) \leq x$ since $d(x) \leq 1_\sigma$ and $x = (x + p) \cdot x = x \cdot x = x \cdot d(x) \cdot x \leq x \cdot d(x)$, whence $x \cdot d(x) = x$.
—$p \cdot d(x) = d(p \cdot d(x)) \cdot p \cdot d(x) = d(p \cdot x) \cdot p \cdot d(x) = d(0) \cdot x \cdot d(x) = 0$.

Therefore, $d(x) = (x + p) \cdot d(x) = x \cdot d(x) + p \cdot d(x) = x$. □

We call an element y of a dp-dioid a *complement* of an element x whenever $x + y = 1_\sigma$, $y \cdot x = 0$, and $x \cdot y = 0$ hold. Thus, if y is a complement of x, then x is a complement of y. We call an element *complemented* if it has a complement. The set of all complemented elements of a dp-dioid S is denoted B_S.

COROLLARY 8.8. *Let S be a dp-dioid. Then $B_S \subseteq d(S)$.*

LEMMA 8.9. *Let S be a dp-dioid. Then B_S is a Boolean algebra.*

PROOF. Since complemented elements are domain elements, they are idempotent and commutative. We use these properties to show that sums and products of complemented elements are complemented. More precisely, if y_1 is a complement of x_1 and y_2 a complement of x_2, then $y_1 \cdot y_2$ is a complement of $x_1 + x_2$ and $y_1 + y_2$ a complement of

$x_1 \cdot x_2$. First,

$$\begin{aligned} x_1 + x_2 + y_1 \cdot y_2 &= x_1 \cdot (x_2 + y_2) + x_2 \cdot (x_1 + y_1) + y_1 \cdot y_2 \\ &= x_1 \cdot x_2 + x_1 \cdot y_2 + x_2 \cdot x_1 + x_2 \cdot y_1 + y_1 \cdot y_2 \\ &= x_1 \cdot x_2 + x_1 \cdot y_2 + x_2 \cdot y_1 + y_1 \cdot y_2 \\ &= (x_1 + y_1) \cdot (x_2 + y_2) \\ &= 1_\sigma . \end{aligned}$$

Second, $(x_1 + x_2) \cdot y_1 \cdot y_2 = x_1 \cdot y_1 \cdot y_2 + x_2 \cdot y_1 \cdot y_2 = 0$. This proves complementation of sums. The proof of complementation of products is dual, starting from $y_1 \cdot y_2$.

These two facts show that B_S is a subalgebra of $d(S)$. It is therefore a bounded distributive sublattice and a Boolean algebra, since all elements are complemented and complements in distributive lattices are unique. □

The following theorem summarizes this investigation of the structure of $d(S)$.

THEOREM 8.10. *Let S be a dp-dioid. Then $d(S)$ contains the greatest Boolean subalgebra of S bounded by 0 and 1_σ.*

It is obvious that this theorem holds in dp-trioids as well. In the abstract setting, it need not be the case that $d(S)$ contains any Boolean algebra apart from $\{0, 1_\sigma\}$. In fact, the sequential subidentities may form a distributive lattice that is not a Boolean algebra, for instance, a chain.

Example 8.11. Consider the structure with addition defined by $0 < a < 1_\sigma < 1_\pi$ and the other operations defined by the following tables.

$\cdot$	0	a	1_σ	1_π
0	0	0	0	0
a	0	a	a	a
1_σ	0	a	1_σ	1_π
1_π	0	a	1_π	1_π

$\parallel$	0	a	1_σ	1_π
0	0	0	0	0
a	0	a	a	a
1_σ	0	a	1_σ	1_σ
1_π	0	a	1_σ	1_π

	d
0	0
a	a
1_σ	1_σ
1_π	1_σ

It can be checked that this structure forms a dp-trioid (in fact, this counterexample was found by Isabelle), but the element $d(a) = a$ is not complemented. For instance, the only element y that satisfies $a + y = 1_\sigma$ is $y = 1_\sigma$, but $1_\sigma \cdot a = a \neq 0$.

Thus B_S need not be equal to $d(S)$, which justifies Corollary 8.8. In the multirelational model, however, the set of all sequential subidentities forms a Boolean algebra, as mentioned in Section 4. In a multirelational dp-trioid S, therefore, $d(S) = \{P \mid P \subseteq 1_\sigma\}$.

9. THE DIAMOND AXIOMS OF STAR-FREE CDL

We are now equipped for deriving algebraic variants of the diamond axioms of concurrent dynamic logic except for the star axioms in dp-trioids. First, note that $\langle x \rangle p = \langle x \rangle d(p)$.

LEMMA 9.1.

(*1*) *In every dp-dioid, the following* CDL *axioms are derivable.*
  (*a*) $\langle x + y \rangle p = \langle x \rangle p + \langle y \rangle p$,
  (*b*) $\langle x \cdot y \rangle p = \langle x \rangle \langle y \rangle p$,
  (*c*) $\langle d(p) \rangle q = d(p) \cdot d(q)$.

(*2*) *In every dp-trioid, the following* CDL *axiom is derivable as well.*
  (*d*) $\langle x \| y \rangle p = \langle x \rangle p \cdot \langle y \rangle p$.

PROOF.

(a) Using right distributivity and additivity of domain, we calculate

$$\langle x+y\rangle p = d((x+y)\cdot p) = d(x\cdot p + y\cdot p) = d(x\cdot p) + d(y\cdot p) = \langle x\rangle p + \langle y\rangle p.$$

(b) Using domain associativity and locality, we calculate

$$\langle x\cdot y\rangle p = d((x\cdot y)\cdot p) = d(x\cdot(y\cdot d(p))) = d(x\cdot d(y\cdot d(p))) = d(x\cdot\langle y\rangle p) = \langle x\rangle\langle y\rangle p.$$

(c) By domain export, $\langle d(p)\rangle q = d(d(p)\cdot q) = d(p)\cdot d(q)$.

(d) Using domain interaction and the first domain concurrency axiom, we calculate

$$\langle x\|y\rangle p = d((x\|y)\cdot d(p)) = d((x\cdot d(p))\|(y\cdot d(p))) = d(x\cdot d(p))\cdot d(y\cdot d(p)) = \langle x\rangle p\cdot\langle y\rangle p.$$

□

We can derive additional diamond laws from the domain laws such as $\langle 0\rangle p = 0$ or $\langle 1_\sigma\rangle p = d(p)$. However, we have a counterexample to $\langle 1_\pi\rangle p = 1_\sigma$, which holds in the multirelational model.

Example 9.2. Consider the structure with addition defined by $0 < 1_\sigma < 1_\pi$, parallel composition defined by meet, and the remaining operations by the conditions $1_\pi\cdot 0 = 0$, $1_\pi\cdot 1_\pi = 1_\pi$, $d(0) = 0$, and $d(1_\sigma) = d(1_\pi) = 1_\sigma$. It can be checked that this defines a dp-trioid, but $\langle 1_\pi\rangle 0 = d(1_\pi\cdot 0) = d(0) = 0 < 1_\sigma$.

The following *demodalization law* is proved in Appendix 2. It is instrumental for deriving the star axioms of CDL.

LEMMA 9.3. *In every dp-dioid,*

$$\langle x\rangle p \le d(q) \Leftrightarrow x\cdot d(p) \le d(q)\cdot x.$$

Finally, we present two important counterexamples.

LEMMA 9.4.

(1) $\langle R\rangle(P\cup Q) \neq \langle R\rangle P\cup\langle R\rangle Q$*, for some* $R, P, Q\in\mathscr{M}(X)$ *and* $P, Q\subseteq 1_\sigma$*,*
(2) $\langle R\rangle\emptyset\neq\emptyset$*, for some* $R\in\mathscr{M}(X)$*.*

PROOF.

(1) Let $R = \{(a,\{a,b\})\}$, $P = \{(a,\{a\})\}$ and $Q = \{(b,\{b\})\}$. Then

$$\langle R\rangle(P\cup Q) = \{(a,\{a,b\})\} \supset \emptyset = \langle R\rangle P\cup\langle R\rangle Q.$$

(2) For $R = \{(a,\emptyset)\}$, we have $\langle R\rangle\emptyset = \{(a,\{a\})\}\neq\emptyset$. □

The additivity and strictness laws just refuted are defining properties of modal algebras in the sense of Jónsson and Tarski (see Blackburn et al. [2011]). Our concurrent dynamic algebra axioms are therefore nonstandard. This situation is analogous to the difference between strict and multiplicative predicate transformers, which arise from relational semantics, and their isotone counterparts, which arise from up-closed multirelations. Predicate transformers are usually obtained from boxes instead of diamonds; the failure of multiplicativity is related to that of additivity by duality.

In the concurrent setting, the earlier multirelation R models an external choice between a and b from input a. Reflecting this, it is not sufficient that one can observe either one of a and b, but not both, after executing R. In contrast to this, $\langle S\rangle(P\cup Q) = \langle S\rangle P\cup\langle S\rangle Q$, for $S = \{(a,\{a\}),(a,\{b\})\}$, models an internal choice.

Finally, $\langle R\|S\rangle P$ holds if there is a parallel terminating execution of concurrent program R and concurrent program S such that P holds of the global concurrent state produced. This is the case if and only if P holds in all states produced by R upon

termination and in all those produced by S upon termination, that is, $\langle R\rangle P \cdot \langle S\rangle P$ holds.

10. THE STAR AXIOMS OF CDL

This section derives the star axioms of CDL in expansions of dp-dioids to variants of Kleene algebras. This is not straightforward due to the lack of associativity and left distributivity laws. As before, we start at the level of multirelations to derive the appropriate star axioms. We then lift the investigation to the algebraic level.

Let R and S be multirelations. Consider the functions

$$F_{RS} = \lambda X.\ S \cup R \cdot X, \qquad F_R = \lambda X.\ 1_\sigma \cup R \cdot X,$$

which generate variants of the Kleene star as their least fixpoints. Existence of these fixpoints is guaranteed by basic fixpoint theory. The universal multirelation U has been introduced in Section 2.

LEMMA 10.1.

(1) *The functions F_{RS} and F_R are isotone.*
(2) *$(\mathscr{M}(X), \cup, \cap, \emptyset, U)$ forms a complete lattice.*
(3) *F_{RS} and F_R have least pre-fixpoints and greatest post-fixpoints, which are also least and greatest fixpoints.*

See Appendix 2 for proofs.

