Math. Struct. in Comp. Science (2013), *vol.* 23, *pp.* 635–674. © Cambridge University Press 2013
doi:10.1017/S0960129512000965 First published online 18 March 2013

The algebra of multirelations

C. E. MARTIN and S. A. CURTIS

Department of Computing and Communication Technologies, Oxford Brookes University, Wheatley, Oxfordshire, OX33 1HX, United Kingdom
Email: {cemartin;sharoncurtis}@brookes.ac.uk

Received 26 October 2009; revised 20 July 2012

Multirelational semantics are well suited to reasoning about programs involving two kinds of non-determinism. This paper lays the categorical foundations for an algebraic calculus of multirelations.

1. Introduction

Multirelations (Rewitzky 2003; Martin *et al.* 2007) provide a mathematical framework for reasoning about processes involving two kinds of non-determinism, such as user/client interactions, communication protocols and two-player games. This paper lays the foundations for an algebraic calculus of multirelations within the setting of allegories (Freyd and Ščedrov 1993). Formal category-theoretic definitions are given for multirelations and their operators, and fundamental algebraic laws are formulated and proved. This provides a solid foundation for further work, both in the theory of multirelations and for the derivation of algorithms for applications.

Multirelations are set-valued relations that satisfy an upclosure condition. Originally introduced in Rewitzky (2003), they are equivalent in expressive power to monotonic predicate transformers, which are total functions on predicates that preserve the implication ordering. Predicate transformers model programs backwards, mapping postconditions on the output to weakest preconditions on the input, but the multirelational model is a little more intuitive because programs are modelled forwards, that is, from input to output. The trade-off is a loss of simplicity since relations are more unwieldy than total functions, and the composition operator of multirelations is quite cumbersome.

This paper simplifies the set-theoretic multirelational model by taking a more abstract view with a clean and simple formalism for calculation. To that end, we focus here on the algebraic theory of binary multirelations. For applications of multirelations, see our previous work Martin *et al.* (2007) and Martin and Curtis (2006).

1.1. *Outline of paper*

In Section 2, we give a brief history of multirelations and related models, and in Section 3 we briefly recap the standard theory of order-enriched categories and allegories, which we will need in Section 4 to place multirelations in an allegorical setting. In Sections 5 and 6, we discuss the relationship of the multirelational model to other models of program transformation, and in Section 7, we summarise the work in this paper and indicate some

future directions for research into multirelations. The proofs not given in the main sections are collected together in an appendix.

2. History and background

The work in this paper draws on the theory of both relations and predicate transformers, the relevant background for which is summarised in this section. We also give a short account of the work that has already been carried out on multirelations, and discuss other models of non-determinism.

2.1. *Relations*

The study of relations goes back to the nineteenth century (de Morgan 1856), but it intensified in the mid-twentieth century when Tarski (1941) suggested two relational models: one being set-theoretic and the other a point-free axiomatic approach. More recently, Maddux (1996) surveyed existing relational theory and set out algebraic laws for the standard relational program semantics, where relations describe the connections between a program's input values and its corresponding output values for terminating computations.

Since Tarksi's work, relational methods have been used for a wide range of applications in computer science. One body of work of particular interest for this paper is the categorical calculus of relations for the derivation of functional programs described in Bird and de Moor (1997). This calculus is based on the concept of an *allegory* (a specialised kind of category with additional relational-style operators) as introduced in Freyd and Ščedrov (1993), but also includes concepts from functional programming, such as sums, products, and iterations like *map* and *fold*. Such constructs are not part of traditional relational algebra, but are used in Bird and de Moor's calculus to describe structured computations over inductive datatypes. Another strength of this approach lies in the use of a point-free style of reasoning, which avoids bound variables and quantifications, and is well suited to mechanisation.

A similar calculus of relations for program development was developed independently in Backhouse *et al.* (1991), but the approach was more lattice theoretic than categorical, and consequently less influential on the algebraic approach adopted in this paper.

2.2. *Predicate transformers*

Dijkstra (Dijkstra 1975) invented predicate transformers to give a non-operational semantics of an imperative programming language, building on previous work on program correctness logic (Floyd 1967; Hoare 1969). Predicate transformers are functions taking predicates as input and producing predicates as output, but not all are suitable for representing programs. Predicate transformers are probably best known for modelling Dijkstra's *weakest precondition* semantics, which can be described as follows: given a program S acting on input values of a source type X and producing output values of a target type Y, and a predicate ψ on Y, the predicate $wp(S, \psi)$ is called the weakest

https://doi.org/10.1017/S0960129512000965 Published online by Cambridge University Press

precondition of S with respect to postcondition ψ. That is, $wp(S, \psi)$ is the weakest predicate such that when satisfied initially, the program S is guaranteed to terminate in a state satisfying ψ. Here the function $wp(S, \_)$ is a predicate transformer of type $\mathbb{P}Y \to \mathbb{P}X$ (representing predicates as sets of values), returning a weakest precondition for any given postcondition. Dijkstra also formulated a set of *healthiness* conditions for predicate transformers, which ensure that they model feasible programs.

From a mathematical perspective, predicate transformers can be described using topological constructs: Plotkin (1979) showed that predicate transformers are elements of the powerdomains of Smyth (1983). Furthermore, Smyth's work helped to shed light on computational concepts: when predicate transformers are expressed topologically, applying Stone duality (Stone 1936) results in an isomorphism between predicate transformer semantics (a form of denotational semantics) and state transformer semantics. More generally, Abramsky had the insight to show that Stone-style dualities exist between denotational semantics and axiomatic program logics (Abramsky 1991) – this is an overarching idea in theoretical computer science that weaves together many different threads in program semantics.

The theory of predicate transformers was further developed by a number of researchers (Back and von Wright 1998; Morgan 1994; Morgan *et al.* 1994; Morris 1987) to include all total functions that are monotonic with respect to the implication ordering on predicates. This meant that predicate transformers could be used to model not just programs, but also their specifications, thereby facilitating the calculation of programs from specifications in a language known as the *refinement calculus*.

The algebraic properties of predicate transformers have been studied in depth in Back and von Wright (1998), which described some of the lattice theoretic properties of the category of predicate transformers and its subcategories. An algebraic construction of predicate transformers was given in Gardiner *et al.* (1994), where it was shown that the category of predicate transformers is related to the category of relations in precisely the same way that the category of relations is related to that of total functions. This relationship was expressed in terms of a unique factorisation property, and that result is reproduced in this paper in the context of multirelations, along with some of the lattice theoretic results from Back and von Wright (1998) – we do this because the setting of allegories is more general and the proofs more succint.

2.3. *Multirelations*

Multirelations were introduced in Rewitzky (2003) to provide a relational model for programs and specifications that may exhibit both angelic and demonic non-determinism. This model relates input values to *predicates* on output values: in set-theoretic terms, a multirelation m with source X and target Y is a subset of the cartesian product $X \times \mathbb{P}Y$. The statement $x\ m\ post$, which can also be written as $(x, post) \in m$, can be interpreted as follows: given x as an input, m can be guaranteed to terminate with some output value $v \in post$, where $post$ is a subset of the type Y representing a predicate.

There is an *upclosure* condition on multirelations corresponding to the monotonicity property of predicate transformers: if a postcondition $post$ can be guaranteed, then weaker

https://doi.org/10.1017/S0960129512000965 Published online by Cambridge University Press

predicates should be guaranteed too. So for all $x \in X$ and $post, post' \in \mathbb{P}Y$, we have

$$x\ m\ post \wedge (post \subseteq post') \Rightarrow x\ m\ post'.$$

The type of all upclosed multirelations from X to Y will be denoted by $X \rightrightarrows Y$.

Whilst standard relational program semantics can capture only one kind of non-determinism, multirelations can model choices made by two 'agents', who are often referred to as the angel and demon. The interpretation of multirelations is as follows: if input x is related by m to several postconditions, then the first agent chooses which postcondition *post* to guarantee, and the second agent chooses an output value from *post*. Whilst the choice of which agent is the angel and which the demon can be made either way, resulting in two possible dual interpretations of multirelations, we find it convenient to have multirelations relate input values to guarantees so that the angelic agent chooses which guarantee is true of a multirelation's output, and the demonic agent chooses the actual output value. Thus the angelic choice of two multirelations $m, n : X \rightrightarrows Y$ is defined to be the (relational) union $m \cup n : X \rightrightarrows Y$, and the demonic choice is their intersection $m \cap n : X \rightrightarrows Y$.

Example 2.1. Consider a confectionery vending machine that on input of a single coin dispenses either a chocolate bar, a packet of toffees or a lollipop. A customer purchase can be represented by a multirelation of type $PAYMENT \rightrightarrows CONFECTIONERY$, where $PAYMENT = \{coin\}$ and $CONFECTIONERY = \{choc, toffees, lollipop\}$. Let us now look at several multirelations of this type of machine, considering the customer as the angel.

The vending machine V_1 is fully-stocked and has three selection buttons for the options so that the customer can (angelically) choose what is dispensed:

$$V_1 = \{(coin, P) \mid choc \in P \ \vee\ toffees \in P \ \vee\ lollipop \in P\},$$

where $P \in \mathbb{P}\{choc, toffees, lollipop\}$ since $V_1 : PAYMENT \rightrightarrows CONFECTIONERY$. In particular, $(coin, \{choc\}) \in V_1$, so a customer preferring a chocolate bar can angelically choose the predicate $\{choc\}$, leaving the demon no choice. Other predicates that a customer can guarantee include $\{toffees\}$ and $\{toffees,\ lollipop\}$.

V_2 is similar to V_1, but is presently out of stock of the chocolate bars:

$$V_2 = \{(coin, P) \mid toffees \in P \ \vee\ lollipop \in P\}.$$

The machine V_3 is fully stocked but less helpful, as it only has two buttons. If the customer presses the first button then a chocolate bar will be dispensed, and pressing the other button results in either a packet of toffees or a lollipop being dispensed, at the machine's (demonic) choice:

$$V_3 = \{(coin, P) \mid choc \in P \ \vee\ \{toffees, lollipop\} \subseteq P\}$$

Finally, this vending machine V_4 has a single dispensing button, and the customer will receive whatever the machine chooses to vend:

$$V_4 = \{\ (coin, \{choc, toffees, lollipop\})\ \}$$

https://doi.org/10.1017/S0960129512000965 Published online by Cambridge University Press

More details of set-theoretic multirelational program semantics can be found in Martin *et al.* (2007) and Martin and Curtis (2006), along with examples of multirelation applications in a broad range of areas, including voting schemes, games and resource sharing protocols.

Monotonic predicate transformers are mathematically equivalent to upclosed multirelations; this duality is shown in Rewitzky (2003) and Düntsch *et al.* (2010). The main difference between the models is that unlike predicate transformers, multirelations model programs in a forwards direction, that is, from input to output. This may offer a small intuitive advantage when it comes to maniplating multirelations for program development. Another advantage of multirelations is that, unlike predicate transformers, there is no separate command language in which to express programs.

Further development of multirelational theory towards a more algebraic style of reasoning can be found in Martin and Curtis (2006) and Martin and Curtis (2010), where the similarities between functions, relations and multirelations have been used to extend standard constructs from functional and relational program semantics to multirelations. In particular, sums, products and operators over inductive datatypes such as *map* and *fold* have been extended to multirelations in a canonical way.

2.4. *Other choice models*

Work on dual non-determinism has not been confined to the models discussed above. Both predicate transformers and multirelations are also mathematically equivalent to another model known as *choice semantics* (Back and von Wright 1998). For a program with input values of type X and output values of type Y, its predicate transformer representation will have type $\mathbb{P}Y \to \mathbb{P}X$, and its multirelation representation will have type $X \rightrightarrows Y$ (that is, $X \times \mathbb{P}Y$), but the choice semantics uses a set-valued function of type $X \to \mathbb{P}\mathbb{P}Y$, which corresponds to the power transpose of the program's multirelation. Whilst the multifunctions of the choice semantics model, like multirelations, describe programs in a forwards direction, multirelations have a simpler algebra because relations are generally considered easier to manipulate than set-valued functions. For more discussion of choice semantics and its equivalence to other semantic models, see Section 6.3.

Naumann (1998) explored the relationship between categories of relations and predicate transformers (which had already been described in Gardiner *et al.* (1994)) using power allegory concepts applied to the base category of monotonic functions between posets. Subsequently, the category of *ideal relations* (not itself an allegory) was used to provide a relational semantics based on predicate transformers (Naumann 2001). This algebraic approach incorporates higher-order functions as well as dual non-determinism.

Morris and Tyrrell (2008a) developed a general theory of dual non-determinism incorporating specifications, programs and refinement. Their model is based on *terms* (which they define to be expressions without side-effects) extended to incorporate both angelic and demonic non-determinism so that functions return values of non-deterministic type. Terms can also be λ-abstractions, which enables the modelling of higher-order functions. Morris and Tyrrell provide axioms and a denotational model, capturing the (unbounded) non-determinism with the use of free completely distributive lattices (FCD) over partially ordered sets. Thus, for X,Y types of terms, each incorporating a suitable

https://doi.org/10.1017/S0960129512000965 Published online by Cambridge University Press

poset, their model uses non-deterministic functions of type $X \to \mathsf{FCD}(Y)$. Also, subsequent work (Morris and Tyrrell 2008b) sought to unify various models of dual non-determinism incorporating higher-order functions, showing that models using predicate transformers, binary multirelations, state transformers and free lattices over a poset are isomorphic. One contribution of their work that is relevant to multirelations was the definition of a set-theoretic multirelational model including higher-order functions.

3. Mathematical foundations

This section covers the standard theory of order-enriched categories and allegories, which we will need to use to model multirelations. Familiarity with basic categorical concepts will be assumed – see, for example, Barr and Wells (1990) for reference.

We begin by describing order-enriched categories, and then focus on allegories, specifically *power allegories*, which are our setting for multirelations. The laws in this section are not exhaustive, but are sufficient for the proofs in this paper.

3.1. *Order-enriched categories*

In several categorical models of program semantics, including multirelations, the arrows of categories are used to model programs and/or specifications, and the objects of the categories represent types. Such categories typically have an ordering on arrows to describe when one program is a *refinement* of another.

