UTP Designs for Binary Multirelations

Pedro Ribeiro and Ana Cavalcanti

Department of Computer Science, University of York, UK
{pfr,alcc}@cs.york.ac.uk

Abstract. The total correctness of sequential computations can be established through different isomorphic models, such as monotonic predicate transformers and binary multirelations, where both angelic and demonic nondeterminism are captured. Assertional models can also be used to characterise process algebras: in Hoare and He's Unifying Theories of Programming, CSP processes can be specified as the range of a healthiness condition over designs, which are pre and postcondition pairs. In this context, we have previously developed a theory of angelic designs that is a stepping stone for the natural extension of the concept of angelic nondeterminism to the theory of CSP. In this paper we present an extended model of upward-closed binary multirelations that is isomorphic to angelic designs. This is a richer model than that of standard binary multirelations, in that we admit preconditions that rely on later or final observations as required for a treatment of processes.

Keywords: semantics, refinement, binary multirelations, UTP.

1 Introduction

In the context of sequential programs, their total correctness can be characterised through well-established models such as monotonic predicate transformers [1]. This model forms a complete lattice, where demonic choice corresponds to the greatest lower bound, while angelic choice is the least upper bound.

In [2] Rewitzky introduces the concept of binary multirelations, where the initial state of a computation is related to a set of final states. Amongst the different models studied [2,3], the theory of upward-closed binary multirelations is the most important as it has a lattice-theoretic structure. In this case, the set of final states corresponds to choices available to the angel, while those over the value of the set itself correspond to demonic choices.

The UTP of Hoare and He [4] is a predicative theory of relations suitable for the combination of refinement languages catering for different programming paradigms. In this context, the total correctness of sequential computations is characterised through the theory of designs, which are pre and postcondition pairs. Since the concept of angelic nondeterminism cannot be captured directly, binary multirelational encodings have been proposed [5,6,7].

While sequential computations can be given semantics using a relation between their initial and final state, reactive systems require a richer model that accounts

G. Ciobanu and D. Méry (Eds.): ICTAC 2014, LNCS 8687, pp. 388–405, 2014.

for the interactions with their environment. This is achieved in the UTP through the theory of reactive processes [4,8]. The combination of this theory and that of designs enables the specification of CSP processes in terms of designs that characterise the pre and postcondition of processes. We observe, however, that the theory of designs encompasses programs whose preconditions may also depend on the final or later observations of a computation. As a consequence, the general theory of designs allows these observations to be ascertained irrespective of termination. For instance, the precondition of the CSP process $a \rightarrow \mathit{Chaos}$ requires that no after observation of the trace of events is prefixed by event a.

In order to extend the concept of angelic nondeterminism to CSP, we have previously developed a theory of angelic designs. The most challenging aspect tackled pertains to the treatment of sequential composition, where it departs from the norm for UTP theories: instead of sequential composition being relational composition we have a different treatment [5] inspired on the definition of sequential composition for binary multirelations.

The main contribution of this work is a new theory of binary multirelations that caters for sets of final states where termination may not be necessarily enforced. Thus is in line with the general notion of UTP designs, with the added benefit that binary multirelations can handle both angelic and demonic nondeterminism. Our contribution is not only an extended model of upward-closed binary multirelations isomorphic to angelic designs, but also a solid basis for understanding the treatment of sequential composition in such models. To facilitate this analysis here, we also present links, Galois connections and isomorphisms, between the theories of interest. The links validate our new theory, and identify its potential role in a treatment of CSP processes.

Our long term aim is the development of a model of CSP where the angelic choice operator is a counterpart to that of the refinement calculus, that is, it avoids divergence [9]. For example, if we consider the angelic choice $a \rightarrow \mathit{Chaos} \sqcup a \rightarrow \mathit{Skip}$, then this would ideally be resolved in favour of $a \rightarrow \mathit{Skip}$. An application of this notion is found, for instance, in the context of a modelling approach for the verification of implementations of control systems [10].

The structure of this paper is as follows. In section 2 we introduce the UTP and the theories of interest. In section 3 the main contribution of this paper is discussed. In section 4 we establish the relationship between the new model and the theory of angelic designs. Finally in section 5 we present our conclusions.

2 Preliminaries

As mentioned before, the UTP is an alphabetized, predicative theory of relations suitable for modelling different programming paradigms [4]. UTP theories are characterised by three components: an alphabet, a set of healthiness conditions and a set of operators. The alphabet $\alpha(P)$ of a relation P can be split into $\mathit{in}\alpha(P)$, which contains undashed variables corresponding to the initial observations of a computation, and $\mathit{out}\alpha(P)$ containing dashed counterparts for the after or final observations. Refinement is defined as universal reverse implication.

2.1 Designs

In the UTP theory of designs [4,11] the alphabet consists of program variables and two auxiliary Boolean variables ok and ok' that record when a program starts, and when it terminates. A design is specified as follows.

Definition 1 (Design). $(P \vdash Q) \mathrel{\widehat=} (ok \land P) \Rightarrow (Q \land ok')$

P and Q are relations that together form a pre and postcondition pair, such that if the program is started, that is ok is *true*, and P is satisfied, then it establishes Q and terminates successfuly, with ok' being *true*.

A design can be expressed in this form if, and only if, it is a fixed point of the healthiness conditions **H1** and **H2** [4], whose functional composition is reproduced below, where $P^o = [o/ok']$, that is o is substituted for ok', with t corresponding to *true* and f to *false*.

Theorem 1. $\mathbf{H1} \circ \mathbf{H2}(P) = (\neg\ P^f \vdash P^t)$

The healthiness condition **H1** states that any observations can be made before a program is started, while **H2** requires that if a program may not terminate, then it must also be possible for it to terminate. In other words, it is not possible to require nontermination explicitly. The healthiness conditions of the theory are monotonic and idempotent, and so the model is a complete lattice [4].

When designs are used to model sequential computations, the precondition $\neg\ P^f$ of a design P is in fact not a relation, but rather a condition that only refers to undashed variables. Designs that observe this property are fixed points of the healthiness condition **H3**, whose definition is reproduced below [4].

Definition 2. $\mathbf{H3}(P) = P\ ;\ \mathit{I\!I}_{\mathcal{D}}$

This is a healthiness condition that requires the skip of the theory, defined below as $\mathit{I\!I}_{\mathcal{D}}$ [4,11], to be a right-unit for sequential composition.