We write (R^*S) or μF_{RS} for the least fixpoint of F_{RS} and R^* or μF_R for the least fixpoint of F_R. We immediately obtain the fixpoint unfold and induction laws

$$S \cup R \cdot (R^*S) \subseteq (R^*S), \qquad S \cup R \cdot T \subseteq T \Rightarrow (R^*S) \subseteq T$$

for F_{RS} and the corresponding laws

$$1_\sigma \cup R \cdot R^* \subseteq R^*S, \qquad 1_\sigma \cup R \cdot T \subseteq T \Rightarrow R^* \subseteq T$$

for F_R. The binary fixpoint (R^*S) is not necessarily equal to $R^* \cdot S$. At least, by definition, $R^* = R^* \cdot 1_\sigma = (R^*1_\sigma)$. The fixpoints μF_R and μF_{RS} can be related by the following well-known *fixpoint fusion* law.

THEOREM 10.2.

(1) *Let f and g be isotone functions and h a continuous function over a complete lattice. If $h \circ g \leq f \circ h$, then $h(\mu g) \leq \mu f$.*
(2) *Let f, g, and h be isotone functions over a complete lattice. If $f \circ h \leq h \circ g$, then $\mu f \leq h(\mu g)$.*

It follows from (1) and (2) that, if f and g are isotone, h is continuous, and $h \circ g = f \circ h$, then $\mu f = h(\mu g)$. Applying fixpoint fusion to F_{RS} and F_R yields the following fact.

COROLLARY 10.3. *Let R, S, and T be multirelations. Then*

$$R^* \cdot S \subseteq (R^*S), \qquad (R^*S) \cdot T \subseteq (R^*(S \cdot T)).$$

PROOF. Let $f = F_{RS}$, $g = F_R$, and $h = H = \lambda X.X \cdot S$.

It is easy to show that H is continuous, that is, $(\bigcup_{i\in I} R_i) \cdot S = \bigcup_{i\in I}(R_i \cdot S)$. The proof is similar to that of Lemma 3.1(4). Moreover,

$$(H \circ F_R)(x) = (1_\sigma \cup R \cdot x) \cdot S = S \cup (R \cdot x) \cdot S \subseteq S \cup R \cdot (x \cdot S) = (F_{RS} \circ H)(x)$$

by weak associativity (Lemma 3.1(3)), so $R^* \cdot S \subseteq (R^*S)$ by fixpoint fusion.

The proof of $(R^*S) \cdot T \subseteq (R^*(S \cdot T))$ follows the same pattern. □

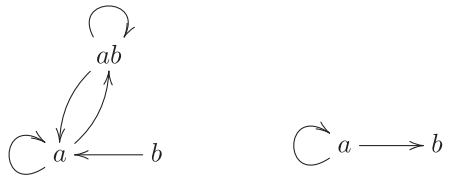

Fig. 4. Diagrams for R and S in the proof of Lemma 3.4(2) (same as Figure 1).

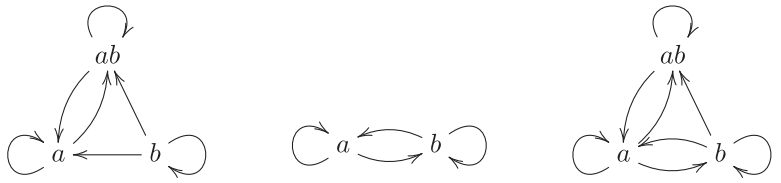

Fig. 5. Diagrams for R^*, $R^* \cdot S$ and R^*S for R and S in the proof of Lemma 3.4(2).

Proving the converse direction, $(R^*S) \subseteq R^* \cdot S$, by fixpoint fusion requires associativity in the other direction, which does not hold in our setting (Lemma 3.4(2), where the counterexample was given for $R \cdot (R \cdot S) \subseteq (R \cdot R) \cdot S$ and extends to the aforementioned case). The following counterexample rules out any other proof of this inclusion.

LEMMA 10.4. *There are multirelations R and S such that $R^*S \neq R^* \cdot S$.*

PROOF. Consider R and S from Lemma 3.4(2) and their diagrams in Figure 4. The multirelations $R^* = 1_\sigma \cup R \cdot (1_\sigma \cup R)$, $R^* \cdot S$ and $R^*S = S \cup R \cdot (S \cup R \cdot (S \cup R)) = R \cdot R \cdot (R \cup S)$ are computed from these diagrams as shown in Figure 5. Clearly, $R^*S \not\subseteq R^* \cdot S$. □

At first sight, Lemma 10.4 seems to invalidate the star-axiom of CDL. However, the identity $R^*S = R^* \cdot S$ is only needed in the modal setting, where S is a subidentity. In this case, as we have seen, stronger algebraic properties for sequential composition are present. We now investigate this restriction.

First, we show that the unfold law for R^*S can be strengthened to an identity.

COROLLARY 10.5. *Let R and S be multirelations. Then $S \cup R \cdot (R^*S) = (R^*S)$.*

This holds since every pre-fixpoint of F_{RS} is also a fixpoint.

We now prove the desired fusion of μF_{RS} with μF_R when S is a subidentity.

PROPOSITION 10.6. *Let R be a multirelation and P a subidentity. Then*

$$R^*P = R^* \cdot P.$$

PROOF. Applying fixpoint fusion, as in Corollary 10.3, but with $H = \lambda X.X \cdot P$, now establishes $H \circ F_R = F_{RP} \circ H$, since we have full associativity for subidentities by Lemma 4.2(1). This suffices to verify the claim. □

We can therefore replace R^*P by $R^* \cdot P$ in the induction law for F_{RP}.

LEMMA 10.7. *Let R and S be multirelations and P be a subidentity. Then*

$$P \cup R \cdot S \subseteq S \Rightarrow R^* \cdot P \subseteq S.$$

Corollary 10.5 and Lemma 10.7 motivate the following algebraic definition. As before, we use domain elements instead of sequential subidentities.

A *proto-Kleene algebra with domain* (*dp-Kleene algebra*) is a dp-dioid expanded by a star operation, which satisfies the *(left) star unfold* and *(left) star induction* axioms

$$1_\sigma + x \cdot x^* \leq x^*, \qquad d(z) + x \cdot y \leq y \Rightarrow x^* \cdot d(z) \leq y.$$

A *proto-bi-Kleene algebra with domain* (*dp-bi-Kleene algebra*) is a dp-Kleene algebra, which is also a dp-trioid[2]. In both cases, the unfold law strengthens to the identity $1_\sigma + x \cdot x^* = x^*$. The full list of dp-bi-Kleene algebra axioms can be found in Appendix 1.

The development so far is summarized in the following soundness result, which links the multirelational layer with the abstract algebraic one.

THEOREM 10.8. *$(\mathscr{M}(X), \cup, \cdot, \|, \emptyset, 1_\sigma, 1_\pi, d, ^*)$ is a dp-bi-Kleene algebra.*

PROOF. The structure is a dp-trioid as a consequence of Theorem 6.1. The star axioms hold by Corollary 10.5 and Lemma 10.7. □

Due to this result, we can now continue at the algebraic level. First, we derive the modal star unfold axiom of CDL.

LEMMA 10.9. *Let K be a dp-Kleene algebra, $x \in K$ and $p \in d(K)$. Then*

$$p + \langle x \rangle \langle x^* \rangle p = \langle x^* \rangle p.$$

PROOF. $p + \langle x \rangle \langle x^* \rangle p = \langle 1_\sigma + x \cdot x^* \rangle p = \langle x^* \rangle p$ by the star unfold axiom and the CDL axioms, which have been verified in Lemma 9.1. □

It remains to verify the star induction axiom of CDL. First we show a simulation law.

LEMMA 10.10. *Let K be a dp-Kleene algebra, $x \in K$ and $p \in d(K)$. Then*

$$x \cdot p \leq p \cdot y \Rightarrow x^* \cdot p \leq p \cdot y^*.$$

See Appendix 2 for a proof. The derivation of an algebraic variant of the star unfold axiom of CDL is then trivial.

PROPOSITION 10.11. *Let K be a dp-Kleene algebra, $x \in K$ and $p \in d(K)$. Then*

$$\langle x \rangle p \leq p \Rightarrow \langle x^* \rangle p \leq p.$$

PROOF.

$$\langle x \rangle p \leq p \Leftrightarrow x \cdot p \leq p \cdot x \Rightarrow x^* \cdot p \leq p \cdot x^* \Leftrightarrow \langle x^* \rangle p \leq p.$$

The first and last step use demodalization (Lemma 9.3); the second step uses Lemma 10.10. □

The first main theorem of this article combines these results.

THEOREM 10.12. *The* CDL *axioms are derivable in dp-bi-Kleene algebras.*

We therefore call dp-bi-Kleene algebras informally *concurrent dynamic algebras*.

Finally, in Appendix 2, we prove a right star unfold law and derive a variant of modal star induction in analogy to the induction axiom of dp-Kleene algebra.

LEMMA 10.13. *Let K be a dp-Kleene algebra, $x \in K$ and $p, q \in d(K)$. Then*

(1) $p + \langle x^* \rangle \langle x \rangle p \leq \langle x^* \rangle p$,
(2) $p + \langle x \rangle q \leq q \Rightarrow \langle x^* \rangle p \leq q$.

[2]In this article, we ignore the star of concurrent composition, which should normally be part of the definition of a bi-Kleene algebra. The reason is that it is not considered in CDL.

11. THE STRUCTURE OF AP-TRIOIDS

Section 8 shows that the domain elements of a dp-dioid or dp-trioid form a distributive lattice. We now revisit this development for antidomain, where the resulting domain algebras are Boolean algebras. We start with a number of auxiliary lemmas. These are needed because the minimality of the axiom set makes it difficult to derive the desirable properties directly.

In the following lemma, we abbreviate $d = a \circ a$. This is justified in Proposition 11.2, which formally verifies that $a(a(x))$ models the domain of element x.

LEMMA 11.1. *In every ap-dioid,*

(1) $a(x) \leq 1_\sigma$,
(2) $a(x) \cdot a(x) = a(x)$,
(3) $a(x) = 1_\sigma \Leftrightarrow x = 0$,
(4) $a(x) \cdot y = 0 \Leftrightarrow a(x) \leq a(y)$,
(5) $x \leq y \Rightarrow a(y) \leq a(x)$,
(6) $a(x) \cdot a(y) \cdot d(x + y) = 0$,
(7) $a(x + y) = a(x) \cdot a(y)$,
(8) $a(a(x) \cdot y) = d(x) + a(y)$.