Definition 3.1. An *order-enriched* category $(\mathsf{C}, \sqsubseteq_{\mathsf{C}})$ is a category C with an additional partial ordering $\sqsubseteq_{\mathsf{C}}$ on the arrows in its homsets, with respect to which composition is monotonic, that is, for any arrows $r, t : W \to X$ and $s, u : X \to Y$,

$$(r \sqsubseteq t \wedge s \sqsubseteq u) \Rightarrow (r \,;s \sqsubseteq t \,;u)$$

As in the above, we will usually omit the subscript from $\sqsubseteq_{\mathsf{C}}$, if the ordering to which it refers is clear from the context.

Example 3.2. The category of relations $(\mathsf{Rel}, \subseteq)$ has as objects the class of all sets, and its arrows are all relations, which we will write in the form $r : X \leftrightarrow Y$. Its composition operator is the standard relational composition, the identity arrow id_X for each object X is the identity function on the set X and the order on arrows is subset inclusion $\subseteq$.

Example 3.3. The category of monotonic predicate transformers $(\mathsf{Tran}, \leqslant)$ has as objects the class of all sets, and its arrows from X to Y are all total functions of the form $p : \mathbb{P}Y \to \mathbb{P}X$ that are monotonic in the sense that for all $U, V : \mathbb{P}Y$,

$$U \subseteq V \Rightarrow p\,U \subseteq p\,V.$$

Instead of $p : \mathbb{P}Y \to \mathbb{P}X$, we will write $p : X \mapsto Y$ for predicate transformer arrows, as in Back and von Wright (1998). The identity arrow id_X for each object X is the identity function on the set $\mathbb{P}X$ and composition is standard functional composition. The order on arrows is pointwise inclusion, denoted here by $\leqslant$.

Example 3.4. The category of upclosed multirelations $(\mathsf{Mul}, \subseteq)$ has as objects the class of all sets, and its arrows are the upclosed multirelations. The composition of two multirelations

https://doi.org/10.1017/S0960129512000965 Published online by Cambridge University Press

$m : X \rightrightarrows Y$ and $n : Y \rightrightarrows Z$ is denoted by $m \fatsemi n : X \rightrightarrows Z$, where for all $x \in X$ and $U \in \mathbb{P}Z$,

$$x\ (m \fatsemi n)\ U \Leftrightarrow (\exists V : x\ m\ V : (\forall y : y \in V : y\ n\ U)).$$

Translating this into words, given input value x, the angel can guarantee that $m \fatsemi n$ will output a value that satisfies U if he can ensure that m will establish some postcondition V such that n must establish U given any value in V. The identity arrow for each object X is the membership relation $\in_X$ and the order on arrows is subset inclusion $\subseteq$.

Examples 3.2–3.4 are all order-enriched categories that are set-theoretic versions of abstract categories that will be discussed thoroughly later.

3.1.1. *Maps.*

Definition 3.5. An arrow $f : X \to Y$ in an order-enriched category is a *map* if and only if it has a right adjoint f^* that is an arrow $f^* : Y \to X$ such that both of the following properties hold:

$$id_X \subseteq f\,;f^* \tag{3.5a}$$

$$f^*\,;f \subseteq id_Y. \tag{3.5b}$$

In this paper, we will use the symbol f to denote a *map*, and will refer to its right adjoint f^* as a *comap*. The maps in a category form a subcategory, and it is immediate from the following laws that each map uniquely determines its comap and *vice versa*.

Laws 3.6. We have,

$$r\,;f \subseteq s \equiv r \subseteq s\,;f^* \tag{3.6a}$$

$$r \subseteq f\,;s \equiv f^*\,;r \subseteq s. \tag{3.6b}$$

These are known as the *shunting laws* for maps.

Example 3.7. In Rel, the category of relations, the maps are the total functions, and the comap of a function is its relational converse. To see that a function f is a map, we can take the relationship $x\ f\ y$ to mean that $f(x) = y$, and then note that from the two defining properties of maps, property (3.5a) ensures that f is total and (3.5b) ensures that for any x, there is at most one y such that $x\ f\ y$. The subcategory of maps in Rel will be referred to as Fun.

Example 3.8. In Mul, the category of (upclosed) multirelations, an arrow $m : X \rightrightarrows Y$ is a map if and only if for all $x : X$ and $Z : \mathbb{P}\mathbb{P}Y$,

$$x\ m\ \left(\bigcap Z\right) \equiv (\forall Y : Y \in Z : x\ m\ Y).$$

Informally, a map is a multirelation that does not involve any angelic choice, such as the vending machine V_4 in Example 2.1. In contrast, an arrow $m : X \rightrightarrows Y$ is a comap if and only if for all $x : X$ and $Z : \mathbb{P}\mathbb{P}Y$,

$$x\ m\ \left(\bigcup Z\right) \equiv (\exists Y : Y \in Z : x\ m\ Y).$$

https://doi.org/10.1017/S0960129512000965 Published online by Cambridge University Press

Informally, a comap is a multirelation where the angel has complete control over the choices made. For example, vending machines V_1 and V_2 of Example 2.1 are comaps, but V_3 and V_4 are not because they involve demonic choice to some extent.

3.1.2. *Meets and joins.* The concepts of *meet* and *join* will be used to model demonic and angelic non-determinism respectively. Their defining axioms are stated below, together with some useful properties.

Definition 3.9. The arrows of an order-enriched category $(\mathsf{C}, \subseteq)$ have binary *meets* if for all arrows $r, s : X \to Y$ in C, there exists an arrow $r \cap s : X \to Y$ such that for all $q : X \to Y$,

$$q \subseteq r \cap s \equiv (q \subseteq r) \wedge (q \subseteq s).$$

If such meets exist, the following laws can be deduced from the above definition.

Laws 3.10.

$$r ; (s \cap t) \subseteq (r ; s) \cap (r ; t) \tag{3.10a}$$
$$(s \cap t) ; r \subseteq (s ; r) \cap (t ; r) \tag{3.10b}$$
$$f ; (s \cap t) = (f ; s) \cap (f ; t) \tag{3.10c}$$
$$(s \cap t) ; f^* = (s ; f^*) \cap (t ; f^*). \tag{3.10d}$$

Example 3.11. In Mul, the meet of two multirelations $m, n : X \rightrightarrows Y$ is their intersection $m \cap n$, which is also their demonic choice.

Definition 3.12. The arrows of an order-enriched category $(\mathsf{C}, \subseteq)$ have binary *joins* if for all arrows $r, s : X \to Y$ in C, there exists an arrow $r \cup s : X \to Y$ such that for all $q : X \to Y$,

$$r \cup s \subseteq q \equiv (r \subseteq q) \wedge (s \subseteq q).$$

Laws 3.13.

$$(r ; s) \cup (r ; t) \subseteq r ; (s \cup t) \tag{3.13a}$$
$$(s ; r) \cup (t ; r) \subseteq (s \cup t) ; r \tag{3.13b}$$
$$(s \cup t) ; f = (s ; f) \cup (t ; f) \tag{3.13c}$$
$$f^* ; (s \cup t) = (f^* ; s) \cup (f^* ; t). \tag{3.13d}$$

Example 3.14. In Mul, the join of two multirelations $m, n : X \rightrightarrows Y$ is their union $m \cup n$, which is also their angelic choice.

3.1.3. *Division.* Division operators are useful for reasoning about universal quantification in a point-free manner. The following left and right division operators are dual to each other.

https://doi.org/10.1017/S0960129512000965 Published online by Cambridge University Press

Definition 3.15. An order-enriched category $(\mathsf{C}, \subseteq)$ has *left division* if, for each pair of arrows $r : X \to Z$ and $s : X \to Y$ in C with common source, there exists an arrow $s\backslash r : Y \to Z$ such that for all $t : Y \to Z$,

$$t \subseteq s\backslash r \equiv s\,;t \subseteq r.$$

Definition 3.16. An order-enriched category $(\mathsf{C}, \subseteq)$ has *right division* if, for each pair of arrows $r : X \to Z$ and $t : Y \to Z$ in C with common target, there exists an arrow $r/t : X \to Y$ such that for all $s : X \to Y$,

$$s \subseteq r/t \equiv s\,;t \subseteq r.$$

Example 3.17. The category of relations Rel has both left and right division. The set-theoretic interpretation of these operators is as follows:

$$x\ (s\backslash r)\ y \equiv (\forall z : z\,s\,x \Rightarrow z\,r\,y)$$
$$x\ (r/t)\ y \equiv (\forall z : y\,t\,z \Rightarrow x\,r\,z).$$

For example, for the set membership relation $\in_X : X \leftrightarrow \mathbb{P}X$, the arrow $\in_X\backslash\in_X$ is the subset relation $\subseteq_X : \mathbb{P}X \leftrightarrow \mathbb{P}X$, and, similarly, $\ni_X/\ni_X$ is the superset relation $\supseteq_X$, where $\ni_X$ denotes the converse of $\in_X$.

Some useful laws of left division are given below – the symmetrical laws involving right division are omitted.

Laws 3.18 (left division).

$$r \subseteq q \ \Rightarrow\ (s\backslash r) \subseteq (s\backslash q) \tag{3.18a}$$
$$w \subseteq s \ \Rightarrow\ (s\backslash r) \subseteq (w\backslash r) \tag{3.18b}$$
$$s\,;(s\backslash r) \subseteq r \tag{3.18c}$$
$$t \subseteq s\backslash(s\,;t) \tag{3.18d}$$
$$id \subseteq r\backslash r \tag{3.18e}$$
$$id\backslash r = r \tag{3.18f}$$
$$(s\,;t)\backslash r = t\backslash(s\backslash r) \tag{3.18g}$$
$$r\,;(r\backslash r) = r \tag{3.18h}$$
$$s\backslash(r/t) = (s\backslash r)/t \tag{3.18i}$$
$$r \subseteq (s/r)\backslash s \tag{3.18j}$$
$$(r\backslash s)\,;t \subseteq r\backslash(s\,;t) \tag{3.18k}$$
$$(r\backslash s)\,;(s\backslash t) \subseteq r\backslash t \tag{3.18l}$$
$$f\,;(r\backslash s) = (r\,;f^*)\backslash s \tag{3.18m}$$
$$(r\backslash s)\,;f^* = r\backslash(s\,;f^*) \tag{3.18n}$$
$$f\,;r = f^*\backslash r. \tag{3.18o}$$

https://doi.org/10.1017/S0960129512000965 Published online by Cambridge University Press

3.2. *Allegories*

In this section we introduce *power allegories*, which contain all the axioms needed to define point-free multirelations. A power allegory is an order-enriched category with meets, joins and division, together with some additional operators and axioms. We will start with the basic definition of an allegory.

Definition 3.19. An allegory A is an order-enriched category $(\mathsf{A},\subseteq_{\mathsf{A}})$ with binary meets given by $\cap_{\mathsf{A}}$ as in Definition 3.9, and an additional operator $^{\circ_{\mathsf{A}}}$, as follows: for each arrow $r : X \to Y$ there is a *converse* arrow $r^\circ : Y \to X$ such that for all

$$s : X \to Y$$
$$t : Y \to Z$$
$$u : X \to Z$$

we have

$$(r^\circ)^\circ = r \tag{3.19a}$$
$$r \subseteq s \;\equiv\; r^\circ \subseteq s^\circ \tag{3.19b}$$
$$(r\,;t)^\circ = t^\circ\,;r^\circ \tag{3.19c}$$
$$(r;t) \cap u \subseteq (r \cap (u;t^\circ));t \qquad \text{(modular law).} \tag{3.19d}$$

Again, we will usually omit the subscripts from $\subseteq_{\mathsf{A}}$, $\cap_{\mathsf{A}}$ and $^{\circ_{\mathsf{A}}}$, where the allegory to which they belong is clear from the context.

The following additional properties of $\cap$ and converse are easy to derive from the axioms of an allegory.

Laws 3.20 (Freyd and Ščedrov 1993).

$$(r \cap s)^\circ = r^\circ \cap s^\circ \tag{3.20a}$$
$$id^\circ = id. \tag{3.20b}$$

The concept of an allegory is in general intended to model sets and relations in the same kind of way that categories model sets and functions. Thus we have the following archetypal example of an allegory.

Example 3.21. The category of relations Rel is an allegory, where its partial ordering on arrows is subset inclusion $\subseteq$, the meet of two arrows is their intersection and converse is relational converse.

In an allegory, the relationship between maps and comaps is easily described as follows.

Lemma 3.22 (Johnstone 2002). In an allegory, the right adjoint (comap) of a map f is necessarily f°. The maps in an allegory are discretely ordered, that is, $f \subseteq g$ implies $f = g$.

Lemma 3.23 (Freyd and Ščedrov 1993). The maps of an allegory A may also be referred to as *function arrows*, and these form a wide subcategory of A, which is to say that the

https://doi.org/10.1017/S0960129512000965 Published online by Cambridge University Press

subcategory has the same collection of objects as A. This category of functions will be denoted by $\mathsf{Fun}(\mathsf{A})$.

Example 3.24. For the allegory Rel, we have $\mathsf{Fun}(\mathsf{Rel}) = \mathsf{Fun}$, the category of sets and total functions.

The operators of an allegory are insufficient for modelling two kinds of non-determinism since joins are needed as well as meets. For this, we use a distributive allegory, where arrows with the same source and target form a distributive lattice.

Definition 3.25. A *distributive allegory* A is an allegory with binary joins given by $\cup_{\mathsf{A}}$ (which we will abbreviate by $\cup$) as in Definition 3.12, and a family of nullary operators $\varnothing_{X,Y} : X \to Y$ (which we will abbreviate by $\varnothing$) such that for every pair of objects and every arrow $r : X \to Y$,

$$\varnothing \subseteq r \tag{3.25a}$$

$$r ; \varnothing = \varnothing = \varnothing ; r. \tag{3.25b}$$

In addition, for all arrows $p : W \to X$ and $q, r, s : X \to Y$, the following laws must hold:

$$p ; (r \cup s) = p ; r \cup p ; s \tag{3.25c}$$

$$q \cap (r \cup s) = (q \cap r) \cup (q \cap s). \tag{3.25d}$$

The following further properties of $\cup$ and composition are easy to derive from the axioms of a distributive allegory.