Definition 3. $\mathit{I\!I}_{\mathcal{D}} \mathrel{\widehat=} (\mathit{true} \vdash x' = x)$

The design $\mathit{I\!I}_{\mathcal{D}}$ once started keeps the value of every program variable x unchanged and terminates successfuly. In order to discuss the consequences of designs that do not satisfy **H3**, we consider the following example.

Example 1. $(x' \neq 2 \vdash x' = 1) = ok \Rightarrow ((x' = 1 \land ok') \lor x' = 2)$

This is a design that once started can either establish the final value of the program variable x as 1 and terminate, or alternatively can establish the final value of x as 2 but then termination is not necessarily required. This is unexpected behaviour in the context of a theory for sequential programs. However, in the theory of CSP [4,8], processes are expressed as the image of non-**H3** designs through the function **R** that characterises reactive programs.

2.2 Binary Multirelations

As mentioned before, the theory of binary multirelations as introduced by Rewitzky [2] is a theory of relations between an initial state and a set of final states.

We define these relations through the following type BM, where $State$ is a type of records with a component for each program variable.

Definition 4 (Binary Multirelation). $BM \mathrel{\widehat{=}} State \leftrightarrow \mathbb{P}\, State$

For instance, the program that assigns the value 1 to the only program variable x when started from any initial state is defined as follows.

Example 2. $x :=_{BM} 1 = \{s : State, ss : \mathbb{P}\, State \mid (x \mapsto 1) \in ss\}$

Following [5], $(x \mapsto 1)$ denotes a record whose only component is x and its respective value is 1. For conciseness, in the definitions that follow, the types of s and ss may be omitted but are exactly the same as in example 2.

The target set of a binary multirelation can be interpreted as either encoding angelic or demonic choices [2,5]. We choose to present a model where the set of final states encodes angelic choices. This choice is justified in [12,5] as maintaining the refinement order of the UTP theories.

Demonic choices are encoded by the different ways in which the set of final states can be chosen. For example, the program that angelically assigns the value 1 or 2 to the only program variable x is specified by the following relation, where $\sqcup_{BM}$ is the angelic choice operator for binary multirelations.

Example 3. $x :=_{BM} 1 \sqcup_{BM} x :=_{BM} 2 = \{s, ss \mid (x \mapsto 1) \in ss \land (x \mapsto 2) \in ss\}$

This definition allows any superset of the set $\{(x \mapsto 1), (x \mapsto 2)\}$ to be chosen. The choice of values 1 and 2 for the program variable x are available in every set of final states ss, and so are available in every demonic choice.

The subset of BM of interest is that of upward-closed multirelations [2,3]. The following predicate [5] characterises this subset for a relation B.

Definition 5. $\mathbf{BMH} \mathrel{\widehat{=}} \forall\, s, ss_0, ss_1 \bullet ((s, ss_0) \in B \land ss_0 \subseteq ss_1) \Rightarrow (s, ss_1) \in B$

If a particular initial state s is related to a set of final states ss_0, then it is also related to any superset of ss_0. This means that if it is possible to terminate in some final state that is in ss_0, then the addition of any other final states to that same set does not change the final states available for angelic choice, which correspond to those in the distributed intersection of all sets of final states available for demonic choice. Alternatively, the set of healthy binary multirelations can be characterised by the fixed points of the following function.

Definition 6. $\mathbf{bmh_{up}}(B) \mathrel{\widehat{=}} \{s, ss \mid \exists\, ss_0 : \mathbb{P}\, State \bullet (s, ss_0) \in B \land ss_0 \subseteq ss\}$

This equivalence is established by the following lemma 1.

Lemma 1. $\mathbf{BMH} \Leftrightarrow \mathbf{bmh_{up}}(B) = B$

Proof of these and other results can be found in [7].

The refinement order for healthy binary multirelations B_0 and B_1 is given by subset inclusion [5], as reproduced below.

Definition 7 ($\sqsubseteq_{BM}$). $B_0 \sqsubseteq_{BM} B_1 \mathrel{\widehat{=}} B_0 \supseteq B_1$

This partial order over BM forms a complete lattice. It allows an increase in the degree of angelic nondeterminism and a decrease in demonic nondeterminism, with angelic choice as set intersection and demonic choice as set union.

For binary multirelations that are upward-closed, that is, which satisfy **BMH**, the definition of sequential composition is as follows.

Lemma 2. *Provided* B_0 *satisfies* **BMH**.

$$B_0 \mathbin{;_{BM}} B_1 = \{s_0 : State, ss : \mathbb{P}\, State \mid (s_0, \{s_1 : State \mid (s_1, ss) \in B_1\}) \in B_0\}$$

It considers every initial state s_0 in B_0 and set of final states ss of B_1, such that ss is a set that could be reached through some initial state s_1 of B_1 that is available to B_0 as a set of final states.

2.3 Angelic Designs

As discussed earlier, both angelic and demonic nondeterminism can be modelled in the UTP through a suitable encoding of multirelations. The first of these has been proposed in [5], where the alphabet consists of input program variables and a sole output variable ac', a set of final states. Those states in ac' correspond to angelic choices, while the choice over the value of ac' itself corresponds to demonic choices. Upward closure is enforced by the following healthiness condition, where v and v' refer to every variable other than ac and ac'.

Definition 8. $\mathbf{PBMH}(P) \mathrel{\widehat{=}} P \mathbin{;} ac \subseteq ac' \land v' = v$

PBMH requires that if it is possible for P to establish a set of final states ac', then any superset can also be established. (In the theory of [5], there are no other variables v', while here we consider a more general theory.)

Following the approach in [5] we have previously developed a theory of angelic designs [6]. The alphabet includes the variables ok and ok' from the theory of designs, a single input state s and a set of final states ac'. The healthiness conditions are **H1** and **H2** and **A**, whose definition is the functional composition of **A0** and **A1** as reproduced below [6].

Definition 9.

$$\mathbf{A0}(P) \mathrel{\widehat{=}} P \land ((ok \land \neg\, P^f) \Rightarrow (ok' \Rightarrow ac' \neq \emptyset))$$
$$\mathbf{A1}(P) \mathrel{\widehat{=}} (\neg\, \mathbf{PBMH}(P^f) \vdash \mathbf{PBMH}(P^t))$$
$$\mathbf{A}(P) \mathrel{\widehat{=}} \mathbf{A0} \circ \mathbf{A1}(P)$$

The healthiness condition **A0** requires that when a design terminates successfully, then there must be some final state in ac' available for angelic choice. **A1** requires that the final set of states in both the postcondition and the negation of the precondition are upward closed. We observe that **A1** can also be expressed as the application of **PBMH** to the whole of the design P.