See Appendix 2 for proofs. The *greatest left annihilation property* (4) is a characteristic property of antidomain elements. It states that $a(y)$ is the greatest antidomain element p that satisfies the left annihilation law $p \cdot y = 0$. By Property (5), the antidomain operation is *antitone*; by Property (7), it is *multiplicative*. Property (8) is an *export* law for antidomain. These laws are helpful in the following proposition, which is proved in Appendix 2.

PROPOSITION 11.2. *Every ap-dioid is a dp-dioid with domain operation $d = a \circ a$.*

As in Section 8, we investigate the structure of domain elements.

PROPOSITION 11.3. *Let S be an ap-dioid with $d = a \circ a$. Then $d(S)$ forms a subalgebra, which is the greatest Boolean algebra in S bounded by 0 and 1_σ.*

PROOF. First, since every ap-dioid is a dp-dioid, $d(S)$ is a bounded distributive lattice. Second, antidomain elements are closed under the operations because $d(a(x)) = a(x)$ by antidomain locality,

$$d(a(x)) = a(a(a(x))) = a(d(x)) = a(1_\sigma \cdot d(x)) = a(1_\sigma \cdot x) = a(x).$$

Third, the operation $\lambda x.a(x)$ is complementation in this algebra. One of the complementation properties, $a(d(x)) + d(x) = a(x) + d(x) = 1_\sigma$, is an axiom. The others, $a(d(x)) \cdot d(x) = a(x) \cdot d(x) = 0$ and $d(x) \cdot a(d(x)) = d(x) \cdot a(x) = 0$, are immediate from antidomain annihilation.

Finally, by Theorem 8.10, $d(S)$ contains the greatest Boolean algebra in S between 0 and 1_σ and is therefore equal to the greatest such Boolean algebra. □

We now expand Proposition 11.2 from the sequential to the concurrent case.

PROPOSITION 11.4. *Every ap-trioid is a dp-trioid.*

The proof can be found in Appendix 2.

Finally, we investigate the star. A *proto-Kleene algebra with antidomain* (*ap-Kleene algebra*) is an ap-dioid expanded by a star operation, which satisfies the *(left) star unfold* and *(left) star induction* axioms

$$1_\sigma + x \cdot x^* \leq x^*, \qquad a(z) + x \cdot y \leq y \Rightarrow x^* \cdot a(z) \leq y.$$

A *proto-bi-Kleene algebra with antidomain* (*ap-bi-Kleene algebra*) is an ap-Kleene algebra, which is also an ap-trioid. A full list of ap-bi-Kleene algebra axioms can be found in Appendix 1.

The following proposition is immediate from Propositions 11.2 and 11.4.

PROPOSITION 11.5.

(*1*) *Every ap-Kleene algebra is a dp-Kleene algebra.*
(*2*) *Every ap-bi-Kleene algebra is a dp-bi-Kleene algebra.*

In combination, these facts establish an analogue to Theorem 10.8.

THEOREM 11.6. $(\mathscr{M}(X), \cup, \cdot, \|, \emptyset, 1_\sigma, 1_\pi, a, ^*)$ *forms an ap-bi-Kleene algebra.*

12. THE BOX AXIOMS OF CDL

The results of the previous section imply that the diamond axioms of concurrent dynamic logic hold in antidomain algebras. In addition, we can now derive algebraic variants of Peleg's De Morgan dual box axioms, which should perhaps be taken with a grain of salt. Since every ap-bi-Kleene algebra is a dp-Kleene algebra, the diamond axioms of concurrent dynamic algebras hold immediately.

LEMMA 12.1.

(*1*) *In every ap-dioid, the following CDL axioms are derivable.*
  (*a*) $\langle x + y\rangle p = \langle x\rangle p + \langle y\rangle p$,
  (*b*) $\langle x \cdot y\rangle p = \langle x\rangle\langle y\rangle p$,
  (*c*) $\langle d(p)\rangle q = d(p) \cdot d(q)$.
(*2*) *In every ap-trioid, the following CDL axiom is derivable.*
  (*d*) $\langle x \| y\rangle p = \langle x\rangle p \cdot \langle y\rangle p$.
(*3*) *In every ap-Kleene algebra, the following star axioms are derivable.*
  (*e*) $1_\sigma + \langle x\rangle\langle x^*\rangle p = \langle x^*\rangle p$,
  (*f*) $\langle x\rangle p \leq p \Rightarrow \langle x^*\rangle p \leq p$.

In addition, the following box axioms follow easily from De Morgan duality.

PROPOSITION 12.2.

(*1*) *In every ap-dioid, the following CDL axioms are derivable.*
  (*a*) $[x + y]p = [x]p \cdot [y]p$,
  (*b*) $[x \cdot y]p = [x][y]p$,
  (*c*) $[d(p)]q = a(p) + d(q)$.
(*2*) *In every ap-trioid, the following CDL axiom is derivable.*
  (*d*) $[x \| y]p = [x]p \cdot [y]p$.
(*3*) *In every ap-Kleene algebra, the following star axioms are derivable.*
  (*e*) $1_\sigma \cdot [x][x^*]p = [x^*]p$,
  (*f*) $p \leq [x]p \Rightarrow p \leq [x^*]p$.

In sum, these results yield the second main theorem of this article.

THEOREM 12.3. *The modal axioms of* CDL *are derivable in ap-bi-Kleene algebras.*

We therefore call ap-bi-Kleene algebras *concurrent dynamic algebras* as well. In contrast to dp-Kleene algebras, these are based on Boolean algebras of domain elements.

Finally, we present counterexamples to multiplicativity and co-strictness of boxes.

LEMMA 12.4. *There are multirelations R, P, and Q such that the following holds.*

(*1*) $[R](P \cdot Q) \neq [R]P \cdot [R]Q$,
(*2*) $[R]1_\sigma \neq 1_\sigma$.

PROOF.

(1) Obviously, $\forall p, q.\ \langle x\rangle(p+q) = \langle x\rangle p + \langle x\rangle q$ if and only if $\forall p, q.\ [x](p \cdot q) = [x]p \cdot [x]q$. Hence, the counterexample from Lemma 9.4 applies.
(2) Similarly, $\langle x\rangle 0 = 0$ if and only if $[x]1_\sigma = 1_\sigma$. □

The following counterexample is directly related to this lemma. According to Jónsson and Tarski, modal boxes and diamonds are conjugate functions on Boolean algebras, that is, they are related by the conjugation law

$$\langle x\rangle p \cdot q = 0 \Leftrightarrow p \cdot [x]q = 0.$$

Conjugate functions are a fortiori additive. By Lemmas 9.4 and 12.4, this cannot be the case in the multirelational setting, hence the conjugation law cannot hold. This is confirmed directly by the multirelation $R = \{(a, \emptyset)\}$ and the subidentity $P = \{(a, \{a\})\}$ over the set $X = \{a\}$, which satisfy

$$\langle R\rangle P \cdot P = d(R \cdot P) \cdot P = P \supset \emptyset = P \cdot a(R \cdot a(P)) = P \cdot [R]P.$$

13. THE STAR AND FINITE ITERATION

It is well known that least fixpoints can be reached by iterating from the least element of a complete lattice up to the first infinite ordinal whenever the function under consideration is not only isotone, but also continuous. Otherwise, if the function is only isotone, transfinite induction beyond the first limit ordinal is required.

Our counterexample to left distributivity rules out continuity in general, but, in fact, chain continuity or directedness suffices for the star. As in Section 10, we consider

$$F_R = \lambda X.1_\sigma \cup R \cdot X.$$

Peleg [1987b] has provided a counterexample even to chain continuity. We display a proof in Appendix 2 to make this article self-contained.

LEMMA 13.1 (PELEG). *There exists a multirelation R and an ascending chain of multirelations S_i, for $i \in \mathbb{N}$, such that $F_R(\bigcup_{i\in\mathbb{N}} S_i) \neq \bigcup_{i\in\mathbb{N}} F_R(S_i)$.*

Chain continuity can, however, be obtained if a multirelation R is *externally image finite*, that is, for all $(a, A) \in R$ the set A has finite cardinality. This notion has been called *finitely branched* by Peleg. We have chosen a different name to distinguish it from *internal image finiteness*, which is the case when for each a, the set of all (a, A) has finite cardinality. From a computational point of view, external image finiteness is not a limitation, since infinite sets A correspond to unbounded external nondeterminism or unbounded parallel composition, which is not implementable.

LEMMA 13.2 (PELEG). *If R is externally image finite, then F_R is chain continuous.*

See Appendix 2 for a proof.

We define powers of F_R inductively as $F_R^0 = \lambda X.X$ and $F_R^{n+1} = F_R \circ F_R^n$ and can then define iteration to the first limit ordinal as

$$F_R^* = \bigcup_{i\in\mathbb{N}} F^i.$$

General fixpoint theory (Kleene's fixpoint theorem) then implies the following fact.

PROPOSITION 13.3. *If R is externally image finite, then $R^* = F_R^*(\emptyset)$.*

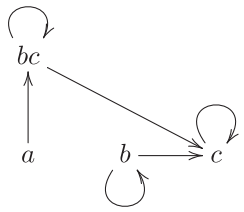

Fig. 6. Diagram for R in the proof of Proposition 14.1.

We now compare this notion of finite iteration with another one.

$$R^{(0)} = \emptyset, \qquad R^{(n+1)} = 1_\sigma \cup R \cdot R^{(n)}, \qquad R^{(*)} = \bigcup_{n\in\mathbb{N}} R^{(n)}.$$

Our next lemma shows that the inductive definition of $R^{(*)}$ captures the iterative function application of F_R^* to $\emptyset$ and hence R^* for external image finiteness. It is proved in Appendix 2.

LEMMA 13.4.

(1) *For all* $n \in \mathbb{N}$, $F_R^n(\emptyset) = R^{(n)}$ *and therefore* $F_R^*(\emptyset) = R^{(*)}$.
(2) *If* R *is externally image finite, then* $R^* = R^{(*)}$.

Finally, we show that external image finiteness in Lemma 13.4(2) is necessary.

LEMMA 13.5. *There exists a multirelation* R *such that* $R^{(*)}$ *is not a fixpoint of* F_R.

PROOF. Consider the multirelation

$$R = \{(m, \{n \mid n < m\}) \mid m \in \mathbb{N} \cup \{\infty\}\}.$$

It follows that $(0, \emptyset) \in R$ and $R \cdot \emptyset = \{(0, \emptyset)\}$.