Laws 3.26 (Freyd and Ščedrov 1993).

$$(r \cup s)^\circ = r^\circ \cup s^\circ \tag{3.26a}$$

$$(s \cup t) ; r = (s ; r) \cup (t ; r). \tag{3.26b}$$

The left division operator will also be required in the definition of multirelations, so we need the following kind of allegory.

Definition 3.27. A *division allegory* A is a distributive allegory with left division given by $\backslash_{\mathsf{A}}$ (which we will abbreviate by $\backslash$), as in Definition 3.15.

Note that a division allegory A also has right division $/_{\mathsf{A}}$, as in Definition 3.16, as the first of the following laws shows.

Laws 3.28 (Freyd and Ščedrov 1993).

$$r/s = (s^\circ \backslash r^\circ)^\circ \tag{3.28a}$$

$$(r \cup s) \backslash t = (r \backslash t) \cap (s \backslash t). \tag{3.28b}$$

All of the remaining concepts we will need for defining multirelations, namely membership, powersets and power transpose, are provided by power allegories.

https://doi.org/10.1017/S0960129512000965 Published online by Cambridge University Press

Definition 3.29. A *power allegory* A is a division allegory such that there is:

— for each object X in A, an object $\mathsf{P}X$ in A called the *power-object* of X;
— a *power transpose* function Λ that, for each arrow $r : X \to Y$ in A, returns a function arrow $\Lambda r : X \to \mathsf{P}Y$ in A;
— for each object X in A, a *membership* arrow $\ni_X : \mathsf{P}X \to X$.

They must also satisfy the following universal property, which defines them up to isomorphism:

$$(f = \Lambda r) \equiv (f \,;\ni \;\; = r). \tag{3.29a}$$

The converse of $\ni$ is denoted by $\in$.

Example 3.30. The allegory Rel is also a power allegory, where the join of two arrows is their union, division is given as in Example 3.17, the power object $\mathsf{P}X$ of a set X is its powerset $\mathbb{P}X$, its $\in$ is the usual set membership and the power transpose function as applied to a relation r is defined by $\Lambda r(x) = \{x \mid x \; r \; y\}$.

There are many useful laws concerning $\in$, Λ and other allegory operators, and they are all straightforwardly derivable from power allegory axioms. Those we will need in the proofs are as follows.

Laws 3.31.

$$id \subseteq \Lambda r \,;(\Lambda r)^\circ \tag{3.31a}$$
$$(\Lambda r)^\circ \,;\Lambda r \subseteq id \tag{3.31b}$$
$$\Lambda r \,;\ni \; = r \tag{3.31c}$$
$$\in \,;(\Lambda r)^\circ = r^\circ \tag{3.31d}$$
$$\Lambda(r^\circ) \subseteq r \backslash \in \tag{3.31e}$$
$$\Lambda(f \,;\ni) = f \tag{3.31f}$$
$$\Lambda(f \,;r) = f \,;\Lambda r \tag{3.31g}$$
$$\Lambda \ni \; = id \tag{3.31h}$$
$$\Lambda r \,;(\in \backslash s) = r^\circ \backslash s \tag{3.31i}$$
$$(r \backslash \in) \,;(\in \backslash s) = r \backslash s \tag{3.31j}$$
$$\in \,;(\in \backslash r) = r \tag{3.31k}$$
$$(\ni / r) \backslash \ni \; = r. \tag{3.31l}$$

The operators of a power allegory can be used to give point-free definitions of some concepts that will be useful for multirelations.

Definition 3.32. For each object Y in a power allegory, the arrow $\eta_Y : Y \to \mathsf{P}Y$ is defined by $\eta = \Lambda id$.

https://doi.org/10.1017/S0960129512000965 Published online by Cambridge University Press

Definition 3.33. For each object Y in a power allegory, the arrow $\sqsubseteq_Y : \mathsf{P}Y \to \mathsf{P}Y$ is defined by

$$\sqsubseteq_Y = \in_Y \backslash \in_Y .$$

The converse of $\sqsubseteq$ is denoted by $\sqsupseteq$.

Note that we use the symbol $\sqsubseteq$ to distinguish the arrow $\sqsubseteq$ from the ordering $\subseteq$ that compares arrows within the homsets of a power allegory. In the power allegory Rel, these are the same subset inclusion ordering, but for more general allegories this is not necessarily the case. An example where $\sqsubseteq$ is different is given in Section 4.1 after Lemma 4.15.

Definition 3.34 (Bird and de Moor 1997). The existential image functor $\mathsf{E} : \mathsf{A} \to \mathsf{Fun}(\mathsf{A})$ is defined by

$$\mathsf{E}r = \Lambda(\ni ; r).$$

Definition 3.35. For each object Y in a power allegory, the arrow $\bigcup_Y : \mathsf{PP}Y \to \mathsf{P}Y$ is defined by

$$\bigcup_Y = \Lambda(\ni_{\mathsf{P}Y} ; \ni_Y).$$

Definition 3.36. For each object Y in a power allegory, the arrow $\bigcap_Y : \mathsf{PP}Y \to \mathsf{P}Y$ is defined by

$$\bigcap_Y = \Lambda(\in_{\mathsf{P}Y} \backslash \ni_Y).$$

In Rel, $\bigcup$ and $\bigcap$ represent generalised union and intersection, as suggested by the symbols, but this is not true for allegories in general. Some additional laws concerning the above operators are as follows.

Laws 3.37.

$$\eta ; \ni = id \tag{3.37a}$$

$$\sqsubseteq ; (\Lambda r^\circ)^\circ = \in \backslash r \tag{3.37b}$$

$$\Lambda r ; \bigcap ; \sqsubseteq = (\in / r) \backslash \in . \tag{3.37c}$$

4. Multirelations

We are now in a position to introduce a categorical definition of multirelations, and will do so by characterising the arrows in a power allegory that have the upclosure property. The resulting point-free definition of multirelations will result in easier algebraic manipulations than are possible using the previous set-theoretic definition.

Definition 4.1. A *multirelation* $m : X \rightrightarrows Y$ is an arrow $m : X \to \mathsf{P}Y$ in a power allegory such that

$$m ; \sqsubseteq_Y = m \qquad \text{(upclosure property)}.$$

https://doi.org/10.1017/S0960129512000965 Published online by Cambridge University Press

One of the simplest examples of a multirelation is the identity, as in the following example.

Example 4.2. The *identity* multirelation is $\in_X$ for each object X. In set-theoretic terms, for any input x, we have $x \in \{x\}$, so the angel can always choose the predicate represented by $\{x\}$, which outputs x. Note also that property (3.31k) ensures that $\in_X$ satisfies the upclosure property of multirelations.

Sequential composition of multirelations is defined as follows.

Definition 4.3. For any two multirelations $m : X \rightrightarrows Y$ and $n : Y \rightrightarrows Z$, their composition is denoted by $m \fatsemi n : X \rightrightarrows Z$ and defined by

$$m \fatsemi n = m \,;(\in \backslash n)$$

The following lemma ensures that this definition is feasible.

Lemma 4.4. For any two multirelations $m : X \rightrightarrows Y$ and $n : Y \rightrightarrows Z$, it is also the case that $m \fatsemi n$ is an (upclosed) multirelation.

Note that the above definition corresponds to the set-theoretic definition of composition (see Example 3.4) when the chosen power allegory is Rel: to see this equivalence, we can expand $\in \backslash n$ using the definition of division in Rel (see Example 3.17). There is also the following alternative (and equivalent) definition of multirelational composition involving power transpose.

Law 4.5. $m \fatsemi n \;=\; m \,;(\Lambda(n^\circ))^\circ$.

Having defined multirelations and their composition operator, we can now construct a category of multirelations.

Lemma 4.6. The collection of objects in a power allegory A form an order-enriched *category of multirelations* $(\mathsf{Mul}(\mathsf{A}), \subseteq_{\mathsf{A}})$, where the arrows are the multirelations and composition is $\fatsemi$ (as in Definition 4.3) with identity $\in_X$ for each object X.

The following proof of this lemma is given to illustrate a calculation using the algebra of multirelations in a point-free style.

Proof. By Lemma 4.4 (which is proved in the appendix), multirelational composition preserves upclosure and is monotonic with respect to $\subseteq$ by the monotonicity of $(\backslash)$ (3.18a) and $(\,;)$. Associativity of $(\fatsemi)$ is proved as follows.

By the definition of $\fatsemi$ (4.3) and alternative definition (4.5),

$$(r \fatsemi s) \fatsemi t = r \fatsemi (s \fatsemi t)$$

is equivalent to

$$(r \,;(\in \backslash s)) \,;(\Lambda(t^\circ))^\circ) = r \,;(\in \backslash (s \,;(\Lambda(t^\circ))^\circ)),$$

and this is true by the property of $\backslash$ and functions (3.18n) together with the associativity of $;$.

https://doi.org/10.1017/S0960129512000965 Published online by Cambridge University Press

Finally, to prove $\in$ is the identity for composition, we have

$$\begin{aligned} r \fatsemi \in &= r \,;(\in \backslash \in) && \text{(definition of composition (4.3))} \\ &= r && \text{(definition of } \sqsubseteq \text{ (3.33); } r \text{ is a multirelation (4.1))} \\ &= \in \,;(\in \backslash r) && \text{(property of } \backslash \text{ and } \in \text{ (3.31k))} \\ &= \in \fatsemi r. && \text{(definition of composition (4.3))} \end{aligned}$$

□

Note that although Mul(A) is a category situated within the power allegory A, it is not a subcategory of A since it does not use the same composition operator. It does, however, have the same ordering relation and meet and join operators as A, the latter representing demonic and angelic choices, respectively, just as they do for set-theoretic multirelations.

Lemma 4.7. The order-enriched category Mul(A) has binary meets given by $\cap$ and binary joins given by $\cup$.

Note that in Mul(A), the laws describing the right-distribution of composition over meets (3.10b) and joins (3.13b) take the stronger form of equalities as follows.

Laws 4.8.

$$(n \cap v) \fatsemi m = (n \fatsemi m) \cap (v \fatsemi m) \tag{4.8a}$$

$$(n \cup v) \fatsemi m = (n \fatsemi v) \cup (n \fatsemi v). \tag{4.8b}$$

4.1. *Lifting relations to multirelations*

Although the traditional relational calculus can only model one kind of non-determinism at once, and cannot distinguish between angelic and demonic choice, relations can be mapped to multirelations in two different ways to model either angelic or demonic non-determinism. Both mappings can be useful in multirelational specifications.

In this section we will introduce these mappings in the context of allegories, and examine their algebraic properties. More specifically, for an arrow r in a power allegory A, we will define multirelations:

— $\langle r \rangle$, which is the *angelic lifting* of r; and
— $[r]$, which is the *demonic lifting*.

To see why these operators are useful in specifications, consider a two-player game, with the angelic player versus the demonic player, and a relation $move : State \leftrightarrow State$ describing the possible changes of game state when a player makes a move. Then $\langle move \rangle$ describes the multirelation corresponding to a move of the angelic player, and $[move]$ describes the move of the demonic player.

The algebraic definitions of both the angelic and demonic liftings are given below, together with some of their properties and laws.

https://doi.org/10.1017/S0960129512000965 Published online by Cambridge University Press

4.1.1. *Angelic lifting.* We begin by motivating the definition of angelic lifting in the set-theoretic context. If $r : X \leftrightarrow Y$ in Rel, and x is some input value in X, then whenever $x\,r\,y$, the multirelation $\langle r \rangle$ should allow the angel to choose $\{y\}$ as a guarantee, given input x, to reflect the fact that the angel can choose to output y; there will also be weaker guarantees because of the upclosure property. Thus we have the following definition.

Definition 4.9. For any arrow $r : X \to Y$ in a power allegory A, its *angelic lifting* $\langle r \rangle : X \rightrightarrows Y$ in $\mathsf{Mul(A)}$ is given by

$$\langle r \rangle = r \,;\in .$$

Law 4.12a below shows that the angelic lifting operator does indeed produce a multirelation. This lifting operator corresponds to the *angelic update* given by Back and von Wright (1998). Intuitively, this is because, for a set-theoretic relation r, the angel can ensure that the angelic lifting $\langle r \rangle$ guarantees postcondition $B \subseteq Y$ from initial state $x \in X$ if and only if there is a value $y \in B$ such that $x\,r\,y$.

Example 4.10. Recall the vending machine V_1 of Example 2.1, which allows an angelic customer to choose freely between chocolate, toffees or a lollipop. We now define a relation $choose : PAYMENT \leftrightarrow CONFECTIONERY$ in the allegory Rel by

$$choose = \{coin\} \times \{choc, toffees, lollipop\}.$$

This means the vending machine V_1 is $\langle choose \rangle$. In particular, note that the predicates that the customer can choose from include $\{choc\}$, $\{toffees\}$ and $\{lollipop\}$, corresponding to the three choices that the customer can angelically choose between.

The vending machine V_2 of Example 2.1 also turns out to be an angelic lifting (of the relation $\{coin\} \times \{toffees, lollipop\}$), but V_3 and V_4 are not.

In general, angelic liftings of ordinary set-theoretic relations produce multirelations that are angelic, that is, where the angel has all the control over the output value and need not offer the demon any choice whatsoever. However, the following example shows an exception.

Example 4.11. The family of nullary operators $\varnothing_{X,Y} : X \to Y$ in an allegory A angelically lifts to a family of arrows in $\mathsf{Mul(A)}$ called $\mathsf{abort}_{X,Y} : X \rightrightarrows Y$. By law (3.25b), together with Definition 4.9, $\mathsf{abort} = \langle \varnothing \rangle = \varnothing$.

However, the multirelation abort is not considered to be angelic in Rel because the angel cannot guarantee anything as a result of this process.

Some laws of the angelic lifting operator are listed below for the category A. In these laws, r and s denote arrows in A, and m, n denote arrows in $\mathsf{Mul(A)}$ (which are also arrows in A by Definition 4.1).