Since all of the healthiness conditions of the theory commute, and they are all idempotent and monotonic [6], so is their functional composition. Furthermore, because the theory of designs is a complete lattice and **A** is both idempotent and monotonic, so is the theory of angelic designs.

The theory of angelic designs is based on non-homogeneous relations. As a consequence the definition of sequential composition departs from the norm for other UTP theories, where usually sequential composition is relational composition. Instead, the definition is layered upon the sequential composition operator $;_{\mathcal{A}}$ of [5], whose definition in the context of this theory, we reproduce below.

Definition 10. $P \;;_{\mathcal{A}}\; Q \mathrel{\widehat{=}} P[\{s \mid Q\}/ac']$

The resulting set of angelic choices is that of Q, such that they can be reached from an initial state of Q that is available for P as a set ac' of angelic choices. This is a result that closely resembles that for binary multirelations, except for the fact that it is expressed using substitution. In the next section, we present a set-theoretic model of binary multirelations, like that in section 2.2, but extended to cater for angelic designs.

3 Extending Binary Multirelations

Based on the theory of binary multirelations, we introduce a new type of relations $BM_\perp$ by considering a different type $State_\perp$ for the target set of states.

Definition 11. $State_\perp == State \cup \{\perp\},\ BM_\perp == State \leftrightarrow \mathbb{P}\, State_\perp$

Each initial state is related to a set of final states of type $State_\perp$, a set that may include the special state $\perp$, which denotes that termination is not guaranteed. If a set of final states does not contain $\perp$, then the program must terminate.

For example, consider the program that assigns the value 1 to the variable x, but may or may not terminate. This is specified by the following relation, where $:=_{BM_\perp}$ is the assignment operator that does not require termination.

Example 4. $x :=_{BM_\perp} 1 = \{s : State, ss : \mathbb{P}\, State_\perp \mid s \oplus (x \mapsto 1) \in ss\}$

Every initial state s is related to a set of final states ss where the state obtained from s by overriding the value of the component x with 1 is included. Since ss is of type $State_\perp$, all sets of final states in ss include those with and without $\perp$.

In the following section 3.1 we define the healthiness conditions of the new theory of binary multirelations of type $BM_\perp$. In section 3.2 we explore important properties of the new model. Finally in section 3.3 we explore the relationship between the new model and the original theory of binary multirelations.

3.1 Healthiness Conditions

Having defined a new type of relations, in what follows we introduce the healthiness conditions that characterise the relations in the theory.

BMH0. The first healthiness condition of interest enforces upward closure [2] for sets of final states that are necessarily terminating, and in addition enforces the same property for sets of final states that are not required to terminate.

Definition 12 (BMH0).

$$\begin{array}{l}\forall s : \mathit{State}, ss_0, ss_1 : \mathbb{P}\, \mathit{State}_\perp \bullet \\ ((s, ss_0) \in B \land ss_0 \subseteq ss_1 \land (\perp \in ss_0 \Leftrightarrow \perp \in ss_1)) \Rightarrow (s, ss_1) \in B\end{array}$$

It states that for every initial state s, and for every set of final states ss_0 in a relation B, any superset ss_1 of that final set of states is also associated with s as long as $\perp$ is in ss_0 if, and only if, it is in ss_1. That is, **BMH0** requires upward closure for sets of final states that terminate, and for those that may or may not terminate, but separately. The definition of **BMH0** can be split into two conjunctions as shown in the following lemma 3.

Lemma 3

$$\mathbf{BMH0} \Leftrightarrow \left(\begin{array}{l}\left(\begin{array}{l}\forall s : \mathit{State}, ss_0, ss_1 : \mathbb{P}\, \mathit{State}_\perp \bullet \\ ((s, ss_0) \in B \land ss_0 \subseteq ss_1 \land \perp \in ss_0 \land \perp \in ss_1) \Rightarrow (s, ss_1) \in B\end{array}\right) \\ \land \\ \mathbf{BMH}\end{array}\right)$$

This confirms that for sets of final states that terminate this healthiness condition enforces **BMH** exactly as in the original theory of binary multirelations [2].

BMH1. The second healthiness condition **BMH1** requires that if it is possible to choose a set of final states where termination is not guaranteed, then it must also be possible to choose an equivalent set of states where termination is guaranteed. This healthiness condition is similar in nature to **H2** of the theory of designs.

Definition 13 (BMH1)

$$\forall s : \mathit{State}, ss : \mathbb{P}\, \mathit{State}_\perp \bullet (s, ss \cup \{\perp\}) \in B \Rightarrow (s, ss) \in B$$

This healthiness condition excludes relations that only offer sets of final states that may not terminate. Consider the following example.

Example 5. $\{s : \mathit{State}, ss : \mathbb{P}\, \mathit{State}_\perp \mid (x \mapsto 1) \in ss \land \perp \in ss\}$

This relation describes an assignment to the only program variable x where termination is not guaranteed. However, it discards the inclusive situation where termination may indeed occur. The inclusion of a corresponding final set of states that requires termination does not change the choices available to the angel as it is still impossible to guarantee termination.

BMH2. The third healthiness condition reflects a redundancy in the model, namely, that both the empty set and $\{\perp\}$ characterise abortion.

Definition 14 (BMH2). $\forall s : State \bullet (s, \emptyset) \in B \Leftrightarrow (s, \{\perp\}) \in B$

Therefore we require that every initial state s is related to the empty set of final states if, and only if, it is also related to the set of final states $\{\perp\}$.

If we consider **BMH1** in isolation, it covers the reverse implication of **BMH2** because if $(s, \{\perp\})$ is in the relation, so is $(s, \emptyset)$. However, **BMH2** is stronger than **BMH1** by requiring $(s, \{\perp\})$ to be in the relation if $(s, \emptyset)$ is also in the relation. The reason for this redundancy is to facilitate the linking between theories, in particular with the original theory. We come back to this point in section 3.3.

The new model of binary multirelations is characterised by the conjunction of the healthiness conditions **BMH0**, **BMH1** and **BMH2**, which we refer to as $\mathbf{BMH_{0,1,2}}$. An alternative characterisation in terms of fixed points is available in [7]. That characterisation has enabled us, for instance, to establish that all healthiness conditions are monotonic.