Then $(m, \{n \mid n \leq m-2\}) \notin R$, but it is in $R^{(2)}$, and $(m, \{n \mid n \leq m-k\}) \notin R^{(i)}$ for $i < k$, but it is in $R^{(k)}$; similarly, $(m, \emptyset) \in R^{(m)}$ but not in $R^{(l)}$ for all $l < m$. Consequently, $(\infty, \emptyset) \notin R^{(n)}$ for all $n \in \mathbb{N}$, therefore $(\infty, \emptyset) \notin R^{(*)}$, but $(\infty, \emptyset) \in F_R(R^{(*)})$. □

14. REFUTATION OF SEGERBERG'S AXIOM

Segerberg's axiom is the induction axiom of (nonconcurrent) propositional dynamic logic (see Harel et al. [2000]). Goldblatt uses its box version—his box semantics is different from ours—but not the diamond one. This section provides a counterexample to Segerberg's axiom in the multirelational model with box-diamond duality.

In diamond form, Segerberg's axiom is

$$\langle x^*\rangle p \leq p + \langle x^*\rangle(\langle x\rangle p - p).$$

In modal Kleene algebra, it is equivalent to the star induction axiom. For multirelations, the situation is different.

PROPOSITION 14.1. *There is a multirelation* R *and a subidentity* P *such that*

$$\langle R^*\rangle P \supset P \cup \langle R^*\rangle(\langle R\rangle P - P).$$

PROOF. Let $R = \{(a, \{b, c\}), (b, \{b\}), (b, \{c\}), (c, \{c\})\}$ and $P = \{(c, \{c\})\}$. As previously, we visualize R in the Hasse diagram in Figure 6. The multirelation R^* can be read off as the relational reflexive transitive closure from this diagram by chasing arrows. One can also use the diagram to check that

$$R \cdot P = \{(b, \{c\}), (c, \{c\})\}, \qquad \langle R\rangle P = \{(b, \{b\}), (c, \{c\})\}, \qquad \langle R\rangle P - P = \{(b, \{b\})\}.$$

In addition, R^* can be computed by iterating with $R^{(*)}$ according to Lemma 13.4(2), since R is externally image finite. Obviously, $R \cdot \emptyset = \emptyset$. Therefore,

$$\begin{aligned}
R^{(1)} &= 1_\sigma,\\
R^{(2)} &= 1_\sigma \cup R \cdot (1_\sigma \cup R) = \{(a, \{a\}), (a, \{c\}), (a, \{b, c\}), (b, \{b\}), (b, \{c\}), (c, \{c\})\},\\
R^{(3)} &= 1_\sigma \cup R \cdot (1_\sigma \cup R \cdot (1_\sigma \cup R)) = R^{(2)},\\
R^{(n)} &= R^{(2)},
\end{aligned}$$

that is, iteration becomes stationary after four steps. Chain continuity implies that

$$R^* = R^{(*)} = R^{(2)} = \{(a, \{a\}), (a, \{c\}), (a, \{b, c\}), (b, \{b\}), (b, \{c\}), (c, \{c\})\}.$$

On the one hand, this result yields

$$\begin{aligned}
\langle R^*\rangle(\langle R\rangle P - P) &= \langle R^*\rangle\{(b, \{b\})\} = \{(b, \{b\})\},\\
P \cup \langle R^*\rangle(\langle R\rangle P - P) &= \{(b, \{b\}), (c, \{c\})\}.
\end{aligned}$$

On the other hand,

$$\begin{aligned}
R^* \cdot P &= \{(a, \{c\}), (b, \{c\}), (c, \{c\})\},\\
\langle R^*\rangle P &= \{(a, \{a\}), (b, \{b\}), (c, \{c\})\}.
\end{aligned}$$

This confirms that $\langle R^*\rangle P \supset P \cup \langle R^*\rangle(\langle R\rangle P - P)$ and falsifies Segerberg's axiom. □

COROLLARY 14.2. *Segerberg's axiom is not derivable in ap-bi-Kleene algebras.*

Obviously, this implies that the axiom is not derivable in ap-Kleene algebras. However, at least its converse is derivable.

LEMMA 14.3. *In every ap-Kleene algebra,*

$$p + \langle x^*\rangle(\langle x\rangle p - p) \leq \langle x^*\rangle p.$$

See Appendix 2 for a proof. Hence, this fact is derivable in ap-bi-Kleene algebras as well.

Segerberg's axiom is usually presented in box form as $p \cdot [x^*](p \to [x]p) \leq [x^*]p$, where $p \to q = a(p) + q$. By De Morgan duality, variants of Proposition 14.1, Corollary 14.2, and Lemma 14.3 hold in the box case. In particular, the box variant of Segerberg's axiom is neither valid in the multirelational model nor derivable in ap-bi-Kleene algebras.

15. CONCLUSION

We have defined weak variants of Kleene algebras with domain and antidomain that capture essential properties of the algebra of multirelations under union, sequential, and parallel composition as well as the sequential Kleene star together with multirelational domain and antidomain operations. The relationships between the different algebraic structures defined in this article are summarized in Figure 7. Both dp-bi-Kleene algebras and ap-bi-Kleene algebras qualify as concurrent dynamic algebras; their axioms are listed in Appendix 1. We have derived algebraic counterparts of Peleg's CDL axioms from these two algebras. We have also proved their soundness with respect to the concrete multirelational model.

The algebra of multirelations is, however, much richer than this article might suggest. First of all, a left interaction law $R \cdot (S \| T) \subseteq (R \cdot S) \| (R \cdot T)$ complements its dextrous counterpart. Second, domain is characterized by the inclusion $1_\sigma \cap R \cdot U \subseteq d(R)$, where U is the universal multirelation defined in Section 2, but an equational definition $d(R) = 1_\sigma \cap R \cdot U$ of domain, as in the relational setting, is impossible. Third,

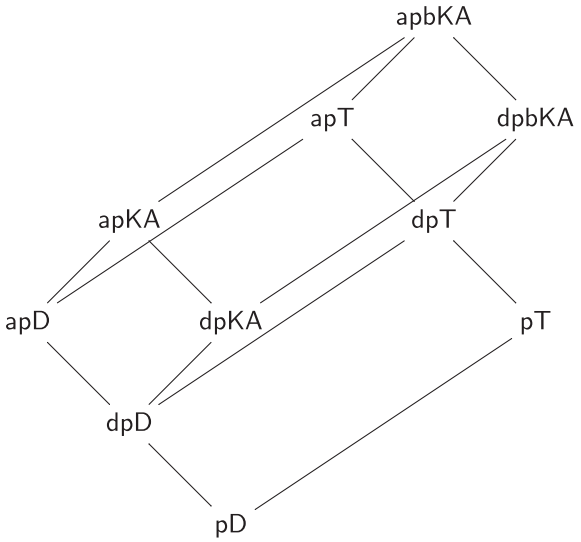

Fig. 7. Summary of algebraic subclass relationships. pD stands for the class of proto-dioids, dpD for domain proto-dioids, apD for antidomain proto-dioids, dpKA for dp-Kleene algebras, apKA for ap-Kleene algebras, pT for proto-trioids, dpT for dp-trioids, apT for ap-trioids, dpbKA for dp-bi-Kleene algebras, and apbKA for ap-bi-Kleene algebras.

sequentiality and concurrency also interact via laws such as $1_\pi \cdot R = 1_\pi$ and in particular $1_\pi \cdot \emptyset = 1_\pi$. In fact, whether a multirelation R satisfies $R \cdot \emptyset = \emptyset$, $R \cdot \emptyset \neq \emptyset$, or even $R \cdot \emptyset = R$ depends on whether or not pairs of the form $(a, \emptyset)$ occur in it. This situation is similar to that of languages with finite and infinite words. In that case, one can define the finite part $\mathsf{fin}(L)$ and the infinite part $\mathsf{inf}(L)$ of a language L and prove laws such as $\mathsf{fin}(L) \cdot \emptyset = \emptyset$ and $\mathsf{inf}(L) \cdot \emptyset = \mathsf{inf}(L)$. Here, we can consider the multirelations $\tau(R) = R \cap 1_\pi$ and $\overline{\tau}(R) = R - 1_\pi$, which satisfy $\tau(R) \cdot \emptyset = \tau(R)$ and $\overline{\tau}(R) \cdot \emptyset = \emptyset$, study the sets of these elements, and derive identities for expressions such as $\tau(R \cdot S)$ or $\overline{\tau}(R \cup S)$ in analogy to the language case. Elements $(a, \emptyset)$ can be interpreted in various ways, for instance, as success states; elements $\tau(R)$ can be seen as terminal elements, since $\tau(R) \cdot S = \tau(R)$ holds for any multirelation S and $\langle \tau(R) \rangle P = d(\tau(R))$. A detailed investigation is the aim of future work.

While up-closed multirelations are unsuitable for concurrency, another subclass is interesting. Call a multirelation R *union-closed* if for all a and $X \neq \emptyset$ the condition $X \subseteq \{A \mid (a, A) \in R\}$ implies $(a, \bigcup X) \in R$. If R has only finite internal nondeterminism, that is, for each a there are only finitely many A with $(a, A) \in R$, then R is union closed if and only if $R||R \subseteq R$. It turns out that sequential composition of union-closed multirelations is associative, while, in contrast to the up-closed case, parallel composition remains nontrivial. In the context of concurrency, it seems natural to require that a multirelation can access the union of two separate sets from some state whenever it can access them individually. Adapting concurrent dynamic algebras to union-closed relations is another promising direction for future work. A further specialization to Parikh's game logic based on proto-Kleene algebras with domain and antidomain seems another feasible restriction.

In conclusion, the results presented in this article lay the foundation for a thorough algebraic exploration of Peleg's concurrent dynamic logic with its extensions and variants, Parikh's game logics, and monotone predicate transformer semantics. Algebra has been instrumental in taming the tedious second-order syntactic manipulations

at the multirelational level in favor of first-order equational reasoning. More succinct descriptions of the algebra of multirelations will be given in future articles. A unification of related approaches to games and concurrency from this basis seems possible. The integration of more advanced concepts such as communication, synchronization, knowledge, or incentive constraints remains to be explored.