Laws 4.12.

$$\langle r \rangle \,;\sqsubseteq = \langle r \rangle \qquad \text{(upclosure)} \tag{4.12a}$$

$$\langle m \fatsemi n \rangle \subseteq m \fatsemi \langle n \rangle \tag{4.12b}$$

https://doi.org/10.1017/S0960129512000965 Published online by Cambridge University Press

$$\langle r \rangle \fatsemi m = r \,;m \tag{4.12c}$$
$$r \,;\langle s \rangle = \langle r \,;s \rangle \tag{4.12d}$$
$$\langle id \rangle = \in \qquad \text{(identity-preserving)} \tag{4.12e}$$
$$\langle r \,;s \rangle = \langle r \rangle \fatsemi \langle s \rangle \qquad \text{(composition-preserving)} \tag{4.12f}$$
$$r \subseteq s \Rightarrow \langle r \rangle \subseteq \langle s \rangle \qquad \text{(monotonicity)} \tag{4.12g}$$
$$\langle r \cup s \rangle = \langle r \rangle \cup \langle s \rangle \qquad \text{(join-preserving).} \tag{4.12h}$$

One immediate consequence of the above laws is that the lifting operator is a functor.

Lemma 4.13. $\langle\ \rangle : \mathsf{A} \to \mathsf{Mul(A)}$ is a monotonic functor.

We can also give a formal point-free characterisation of the multirelations that are angelic liftings.

Lemma 4.14. A multirelation $m : X \rightrightarrows Y$ in a power allegory is an angelic lifting if and only if

$$m \,;\bigcup^{\circ} = m \,;\in .$$

Rewitzky (2003) described such multirelations as total and completely additive. We will now discuss the properties of angelic liftings in a set-theoretic context to illustrate the above lemma.

In Rel, a *strongest postcondition* of a multirelation is defined as follows. For $m : X \rightrightarrows Y$, a subset V of Y is a strongest postcondition of m with respect to x if $x\, m\, V$, and whenever W is another subset of Y such that $x\, m\, W$, then $W \not\subset V$. Thus, given a relation $r : X \leftrightarrow Y$, if $x\, r\, y$, then $\{y\}$ is a strongest postcondition of $\langle r \rangle$ with respect to x. Hence, when all the strongest postconditions of a multirelation $m : X \rightrightarrows Y$ are of the form $\{y\}$ for some $y \in Y$, the multirelation m can be described as angelic since the angel need not offer the demon any choice whatsoever. One way of expressing this property is to say that for all $Z : \mathbb{PP}Y$,

$$x\ m\ \left(\bigcup Z\right) \equiv (\exists Y : Y \in Z : x\ m\ Y).$$

This equivalence is the set-theoretic version of the equation in Lemma 4.14.

Given that angelic liftings only model one type of choice, it is unsurprising that they are equivalent to arrows in the original allegory.

Lemma 4.15. The angelic liftings in $(\mathsf{Mul(A)}, \subseteq_{\mathsf{A}})$ form a subcategory, which will be denoted by $(\mathsf{Ang(A)}, \subseteq_{\mathsf{A}})$, and there is an order-isomorphism of categories $\mathsf{A} \cong \mathsf{Ang(A)}$.

Since A is a power allegory, the order-enriched category $\mathsf{Ang(A)}$ must also be a power allegory, so it must have meets and joins. The join operator for $\mathsf{Ang(A)}$ is the same as for A, that is,

$$\cup_{\mathsf{Ang(A)}} \ = \ \cup_{\mathsf{A}},$$

https://doi.org/10.1017/S0960129512000965 Published online by Cambridge University Press

by property (4.12h). However, $\mathsf{Ang(A)}$ is not closed under $\cap_{\mathsf{A}}$; its meet operator $\cap_{\mathsf{Ang(A)}}$ turns out to be

$$m \cap_{\mathsf{Ang(A)}} n = (m ; \eta^{\circ} \cap_{\mathsf{A}} n ; \eta^{\circ}) ; \in$$

for two multirelations $m, n : X \rightrightarrows Y$ that are angelic liftings. Note also that $\sqsubseteq_{\mathsf{Ang(A)}}$ is not the same as $\subseteq_{\mathsf{A}}$ in this power allegory, but we have

$$\sqsubseteq_{\mathsf{Ang(A)}} \quad = \quad \sqsubseteq_{\mathsf{A}} ; \in_{\mathsf{A}}$$

instead.

4.1.2. *Demonic lifting.* We now turn to demonic liftings. If a relation $r : X \leftrightarrow Y$ in Rel is to be interpreted as describing demonic choice, then, given input value x, the angel should not be able to influence the choice of which y to output from the set of all y such that $x\, r\, y$. In other words, the angel should not be able to choose a predicate stronger than $\{y \mid x\, r\, y\}$. Thus we have the following definition.

Definition 4.16. For any arrow $r : X \to Y$ in a power allegory A, its *demonic lifting* $[r] : X \rightrightarrows Y$ is given by

$$[r] = r^{\circ} \backslash \in .$$

This lifting operator corresponds to the *demonic update* of Back and von Wright (1998). Intuitively, this is because for a set-theoretic relation r, the angel can ensure that the demonic lifting $[r]$ guarantees postcondition $B \subseteq Y$ from initial state $x \in X$ if and only if $x\, r\, y$ for every value $y \in B$.

Example 4.17. Recall the vending machine V_4 of Example 2.1, which on insertion of a coin allowed the angelic customer no choice at all, and would demonically choose to dispense either chocolate, toffees or a lollipop. The vending machine V_4 is $[\mathit{choose}]$, where the relation *choose* is defined as in Example 4.10. Note that the machine has a single strongest postcondition, namely $\{\mathit{choc}, \mathit{toffees}, \mathit{lollipop}\}$.

Note that demonic liftings generally produce demonic multirelations, that is, where the demon has complete control over the output value. However, once again there is an exception.

Example 4.18. The family of nullary operators $\varnothing_{X,Y} : X \to Y$ demonically lifts to a family of arrows $\mathsf{magic}_{X,Y} : X \rightrightarrows Y$, where, by laws (3.25a) and (3.25b), together with Definition 4.16, and the definition of left division, we have $m \subseteq \mathsf{magic}_{X,Y}$ for all $m : X \rightrightarrows Y$.

In Rel, the multirelation magic is not considered demonic despite being a demonic lifting since it offers the angel the strongest guarantee of all: the postcondition false, represented by $\{\ \}$.

Some laws for the demonic lifting operator are listed below. These take place in the power allegory A, where r, s denote arrows in A and m, n denote arrows in $\mathsf{Mul(A)}$ (which are also arrows in A by Definition 4.1).

https://doi.org/10.1017/S0960129512000965 Published online by Cambridge University Press

Laws 4.19.

$$[r] = [r]\,;\sqsubseteq \qquad \text{(upclosure)} \tag{4.19a}$$

$$[r] \wr m = r^\circ \setminus m \tag{4.19b}$$

$$[id] = \in \qquad \text{(identity-preserving)} \tag{4.19c}$$

$$[r\,;s] = [r] \wr [s] \qquad \text{(composition-preserving)} \tag{4.19d}$$

$$r \subseteq s \Rightarrow [s] \subseteq [r] \qquad \text{(anti-monotonicity)} \tag{4.19e}$$

$$[r \cup s] = [r] \cap [s] \qquad \text{(meet-preserving)} \tag{4.19f}$$

$$\in \subseteq [r] \wr \langle r^\circ \rangle \tag{4.19g}$$

$$\langle r^\circ \rangle \wr [r] \subseteq \in \tag{4.19h}$$

$$m = \langle m \rangle \wr [\ni] \tag{4.19i}$$

$$[r]\,;\bigcap^\circ = [r]/\ni\,. \tag{4.19j}$$

The properties of angelic liftings discussed in Section 4.1.1 all have the following counterparts for demonic liftings.

Lemma 4.20. $[\,] : \mathsf{A} \to \mathsf{Mul}(\mathsf{A})$ is an anti-monotonic functor.

We also want to be able to characterise multirelations that are demonic liftings.

Lemma 4.21. A multirelation $m : X \rightrightarrows Y$ in a power allegory is a demonic lifting if and only if

$$m\,;\bigcap^\circ = m/\ni\,.$$

Rewitzky (2003) describes such multirelations as proper and completely multiplicative. We will now discuss the properties of demonic liftings in a set-theoretic context to illustrate the above lemma.

If a set-theoretic multirelation $m : X \rightrightarrows Y$ always has just one strongest postcondition that the angel can choose to guarantee given some input x, then the angel has no control over what the demon chooses and this multirelation would be described as demonic. Another way of expressing this property is to say that for all $Z : \mathbb{PP}Y$,

$$x\ m\ \left(\bigcap Z\right) \equiv (\forall Y : Y \in Z : x\ m\ Y)$$

This equivalence is the set-theoretic version of the equation in Lemma 4.21.

As well as a category of multirelations that are angelic liftings, we also have a category of demonic liftings.

Lemma 4.22. The demonic liftings in $(\mathsf{Mul}(\mathsf{A}), \subseteq_{\mathsf{A}})$ form a subcategory, which will be denoted by $(\mathsf{Dem}(\mathsf{A})), \subseteq_{\mathsf{A}})$. Furthermore, there is an anti-monotonic order-isomorphism of categories $\mathsf{A} \cong \mathsf{Dem}(\mathsf{A})$.

From the above isomorphism, we deduce that $\mathsf{Dem}(\mathsf{A})$ is a power allegory so it has both meets and joins. Its meet operator $\cap_{\mathsf{Dem}(\mathsf{A})}$ is the same as $\cap_{\mathsf{A}}$, as can be seen from the

https://doi.org/10.1017/S0960129512000965 Published online by Cambridge University Press

property (4.19f), which shows that the meet of two demonic liftings is itself a demonic lifting. However, the join operator for Dem(A) is given by

$$m \cup_{\mathsf{Dem(A)}} n = [m ; \ni \cup_{\mathsf{A}} n ; \ni]$$

for two multirelations $m, n : X \rightrightarrows Y$ that are demonic liftings.

One final observation is that functions lift to multirelations that are both angelic and demonic liftings.

Lemma 4.23. For any function $f : X \to Y$ in a power allegory A, its angelic and demonic liftings coincide. Furthermore, Fun(A) is isomorphic to the category Ang(A) ∩ Dem(A).

5. A hierarchy of categories

The order-enriched categories of total functions (Fun, $=$), relations (Rel, $\subseteq$) and predicate transformers (Tran, $\leqslant$) are related in a systematic way: Rel is related to Fun as each arrow in Rel can be factorised into a pair of functions, and in precisely the same way, Tran can be built from Rel. This three-level hierarchy cannot be extended in either direction (Gardiner *et al.* 1994).

The category of predicate transformers in a power allegory, Tran(A), will be defined in Section 6.1, where it will also be shown that it is order-isomorphic to Mul(A). It has been shown previously that arrows in Tran(A) can be built from those in A in precisely the same way that Tran is built from Rel (de Moor *et al.* 1991). In this section, we explore the analogous factorisation of arrows in Mul(A) into those from A, and compare it with standard results relating Fun(A) and A in certain allegories.

The reason that this relationship is of interest here is that it has practical implications: it means that both functors and initial algebras, which are important concepts for modelling datatypes in algebraic program semantics, can be extended from Fun(A), via A, to Mul(A) in a suitable allegory A in a well-defined way. The details of these constructions are beyond the scope of this paper – see Martin and Curtis (2006) for further information. Although most of the proofs in Martin and Curtis (2006) are situated in Rel, the one concerning the lifting of initial algebras is point-free, and could therefore be translated to apply to any power allegory.

5.1. *Factorisation*

The factorisation property we shall use is that in a power allegory A, each arrow in Mul(A) is equivalent to a pair of arrows in A, which are unique up to equivalence. This factorisation is expressed in terms of maps, so we begin by identifying the maps and comaps in this allegory.

Lemma 5.1. The maps in Mul(A) are precisely the demonic liftings, and the comaps are the angelic liftings.

The following laws are now immediate from the preceding laws of maps with meet (3.10) and join (3.13).

https://doi.org/10.1017/S0960129512000965 Published online by Cambridge University Press

Laws 5.2.

$$[r] \fatsemi (m \cap n) = ([r] \fatsemi m) \cap ([r] \fatsemi n) \tag{5.2a}$$

$$\langle r \rangle \fatsemi (m \cup n) = (\langle r \rangle \fatsemi m) \cup (\langle r \rangle \fatsemi n). \tag{5.2b}$$

The unique factorisation property is defined as follows.

Definition 5.3. Let $(\mathsf{C}, \subseteq)$ be an order-enriched category. Then C has *map factorisation* if every arrow m has a factorisation $m = t^* \,;u$, where t and u are maps. This factorisation is *unique up to equivalence* if whenever $m = t^* \,;u$ is a map factorisation and r, s are maps, then $r^* \,;s \subseteq m$ if and only if there exists a map h such that $h \,;t \subseteq r$ and $s \subseteq h \,;u$.

Lemma 5.4. $\mathsf{Mul}(\mathsf{A})$ has a map factorisation that is unique up to equivalence.

This result, together with the map characterisation of Lemma 5.1 and the isomorphisms of Lemmas 4.15 and 4.22, shows that every multirelation in a power allegory A is equivalent to a pair of arrows in A, and that pair is unique up to equivalence. So, in particular, each set-theoretic multirelation can be factorised uniquely into a pair of relations. This observation is similar to the one made in Back and von Wright (1998, Theorem 13.10), except that the uniqueness condition is omitted there, as is the property that the factors are maps and comaps. It is this last property that facilitates the lifting of functors and initial algebras (Martin and Curtis 2010).

Example 5.5. Recall the vending machine V_3 of Example 2.1, which only has two buttons: one for a chocolate bar, and the other resulting in the machine's demonic choice of either a packet of toffees or a lollipop being dispensed:

$$V_3 = \{(coin, P) \mid \{choc\} \subseteq P \vee \{toffees, lollipop\} \subseteq P\}.$$

This machine is neither an angelic nor a demonic lifting. By (4.19i), this can be factorised as $V_3 = \langle V_3 \rangle \fatsemi [\ni]$. This expression can be thought of as follows. The first step $\langle V_3 \rangle$ involves an angelic choice of guarantee: either $\{choc\}$, $\{toffees, lollipop\}$, or a weaker predicate. Then the $[\ni]$ step describes the demonic choice of an element from whichever set/guarantee was selected by the angel with $\langle V_3 \rangle$.

As mentioned above, each arrow in Rel can then be factorised further into a pair of functions. More generally, we can factorise arrows of a power allegory A into arrows of $\mathsf{Fun}(\mathsf{A})$ if that allegory is *tabular*.