BMH3. The fourth healthiness condition characterises a subset of the model that corresponds to the original theory of binary multirelations.

Definition 15 (BMH3)

$$\forall s : State \bullet (s, \emptyset) \notin B \Rightarrow (\forall ss : \mathbb{P}\, State_\perp \bullet (s, ss) \in B \Rightarrow \perp \notin ss)$$

If an initial state s is not related to the empty set, then it must be the case that for all sets of final states ss related to s, $\perp$ is not included in the set ss.

This healthiness condition excludes relations that do not guarantee termination for particular initial states, yet establish some set of final states. example 4 is an example of such a relation. This is also the case for the original theory of binary multirelations. If it is possible for a program not to terminate when started from some initial state, then execution from that state must lead to arbitrary behaviour. This is the same intuition for **H3** of the theory of designs [4].

This concludes the discussion of the healthiness conditions. The relationship with the original model of binary multirelations is discussed in section 3.3.

3.2 Operators

Having defined the healthiness conditions, in this section we introduce the most important operators of the theory. These enable the discussion of interesting properties observed in the new model.

Assignment. In this model there is in fact the possibility to define two distinct assignment operators. The first one behaves exactly as in the original theory of binary multirelations $x :=_{BM} e$. This operator does not need to be redefined, since $BM \subseteq BM_\perp$. The new operator that we define below, however, behaves rather differently, in that it may or may not terminate.

Definition 16. $x :=_{BM_\perp} e \mathrel{\widehat=} \{s : State, ss : \mathbb{P}\, State_\perp \mid s \oplus (x \mapsto e) \in ss\}$

This assignment guarantees that for every initial state s, there is some set of final states available for angelic choice where x has the value of expression e. However, termination is not guaranteed. While the angel can choose the final value of x it cannot possibly guarantee termination in this case.

Angelic Choice. Angelic choice is defined as set intersection just like in the original theory of binary multirelations.

Definition 17. $B_0 \sqcup_{BM_\perp} B_1 \mathrel{\widehat=} B_0 \cap B_1$

For every set of final states available for demonic choice in B_0 and B_1, only those that can be chosen both in B_0 and B_1 are available. As the refinement ordering in the new model is exactly the same as in the theory of binary multirelations, the angelic choice operator, being the least upper bound, has the same properties with respect to the extreme points of the lattice.

An interesting property of angelic choice that is observed in this model is illustrated by the following lemma 4. It considers the angelic choice between two assignments of the same expression, yet only one is guaranteed to terminate.

Lemma 4. $(x :=_{BM_\perp} e) \sqcup_{BM_\perp} (x :=_{BM} e) = (x :=_{BM} e)$

This result can be interpreted as follows: given an assignment which is guaranteed to terminate, adding a corresponding angelic choice that is potentially non-terminating does not in fact introduce any new choices.

Demonic Choice. The demonic choice operator is defined by set union, exactly as in the original theory of binary multirelations.

Definition 18. $B_0 \sqcap_{BM_\perp} B_1 \mathrel{\widehat=} B_0 \cup B_1$

For every initial state, a corresponding set of final states available for demonic choice in either, or both, of B_0 and B_1, is included in the result.

Similarly to the angelic choice operator, there is a general result regarding the demonic choice over the two assignment operators, terminating and not necessarily terminating. This is shown in the following lemma 5.

Lemma 5. $(x :=_{BM} e) \sqcap_{BM_\perp} (x :=_{BM_\perp} e) = (x :=_{BM_\perp} e)$

If there is an assignment for which termination is not guaranteed, then the demonic choice over this assignment and a corresponding one that is guaranteed to terminate is the same as the assignment that does not require termination. In other words, if it is possible for the demon to choose between two similar sets of final states, one that is possibly non-terminating and one that terminates, then the one for which termination is not guaranteed dominates the choice.

Sequential Composition. The definition of sequential composition in this new model is not immediately obvious. In fact, one of the reasons for developing this theory is that it provides a more intuitive approach to the definition of sequential composition in the theory of angelic designs. To illustrate the issue, we consider the following example from the theory of designs, where a non-**H3**-design is sequentially composed with $\mathit{II}_{\mathcal{D}}$, the Skip of the theory.

Example 6.

$$\begin{aligned}
&(x' = 1 \vdash \mathit{true}) \ ; \ \mathit{II}_{\mathcal{D}} && \{\text{Definition of } \mathit{II}_{\mathcal{D}}\}\\
&= (x' = 1 \vdash \mathit{true}) \ ; \ (\mathit{true} \vdash x' = x) && \{\text{Sequential composition for designs}\}\\
&= (\neg\ (x' \neq 1 \ ; \ \mathit{true}) \land \neg\ (\mathit{true} \ ; \ \mathit{false}) \vdash \mathit{true} \ ; \ x' = x) && \{\text{Sequential composition}\}\\
&= (\neg\ (\exists\, x_0 \bullet x_0 \neq 1 \land \mathit{true}) \land \neg\ (\exists\, x_0 \bullet \mathit{true} \land \mathit{false}) \vdash \exists\, x_0 \bullet \mathit{true} \land x' = x_0) &&\\
& && \{\text{Predicate calculus and one-point rule}\}\\
&= (\neg\ \mathit{true} \land \neg\ \mathit{false} \vdash \mathit{true}) && \{\text{Predicate calculus and property of designs}\}\\
&= \mathit{true}
\end{aligned}$$

The result is *true*, the bottom of designs [4], whose behaviour is arbitrary. This result can be generalised for the sequential composition of any non-**H3**-design.

The behaviour just described provides the motivation for the definition of sequential composition in the new binary multirelational model.

Definition 19

$$B_0 \ ;_{BM_\perp} \ B_1 \mathrel{\widehat{=}} \left\{ \begin{array}{l|l} \multicolumn{2}{l}{s_0 : \mathit{State}, ss_0 : \mathbb{P}\, \mathit{State}_\perp} \\ & \exists\, ss : \mathbb{P}\, \mathit{State}_\perp \bullet (s_0, ss) \in B_0 \land \\ & (\perp \in ss \lor ss \subseteq \{s_1 : \mathit{State} \mid (s_1, ss_0) \in B_1\}) \end{array} \right\}$$

For sets of final states where termination is guaranteed, that is, $\perp$ is not in the set of intermediate states ss, this definition matches that of the original theory. If $\perp$ is in ss, and hence termination is not guaranteed, then the result of the sequential composition is arbitrary as it can include any set of final states.