APPENDIX 1: AXIOMS OF CONCURRENT DYNAMIC ALGEBRAS

First, we list the complete set of proto-trioid axioms.

$$\begin{aligned}
x + (y + z) &= (x + y) + z \\
x + y &= y + x \\
x + 0 &= x \\
x + x &= x \\
1_\sigma \cdot x &= x \\
x \cdot 1_\sigma &= x \\
x \cdot y + x \cdot z &\leq x \cdot (y + z) \\
(x + y) \cdot z &= x \cdot z + y \cdot z \\
0 \cdot x &= 0 \\
x \| (y \| z) &= (x \| y) \| z \\
x \| y &= y \| x \\
1_\pi \| x &= x \\
x \| (y + z) &= x \| y + x \| z \\
0 \| x &= 0
\end{aligned}$$

Next, we list the concurrent dynamic algebra axioms for distributive lattices and Boolean algebras. The left-hand column contains the axioms for dp-bi-Kleene algebras, the right-hand column those for ap-bi-Kleene algebras.

$$\begin{aligned}
d(x) \cdot (y \cdot z) &= (d(x) \cdot y) \cdot z \\
x \cdot (d(y) \cdot z) &= (x \cdot d(y)) \cdot z \\
x \cdot (y \cdot d(z)) &= (x \cdot y) \cdot d(z) \\
x &\leq d(x) \cdot x \\
d(x \cdot y) &= d(x \cdot d(y)) \\
d(x + y) &= d(x) + d(y) \\
d(x) &\leq 1_\sigma \\
d(0) &= 0 \\
(x \| y) \cdot d(z) &= (x \cdot d(z)) \| (y \cdot d(z)) \\
d(x \| y) &= d(x) \cdot d(y) \\
d(x) \| d(y) &= d(x) \cdot d(y) \\
1_\sigma + x \cdot x^* &\leq x^* \\
d(z) + x \cdot y \leq y &\Rightarrow x^* \cdot d(z) \leq y
\end{aligned}$$

$$\begin{aligned}
a(x) \cdot (y \cdot z) &= (a(x) \cdot y) \cdot z \\
x \cdot (a(y) \cdot z) &= (x \cdot a(y)) \cdot z \\
x \cdot (y \cdot a(z)) &= (x \cdot y) \cdot a(z) \\
a(x) \cdot x &= 0 \\
a(x \cdot y) &= a(x \cdot a(a(y)) \\
a(x) + a(a(x)) &= 1_\sigma \\
a(x) \cdot (y + z) &= a(x) \cdot y + a(x) \cdot z \\
(x \| y) \cdot a(z) &= (x \cdot a(z)) \| (y \cdot a(z)) \\
a(x \| y) &= a(x) + a(y) \\
a(x) \| a(y) &= a(x) \cdot a(y) \\
1_\sigma + x \cdot x^* &\leq x^* \\
a(z) + x \cdot y \leq y &\Rightarrow x^* \cdot a(z) \leq y
\end{aligned}$$

To obtain dp-trioids and ap-trioids, the star axioms must be dropped. To obtain proto-algebras, the concurrency axioms must be dropped.

Finally, we show, for ap-bi-Kleene algebras, the definition of domain from antidomain and those for the diamond and box operators.

$$a(a(x)) = d(x) \qquad \langle x\rangle y = d(x \cdot y) \qquad [x]y = a(\langle x\rangle a(y))$$

APPENDIX 2: PROOFS

Proof of Lemma 3.1

(1) The two facts follow directly from the definition of sequential composition.
(2) By definition, $(a, A) \notin \emptyset$ for all $a \in X$ and $A \subseteq X$, hence $\emptyset \cdot R = \emptyset$.
(3)

$$\begin{aligned}
&(a, A) \in (R \cdot S) \cdot T \\
&\Leftrightarrow \exists B, C.\ (a, C) \in R \wedge \exists g.\ G_g(C) \subseteq S \wedge B = \bigcup g(C) \wedge \exists f.\ G_f(B) \subseteq T \\
&\quad \wedge A = \bigcup f(B) \\
&\Leftrightarrow \exists C.\ (a, C) \in R \wedge \exists g.\ G_g(C) \subseteq S \wedge \exists f.\ G_f\left(\bigcup g(C)\right) \subseteq T \\
&\quad \wedge A = \bigcup_{c\in C} \bigcup_{x\in g(c)} f(x) \\
&\Leftrightarrow \exists C.\ (a, C) \in R \wedge \exists f, g.\ (\forall c \in C.\ G_g(c) \in S \wedge G_f(g(c)) \subseteq T) \\
&\quad \wedge A = \bigcup_{c\in C} \bigcup_{x\in g(c)} f(x) \\
&\Leftrightarrow \exists C.\ (a, C) \in R \wedge \exists f.\ \forall c \in C. \exists D.\ (c, D) \in S \wedge G_f(D) \subseteq T \\
&\quad \wedge A = \bigcup_{c\in C} \bigcup_{d\in D} f(d) \\
&\Rightarrow \exists C.\ (a, C) \in R \wedge \exists h.\ (\forall c \in C. \exists D.\ (c, D) \in S) \\
&\quad \wedge (\forall d \in D.\ (d, h(d, c)) \in T) \wedge A = \bigcup_{c\in C} \bigcup_{d\in D} h(d, c) \\
&\Rightarrow \exists C.\ (a, C) \in R \wedge \exists f, h.\ \forall c \in C. \exists D.\ (c, D) \in S \\
&\quad \wedge \forall d \in D.\ (d, h(d, c)) \in T \wedge f(c) = \bigcup_{d\in D} h(d, c) \wedge A = \bigcup_{c\in C} f(c) \\
&\Rightarrow \exists C.\ (a, C) \in R \wedge \exists f.\ \forall c \in C. \exists D.\ (c, D) \in S \\
&\quad \wedge \exists g.\ G_g(D) \subseteq T \wedge f(c) = \bigcup_{d\in D} g(d) \wedge A = \bigcup_{c\in C} f(c) \\
&\Leftrightarrow (a, A) \in R \cdot (S \cdot T).
\end{aligned}$$

(4)

$$\begin{aligned}
(a, A) \in (R \cup S) \cdot T &\Leftrightarrow \exists B.\ (a, B) \in R \cup S \wedge \exists f.\ G_f(B) \subseteq T \wedge A = \bigcup f(B) \\
&\Leftrightarrow (\exists B.\ (a, B) \in R \wedge \exists f.\ G_f(B) \subseteq T \wedge A = \bigcup f(B)) \\
&\quad \vee (\exists B.\ (a, B) \in S \wedge \exists f.\ G_f(B) \subseteq T \wedge A = \bigcup f(B)) \\
&\Leftrightarrow (a, A) \in R \cdot T \vee (a, A) \in S \cdot T \\
&\Leftrightarrow (a, A) \in R \cdot T \cup R \cdot T.
\end{aligned}$$

(5) We show that $R \cdot S \subseteq R \cdot (S \cup T)$. The claim then follows by symmetry and properties of least upper bounds.

$$\begin{aligned}(a, A) \in R \cdot S &\Leftrightarrow \exists B.\ (a, B) \in R \wedge \exists f.\ G_f(B) \subseteq S \wedge A = \bigcup f(B)\\ &\Rightarrow \exists B.\ (a, B) \in R \wedge \exists f.\ G_f(B) \subseteq S \cup T \wedge A = \bigcup f(B)\\ &\Leftrightarrow (a, A) \in R \cdot (S \cup T).\quad \square\end{aligned}$$

Proof of Lemma 3.2

(1)

$$\begin{aligned}(a, A) \in (R \| S) \| T &\Leftrightarrow \exists B, C, D.\ A = B \cup C \cup D \wedge (a, B) \in R \wedge (a, C) \in S \wedge (a, D) \in T\\ &\Leftrightarrow (a, A) \in R \| (S \| T).\end{aligned}$$

(2) $(a, A) \in R \| S \Leftrightarrow \exists B, C.\ A = B \cup C \wedge (a, B) \in R \wedge (a, C) \in S \Leftrightarrow (a, A) \in S \| R$.
(3) Immediate from the definition of parallel composition and 1_π.
(4) Immediate from the definition of parallel composition.
(5)

$$\begin{aligned}&(a, A) \in R \| (S \cup T)\\ &\quad\Leftrightarrow \exists B, C.\ A = B \cup C \wedge (a, B) \in R \wedge ((a, C) \in S \vee (a, C) \in T)\\ &\quad\Leftrightarrow \exists B, C.\ A = B \cup C \wedge ((a, B) \in R \wedge (a, C) \in S) \vee ((a, B) \in R \wedge (a, C) \in T)\\ &\quad\Leftrightarrow (a, A) \in R \| S \cup R \| T.\quad \square\end{aligned}$$

Proof of Lemma 3.3
Since $G_f(A \cup B) \subseteq R \Leftrightarrow G_f(A) \subseteq R \wedge G_f(B) \subseteq R$, it follows that

$$\begin{aligned}(a, A) \in (R \| S) \cdot T &\Leftrightarrow \exists B, C.\ (a, B \cup C) \in R \| S \wedge \exists f.\ G_f(B \cup C) \subseteq T \wedge A = \bigcup f(B \cup C)\\ &\Rightarrow \exists X, Y.\ A = X \cup Y\\ &\quad \wedge (\exists B.\ (a, B) \in R \wedge \exists f.\ G_f(B) \subseteq T \wedge X = \bigcup f(B))\\ &\quad \wedge (\exists C.\ (a, C) \in S \wedge \exists f.\ G_f(C) \subseteq T \wedge Y = \bigcup f(C))\\ &\Leftrightarrow (a, A) \in (R \cdot T) \| (S \cdot T).\quad \square\end{aligned}$$

Proof of Lemma 4.1

(1) Suppose that $(a, A) \in R \cdot P$. Then there exists a set B such that $(a, B) \in R$ and, for all $b \in B$, $G_\iota(b) \in P$, and $A = \bigcup_{b \in B} \{b\} = B$. Thus, $(a, A) \in R$ and $G_\iota(A) \subseteq P$.
Suppose $(a, A) \in R$ and $G_\iota(a) \in P$ for all $a \in A$. Then $(a, A) \in R \cdot P$ by definition of sequential composition with $f = \iota$.
(2) Suppose that $(a, A) \in P \cdot R$. Then $G_\iota(a) \in P$ and $(a, A) \in R$ by definition of sequential composition. Suppose that $G_\iota(a) \in P$ and $(a, A) \in R$. Then $(a, A) \in P \cdot R$, using $f = \lambda x.A$. $\square$