Definition 5.6. An allegory A is tabular if every arrow $r : A \to B$ has a map factorisation $f^\circ \,;g$ where arrows $f : T \to A$ and $g : T \to B$ satisfy the jointly monic condition, that is,

$$f \,;f^\circ \cap g \,;g^\circ = id_T.$$

Lemma 5.7 (Johnstone 2002, Lemma 3.2.4). If A is a tabular allegory, then whenever $r = f^* \,;g$ is a tabulation and x, y are maps, we have $x^* \,;y \subseteq m$ if and only if there exists a map h such that $h \,;f = x$ and $y = h \,;g$.

https://doi.org/10.1017/S0960129512000965 Published online by Cambridge University Press

Since the ordering on maps in an allegory is the discrete one (see Lemma 3.22), the above uniqueness property is identical to that of Definition 5.3.

6. Equivalent models

In this section we will define two other categories that are each equivalent to the category of multirelations, and discuss their comparative advantages and disadvantages.

6.1. *Predicate transformers*

Recall from Example 3.3 that the category of predicate transformers Tran has sets as objects, and its arrows are total functions on powersets that are monotonic with respect to set inclusion $\subseteq$. A formal point-free definition is as follows.

Definition 6.1 (Bird and de Moor 1997). A *predicate transformer* $p : X \mapsto Y$ is a function arrow $p : \mathsf{P}Y \to \mathsf{P}X$ in a power allegory such that

$$\sqsupseteq ; p \ \subseteq \ p ; \sqsupseteq \qquad \text{(monotonicity property)}$$

where $\sqsupseteq$ is the converse of $\sqsubseteq$.

This is an abstract model of weakest precondition predicate transformer semantics. In the power allegory Rel, the above monotonicity condition equates to the following more familiar condition from Example 3.3:

$$U \subseteq V \Rightarrow p\, U \subseteq p\, V.$$

Predicate transformer arrows can be compared using an ordering that corresponds to pointwise inclusion in set-theoretic terms.

Definition 6.2. For each pair of arrows $p, q : X \mapsto Y$ in a power allegory, the ordering $\leqslant$ is defined by

$$p \leqslant q \equiv (p ; \ni \ \subseteq \ q ; \ni).$$

With this ordering, predicate transformers form an order-enriched category.

Lemma 6.3. The objects and predicate transformers in a power allegory A form an order-enriched *category of predicate transformers* $(\mathsf{Tran}(\mathsf{A}), \leqslant)$ with composition $\circ$ the converse of composition in A, which is to say that for $p : X \mapsto Y$ and $q : Y \mapsto Z$, we have $p \circ q : X \mapsto Z$ given by $p \circ q = q ; p$. The identity arrow id_X for each object X is the arrow $id_{\mathsf{P}X}$ from the underlying allegory A.

The equivalence between this model and that of multirelations is formalised by the following lemma.

Lemma 6.4. There is an order-isomorphism of categories $\mathsf{Mul}(\mathsf{A}) \cong \mathsf{Tran}(\mathsf{A})$. Specifically, the isomorphism is given by $\Phi : \mathsf{Mul}(\mathsf{A}) \to \mathsf{Tran}(\mathsf{A})$, where $\Phi(m) = \Lambda(m^\circ)$.

https://doi.org/10.1017/S0960129512000965 Published online by Cambridge University Press

So all of the foregoing definitions and results for multirelations have an equivalent formulation for predicate transformers. In particular, it is reassuring to observe that the algebraic characterisations of angelic and demonic liftings given in Definitions 4.14 and 4.21 translate to the more well-known characterisation in terms of universal disjunction and conjunction (Back and von Wright 1992), which is given below. These point-free definitions are phrased in terms of the existential image functor introduced in Definition 3.34: a predicate transformer $p : X \mapsto Y$ is *universally disjunctive* if

$$\bigcup ; p = \mathsf{E}p ; \bigcup$$

and *universally conjunctive* if

$$\bigcap ; p = \mathsf{E}p ; \bigcap.$$

The angelic and demonic liftings of an arrow r in a power allegory translate to the predicate transformers $\mathsf{E}(r^\circ)$ and $\Lambda(\ni / r)$, respectively, using Lemma 6.4.

6.2. *Multifunctions*

A different representation of multirelations is generated by the standard mapping from relations to set-valued functions (multifunctions) using the power transpose (Λ). The resulting model is essentially the choice semantics of Back and von Wright (1998).

Definition 6.5. An *upclosed multifunction* with source X and target Y in a power allegory is a function arrow $p : X \to \mathsf{PP}Y$ such that

$$p ; \uparrow_Y = p,$$

where the upclosure operator is defined by $\uparrow_Y = \mathsf{E} \sqsubseteq_Y$.

The interpretation of $\uparrow_Y$ in set-theory is standard (Davey and Priestley 2002): for all $W \in \mathbb{PPP}Y$,

$$\uparrow_Y W \;=\; \{V \mid (\exists U : U \in W : U \subseteq V)\}.$$

So a total function $p : X \to \mathbb{PPP}Y$ is an upclosed multifunction if and only if for all $x \in X$, the set $p\,x$ is upclosed in the sense that if $U \in p\,x$ and $U \subseteq V$, then $V \in p\,x$. Multifunctions also form a category within a power allegory.

Lemma 6.6 (Martin and Curtis 2010). The upclosed multifunctions in a power allegory A form an order-enriched category $(\mathsf{MFun}(\mathsf{A}), \leqslant)$, where the composition of each pair of upclosed multifunctions $p : X \to \mathsf{PP}Y$ and $q : Y \to \mathsf{PP}Z$ is defined by

$$p \star q = p ; \mathsf{EE}q ; \mathsf{E}\bigcap ; \bigcup,$$

and the identity is $\Lambda{\in_X}$ for each object X. The ordering ($\leqslant$) is the same as that on predicate transformers (see Definition 6.2).

https://doi.org/10.1017/S0960129512000965 Published online by Cambridge University Press

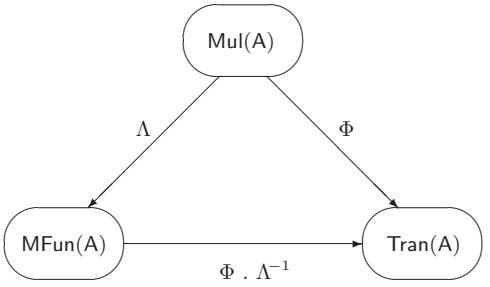

Fig. 1. Order-isomorphisms between Mul(A), MFun(A) and Tran(A).

Expanding this definition of composition gives

$$(p \star q)x = \bigcup\{\bigcap\{q\, w \mid w \in W\} \mid W \in p\, x\}$$

in set-theoretic terms. So given input x, the angel can ensure that $p \star q$ will establish postcondition U if and only if he can choose a postcondition W for p such that for every input value in W, q can be guaranteed to establish U. The isomorphism between multirelations and multifunctions is stated in the following lemma.

Lemma 6.7 (Martin and Curtis 2010). There is an order-isomorphism MFun(A) ≅ Mul(A) of categories, as given by the universal property (3.29a) for Λ and $\ni$.

6.3. *Comparison of models*

Figure 1 summarises the isomorphisms between the three equivalent models of predicate transformers, multirelations and multifunctions, all of which are useful for different reasons. The predicate transformer model has the simplest composition operator, and the most established body of theory; it has been studied in depth by the designers of the various refinement calculi for which it is the semantic model (see, for example, Back and von Wright (1998), Morgan (1994) and Morris (1987)). Its main disadvantage is that it is used to model programs and specifications backwards, rather than forwards. This was not a handicap for the developers of the refinement calculi because each calculus consisted of a separate command language and associated laws, where specifications were modelled forwards. It is a problem here, however, because our goal is to develop a single mathematical language in which a process can be expressed, and then manipulated into another process that is either equivalent to, or a refinement of, the original, without the need for a separate semantic model.

The solution to this problem is to switch to multirelations, which model processes forwards. The hierarchy of the three models of functions, relations and multirelations described in Section 5 can be exploited more usefully in this model because familiar operators can be extended to multirelations in a natural way that can be used immediately in the calculus. Previous attempts (Martin 1995) to extend operators like map and fold to predicate transformers were less successful because the resulting constructs then needed to

https://doi.org/10.1017/S0960129512000965 Published online by Cambridge University Press

be translated back from the semantic model into the command language, and there was no obvious mechanism for doing this. So in some ways it is simpler to work entirely within one space than to swap between a command language and semantic model. However, the language of multirelations bears far less resemblance to a programming language than the command language of Morgan (1994), for example. On the other hand, the calculus of multirelations does have similarities to the calculus of relations, and thus has a familiar feel, which could make it a valuable tool.

Some of our previous calculations with set-theoretic multirelations have involved some slightly cumbersome manipulations (Martin *et al.* 2007). This is mainly because of the unwieldy composition operator (see Example 3.4), and it is one of the reasons for the current change to a point-free approach. Most of the previous work on predicate transformers has been set in the realm of set theory and logic, and there has been very little study of predicate transformers in allegories, perhaps because there was no need for it. But the allegorical approach is almost essential for multirelations because it removes the need for the quantifiers used in the set-theoretic model. The result, as introduced in this paper, is starting to look like the core of a workable calculus, which is similar, in some respects, to the relational calculus of Bird and de Moor (1997).

So what use are multifunctions? They are harder to use than multirelations, partly because the essential operators of composition, meet and join are more difficult to express. But the model is still useful because the category $\mathsf{MFun}(A)$ can be constructed as a Kleisli category of $\mathsf{Fun}(A)$ (Martin and Curtis 2010), so all of the associated theory, such as that described in Fokkinga (1994), is applicable. In particular, this construction may hold the key to the definition of the elusive *unfold* operator.

6.4. *Refinement*

This paper contains some basic laws of the category of multirelations in a power allegory, but there is insufficient space in this paper to show how these laws might be used in a derivation involving refinement. The calculus of multirelations is not intended to supersede the refinement calculi of Back and von Wright (1998), Morgan (1994) and Morris (1987), but instead we expect it to be used in a slightly different way, *viz*. for algebraic reasoning about the guarantees of processes that exhibit both angelic and demonic non-determinism. The subset inclusion ordering on multirelations has the same meaning as the standard refinement ordering: it represents a possible increase in angelic non-determinism and decrease in demonic non-determinism. So equational reasoning can be used to show that two processes offer the same guarantees, and inequational reasoning can show that one process has stronger guarantees than another.

7. Conclusions

The contribution of this paper is to collate the central definitions and laws of the theory of multirelations and place them in the categorical setting of allegories. The result is a clear and succint algebraic formalism that is much more concise than its set-theoretic counterpart, partly because it avoids the use of quantifiers. The proofs in the

https://doi.org/10.1017/S0960129512000965 Published online by Cambridge University Press

appendix demonstrate how the axiomatic approach taken here leads to short and rigorous calculations.

In addition, we have put multirelations into historical context and compared them with other models. All of the results in this paper already exist for set-theoretic predicate transformers (Back and von Wright 1998; Gardiner *et al.* 1994), and some also exist for set-theoretic multirelations (Martin and Curtis 2006; Martin *et al.* 2007). Many have also been proved for predicate transformers, both in an allegory (de Moor *et al.* 1991) and over posets (Naumann 1998), so there is an element of repackaging to this paper. However, we think that this work is worthwhile because the algebraic calculus of multirelations has great potential and deserves much more attention than it has received so far. It offers the abstraction of the relational calculus of allegories together with the expressive power of predicate transformers: every multirelation in a power allegory is equivalent to a pair of arrows in the allegory, and that pair is essentially unique, as Lemma 5.4 showed. Likewise, the arrows in a tabular allegory are equivalent to a pair of function arrows that satisfy the same uniqueness condition, so there is a hierarchy of models.

This paper has described some basic theory of categorical multirelations, but the real challenge lies ahead. We now need to extend the theory, building it into a workable calculus for algorithm derivation using case studies from various branches of computer science and game theory. We have already identified some interesting avenues for exploration, such as products, conjugates and coalgebras. Further investigation is sure to reveal more problems to solve, but we hope that this paper lays a solid foundation from which to tackle these questions in a secure and reliable way.

Appendix: Proofs.

Much of Section 3 is standard theory, and the proofs of most of the laws in that section can be found in Martin and Curtis (2009) and the standard references Bird and de Moor (1997) and Freyd and Ščedrov (1993). In this appendix, we have gathered together the proofs for the remaining claims in Section 3, though in some cases we have just given proof hints for derivations that are very straightforward. We also give here the proofs of the claims in Sections 4, 5 and 6 that are not already referenced to another source.

Proof of Laws 3.10

(3.10d) This proof follows straightforwardly from the shunting rule (3.6a) and property (3.5b).

Proof of Laws 3.13

The proofs of all these properties follow straightforwardly from the shunting rules (3.6), the definition of join (3.12) and the monotonicity of composition.

Proof of Laws 3.18

(3.18j) This is immediate from the definition of $\backslash$ (3.15) and the dual of law (3.18c).

https://doi.org/10.1017/S0960129512000965 Published online by Cambridge University Press

(3.18k) We have

$$\begin{aligned}(r\backslash s)\,;t \;\subseteq\; r\backslash(s\,;t) \;&\equiv\; r\,;((r\backslash s)\,;t) \;\subseteq\; s\,;t && \text{(definition of } \backslash \text{ (3.15))}\\ &\Leftarrow\; s\,;t \;\subseteq\; s\,;t\\ &&& \text{(associativity of composition and property of } \backslash \text{ (3.18c))}\\ &\Leftarrow\; True. && (\subseteq \text{ is a partial order})\end{aligned}$$

(3.18o) This is immediate from laws (3.18m) and (3.18f).

Proof of Laws 3.31

(3.31a, 3.31b) These follow from the definition of a power allegory since Λ returns a function arrow.

(3.31d) This is proved by taking converses of (3.31c).

(3.31e) We have

$$\begin{aligned}\Lambda(r^\circ) \;\subseteq\; (r\backslash\in) \;&\equiv\; (r\,;\Lambda(r^\circ)) \;\subseteq\; \in && \text{(definition of } \backslash \text{ (3.15))}\\ &\equiv\; r \;\subseteq\; (\in\,;(\Lambda(r^\circ))^\circ) && \text{(shunting (3.6a))}\\ &\equiv\; True. && (\text{(3.31d) and idempotence of } {}^\circ \text{ (3.19a)})\end{aligned}$$

(3.31f) This is proved by taking $r = f\,;\ni$ in the universal property (3.29a).