If we assume that B_0 is **BMH0**-healthy, then the definition of sequential composition can be split into the set union of two sets as shown in theorem 2.

Theorem 2. *Provided* B_0 *is* **BMH0**-*healthy.*

$$B_0 \ ;_{BM_\perp} \ B_1 = \left(\begin{array}{l} \{s_0, ss_0 \mid (s_0, \mathit{State}_\perp) \in B_0\} \\ \cup \\ \{s_0, ss_0 \mid (s_0, \{s_1 \mid (s_1, ss_0) \in B_1\}) \in B_0\} \end{array} \right)$$

The first set considers the case when B_0 leads to sets of final states where termination is not required ($\mathit{State}_\perp$). The second set considers the case where termination is required and matches the result of lemma 2. This concludes our discussion of the main results regarding the operators of the theory.

3.3 Relationship with Binary Multirelations

Having presented the most important operators of the theory, in this section we focus our attention on the relationship between the new model and the original theory of binary multirelations. The first step consists in the definition of a pair of linking functions, *bmb2bm* that maps from the new model into the original theory of binary multirelations, and *bm2bm*, a mapping in the opposite direction.

The relationship between the theories of interest is illustrated in fig. 1 where each theory is labelled according to its healthiness conditions. In addition to the relationship between both models of binary multirelations, fig. 1 also shows the relationship between the new model of binary multirelations and the theory of angelic designs characterised by **A**. The latter is the focus of section 4.

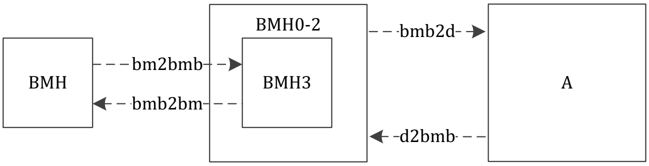

Fig. 1. Theories and links

From $BM_{\perp}$ to BM. The function *bmb2bm*, defined below, maps binary multirelations in the new model, of type $BM_{\perp}$, to those in the original model.

Definition 20 (*bmb2bm*)

$$bmb2bm : BM_{\perp} \pfun BM$$
$$bmb2bm(B) \mathrel{\widehat=} \{s : State, ss : \mathbb{P}\, State_{\perp} \mid ((s, ss) \in B \land \perp \notin ss)\}$$

It is defined by considering every pair (s, ss) in B such that $\perp$ is not in ss. We consider the following example, where *bmb2bm* is applied to the potentially non-terminating assignment of e to the program variable x.

Example 7. $bmb2bm(x :=_{BM_{\perp}} e) = (x :=_{BM} e)$

The results corresponds to assignment in the original theory. theorem 3 shows that the application of *bmb2bm* to an $\mathbf{BMH_{0,1,2,3}}$-healthy relation yields a **BMH**-healthy relation.

Theorem 3. *Provided B is $\mathbf{BMH_{0,1,2,3}}$-healthy.*

$$\mathbf{bmh_{up}} \circ bmb2bm(B) = bmb2bm(B)$$

This result confirms that *bmb2bm* yields relations that are in the original theory. The proof of this theorem and other proofs omitted below are found in [7].

From BM **to** $BM_{\perp}$**.** The function $bm2bmb$ maps from relations in the original model, of type BM, into the new theory. Its definition is presented below.

Definition 21 ($bm2bmb$)

$$bm2bmb : BM \nrightarrow BM_{\perp}$$
$$bm2bmb(B) \mathrel{\widehat{=}} \{\, s : State, ss : \mathbb{P}\, State_{\perp} \mid ((s, ss) \in B \land \perp \notin ss) \lor (s, \emptyset) \in B \,\}$$

It considers every pair (s, ss) in a relation B where $\perp$ is not in the set of final states ss, or if B is aborting for a particular initial state s, then the result is the universal relation of type $BM_{\perp}$. A similar result to theorem 3 exists for the application of $bm2bmb$ [7], where it yields $\mathbf{BMH_{0,1,2,3}}$-healthy relations.

Based on these results we can establish that $bm2bmb$ and $bmb2bm$ form a bijection for healthy relations as ascertained the following theorems 4 and 5.

Theorem 4. *Provided B is $\mathbf{BMH_{0,1,2,3}}$-healthy.* $bm2bmb \circ bmb2bm(B) = B$

Theorem 5. *Provided B is $\mathbf{BMH}$-healthy.* $bmb2bm \circ bm2bmb(B) = B$

These results show that the subset of the theory that is **BMH0-BMH3**-healthy is isomorphic to the original theory of binary multirelations [2]. This confirms that while our model is more expressive, it is still possible to express every program that could be specified using the original model. This concludes the discussion of the new theory. In the following section we discuss the relationship with the theory of angelic designs.

4 Relationship with UTP Designs

In this section we establish that the predicative model of **A**-healthy designs is isomorphic to the new theory of binary multirelations. We begin our discussion by defining a pair of linking functions: $d2bmb$, that maps from **A**-healthy designs into the new model of binary multirelations, and $bmb2d$, mapping in the opposite direction. The relationship between the theories is illustrated in fig. 1.

4.1 From Designs to Binary Multirelations

The first function of interest is $d2bmb$, whose definition is presented below.

Definition 22 (d2bmb)

$$d2bmb : \mathbf{A} \nrightarrow BM_{\perp}$$
$$d2bmb(P) \mathrel{\widehat{=}} \left\{ s : State, ss : \mathbb{P}\, State_{\perp} \;\middle|\; \begin{array}{l} ((\neg\, P^{f} \Rightarrow P^{t})[ss/ac'] \land \perp \notin ss) \\ \lor \\ (P^{f}[ss \setminus \{\perp\}/ac'] \land \perp \in ss) \end{array} \right\}$$

For a given design $P = (\neg\, P^f \vdash P^t)$, the set construction of $d2bmb(P)$ is split into two disjuncts. In the first disjunct, we consider the case where P is started and terminates successfully, with *ok* and *ok′* both being substituted with *true*. The resulting set of final states *ss*, for which termination is required ($\perp \notin ss$) is obtained by substituting *ss* for ac' in P. The second disjunct considers the case where *ok* is also *true*, but *ok′* is *false*. This corresponds to the situation where P does not terminate. In this case, the set of final states is obtained by substituting $ss \setminus \{\perp\}$ for ac' and requiring $\perp$ to be in the set of final states *ss*.