Proof of Lemma 4.2

(1) Let $R \subseteq 1_\sigma$. Then

$$\begin{aligned}(a, A) \in (R \cdot S) \cdot T &\Leftrightarrow \exists B.\ G_\iota(a) \in R \ \wedge (a, B) \in S \wedge \exists f.\ G_f(B) \subseteq T \wedge A = \bigcup f(B)\\ &\Leftrightarrow G_\iota(a) \in R \ \wedge \exists B.(a, B) \in S \wedge \exists f.\ G_f(B) \subseteq T \wedge A = \bigcup f(B)\\ &\Leftrightarrow G_\iota(a) \in R \wedge (a, A) \in S \cdot T\\ &\Leftrightarrow (a, A) \in R \cdot (S \cdot T).\end{aligned}$$

Let $S \subseteq 1_\sigma$. Then

$$\begin{aligned}
&(a, A) \in (R \cdot S) \cdot T \\
&\quad \Leftrightarrow \exists B.\ (a, B) \in R \wedge G_\iota(B) \subseteq S \wedge \exists f.\ G_f(B) \in T \wedge A = \bigcup f(B) \\
&\quad \Leftrightarrow \exists B.\ (a, B) \in R \wedge \exists f.\ G_\iota(B) \subseteq S \wedge G_f(B) \subseteq T \wedge A = \bigcup f(B) \\
&\quad \Leftrightarrow \exists B.\ (a, B) \in R \wedge \exists f.\ G_f(B) \subseteq S \cdot T \wedge A = \bigcup f(B) \\
&\quad \Leftrightarrow (a, A) \in R \cdot (S \cdot T).
\end{aligned}$$

Let $T \subseteq 1_\sigma$. Then

$$\begin{aligned}
&(a, A) \in (R \cdot S) \cdot T \\
&\quad \Leftrightarrow (a, A) \in R \cdot S \wedge G_\iota(A) \subseteq T \\
&\quad \Leftrightarrow \exists B.\ (a, B) \in R \wedge \exists f.\ G_f(B) \subseteq S \wedge A = \bigcup f(B) \wedge G_\iota(A) \subseteq T \\
&\quad \Leftrightarrow \exists B.\ (a, B) \in R \wedge \exists f.\ G_f(B) \subseteq S \wedge G_\iota(A) \subseteq T \wedge A = \bigcup f(B) \\
&\quad \Leftrightarrow \exists B.\ (a, B) \in R \wedge \exists f.\ G_f(B) \subseteq S \wedge G_\iota(f(b)) \subseteq T \wedge A = \bigcup f(B) \\
&\quad \Leftrightarrow \exists B.\ (a, B) \in R \wedge \exists f.\ G_f(B) \subseteq S \cdot T \wedge A = \bigcup f(B) \\
&\quad \Leftrightarrow (a, A) \in R \cdot (S \cdot T).
\end{aligned}$$

(2) Let $P \subseteq 1_\sigma$.

$$\begin{aligned}
&(a, A) \in (R \| S) \cdot P \\
&\quad \Leftrightarrow \exists B, C.\ A = B \cup C \wedge (a, B) \in R \wedge (a, C) \in S \wedge G_\iota(A \cup B) \subseteq P \\
&\quad \Leftrightarrow \exists B, C.\ A = B \cup C \wedge (a, B) \in R \wedge (a, C) \in S \wedge G_\iota(A) \subseteq P \wedge G_\iota(B) \subseteq P \\
&\quad \Leftrightarrow \exists B, C.\ A = B \cup C \wedge (a, B) \in R \cdot P \wedge (a, C) \in S \cdot P \\
&\quad \Leftrightarrow (a, A) \in (R \cdot P) \| (S \cdot P).
\end{aligned}$$

(3) Let again $P \subseteq 1_\sigma$.

$$\begin{aligned}
(a, A) \in P \cdot (R \cup S) &\Leftrightarrow G_\iota(a) \in P \wedge ((a, A) \in R \vee (a, A) \in S) \\
&\Leftrightarrow (G_\iota(a) \in P \wedge (a, A) \in R) \vee (G_\iota(a) \in P \wedge (a, A) \in S) \\
&\Leftrightarrow (a, A) \in P \cdot R \vee (a, A) \in P \cdot S \\
&\Leftrightarrow (a, A) \in P \cdot R \cup P \cdot S. \quad \square
\end{aligned}$$

Proof of Lemma 5.1

(1) Obvious.
(2) $(a, A) \in d(R) \cdot R \Leftrightarrow G_\iota(a) \in d(R) \wedge (a, A) \in R \Leftrightarrow (a, A) \in R$.
(3)

$$\begin{aligned}
G_\iota(a) \in d(R \cup S) &\Leftrightarrow \exists B.\ (a, B) \in R \vee (a, B) \in S \\
&\Leftrightarrow \exists B.\ (a, B) \in R \vee \exists B.(a, B) \in S \\
&\Leftrightarrow G_\iota(a) \in d(R) \vee G_\iota(a) \in d(S) \\
&\Leftrightarrow G_\iota(a) \in d(R) \cup d(S).
\end{aligned}$$

(4) Obvious from the definition of domain.

(5)

$$\begin{aligned} G_\iota(a) \in d(R \cdot S) &\Leftrightarrow \exists B.\ (a, B) \in R \cdot S \\ &\Leftrightarrow \exists B, C.\ (a, C) \in R \wedge \exists f.\ G_f(C) \subseteq S \wedge B = \bigcup f(C) \\ &\Leftrightarrow \exists C.\ (a, C) \in R \wedge \exists f.\ G_f(C) \subseteq S \\ &\Leftrightarrow \exists C.\ (a, C) \in R \wedge G_\iota(C) \subseteq d(S) \\ &\Leftrightarrow \exists C.\ (a, C) \in R \cdot d(S) \\ &\Leftrightarrow G_\iota(a) \in d(R \cdot d(S)). \end{aligned}$$

(6)

$$\begin{aligned} G_\iota(a) \in d(R \| S) &\Leftrightarrow \exists B.\ (a, B) \in R \| S \\ &\Leftrightarrow \exists C, D.\ (a, C) \in R \wedge (a, D) \in S \\ &\Leftrightarrow \exists C.\ (a, C) \in R \wedge \exists D.\ (a, D) \in S \\ &\Leftrightarrow G_\iota(a) \in d(R) \wedge G_\iota(a) \in d(S) \\ &\Leftrightarrow G_\iota(a) \in d(R) \cap d(S). \end{aligned}$$

(7) Obvious. □

Proof of Lemma 5.2

(1) Obviously, $(a, A) \in a(R)$ if and only if $A = \{a\}$ and $(a, A) \notin d(R)$, which holds if and only if $(a, A) \in 1_\sigma$ and $(a, A) \notin R$.
(2) $G_\iota(a) \in a(a(R)) \Leftrightarrow \neg\neg\exists A.(a, A) \in R \Leftrightarrow \exists A, (a, A) \in R \Leftrightarrow G_\iota(a) \in d(R)$.
(3) $G_\iota(a) \in d(a(R)) \Leftrightarrow G_\iota(a) \in a(a(a(R))) \Leftrightarrow \neg\neg\neg\exists A.\ (a, A) \in R \Leftrightarrow G_\iota(a) \in a(R)$. □

Proof of Lemma 5.3

(1) $(a, A) \in a(R) \cdot R \Leftrightarrow G_\iota(a) \in a(R) \wedge (a, A) \in S \Leftrightarrow \neg\exists B.(a, B) \in R \wedge (a, A) \in R$, which is false.
(2) $a(R \cdot S) = 1_\sigma \cap -d(R \cdot S) = 1_\sigma \cap -d(R \cdot d(S)) = a(R \cdot d(S))$.
(3) $a(R) \cup d(R) = (1_\sigma \cap -d(R)) \cup d(R) = 1_\sigma \cap (-d(R) \cup d(R)) = 1_\sigma \cap U = 1_\sigma$.
(4)

$$\begin{aligned} a(R \cup S) &= 1_\sigma \cap -d(R \cup S) \\ &= 1_\sigma \cap -(d(R) \cup d(S)) \\ &= 1_\sigma \cap -d(R) \cap -d(S) \\ &= (1_\sigma \cap -d(R)) \cap (1_\sigma \cap -d(S)) \\ &= a(R) \cap a(S) \\ &= a(R) \cdot a(S). \end{aligned}$$

(5)

$$\begin{aligned} a(R \| S) &= 1_\sigma \cap -d(R \| S) \\ &= 1_\sigma \cap -(d(R) \cap d(S)) \\ &= (1_\sigma \cap -d(R)) \cup (1_\sigma \cap -d(S)) \\ &= a(R) \cup a(S). \end{aligned}$$

(6) $a(R) \| a(S) = d(a(R)) \| d(a(S)) = d(a(R)) \cdot d(a(S)) = a(R) \cdot a(S)$. □

Proof of Lemma 8.3

(1) Immediate from additivity of domain.
(2) $x \leq d(x) \cdot x$ is an axiom; $d(x) \cdot x \leq x$ holds since $d(x) \leq 1_\sigma$.