(3.31h) This is proved by taking $f = id$ and $r = \ni$ in the universal property (3.29a).

(3.31i) We have

$$\begin{aligned}\Lambda r\,;(\in\backslash s) \;&=\; (\in\,;(\Lambda r)^\circ)\backslash s && (\Lambda r \text{ is a map and property of } \backslash \text{ (3.18m))}\\ &=\; r^\circ\backslash s. && \text{(property of } \Lambda \text{ (3.31d)}\end{aligned}$$

(3.31j) By (3.18l), it is sufficient to show

$$\begin{aligned}(r\backslash s) \;\subseteq\; (r\backslash\in)\,;(\in\backslash s) \;&\Leftarrow\; (r\backslash s) \;\subseteq\; \Lambda(r^\circ)\,;(\in\backslash s)\\ &&& \text{(property of } \Lambda \text{ (3.31e) and monotonicity of composition)}\\ &\equiv\; True. && (\text{(3.31i) and idempotence of } {}^\circ \text{ (3.19a)})\end{aligned}$$

(3.31k) This follows from (3.31j) and (3.18f).

Proof of Laws 3.37

(3.37a) This is an instance of (3.31c).

(3.37b) This follows from the definition of $\sqsubseteq$ (3.33), with (3.18n) and (3.31d).

https://doi.org/10.1017/S0960129512000965 Published online by Cambridge University Press

(3.37c) We have

$$\begin{aligned}
\Lambda r\,;\bigcap;\sqsubseteq &= \Lambda r\,;\Lambda(\in\backslash\ni)\,;(\in\backslash\in) && \text{(definitions of } \bigcap \text{ (3.36) and } \sqsubseteq \text{ (3.33))}\\
&= \Lambda(\Lambda r\,;(\in\backslash\ni))\,;(\in\backslash\in) && \text{(property of } \Lambda \text{ (3.31g))}\\
&= \Lambda(r^{\circ}\backslash\ni)\,;(\in\backslash\in) && \text{(property of } \Lambda \text{ (3.31i))}\\
&= (r^{\circ}\backslash\ni)^{\circ}\backslash\in && \text{(property of } \Lambda \text{ (3.31i))}\\
&= (\in/r)\backslash\in. && \text{(property of } \backslash \text{ (3.28a))}
\end{aligned}$$

Proof of Lemma 4.4

We need to show that $m \fatsemi n$ is upclosed, given the upclosure of m and n. By Definition 4.3,

$$m \fatsemi n = m\,;(\in\backslash n),$$

so by Definition 4.1 of upclosure, it is sufficient to show that

$$((\in\backslash n)\,;\sqsubseteq) \;\subseteq\; \in\backslash n.$$

We have

$$\begin{aligned}
((\in\backslash n)\,;\sqsubseteq) \;\subseteq\; \in\backslash n &\equiv (\in\,;(\in\backslash n)\,;\sqsubseteq) \;\subseteq\; n && \text{(definition of } \backslash \text{ (3.15))}\\
&\Leftarrow (n\,;\sqsubseteq) \;\subseteq\; n && \text{(property of } \backslash \text{ (3.18c))}\\
&\equiv \mathit{True}. && (n \text{ is a multirelation (4.1) and therefore upclosed})
\end{aligned}$$

Proof of Law 4.5

This is immediate from the upclosure of m and property (3.37b).

Proof of Lemma 4.7

As the universal properties for meets (3.9) and joins (3.12) are inherited from the underlying power allegory, it suffices to show that $\cup$ and $\cap$ preserve the upclosure property of multirelations. For multirelations $m, n : X \rightrightarrows Y$ in a power allegory,

$$\begin{aligned}
(m \cap n)\,;\sqsubseteq \;&\subseteq\; (m\,;\sqsubseteq) \cap (n\,;\sqsubseteq) && \text{(distribution of ; over } \cap \text{ (3.10b))}\\
&= m \cap n. && (m \text{ and } n \text{ are multirelations (4.1))}
\end{aligned}$$

The reverse inclusion follows from the definition of $\sqsubseteq$ (3.33), property (3.18e) and the monotonicity of composition. For joins, we have:

$$\begin{aligned}
(m \cup n)\,;\sqsubseteq &= (m\,;\sqsubseteq) \cup (n\,;\sqsubseteq) && \text{(distribution of ; over } \cup \text{ (3.25c))}\\
&= m \cup n. && (m \text{ and } n \text{ are multirelations (4.1))}
\end{aligned}$$

https://doi.org/10.1017/S0960129512000965 Published online by Cambridge University Press

Proof of Laws 4.8

(4.8a) We have

$$\begin{aligned}(n \cap v) \wr m &= (n \wr m) \cap (v \wr m) \\ &\equiv (n \cap v) ; (\Lambda(m^\circ))^\circ = (n ; (\Lambda(m^\circ))^\circ) \cap (v ; (\Lambda(m^\circ))^\circ) \\ &\qquad \text{(alternative definition of } \wr \text{ (4.5))} \\ &\Leftarrow True. \qquad \text{(property of meets and maps (3.10d))}\end{aligned}$$

(4.8b) We have

$$\begin{aligned}(n \cup v) \wr m &= (n \wr m) \cup (v \wr m) \\ &\equiv (n \cup v) ; (\in \backslash m) = (n ; (\in \backslash m)) \cup (v ; (\in \backslash m)) \\ &\qquad \text{(definition of } \wr \text{ (4.3))} \\ &\Leftarrow True. \qquad \text{(composition distributes over join (3.26b))}\end{aligned}$$

Proof of Laws 4.12

(4.12a) This follows from the angelic lifting definition (4.9) and a property of division (3.18h).

(4.12b) We have

$$\begin{aligned}\langle m \wr n \rangle \subseteq m \wr \langle n \rangle &\equiv (m \wr n) ; \in \subseteq m \wr (n ; \in) \qquad \text{(definition of angelic lifting (4.9))} \\ &\equiv m ; (\in \backslash n) ; \in \subseteq m ; (\in \backslash (n ; \in)) \qquad \text{(definition of composition (4.3))} \\ &\Leftarrow True. \qquad \text{((3.18k) and the monotonicity of ;)}\end{aligned}$$

(4.12c) We have

$$\begin{aligned}\langle r \rangle \wr m &= r ; \in ; (\in \backslash m) \qquad \text{(definitions of angelic lifting (4.9) and } \wr \text{ (4.3))} \\ &= r ; m. \qquad \text{(cancellation property (3.31k))}\end{aligned}$$

(4.12d) This is immediate from the definition of angelic lifting (4.9) and the associativity of composition.

(4.12e) This is immediate from the definition of angelic lifting (4.9).

(4.12f) We have

$$\begin{aligned}\langle r ; s \rangle &= r ; \langle s \rangle \qquad \text{(property of angelic lifting (4.12d))} \\ &= \langle r \rangle \wr \langle s \rangle. \qquad \text{(property of angelic lifting (4.12c))}\end{aligned}$$

(4.12g) This follows from the definition of angelic lifting (4.9) and the monotonicity of ;.

(4.12h) We have

$$\begin{aligned}\langle r \cup s \rangle = \langle r \rangle \cup \langle s \rangle &\equiv (r \cup s) ; \in = (r ; \in) \cup (s ; \in) \qquad \text{(definition of angelic lifting (4.9))} \\ &\Leftarrow True. \qquad \text{(distribution of composition over join (3.26b))}\end{aligned}$$

https://doi.org/10.1017/S0960129512000965 Published online by Cambridge University Press

Proof of Lemma 4.13

This follows from properties of $\langle\ \rangle$, namely, identity-preserving (4.12e), composition-preserving (4.12f) and monotonicity (4.12g).

Proof of Lemma 4.14

First we show that for any multirelation m,

$$m\,;\bigcup^{\circ} = m \fatsemi \langle\in\rangle. \tag{A.1}$$

We have

$$\begin{aligned} m\,;\bigcup^{\circ} &= m\,;(\Lambda(\ni\,;\ni))^{\circ} && \text{(definition of } \bigcup \text{ (3.35))} \\ &= m \fatsemi (\in\,;\in) && \text{(alternative definition of } \fatsemi \text{ (4.5))} \\ &= m \fatsemi \langle\in\rangle. && \text{(definition of angelic lifting (4.9))} \end{aligned}$$

For any arrow $r : X \to Y$ in a power allegory A, the lifting $\langle r\rangle$ satisfies the condition of Lemma 4.14 since

$$\begin{aligned} \langle r\rangle\,;\bigcup^{\circ} &= \langle r\rangle \fatsemi \langle\in\rangle && \text{(property of } \bigcup \text{ (A.1))} \\ &= r\,;\langle\in\rangle && \text{(property of angelic lifting (4.12c))} \\ &= \langle r\rangle\,;\in. && \text{(definition of angelic lifting (4.9), twice)} \end{aligned}$$

Conversely, if m satisfies the condition of Lemma 4.14, we will show that it is the lifting

$$m = \langle m\,;\eta^{\circ}\rangle. \tag{A.2}$$

We have

$$\begin{aligned} \langle m\,;\eta^{\circ}\rangle &= (m\,;\in) \fatsemi \langle\eta^{\circ}\rangle && (\langle\ \rangle \text{ preserves composition (4.12f) and definition of } \langle\ \rangle \text{ (4.9))} \\ &= (m\,;\bigcup^{\circ}) \fatsemi \langle\eta^{\circ}\rangle && (m \text{ satisfies the condition of Lemma 4.14}) \\ &= m \fatsemi \langle\in\rangle \fatsemi \langle\eta^{\circ}\rangle && (\text{property of } \bigcup \text{ (A.1)}) \\ &= m \fatsemi \langle\in\,;\eta^{\circ}\rangle && (\langle\ \rangle \text{ preserves composition (4.12f)}) \\ &= m \fatsemi \langle id\rangle && (\text{converse (3.19c) and property of } \eta \text{ (3.37a)}) \\ &= m. && (\text{identity preservation (4.12e) and identity multirelation}) \end{aligned}$$

Proof of Lemma 4.15

The function $\langle\ \rangle : \mathsf{A} \to \mathsf{Mul}(\mathsf{A})$ is a monotonic functor (by Lemma 4.13) that maps onto $\mathsf{Ang}(\mathsf{A})$,which is therefore a category. The inverse of $\langle\ \rangle$ is given by a function

https://doi.org/10.1017/S0960129512000965 Published online by Cambridge University Press

$$\mathsf{a} : \mathsf{Mul}(\mathsf{A}) \to \mathsf{A},$$

which is defined for each multirelation m by $\mathsf{a}(m) = m\,;\eta^\circ$. This function is monotonic since η° has left inverse $\in$ by the converse of (3.37a). To see that a is the inverse of $\langle\ \rangle$, note that by (A.2) we have $\langle \mathsf{a}(m)\rangle = m$, and, conversely,

$$\begin{array}{lll} \mathsf{a}(\langle r\rangle) & = & r\,;\in\,;\eta^\circ \qquad \text{(definitions of } \mathsf{a} \text{ and } \langle\ \rangle \text{ (4.9))} \\ & = & r. \qquad \text{(converse (3.19c) and property of } \eta \text{ (3.37a))} \end{array}$$

So the monotonic function a is the inverse of $\langle\ \rangle$, and since $\langle\ \rangle$ is a functor, it follows that a is also a functor, which establishes the order-isomorphism.

Proof of Laws 4.19

(4.19a) The fact that $[r]\,;\sqsubseteq\ = [r]$ (the upclosure property) is immediate from the definition of demonic lifting (4.16) and a cancellation property of $\in$ (3.31j).

(4.19b) We have

$$\begin{array}{lll} [r]\fatsemi m & = & (r^\circ\backslash\in)\,;(\in\backslash m) \qquad \text{(definitions of demonic lifting (4.16) and } \fatsemi \text{ (4.3))} \\ & = & r^\circ\backslash m. \qquad \text{(cancellation property of } \in \text{ (3.31j))} \end{array}$$

(4.19c) We have

$$\begin{array}{lll} [id] & = & id^\circ\backslash\in \qquad \text{(definition of demonic lifting (4.16))} \\ & = & id\backslash\in \qquad \text{(converse preserves identity (3.20b))} \\ & = & \in. \qquad \text{(property of } \backslash \text{ (3.18f))} \end{array}$$

(4.19d) We have

$$\begin{array}{lll} [r]\fatsemi[s] & = & r^\circ\backslash[s] \qquad \text{(property of demonic lifting (4.19b))} \\ & = & r^\circ\backslash(s^\circ\backslash\in) \qquad \text{(definition of demonic lifting (4.16))} \\ & = & (s^\circ\,;r^\circ)\backslash\in \qquad \text{(property of } \backslash \text{ (3.18g))} \\ & = & (r\,;s)^\circ\backslash\in \qquad \text{(property of converse (3.19c)} \\ & = & [r\,;s]. \qquad \text{(definition of demonic lifting (4.16))} \end{array}$$

(4.19e) We have

$$\begin{array}{lll} [s]\subseteq[r] & \equiv & s^\circ\backslash\in\ \subseteq\ r^\circ\backslash\in \qquad \text{(definition of demonic lifting (4.16))} \\ & \Leftarrow & r\subseteq s. \quad \text{(anti-monotonicity of } \backslash \text{ (3.18b) and monotonicity of } {}^\circ \text{ (3.19b))} \end{array}$$

https://doi.org/10.1017/S0960129512000965 Published online by Cambridge University Press

(4.19f) We have

$$\begin{aligned}
[r \cup s] &= (r \cup s)^\circ \backslash \in && \text{(definition of demonic lifting (4.16))}\\
&= (r^\circ \cup s^\circ) \backslash \in && \text{(converse distributes through join (3.26a))}\\
&= (r^\circ \backslash \in) \cap (s^\circ \backslash \in) && \text{(property of meet, join and } \backslash \text{ (3.28b))}\\
&= [r] \cap [s]. && \text{(definition of demonic lifting (4.16))}
\end{aligned}$$