As a consequence of P satisfying **H2**, we ensure that if there is some set of final states captured by the second disjunct with $\perp$, then there is also a corresponding set of final states without $\perp$ that is captured by the first disjunct.

In order to illustrate the result of applying *d2bmb*, we consider the following example 8. It specifies a program that either assigns the value 1 to the sole program variable x and successfully terminates, or assigns the value 2 to x, in which case termination is not required.

Example 8

$$d2bmb((x \mapsto 2) \notin ac' \vdash (x \mapsto 1) \in ac') \qquad \{\text{Definition of } d2bmb \text{ and designs}\}$$

$$= \left\{\begin{array}{l} s : State, ss : \mathbb{P}\, State_{\perp} \\ \mid ((x \mapsto 2) \notin ac' \Rightarrow (x \mapsto 1) \in ac')[ss/ac'] \land \perp \notin ss) \\ \mid \lor \\ \mid (((x \mapsto 2) \in ac')[ss \setminus \{\perp\}/ac'] \land \perp \in ss) \end{array}\right\}$$

$$\{\text{Predicate calculus and substitution}\}$$

$$= \left\{\begin{array}{l} s : State, ss : \mathbb{P}\, State_{\perp} \\ \mid ((x \mapsto 2) \in ss \land \perp \notin ss) \lor ((x \mapsto 1) \in ss \land \perp \notin ss) \\ \mid \lor \\ \mid ((x \mapsto 2) \in (ss \setminus \{\perp\}) \land \perp \in ss) \end{array}\right\}$$

$$\{\text{Property of sets and predicate calculus}\}$$

$$= \{s : State, ss : \mathbb{P}\, State_{\perp} \mid (x \mapsto 2) \in ss \lor ((x \mapsto 1) \in ss \land \perp \notin ss)\}$$

$$\{\text{Definition of } \sqcap_{BM_{\perp}} \text{ and } :=_{BM_{\perp}} \text{ and } :=_{BM}\}$$

$$= (x :=_{BM_{\perp}} 2) \sqcap_{BM_{\perp}} (x :=_{BM} 1)$$

The function *d2bmb* yields a program with the same behaviour, but specified using the binary multirelational model. It is the demonic choice over two assignments, one requires termination while the other does not.

The following theorem 6 establishes that the application of *d2bmb* to **A**-healthy designs yields relations that are **BMH0**-**BMH2**-healthy.

Theorem 6. $\mathbf{bmh_{0,1,2}} \circ d2bmb(\mathbf{A}(P)) = d2bmb(\mathbf{A}(P))$

This concludes our discussion regarding the linking function *d2bmb*.

4.2 From Binary Multirelations to Designs

The second linking function of interest is *bmb2d*, which maps binary multirelations to **A**-healthy predicates. Its definition is presented below.

Definition 23 (*bmb*2*d*)

$$bmb2d : BM_{\perp} \rightarrow\!\!\!\!\!+ \mathbf{A} \qquad bmb2d(B) \mathrel{\widehat=} ((s, ac' \cup \{\perp\}) \notin B \vdash (s, ac') \in B)$$

It is defined as a design, such that for a particular initial state s, the precondition requires $(s, ac' \cup \{\perp\})$ not to be in B, while the postcondition establishes that (s, ac') is in B. This definition can be expanded into a more intuitive representation, by expanding the design, according to the following lemma 6.

Lemma 6. $bmb2d(B) = ok \Rightarrow \begin{pmatrix} ((s, ac') \in B \land \perp \notin ac' \land ok') \\ \lor \\ (s, ac' \cup \{\perp\}) \in B \end{pmatrix}$

The behaviour of *bmb*2*d* is defined by two disjuncts. The first one considers the case where B requires termination, and hence $\perp$ is not part of the set of final states of the pair in B. The second disjunct considers sets of final states that do not require termination, in which case ok' can be either *true* or *false*.

The following theorem 7 establishes that $bmb2d(B)$ yields **A**-healthy designs provided that B is **BMH0**-**BMH2**-healthy.

Theorem 7. *Provided B is* $\mathbf{BMH_{0,1,2}}$*-healthy.* $\mathbf{A} \circ bmb2d(B) = bmb2d(B)$

This result confirms that *bmb*2*d* is closed with respect to **A** when applied to relations that are **BMH0**-**BMH2**-healthy. This concludes our discussion of *bmb*2*d*. In the following section 4.3 we focus our attention on the isomorphism.

4.3 Isomorphism

In this section we show that *d*2*bmb* and *bmb*2*d* form a bijection. The following theorem 8 establishes that *d*2*bmb* is the inverse function of *bmb*2*d* for relations that are **BMH0**-**BMH2**-healthy. While theorem 9 establishes that *bmb*2*d* is the inverse function of *d*2*bmb* for designs that are **A**-healthy. Together these results establish that the models are isomorphic.

Theorem 8. *Provided B is* **BMH0**-**BMH2***-healthy.* $d2bmb \circ bmb2d(B) = B$

Theorem 9. *Provided P is* **A***-healthy.* $bmb2d \circ d2bmb(P) = P$

These results establish that the same programs can be characterised using two different approaches. The binary multirelational model provides a set-theoretic approach, while the predicative theory proposed can easily be linked with other UTP theories of interest. This dual approach enables us to justify the definitions of certain aspects of the theory. This includes the healthiness conditions, and the operators, which we discuss in the following section 4.4. The most intuitive and appropriate model can be used in each case. The results obtained in either model can then be related using the linking functions.

4.4 Linking Results

In this section we discuss the most important results obtained from linking both the theory of angelic designs and the new model of binary multirelations.

Refinement. As discussed earlier, the theory of angelic designs [6] is a complete lattice under the refinement ordering, here denoted by $\sqsubseteq_{\mathcal{D}}$, which is universal reverse implication. In the theory of binary multirelations, refinement is subset inclusion, as denoted by $\sqsubseteq_{BM_\perp}$. theorem 10 establishes their correspondence.

Theorem 10. *Provided* B_0 *and* B_1 *are* **BMH0**-**BMH2**-*healthy.*

$$bmb2d(B_0) \sqsubseteq_{\mathcal{D}} bmb2d(B_1) \Leftrightarrow B_0 \sqsubseteq_{BM_\perp} B_1$$

It is reassuring to find that the refinement ordering of the theory of angelic designs corresponds to the subset ordering in the binary multirelational model.