(3) $d(x \cdot y) = d(x \cdot d(y)) \leq d(x \cdot 1_\sigma) = d(x)$.
(4) Let $x \leq 1_\sigma$. Then $x = d(x) \cdot x \leq d(x) \cdot 1_\sigma = d(x)$.
(5)

$$\begin{aligned} d(d(x) \cdot y) &= d(d(d(x) \cdot y)) \cdot d(d(x) \cdot y) \\ &= d(d(x) \cdot y) \cdot d(d(x) \cdot y) \\ &= d(d(x) \cdot d(y)) \cdot d(d(x) \cdot y) \\ &\leq d(d(x)) \cdot d(y) \\ &= d(x) \cdot d(y), \end{aligned}$$

using (1), (2), and (3). For the converse direction, $d(x) \cdot d(y) \leq 1_\sigma$, and therefore $d(x) \cdot d(y) \leq d(d(x) \cdot d(y)) = d(d(x) \cdot y)$ by (4). □

Proof of Lemma 8.5

We consider only the first property. Let $x \leq d(y) \cdot x$. Then

$$d(x) \leq d(d(y) \cdot x) = d(y) \cdot d(x) \leq d(x).$$

Let $d(x) \leq d(y)$. Then $x = d(x) \cdot x \leq d(y) \cdot x$. □

Proof of Lemma 8.6

(1) $1_\sigma = d(1_\sigma) = d(1_\sigma \| 1_\pi) = d(1_\sigma) \cdot d(1_\pi) \leq d(1_\pi)$. The converse direction is obvious.
(2) $d(d(x) \| d(y)) = d(d(x) \cdot d(y)) = d(x) \cdot d(y) = d(x) \| d(y)$ by meet closure.
(3) $d(x) \| d(x) = d(x) \cdot d(x) = d(x)$. □

Proof of Lemma 9.3

Suppose $\langle x \rangle p \leq d(q)$, that is, $d(x \cdot p) \leq d(q)$. Then, by Lemma 8.3(2),

$$x \cdot d(p) = d(x \cdot p) \cdot x \cdot d(p) \leq d(q) \cdot x \cdot d(p) \leq d(q) \cdot x.$$

For the converse implication, suppose that $x \cdot d(p) \leq d(q) \cdot x$. Then $(x \cdot d(p)) \cdot d(p) \leq (d(q) \cdot x) \cdot d(p)$ and therefore $x \cdot d(p) \leq d(q) \cdot (x \cdot d(p))$ by domain associativity and idempotency. Hence,

$$\langle x \rangle p = d(x \cdot p) \leq d(d(q) \cdot x \cdot d(p)) = d(q) \cdot d(x \cdot d(p)) \leq d(q) = q$$

by isotonicity of domain, domain export, and properties of meet. □

Proof of Lemma 10.1

(1) The functions $\lambda X.\ R \cdot X$ and $\lambda X.\ S \cup X$ are isotone for all R and S; hence, so are their compositions.
(2) Every ring of sets forms a complete lattice.
(3) This follows from (1) and (2) by standard fixpoint theory (Knaster-Tarski Theorem). □

Proof of Lemma 10.10

Suppose that $x \cdot p \leq p \cdot y$. For $x^* \cdot p \leq p \cdot y^*$, it suffices to show that $p + x \cdot (p \cdot y^*) \leq p \cdot y^*$ by star induction. First, $p \leq p \cdot y^*$ by left isotonicity of multiplication and star unfold. Moreover, by the assumption and domain associativity,

$$x \cdot (p \cdot y^*) = (x \cdot p) \cdot y^* \leq (p \cdot y) \cdot y^* = p \cdot (y \cdot y^*) \leq p \cdot y^*. \quad \square$$

PROOF OF LEMMA 10.13

(1) Obviously, $p \leq \langle x^* \rangle p$ by the left unfold law. For $\langle x^* \rangle \langle x \rangle p \leq \langle x^* \rangle p$ it suffices, by star induction, to show that $\langle x \rangle p \leq \langle x^* \rangle p$ and $\langle x \rangle \langle x^* \rangle p \leq \langle x^* \rangle p$. The first inequality follows from $\langle 1_\sigma \rangle p \leq \langle x^* \rangle p$ and $\langle x \rangle p = \langle x \rangle \langle 1_\sigma \rangle p$ by isotonicity. The second one holds by left star unfold.
(2) Let $p \leq q$ and $\langle x \rangle q \leq q$. Hence, $\langle x^* \rangle q \leq q$ by Proposition 10.11 and the claim follows by domain isotonicity. □

PROOF OF LEMMA 11.1. Note that d is an abbreviation of $a \circ a$.

(1) Obvious from the third antidomain axiom.
(2) $a(x) = (a(x) + d(x)) \cdot a(x) = a(x) \cdot a(x) + a(a(x)) \cdot a(x) = a(x) \cdot a(x) + 0 = a(x) \cdot a(x)$.
(3) This holds since $a(1_\sigma) = 0$ and $1_\sigma \cdot x = 0$ implies $x = 0$.
(4) Let $a(x) \leq a(y)$. Then $a(x) \cdot y \leq a(y) \cdot y = 0$.
For the converse direction,

$$a(x) \cdot y = 0 \Leftrightarrow a(a(x) \cdot y) = 1_\sigma \Leftrightarrow a(a(x) \cdot d(y)) = 1_\sigma \Leftrightarrow a(x) \cdot d(y) = 0,$$

therefore,

$$a(x) = a(x) \cdot (d(y) + a(y)) = a(x) \cdot d(y) + a(x) \cdot a(y) = a(x) \cdot a(y) \leq a(y).$$

(5) $a(y) \cdot x \leq a(y) \cdot y = 0$, so $a(y) \leq a(x)$ by (4).
(6)

$$a(x) \cdot a(y) \cdot (x + y) = a(x) \cdot a(y) \cdot x + a(x) \cdot a(y) \cdot y \leq a(x) \cdot x + a(y) \cdot y = 0.$$

Moreover, by (3),

$$\begin{aligned} a(x) \cdot a(y) \cdot (x + y) = 0 &\Leftrightarrow a(a(x) \cdot a(y) \cdot (x + y)) = 1_\sigma \\ &\Leftrightarrow a(a(x) \cdot a(y) \cdot d(x + y)) = 1_\sigma \\ &\Leftrightarrow a(x) \cdot a(y) \cdot d(x + y) = 0. \end{aligned}$$

(7) $a(x + y) \leq a(x)$ and $a(x + y) \leq a(y)$ by (5), thus,

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

For the converse direction, by (6),

$$\begin{aligned} a(x) \cdot a(y) &= a(x) \cdot a(y) \cdot a(x + y) + a(x) \cdot a(y) \cdot d(x + y) \\ &= a(x) \cdot a(y) \cdot a(x + y) \leq a(x + y). \end{aligned}$$

(8) First, $a(y) \leq a(a(x) \cdot y)$ and $d(x) \leq a(a(x) \cdot y)$ by antitonicity, thus,

$$d(x) + a(y) \leq a(a(x) \cdot y)$$

by properties of least upper bounds.
For the converse direction, we have $a(a(x) \cdot y) \cdot a(x) \cdot d(y) = 0$. Therefore,

$$\begin{aligned} a(a(x) \cdot y) &= a(a(x) \cdot y) \cdot d(y) + a(a(x) \cdot y) \cdot a(y) \\ &\leq a(a(x) \cdot y) \cdot d(y) + a(y) \\ &= a(a(x) \cdot y) \cdot a(x) \cdot d(y) + a(a(x) \cdot y) \cdot d(x) \cdot d(y) + a(y) \\ &= a(a(x) \cdot y) \cdot d(x) \cdot d(y) + a(y) \\ &\leq d(x) + a(y). \quad \square \end{aligned}$$

PROOF OF PROPOSITION 11.2

We verify the domain axioms in the setting of ap-dioids.

—The associativity laws

$$d(x)\cdot(y\cdot z)=(d(x)\cdot y)\cdot z,\qquad x\cdot(d(y)\cdot z)=(x\cdot d(y))\cdot z,\qquad x\cdot(y\cdot d(z))=(x\cdot y)\cdot d(z)$$

are immediate from antidomain associativity.
—$d(x)\leq 1_\sigma$ is immediate from the complementation axiom.
—$d(x)\cdot x=x$ holds because $x=(d(x)+a(x))\cdot x=d(x)\cdot x+0$ by the complementation and left annihilation axiom.
—$d(x\cdot y)=d(x\cdot d(y))$ is immediate from antidomain locality.
—$d(0)=0$ holds because $a(0)=1_\sigma$ and $a(1_\sigma)=0$.
—$d(x+y)=d(x)+d(y)$ holds because, by antidomain multiplicativity and export,

$$d(x+y)=a(a(x+y))=a(a(x)\cdot a(y))=d(x)+a(a(y))=d(x)+d(y).\quad\square$$

Proof of Proposition 11.4

Every ap-dioid is a dp-dioid by Proposition 11.2. We verify the remaining axioms for parallel composition.

—The domain interaction axiom $(x\cdot d(z))\|(y\cdot d(z))=(x\|y)\cdot d(z)$ follows immediately from the antidomain interaction axiom.
—$d(x||y)=d(x)\cdot d(y)$ holds because

$$d(x\|y)=a(a(x\|y))=a(a(x)+a(y))=a(a(x))\cdot a(a(y))=d(x)\cdot d(y),$$

using the De Morgan law for a and the first antidomain concurrency axiom.
—$d(x)\|d(y)=d(x)\cdot d(y)$ is immediate from the second antidomain concurrency axiom. □

Proof of Lemma 13.1

Let $R=\{(n,\mathbb{N})\mid n\in\mathbb{N}\}$ and $S_i=\{(n,\{m\})\mid n\in\mathbb{N}\wedge 0\leq m\leq i\}$. Thus, clearly $S_i\subset S_j$ whenever $i<j$. Moreover,

$$\begin{aligned}(n,A)\in R\cdot\bigcup_{i\in\mathbb{N}}S_i &\Leftrightarrow (n,\mathbb{N})\in R\wedge\exists f.\ G_f(\mathbb{N})\subseteq\bigcup_{i\in\mathbb{N}}S_i\wedge A=\bigcup_{n\in\mathbb{N}}f(n)\\ &\Leftrightarrow (n,\mathbb{N})\in R\wedge\exists m\in\mathbb{N}.\ \left(\forall n\in\mathbb{N}.\ (n,\{m\})\in\bigcup_{i\in\mathbb{N}}S_i\right)\wedge A=\bigcup_{n\in\mathbb{N}}\{n\}\\ &\Leftrightarrow (n,\mathbb{N})\in R\wedge\exists m\in\mathbb{N}.\ \left(\forall n\in\mathbb{N}.\ (n,\{m\})\in\bigcup_{i\in\mathbb{N}}S_i\right)\wedge A=\mathbb{N}\end{aligned}$$

therefore $(n,\mathbb{N})\in F_R(\bigcup_{i\in\mathbb{N}}R_i)$ for all $(n,\mathbb{N})$. However,

$$(n,A)\in R\cdot S_i\Leftrightarrow(n,\mathbb{N})\in R\wedge\exists m\leq i.(\forall n\in\mathbb{N}.(n,\{m\})\in R_i)\wedge A=\bigcup_{0\leq k\leq i}\{k\},$$

hence no $F_R(R_i)$ contains $(n,\mathbb{N})$ for any n and therefore also not the union $\bigcup_{i\in\mathbb{N}}F_R(R_i)$. □

Proof of Lemma 13.2

Suppose that a family $\{S_i\mid i\in\mathbb{N}\}$ such that $S_i\subset S_j$ whenever $i<j$. We must show that $F_R(\bigcup_{i\in\mathbb{N}}S_i)\subseteq\bigcup_{i\in\mathbb{N}}F_R(S_i)$. Therefore, suppose that $(a,A)\in F_R(\bigcup_{i\in\mathbb{N}}S_i)$. If $(a,A)\in 1_\sigma$, then $(a,A)\in\bigcup_{i\in\mathbb{N}}F_R(S_i)$.