(4.19g) We have

$$\begin{aligned}
[r] \fatsemi \langle r^\circ \rangle &= r^\circ \backslash \langle r^\circ \rangle && \text{(property of demonic lifting (4.19b))}\\
&= r^\circ \backslash (r^\circ ; \in) && \text{(definition of angelic lifting (4.9))}\\
&\supseteq \in. && \text{(cancellation property of } \backslash \text{ (3.18d))}
\end{aligned}$$

(4.19h) We have

$$\begin{aligned}
\langle r^\circ \rangle \fatsemi [r] &= r^\circ ; [r] && \text{(property of angelic lifting (4.12c))}\\
&= r^\circ ; (r^\circ \backslash \in) && \text{(definition of demonic lifting (4.16))}\\
&\subseteq \in. && \text{(cancellation property of } \backslash \text{ (3.18c))}
\end{aligned}$$

(4.19i) We have

$$\begin{aligned}
m &= m ; (\in \backslash \in) && (m \text{ is a multirelation (4.1) and definition of } \sqsubseteq \text{ (3.33))}\\
&= m ; [\ni] && \text{(definition of demonic lifting (4.16))}\\
&= \langle m \rangle \fatsemi [\ni]. && \text{(property of angelic lifting (4.12c))}
\end{aligned}$$

(4.19j) We have

$$\begin{aligned}
[r] ; \bigcap^\circ = [r] / \ni \;\equiv\; & (r^\circ \backslash \in) ; \bigcap^\circ = (r^\circ \backslash \in) / \ni && \text{(definition of demonic lifting (4.16))}\\
\equiv\; & r^\circ \backslash (\in ; \bigcap^\circ) = r^\circ \backslash (\in / \ni) && \text{(properties of } \backslash \text{ (3.18n, 3.18i))}\\
\equiv\; & r^\circ \backslash (\in \backslash \ni)^\circ = r^\circ \backslash (\in / \ni) && \\
& && \text{(definition of } \bigcap \text{ (3.36) and property (3.31d) of } \in)\\
\equiv\; & True. && \text{(property of } \backslash \text{ and } / \text{ (3.28a))}
\end{aligned}$$

Proof of Lemma 4.20

The statement follows from properties of [ ]: specifically, identity-preserving (4.19c), composition-preserving (4.19d) and anti-monotonicity (4.19e).

https://doi.org/10.1017/S0960129512000965 Published online by Cambridge University Press

Proof of Lemma 4.21

For any lifting $[r]$ of an arrow $r : X \to Y$ in a power allegory A, the fact that

$$[r] \,;\bigcap^{\circ} \;=\; [r] \,/\ni$$

is stated in the property (4.19j).
Conversely, let m be a multirelation such that $m \,;\bigcap^{\circ} \;=\; m/\ni$. We will show that

$$m = (\in /m)\backslash \in, \tag{A.3}$$

and it will then follow that

$$m \;=\; [(\in /m)^{\circ}]$$

from the definition of demonic lifting (4.16). By (3.18j), we have $m \subseteq (\in /m)\backslash \in$, and for the reverse inclusion, we have

$$\begin{aligned}
(\in /m)\backslash \in \;\subseteq\; m \;&\equiv\; \Lambda m \,;\bigcap \,;\sqsubseteq \;\subseteq\; m && \text{(property of } \textstyle\bigcap \text{ (3.37c))}\\
&\Leftarrow\; \Lambda m \,;\bigcap \;\subseteq\; m && \text{(Upclosure of } m \text{ (4.1))}\\
&\equiv\; \Lambda m \;\subseteq\; m \,;\bigcap^{\circ} && \text{(shunting (3.6a))}\\
&\equiv\; \Lambda m \;\subseteq\; m/\ni && \text{(assumption)}\\
&\equiv\; \Lambda m \,;\ni \;\subseteq\; m && \text{(definition of / (3.16))}\\
&\equiv\; \mathit{True}. && \text{(property of } \Lambda \text{ (3.31c))}
\end{aligned}$$

Proof of Lemma 4.22

We need to prove that there is an anti-monotonic order-isomorphism between $(\mathsf{A}, \subseteq_{\mathsf{A}})$ and $(\mathsf{Dem}(\mathsf{A})), \subseteq_{\mathsf{A}})$ (to be clear about what we mean by 'anti-monotonic', this would be the same as proving that $(\mathsf{A}, \subseteq_{\mathsf{A}})$ and $(\mathsf{Dem}(\mathsf{A})), \supseteq_{\mathsf{A}})$ are order-isomorphic).

The function $[\,] : \mathsf{A} \to \mathsf{Mul}(\mathsf{A})$ is an anti-monotonic functor (by Lemma 4.20) that maps onto $\mathsf{Dem}(\mathsf{A})$, which is therefore a category. Its inverse function is given by a function $\mathsf{d} : \mathsf{Mul}(\mathsf{A}) \to \mathsf{A}$, which is defined for each multirelation m by $\mathsf{d}(m) = m^{\circ}\backslash \ni$. This function is anti-monotonic by (3.18b). To see that d is the inverse of $[\,]$, we will first show that for a multirelation m that is a demonic lifting, we have $[\mathsf{d}(m)] \;=\; m$:

$$\begin{aligned}
[\mathsf{d}(m)] \;&=\; (m^{\circ}\backslash \ni)^{\circ}\backslash \in && \text{(definitions of } \mathsf{d} \text{ and demonic lifting (4.16))}\\
&=\; (\in /m)\backslash \in && \text{(property of } \backslash \text{ (3.28a))}\\
&=\; m. && (m \text{ is a demonic lifting, Lemma 4.21, and property (A.3))}
\end{aligned}$$

https://doi.org/10.1017/S0960129512000965 Published online by Cambridge University Press

Conversely, we show that for a relation r, we have $\mathsf{d}[r] = r$:

$$\begin{aligned}
\mathsf{d}[r] &= (r^{\circ}\backslash\in)^{\circ}\backslash\ni && \text{(definitions of } \mathsf{d} \text{ and demonic lifting (4.16))}\\
&= (\ni/r)\backslash\ni && \text{(property of } \backslash \text{ (3.28a))}\\
&= r. && \text{(property of } \backslash \text{ (3.31l))}
\end{aligned}$$

So the anti-monotonic function d is the inverse of [ ], and since [ ] is a functor, it follows that d is also a functor, which establishes the anti-monotonic order-isomorphism.

Lemma 4.23

The proof of Lemma 4.23 is given after the proof of Lemma 5.1.

Proof of Lemma 5.1

By (4.19g) and (4.19h), all demonic liftings are maps and all angelic liftings are comaps. Conversely, suppose m is a map. We will prove that its comap m^* is an angelic lifting. By Lemma 4.14, it is sufficient to show

$$\begin{aligned}
m^*;\bigcup^{\circ} = m^*;\in \;&\equiv\; m^* \fatsemi \langle\in\rangle = \langle m^*\rangle && \text{((A.1) and the definition of angelic lifting (4.9))}\\
&\Leftarrow\; m^* \fatsemi \langle\in\rangle \subseteq \langle m^*\rangle && \text{((4.12b), since } \in \text{ is the identity of } \fatsemi)\\
&\equiv\; \langle\in\rangle \subseteq m \fatsemi \langle m^*\rangle && \text{(shunting (3.6b))}\\
&\Leftarrow\; \langle\in\rangle \subseteq \langle m \fatsemi m^*\rangle && \text{(property of angelic lifting (4.12b))}\\
&\equiv\; \mathit{True}. && \text{(definition of map (3.5) and monotonicity of } \langle\ \rangle)
\end{aligned}$$

Therefore, by Lemma 4.14, m^* is an angelic lifting. Since every map uniquely determines its comap and *vice versa*, it follows from (4.19g) and (4.19h) that m is a demonic lifting.

Proof of Lemma 4.23

First we show that the lifting of a function produces a multirelation that is both an angelic lifting and a demonic lifting:

$$\begin{aligned}
\langle f\rangle &= f;\in && \text{(definition of angelic lifting (4.9))}\\
&= f^{\circ}\backslash\in && \text{(property of } \backslash \text{ (3.18o) and adjoints are converses (Lemma 3.22))}\\
&= [f]. && \text{(definition of demonic lifting (4.16))}
\end{aligned}$$

The categories $\mathsf{Fun(A)}$ and $\mathsf{Ang(A)} \cap \mathsf{Dem(A)}$ share the same objects and ordering ($\subseteq_{\mathsf{A}}$). The above shows that all arrows of $\mathsf{Fun(A)}$ are lifted to both $\mathsf{Ang(A)}$ and $\mathsf{Dem(A)}$, so it remains to prove the converse, namely, that every arrow in $\mathsf{Ang(A)} \cap \mathsf{Dem(A)}$ is a lifting of an arrow in $\mathsf{Fun(A)}$.

https://doi.org/10.1017/S0960129512000965 Published online by Cambridge University Press

Let $m \in \mathsf{Ang(A)}$ and $m \in \mathsf{Dem(A)}$. Since m is an angelic lifting, it is a comap by Lemma 5.1. By the definition of comaps (3.5), there must then exist s such that

$$id \subseteq [s] \fatsemi m \ \wedge \ m \fatsemi [s] \subseteq id$$

because, from Lemma 5.1, maps are demonic liftings (here id refers to the identity with respect to $\fatsemi$, which is $\in$).

Since m is also a demonic lifting, there must exist r such that $m = [r]$. Thus we have

$$id \subseteq [s] \fatsemi [r] \ \wedge \ [r] \fatsemi [s] \subseteq id.$$

By the anti-monotonic order-isomorphism between A and $\mathsf{Dem(A)}$ (see Lemma 4.22), this is equivalent to

$$id \subseteq r \,;s \ \wedge \ s \,;r \subseteq id$$

(here, id refers to the original identity arrows of A). Thus, by Lemma 3.22, r is a function and is thus in $\mathsf{Fun(A)}$.

Proof of Laws 5.2

(5.2a) This is a consequence of Lemmas 4.7 and 5.1 and a property of meets (3.10c).

(5.2b) This is a consequence of Lemmas 4.7 and 5.1 and a property of joins (3.13d).

Proof of Lemma 5.4

By Lemma 5.1, the maps in $\mathsf{Mul(A)}$ are the demonic liftings and the comaps are the angelic liftings, so the existence of map factorisation is immediate from (4.19i). Recall from Definition 5.3 that a map factorisation is unique up to equivalence if whenever $m = t^* \,;u$ is a map factorisation, and r, s are maps, then $r^* \,;s \subseteq m$ if and only if there exists a map h such that $h \,;t \subseteq r$ and $s \subseteq h \,;u$. It follows from the properties of maps that if such an h exists, then $r^* \,;s \subseteq t^* \,;u$, so it is sufficient to prove the converse, that is,

$$r^* \,;s \subseteq t^* \,;u \ \Rightarrow \ (\exists\, h : h \,;t \subseteq r \text{ and } s \subseteq h \,;u) \tag{A.4}$$

where r, s, t, u and h are all maps. By laws (4.19g) and (4.19h), the comap of each map $[m]$ in $\mathsf{Mul(A)}$ is $\langle m^\circ \rangle$, so to prove the above, it is sufficient to show that for all a, b, c and d in A,

$$\langle a \rangle \fatsemi [c] \subseteq \langle b \rangle \fatsemi [d] \ \Rightarrow \ (\exists\, q : [q] \fatsemi [b^\circ] \subseteq [a^\circ] \text{ and } [c] \subseteq [q] \fatsemi [d]).$$

Since [ ] is an anti-monotonic functor by Lemma 4.20, this is equivalent to

$$\langle a \rangle \fatsemi [c] \subseteq \langle b \rangle \fatsemi [d] \ \Rightarrow \ (\exists\, q : a^\circ \subseteq q \,;b^\circ \text{ and } q \,;d \subseteq c). \tag{A.5}$$

https://doi.org/10.1017/S0960129512000965 Published online by Cambridge University Press

We can calculate:

$$\begin{aligned}
\langle a\rangle \fatsemi [c] \subseteq \langle b\rangle \fatsemi [d] &\equiv \in \subseteq [a^\circ] \fatsemi \langle b\rangle \fatsemi [d] \fatsemi \langle c^\circ\rangle && \text{(shunting (3.6a) and (3.6b))}\\
&\equiv \in \subseteq (a\backslash\langle b\rangle) \fatsemi [d] \fatsemi \langle c^\circ\rangle && \text{(property of demonic lifting (4.19b))}\\
&\equiv \in \subseteq \langle a\backslash\langle b\rangle\rangle \fatsemi [\ni] \fatsemi [d] \fatsemi \langle c^\circ\rangle && \text{(map factorisation (4.19i))}\\
&\equiv \in \subseteq \langle a\backslash\langle b\rangle\rangle \fatsemi [\ni ; d] \fatsemi \langle c^\circ\rangle && \text{(demonic lifting is a functor (Lemma 4.20))}\\
&\equiv \in \subseteq \langle a\backslash\langle b\rangle\rangle \fatsemi (\langle d^\circ\rangle\backslash\langle c^\circ\rangle) && \text{(property of demonic lifting (4.19b) and definition of angelic lifting (4.9))}\\
&\equiv \in \subseteq \langle a\backslash\langle b\rangle\rangle \fatsemi p && \text{(letting } p = \langle d^\circ\rangle\backslash\langle c^\circ\rangle)\\
&\equiv \in \subseteq (a\backslash\langle b\rangle) ; p && \text{(property of } \langle\ \rangle \text{ (4.12c))}\\
&\Rightarrow \eta \subseteq (a\backslash\langle b\rangle) ; p && (\eta \subseteq \in \text{ by (3.37a), with shunting (3.6a) and converses (3.19c))}\\
&\Rightarrow \eta \subseteq a\backslash(\langle b\rangle ; p) && \text{(property of } \backslash \text{ (3.18k))}\\
&\equiv \eta \subseteq a\backslash(b ; \in ; p) && \text{(definition of angelic lifting (4.9))}\\
&\equiv a ; \eta \subseteq b ; \in ; p && \text{(definition of } \backslash \text{ (3.15))}\\
&\equiv \eta^\circ ; a^\circ \subseteq p^\circ ; \ni ; b^\circ && \text{(converses (3.19b) and (3.19c))}\\
&\equiv a^\circ \subseteq \eta ; p^\circ ; \ni ; b^\circ. && \text{(shunting (3.6b))}
\end{aligned}$$