Sequential Composition. Amongst the operators discussed in the context of the theories of interest, sequential composition is, perhaps, the most challenging. In the new model of binary multirelations, this is due to the addition of potential non-termination, while in the theory of angelic designs, the difficulty pertains to the use of non-homogenenous relations and the definition of $;_{\mathcal{A}}$.

In the theory of angelic designs, sequential composition is defined as follows.

Definition 24. $P \;;_{\mathcal{D}\mathbf{ac}}\; Q \mathrel{\widehat=} \exists\, ok_0 \bullet P[ok_0/ok'] \;;_{\mathcal{A}}\; Q[ok_0/ok]$

As discussed earlier, this is a definition that is layered upon $;_{\mathcal{A}}$ [6]. It resembles relational composition, with the notable difference that instead of conjunction we use the operator $;_{\mathcal{A}}$. When considering **A**-healthy designs, sequential composition can be expressed as an **A**-healthy design as established by theorem 11.

Theorem 11. *Provided* P *and* Q *are* **A**-*healthy designs.*

$$P \;;_{\mathcal{D}\mathbf{ac}}\; Q = (\neg\,(P^f \;;_{\mathcal{A}}\; true) \land \neg\,(P^t \;;_{\mathcal{A}}\; Q^f) \vdash P^t \;;_{\mathcal{A}}\; (\neg\, Q^f \Rightarrow Q^t))$$

This is a result similar to the one for designs [4,11], except for the use of the operator $;_{\mathcal{A}}$ and the postcondition, which is different. The implication in the postcondition acts as a filter that eliminates final states of P that fail to satisfy the precondition of Q. We consider the following example, where there is an angelic choice between assigning 1 and 2 to the only program variable b, followed by the program that maintains the state unchanged provided b is 1.

Example 9.

$$\begin{pmatrix} (true \vdash \{b \mapsto 1\} \in ac') \\ \sqcup \\ (true \vdash \{b \mapsto 2\} \in ac') \end{pmatrix} ;_{\mathcal{D}\mathbf{ac}} (s.b = 1 \vdash s \in ac') = (true \vdash \{b \mapsto 1\} \in ac')$$

The angelic choice is resolved as the assignment of 1 to b, which avoids aborting.

Finally, we have established through theorem 12 that the sequential composition operators of our theories are in correspondence.

Theorem 12. *Provided* P *and* Q *are* **A**-*healthy designs.*

$$bmb2d(d2bmb(P) \;;_{BM_\perp}\; d2bmb(Q)) = P \;;_{\mathcal{D}\mathbf{ac}}\; Q$$

This is a reassuring result that provides a dual characterisation for the sequential composition of angelic designs, both in a predicative model and in terms of sets.

Demonic Choice. The demonic choice operator of angelic designs ($\sqcap_{\mathcal{D}\mathbf{ac}}$) defined as disjunction, corresponds exactly to the demonic choice operator ($\sqcap_{BM_\perp}$) of the binary multirelational model, defined as set union.

Theorem 13. $bmb2p(B_0 \sqcap_{BM_\perp} B_1) = bmb2p(B_0) \sqcap_{\mathcal{D}\mathbf{ac}} bmb2p(B_1)$

This result confirms the correspondence of demonic choice in both models.

Angelic Choice. Similarly, the angelic choice operator ($\sqcup_{\mathcal{D}\mathbf{ac}}$), defined as conjunction, is in correspondence with that of binary multirelations, ($\sqcup_{BM_\perp}$) which is defined as set intersection.

Theorem 14. $bmb2p(B_0 \sqcup_{BM_\perp} B_1) = bmb2p(B_0) \sqcup_{\mathcal{D}\mathbf{ac}} bmb2p(B_1)$

Proof.

$bmb2p(B_0) \sqcup_{\mathcal{D}\mathbf{ac}} bmb2p(B_1)$ {Definition of $bmb2p$}

$$= \left(\begin{array}{l} ((s, ac' \cup \{\perp\}) \notin B_0 \lor \perp \in ac' \vdash (s, ac') \in B_0 \land \perp \notin ac') \\ \sqcup_{\mathcal{D}\mathbf{ac}} \\ ((s, ac' \cup \{\perp\}) \notin B_1 \lor \perp \in ac' \vdash (s, ac') \in B_1 \land \perp \notin ac') \end{array}\right)$$

{Definition of $\sqcup_{\mathcal{D}\mathbf{ac}}$}

$$= \left(\begin{array}{l} ((s, ac' \cup \{\perp\}) \notin B_0 \lor \perp \in ac' \lor (s, ac' \cup \{\perp\}) \notin B_1 \lor \perp \in ac') \\ \vdash \\ \left(\begin{array}{l} ((s, ac' \cup \{\perp\}) \notin B_0 \lor \perp \in ac') \Rightarrow ((s, ac') \in B_0 \land \perp \notin ac') \\ \land \\ ((s, ac' \cup \{\perp\}) \notin B_1 \lor \perp \in ac') \Rightarrow ((s, ac') \in B_1 \land \perp \notin ac') \end{array}\right) \end{array}\right)$$

{Predicate calculus}

$$= \left(\begin{array}{l} ((s, ac' \cup \{\perp\}) \notin B_0 \lor \perp \in ac' \lor (s, ac' \cup \{\perp\}) \notin B_1) \\ \vdash \\ \left(\begin{array}{l} ((s, ac' \cup \{\perp\}) \in B_0 \lor (s, ac') \in B_0) \\ \land \\ ((s, ac' \cup \{\perp\}) \in B_1 \lor (s, ac') \in B_1) \end{array}\right) \land \perp \notin ac' \end{array}\right)$$

{Assumption: B_0 and B_1 are **BMH1**-healthy}

$$= \left(\begin{array}{l} ((s, ac' \cup \{\perp\}) \notin B_0 \lor \perp \in ac' \lor (s, ac' \cup \{\perp\}) \notin B_1) \\ \vdash \\ \left(\begin{array}{l} (((s, ac' \cup \{\perp\}) \in B_0 \land (s, ac') \in B_0) \lor (s, ac') \in B_0) \\ \land \\ (((s, ac' \cup \{\perp\}) \in B_1 \land (s, ac') \in B_1) \lor (s, ac') \in B_1) \end{array}\right) \land \perp \notin ac' \end{array}\right)$$