Otherwise, if $(a,A)\in R\cdot\bigcup_{i\in\mathbb{N}}R_i$, then there is a finite set $B=\{b_1,\ldots b_k\}$ and there are sets $A_1,\ldots,A_k$ such that $(a,B)\in R$, all $(b_i,A_i)\in\bigcup_{i\in\mathbb{N}}R_i$, and $A=\bigcup_{i\in\mathbb{N}}A_i$. Hence, for all $1\leq i\leq k$ there exists an l_i such that $(b_i,A_i)\in S_{l_i}$. Because of the ascending chain

condition, there exists a maximal S_m such that all $(b_i, A_i) \in S_m$. Then $(a, A) \in F_R(S_m)$ and, finally, also $(a, A) \in \bigcup_{i\in\mathbb{B}} F_R(S_i)$. □

PROOF OF LEMMA 13.4

(1) In the base case, $F_R^0(\emptyset) = \emptyset = R^{(0)}$. In the induction step,

$$F_R^{(n+1)}(\emptyset) = F_R\big(F_R^n(\emptyset)\big) = 1_\sigma \cup R \cdot R^{(n)} = R^{(n+1)}.$$

Finally, $F_R^*(\emptyset) = \bigcup_{n\in\mathbb{N}} F_R^n(\emptyset) = \bigcup_{n\in\mathbb{N}} R^{(n)} = R^{(*)}$.

(2) Immediate from (1). □

PROOF OF LEMMA 14.3

$p + \langle x^*\rangle(\langle x\rangle p - p) \leq p + \langle x^*\rangle\langle x\rangle p \leq \langle x^*\rangle p$, by Lemma 10.13(1). □

APPENDIX 3: PROOF AUTOMATION WITH ISABELLE/HOL

Some of the proofs at the multirelational level in this article are technically tedious, in particular, those using second-order Skolemization, that is, the Axiom of Choice. Reasoning algebraically about domain and antidomain in the absence of associativity of sequential composition is intricate for different reasons. We have therefore formalized the mathematical structures used in this article and verified many of our proofs with the interactive proof assistant Isabelle/HOL [Nipkow et al. 2002]. In particular, the complete technical development in this article, from multirelations to star-free concurrent dynamic algebras and the complete algebraic layer, have been formally verified. Finally, Isabelle's built-in counterexample generators Quickcheck and Nitpick have helped in finding some counterexamples.

We now list in detail the facts that have and have not been formally verified.

Section 3. We have verified Lemma 3.1, except for Part (3), which is not needed for our results, the isotonicity properties of sequential composition, Lemma 3.2, isotonicity of parallel composition, and Lemma 3.3. Isabelle also provided the counterexamples in Lemma 3.4.

Section 4. All statements (Lemma 4.1 and 4.2) have been verified. The subalgebra of subidentities has not been formalized.

Section 5. All statements, Lemma 5.1 to Corollary 5.4, have been verified.

Section 6. We have verified irredundancy of the domain and antidomain axiom sets of domain and antidomain proto-dioids and proto-trioids. We have not explicitly formalized Theorem 6.1, but all facts needed in the proof have been verified.

Section 8. Lemma 8.1 has been verified, but not Proposition 8.2, which is a well-known consequence. Lemma 8.3 and the individual equational proof steps for Proposition 8.4 have been verified; the precise statement of Proposition 8.4 has not been formalized. Lemma 8.5 and Lemma 8.6 have been verified. The remaining facts in this section (Proposition 8.7 to Theorem 8.10) have not been verified.

Section 9. All proofs and counterexamples, Lemma 9.1 to 9.4, have been verified.

Section 10. Lemma 10.1 to Theorem 10.8 have not been verified; formalizing the underlying concepts seems excessive relative to the moderate difficulty of proofs. Lemma 10.9 to Lemma 10.13 have been verified. Theorem 10.12, which combines these results, as not been formalized as such.

Section 11. Lemma 11.1 has been verified. All the equational proof steps for Proposition 11.2, Proposition 11.3, and Proposition 11.5 have been verified, but the individual statements have not been formalized. Proposition 11.3 has not been verified. Theorem 10.8 has not been verified, because the star in the multirelational model has not been formalized.

Section 12. Lemma 12.1 and Proposition 12.2 have been verified. Theorem 12.3 has not been formalized as yet, but individual proof steps have been verified. Lemma 12.4 has not been verified because it holds by duality between box and diamonds.
Section 13. No results have been verified.
Section 14. No results have been verified.

As mentioned in the Introduction, the complete Isabelle development with all proofs listed earlier can be found online.

ACKNOWLEDGMENTS

The authors are grateful to Yde Venema for drawing their attention to concurrent dynamic logic, and to Yasuo Kawahara, Koki Nishizawa, Toshinori Takai and Norihiro Tsumagari for enlightening discussions and comments on previous variants of this article. The second author would like to thank the Department of Mathematics and Computer Science at Kagoshima University, where much of this work has been conducted, for its hospitality, and the Department of Mathematics at Kyushu University for a pleasant short stay and financial support. Last, but not least, the presentation of this article has benefited to a great extent from the suggestions and constructive criticism of the anonymous reviewers.

REFERENCES

R.-J. Back and J. von Wright. 1998. *Refinement Calculus: A Systematic Introduction*. Springer, New York, NY.

P. Blackburn, M. de Rijke, and Y. Venema. 2011. *Modal Logic*. Cambridge University Press, New York, NY.

J. A. Brzozowski and E. L. Leiss. 1980. On equations for regular languages, finite automata, and sequential networks. *Theoretical Computer Science* 10, 19–35.

A. K. Chandra, D. Kozen, and L. J. Stockmeyer. 1981. Alternation. *Journal of the ACM* 28, 1, 114–133.

J. Desharnais, B. Möller, and G. Struth. 2006. Kleene algebra with domain. *ACM Transactions on Computational Logic* 7, 4, 798–833.

J. Desharnais and G. Struth. 2008. Domain axioms for a family of near-semirings. In *AMAST 08 (LNCS)*, J. Meseguer and G. Rosu (Eds.), Vol. 5140. Springer, 330–345.

J. Desharnais and G. Struth. 2011. Internal axioms for domain semirings. *Science of Computer Programming* 76, 3, 181–203.

H. Furusawa, K. Nishizawa, and N. Tsumagari. 2009. Multirelational models of lazy, monodic tree and probabilistic Kleene algebras. *Bulletin of Informatics and Cybernetics* 41, 11–24.

R. Goldblatt. 1992. Parallel action: Concurrent dynamic logic with independent modalities. *Studia Logica* 51, 3/4, 551–578.

D. Harel, D. Kozen, and J. Tiuryn. 2000. *Dynamic Logic*. MIT Press, Cambridge MA.

D. Kozen. 1976. *On Parallelism in Turing Machines*. Technical Report. Technical Report TR 76-282, Computer Science Department, Cornell University, Ithaca, NY.

D. Kozen. 1994. A completeness theorem for Kleene algebras and the algebra of regular events. *Information and Computation* 110, 2, 366–390.

R. D. Maddux. 2006. *Relation Algebras*. Elsevier.

C. E. Martin, S. A. Curtis, and I. Rewitzky. 2007. Modelling angelic and demonic nondeterminism with multirelations. *Science of Computer Programming* 65, 2, 140–158.

I. Németi. 1981. Dynamic algebras of programs. In *Fundamentals of Computation Theory (LNCS)*, F. Gécseg (Ed.), Vol. 117. Springer, 281–290.

A. Nerode and D. Wijesekera. 1990. *Constructive Concurrent Dynamic Logic I*. Technical Report 90-43. Mathematical Sciences Institute, Cornell University, Ithaca, NY.

T. Nipkow, L. C. Paulson, and M. Wenzel. 2002. *Isabelle/HOL - A Proof Assistant for Higher-Order Logic*. LNCS, Vol. 2283. Springer.

K. Nishizawa, N. Tsumagari, and H. Furusawa. 2009. The cube of Kleene algebras and the triangular prism of multirelations. In *Relational Methods in Computer Science (LNCS)*, R. Berghammer, A. Jaoua, and B. Möller (Eds.), Vol. 5827. Springer, Berliln, 276–290.

R. Parikh. 1983. Propositional game logic. In *FOCS*. IEEE Computer Society, 195–200.

R. Parikh. 1985. The logic of games and its applications. In *Topics in the Theory of Computation (Mathematics Studies)*, M. Karpinsky and J. van Leeuwen (Eds.), Vol. 102. North-Holland, 111–135.

D. Peleg. 1987a. Communication in concurrent dynamic logic. *Journal of Computer System Sciences* 35, 23–58.

D. Peleg. 1987b. Concurrent dynamic logic. *Journal of the ACM* 34, 2, 450–479.

V. Pratt. 1991. Dynamic algebras: Examples, constructions, applications. *Studia Logica* 50, 3–4, 571–605.

V. R. Pratt. 1980. Dynamic algebras and the nature of induction. In *STOC 1980*, R. E. Miller, S. Ginsburg, W. A. Burkhard, and R. J. Lipton (Eds.). ACM Press, New York, NY, 22–28.

I. Rewitzky. 2003. Binary multirelations. In *Theory and Applications of Relational Structures as Knowledge Instruments (LNCS)*, H. C. M. de Swart, E. Orlowska, G. Schmidt, and M. Roubens (Eds.), Vol. 2929. Springer, Berlin, 256–271.

I. Rewitzky and C. Brink. 2006. Monotone predicate transformers as up-closed multirelations. In *Relations and Kleene Algebra in Computer Science (LNCS)*, R. A. Schmidt (Ed.), Vol. 4136. Springer, Berlin, 311–327.

V. Trnková and J. Reiterman. 1987. Dynamic algebras with test. *Journal of Computer System Sciences* 35, 2, 229–242.

J. van Benthem, S. Ghosh, and F. Liu. 2008. Modelling simultaneous games in dynamic logic. *Synthese* 165, 2, 247–268.

D. Wijesekera and A. Nerode. 2005. Tableaux for constructive concurrent dynamic logic. *Annals of Pure and Applied Logic* 135, 1–3, 1–72.

Received July 2014; revised December 2014; accepted May 2015