Thus, taking $q = \eta ; p^\circ ; \ni$ establishes the first part of (A.5). We still need to show that $q ; d \subseteq c$. We have

$$\begin{aligned}
q ; d \subseteq c &\equiv d^\circ ; q^\circ \subseteq c^\circ && \text{(converses (3.19b))}\\
&\equiv d^\circ ; \in ; (\langle d^\circ\rangle\backslash\langle c^\circ\rangle) ; \eta^\circ \subseteq c^\circ && \text{(converses (3.19c) and definitions of } p \text{ and } q)\\
&\equiv d^\circ ; \in ; (\langle d^\circ\rangle\backslash(\langle c^\circ\rangle ; \eta^\circ)) \subseteq c^\circ && \text{(property of } \backslash \text{ (3.18n))}\\
&\equiv \langle d^\circ\rangle ; (\langle d^\circ\rangle\backslash(c^\circ ; \in ; \eta^\circ)) \subseteq c^\circ && \text{(definition of angelic lifting (4.9))}\\
&\equiv \langle d^\circ\rangle ; (\langle d^\circ\rangle\backslash c^\circ) \subseteq c^\circ && \text{(converse of (3.37a))}\\
&\equiv \mathit{True}. && \text{(property of } \backslash \text{ (3.18c))}
\end{aligned}$$

Proof of Lemma 6.3

For an object X, its identity arrow in **Tran**(A), which is the arrow $id_{\mathsf{P}X}$ in A, satisfies the monotonicity property for predicate transformer arrows (see Definition 6.1) since

$$\sqsupseteq ; id \;=\; \sqsupseteq \;=$$

https://doi.org/10.1017/S0960129512000965 Published online by Cambridge University Press

The associativity of composition in **Tran**(A) is inherited from A. Composition preserves the monotonicity property (Definition 6.1) since for all $p : X \mapsto Y$, $q : Y \mapsto Z$,

$$\begin{array}{lll} \sqsupseteq ; (p \circ q) & \subseteq & \sqsupseteq ; q ; p \qquad \text{(composition in Tran(A))} \\ & \subseteq & q ; \sqsupseteq ; p \qquad \text{(monotonicity of } q \text{ (Definition 6.1))} \\ & \subseteq & q ; p ; \sqsupseteq \qquad \text{(monotonicity of } p \text{ (Definition 6.1))} \\ & \subseteq & (p \circ q) ; \sqsupseteq . \qquad \text{(composition in Tran(A))} \end{array}$$

We will now give an alternative definition for $\leqslant$, which is equivalent to Definition 6.2. For all predicate transformer arrows $p, q : X \mapsto Y$,

$$p \leqslant q \equiv p \subseteq (q ; \sqsupseteq). \tag{A.6}$$

This is equivalent to Definition 6.2 by Definition 3.15 and the dual of (3.18k). This can be used to show that composition is monotonic with respect to $\leqslant$. Let $p, q : X \mapsto Y$ and $t, u : Y \mapsto Z$ be such that $p \leqslant q \ \wedge \ t \leqslant u$. It is required to prove that $p \circ t \leqslant q \circ u$:

$$\begin{array}{lll} p \circ t \leqslant q \circ u & \equiv & t ; p \leqslant u ; q \qquad \text{(composition in Tran(A))} \\ & \equiv & t ; p \ \subseteq \ u ; q ; \sqsupseteq \qquad \text{(alternative definition of } \leqslant \text{ (A.6))} \\ & \equiv & t ; p \ \subseteq \ u ; q ; \sqsupseteq ; \sqsupseteq \qquad \text{(dual of (3.31j))} \\ & \Leftarrow & t ; p \ \subseteq \ u ; \sqsupseteq ; q ; \sqsupseteq \qquad \text{(monotonicity of } q \text{ (Definition 6.1))} \\ & \Leftarrow & t \ \subseteq \ (u ; \sqsupseteq) \ \wedge \ p \ \subseteq \ (q ; \sqsupseteq) \qquad \text{(monotonicity of ;)} \\ & \equiv & t \leqslant u \ \wedge \ p \leqslant q. \qquad \text{(alternative definition of } \leqslant \text{ (A.6))} \end{array}$$

Proof of Lemma 6.4

First we show that if m is a multirelation then $\Phi(m)$ is a predicate transformer:

$$\begin{array}{lll} \sqsupseteq ; \Phi(m) \ \subseteq \ \Phi(m) ; \sqsupseteq & \equiv & \sqsupseteq ; \Lambda(m^\circ) \ \subseteq \ \Lambda(m^\circ) ; (\ni / \ni) \\ & & \qquad \text{(definitions of } \Phi \text{ (6.4) and } \sqsupseteq \text{ (3.33), and law (3.28a))} \\ & \equiv & \sqsupseteq ; \Lambda(m^\circ) \ \subseteq \ (\Lambda(m^\circ) ; \ni) / \ni \\ & & \qquad (\Lambda(m^\circ) \text{ is a map; dual of property (3.18n))} \\ & \equiv & \sqsupseteq ; \Lambda(m^\circ) ; \ni \ \subseteq \ \Lambda(m^\circ) ; \ni \qquad \text{(definition of / (3.16))} \\ & \equiv & \sqsupseteq ; m^\circ \ \subseteq \ m^\circ \qquad \text{(property of } \Lambda \text{ (3.31d))} \\ & \equiv & True. \quad \text{(converses (3.19b) and upclosure of multirelation } m) \end{array}$$

Identities are preserved by Φ, since

$$\begin{array}{lll} \Phi(\in) & = & \Lambda \ni \qquad \text{(definition of } \Phi \text{ (6.4))} \\ & = & id. \qquad \text{(property of } \Lambda \text{ (3.31h))} \end{array}$$

https://doi.org/10.1017/S0960129512000965 Published online by Cambridge University Press

Composition is preserved by Φ, since

$$\begin{aligned}
\Phi(r \fatsemi s) &= \Lambda((r \fatsemi s)^\circ) && \text{(definition of } \Phi \text{ (6.4))}\\
&= \Lambda(\ (r\ ;(\Lambda(s^\circ))^\circ)^\circ) && \text{(alternative definition of composition (4.5))}\\
&= \Lambda(\Lambda(s^\circ)\ ;r^\circ) && \text{(converse (3.19c) and (3.19a))}\\
&= \Lambda(s^\circ)\ ;\Lambda(r^\circ) && (\Lambda(s^\circ) \text{ is a map and property of } \Lambda \text{ (3.31g))}\\
&= \Phi(s)\ ;\Phi(r) && \text{(definition of } \Phi \text{ (6.4))}\\
&= \Phi(r) \circ \Phi(s). && \text{(composition in } \mathsf{Tran(A)})
\end{aligned}$$

Thus Φ is a functor. It is monotonic because

$$\begin{aligned}
\Phi(m) \leqslant \Phi(n) &\equiv \Lambda(m^\circ)\ ;\ni \subseteq \Lambda(n^\circ)\ ;\ni && \text{(definitions of } \leqslant \text{ (6.2) and } \Phi \text{ (6.4))}\\
&\equiv m^\circ \subseteq n^\circ && \text{(property of } \Lambda \text{ (3.31c))}\\
&\equiv m \subseteq n. && \text{(converse (3.19b))}
\end{aligned}$$

We still need to show that Φ is an isomorphism. Let $\Phi^{-1}(p) = (p\ ;\ni)^\circ$. We show that Φ and Φ^{-1} are mutual inverses:

$$\begin{aligned}
\Phi^{-1}(\Phi\ (m))) &= (\Lambda(m^\circ)\ ;\ni)^\circ && \text{(definitions of } \Phi \text{ (6.4) and } \Phi^{-1})\\
&= m^{\circ\circ} && \text{(property of } \Lambda \text{ (3.31c))}\\
&= m && \text{(converse (3.19a))}
\end{aligned}$$

and

$$\begin{aligned}
\Phi\,(\Phi^{-1}\ (p)) &= \Lambda((p\ ;\ni)^{\circ\circ}) && \text{(definitions of } \Phi \text{ (6.4) and } \Phi^{-1})\\
&= \Lambda(p\ ;\ni) && \text{(converse (3.19a))}\\
&= p. && \text{(property of } \Lambda \text{ (3.31f) since } p \text{ is a function arrow)}
\end{aligned}$$

Acknowledgements

We are grateful to the anonymous referees for their detailed comments, which helped to improve this paper.

References

Abramsky, S. (1991) Domain Theory in Logical Form. *Annals of Pure and Applied Logic* **51** 1–77.

Back, R. J. R. and von Wright, J. (1992) Combining angels, demons and miracles in program specifications. *Theoretical Computer Science* **100** (2) 365–383.

Back, R. J. R. and von Wright, J. (1998) *Refinement Calculus: A Systematic Introduction*, Springer-Verlag.

Backhouse, R. C., de Bruin, P., Malcolm, G. Voermans, T. S. and van der Woude, J. C. S. P. (1991) Relational catamorphisms. In: Möller, B. (ed.) *Constructing Programs from Specifications*, North-Holland 287–318.

https://doi.org/10.1017/S0960129512000965 Published online by Cambridge University Press

Barr, M. and Wells, C. (1990) *Category theory for computing science*, Prentice-Hall.
Bird, R. S. and de Moor, O. (1997) *The Algebra of Programming*, Prentice Hall.
Davey, B. A. and Priestley, H. A. (2002) *Introduction to Lattices and Order*, second edition, Cambridge University Press.
Dijkstra, E. (1975) Guarded commands, nondeterminacy and formal derivation of programs. *Communications of the ACM* **18** (8) 453–457.
de Moor, O., Gardiner, P. and Martin, C. (1991) Factorizing predicate transformers in a topos (unpublished note).
de Morgan, A. (1856) On the symbols of logic, the theory of the syllogism, and in particular of the copula, and the application of the theory of probability to some questions in the theory of evidence. *Transactions of the Cambridge Philosophical Society* **9** 79–127.
Düntsch, O., Orłowska, E. and Rewitsky, I. (2010) Structures with Multirelations, their Discrete Dualities and Applications *Fundamenta Informaticae* **100** 77–98.
Floyd, R. W. (1967) Assigning meanings to programs. *Proceedings Symposia in Applied Mathematics*, AMS **19** 19–31.
Fokkinga, M. (1994) Monadic maps and folds for arbitrary datatypes. Memoranda Informatica, Department of Computer Science, University of Twente (94-28).
Freyd, P. and Ščedrov, A. (1993) *Categories, Allegories*, Springer-Verlag.
Gardiner, P. H. B., Martin, C. E. and de Moor, O. (1994) An algebraic construction of predicate transformers. *Science of Computer Programming* **22** (1–2) 21–44.
Hoare, C. A. R. (1969) An axiomatic basis for computer programming. *Communications of the ACM* **12** (10) 576–583.
Johnstone, P. T. (2002) *Sketches of an Elephant: A Topos Theory Compendium*, Oxford University Press.
Maddux, R. D. (1996) Relation-Algebraic Semantics. *Theoretical Computer Science* **160** (1) 1–85.
Martin, C. E. (1995) Towards a calculus of predicate transformers. In: Wiedermann, J. and Hájek, P. (eds.) Mathematical Foundations of Computer Science 1995: 20th International Symposium, MFCS '95. *Springer-Verlag Lecture Notes in Computer Science* **969** 489–498.
Martin, C. E. and Curtis, S. A. (2006) Nondeterministic folds. In: Uustalu, T. (ed.) Proceedings of the 8th Mathematics of Program Construction conference. *Springer-Verlag Lecture Notes in Computer Science* **4014** 274–298.
Martin, C. E. and Curtis, S. A. (2009) Supplement to the paper 'Monadic maps and folds for multirelations in an allegory'. Available at http://cms.brookes.ac.uk/staff/SharonCurtis/publications/mf-supp.pdf.
Martin, C. E. and Curtis, S. A. (2010) Monadic maps and folds for multirelations in an allegory. In: Butterfield, A. (ed.) Unifying Theories of Programming: Second International Symposium, UTP 2008. *Springer-Verlag Lecture Notes in Computer Science* **5713** 102–121.
Martin, C. E., Curtis, S. A. and Rewitzky, I. (2007) Modelling angelic and demonic nondeterminism with multirelations. *Science of Computer Programming* **65** (2) 140–158.
Morgan, C. C. (1994) *Programming from Specifications*, second edition, Prentice-Hall.
Morgan, C. C., Gardiner, P., Vickers, T. and Robinson, K. (1994) *On the Refinement Calculus*, first edition, Springer-Verlag.
Morris, J. (1987) A theoretical basis for stepwise refinement and the programming calculus. *Science of Computer Programming* **9** 287–3067.
Morris, J. M. and Tyrrell, M. (2008a) Dually Nondeterministic functions. *ACM Transactions on Programming Languges and Systems* **30** (6).
Morris, J. M. and Tyrrell, M. (2008b) Modelling higher-order dual nondeterminacy. *Acta Informatica* **45** 441–465.

Naumann, D. A. (1998) A Categorical Model for Higher Order Imperative Programming. *Mathematical Structures in Computer Science* **8** 351–399.

Naumann, D. A. (2001) Ideal models for pointwise relational and state-free imperative programming. In: *Proceedings of the 3rd ACM SIGPLAN international conference on Principles and practice of declarative programming* 4–15.

Plotkin, G. D. (1979) Dijkstra's predicate transformers and Smyth's powerdomains. In: Bjorner, D. (ed.) Abstract Software Specifications: Proceedings 1979 Copenhagen Winter School. *Springer-Verlag Lecture Notes in Computer Science* **86** 527–553.

Rewitzky, I. (2003) Binary multirelations. In: Schmidt, G., de Swart, H., Orlowska, E. and Roubens, M. (eds.) *Theory and Application of Relational Structures as Knowledge Instruments* **2929** 259–274.

Smyth, M. B. (1983) Power Domains and Predicate Transformers: A Topological View. In: Diaz, J. (ed.) Proceedings of the 10th Colloquium on Automata, Languages and Programming. *Springer-Verlag Lecture Notes in Computer Science* **154** 662–675.

Stone, M. H. (1936) The theory of representations for Boolean algebras. *Transactions of the American Mathematical Society* **40** 37–111.

Tarski, A. (1941) On the calculus of relations. *Journal of Symbolic Logic* **6** (3) 73–89.