{Predicate calculus: absorption law}

$$= \left(\begin{array}{l} ((s, ac' \cup \{\perp\}) \notin B_0 \lor \perp \in ac' \lor (s, ac' \cup \{\perp\}) \notin B_1) \\ \vdash \\ (s, ac') \in B_0 \land (s, ac') \in B_1 \land \perp \notin ac' \end{array}\right)$$

{Predicate calculus and property of sets}

$= ((s, ac' \cup \{\perp\}) \notin (B_0 \cap B_1) \lor \perp \in ac' \vdash (s, ac') \in (B_0 \cap B_1) \land \perp \notin ac')$

{Definition of $bmb2p$ and $\sqcup_{BM_\perp}$}

$= bmb2p(B_0 \sqcup_{BM_\perp} B_1)$ □

In [7] we have established a number of other properties regarding the angelic choice operator and sequential composition, namely that sequential composition does not, in general, distribute through angelic choice from neither the left nor the right, and that angelic and demonic choice distribute through one another. The latter follows directly from the properties of sets and the characterisation of angelic and demonic choice in the binary multirelational model.

5 Conclusion

Angelic nondeterminism has traditionally been considered in the context of theories of total correctness for sequential computations. Amongst these, isomorphic models include the universal monotonic predicate transformers of the refinement calculus [1,13,14], and binary multirelations [2], where both angelic and demonic nondeterminism are captured. The corresponding characterisation in a relational setting, such as the UTP, has been achieved via multirelational encodings [5,6].

Morris and Tyrrel [15,16], and Hesselink [17], have considered angelic nondeterminism in the context of functional languages, by characterising it at the expression or term level. A generalised algebraic structure has been proposed by Guttmann [18], where both the monotonic predicate transformers and multirelations are characterised as instances.

Tyrrell et al. [19] have proposed an axiomatized algebra of processes resembling CSP where external choice is angelic choice, however, in their model deadlock is indistinguishable from divergence. Roscoe [20] has proposed an angelic choice operator in the context of an operational combinator semantics for CSP. However, its semantics is far from being a counterpart to the angelic choice operator of the refinement calculus, where, if possible, abortion can be avoided.

The theory that we have introduced here presents itself as a natural extension of Rewitzky's [2] binary multirelations, by including information pertaining to the possibility for non-termination. This is a concept found in the general theory of UTP designs, where preconditions can refer to the value of later or final states, an essential property for the characterisation of CSP processes.

The development of links between the new theory and angelic designs provides two complementary views of the same computations. This dual approach has enabled us to characterise certain aspects more easily by choosing the most appropriate model. It is reassuring that the healthiness conditions and operators of both models are in correspondence. Our long term aim is the definition of a UTP theory of CSP that includes all standard CSP operators, and, additionally, an angelic choice operator that avoids divergence.

References

1. Back, R., Wright, J.: Refinement calculus: a systematic introduction. Graduate texts in computer science. Springer (1998)
2. Rewitzky, I.: Binary Multirelations. In: de Swart, H., Orłowska, E., Schmidt, G., Roubens, M. (eds.) Theory and Applications of Relational Structures as Knowledge Instruments. LNCS, vol. 2929, pp. 256–271. Springer, Heidelberg (2003)

3. Martin, C.E., Curtis, S.A., Rewitzky, I.: Modelling Nondeterminism. In: Kozen, D. (ed.) MPC 2004. LNCS, vol. 3125, pp. 228–251. Springer, Heidelberg (2004)
4. Hoare, C.A.R., Jifeng, H.: Unifying Theories of Programming. Prentice Hall International Series in Computer Science (1998)
5. Cavalcanti, A., Woodcock, J., Dunne, S.: Angelic nondeterminism in the unifying theories of programming. Formal Aspects of Computing 18, 288–307 (2006)
6. Ribeiro, P., Cavalcanti, A.: Designs with Angelic Nondeterminism. In: 2013 International Symposium on Theoretical Aspects of Software Engineering (TASE), pp. 71–78 (2013)
7. Ribeiro, P.: Designs with Angelic Nondeterminism. Technical report, University of York (February 2013), `http://www-users.cs.york.ac.uk/pfr/reports/dac.pdf`
8. Cavalcanti, A., Woodcock, J.: A Tutorial Introduction to CSP in *Unifying Theories of Programming*. In: Cavalcanti, A., Sampaio, A., Woodcock, J. (eds.) PSSE 2004. LNCS, vol. 3167, pp. 220–268. Springer, Heidelberg (2006)
9. Ribeiro, P., Cavalcanti, A.: Angelicism in the Theory of Reactive Processes. In: Unifying Theories of Programming (to appear, 2014)
10. Cavalcanti, A., Mota, A., Woodcock, J.: Simulink Timed Models for Program Verification. In: Liu, Z., Woodcock, J., Zhu, H. (eds.) Theories of Programming and Formal Methods. LNCS, vol. 8051, pp. 82–99. Springer, Heidelberg (2013)
11. Woodcock, J., Cavalcanti, A.: A Tutorial Introduction to Designs in Unifying Theories of Programming. In: Boiten, E.A., Derrick, J., Smith, G.P. (eds.) IFM 2004. LNCS, vol. 2999, pp. 40–66. Springer, Heidelberg (2004)
12. Cavalcanti, A., Woodcock, J.: Angelic Nondeterminism and Unifying Theories of Programming. Technical report, University of Kent (2004)
13. Morgan, C.: Programming from specifications. Prentice Hall (1994)
14. Morris, J.M.: A theoretical basis for stepwise refinement and the programming calculus. Sci. Comput. Program. 9, 287–306 (1987)
15. Morris, J.M.: Augmenting Types with Unbounded Demonic and Angelic Nondeterminacy. In: Kozen, D. (ed.) MPC 2004. LNCS, vol. 3125, pp. 274–288. Springer, Heidelberg (2004)
16. Morris, J.M., Tyrrell, M.: Terms with unbounded demonic and angelic nondeterminacy. Science of Computer Programming 65(2), 159–172 (2007)
17. Hesselink, W.H.: Alternating states for dual nondeterminism in imperative programming. Theoretical Computer Science 411(22-24), 2317–2330 (2010)
18. Guttmann, W.: Algebras for correctness of sequential computations. Science of Computer Programming 85(Pt. B), 224–240 (2014); Special Issue on Mathematics of Program Construction (2012)
19. Tyrrell, M., Morris, J.M., Butterfield, A., Hughes, A.: A Lattice-Theoretic Model for an Algebra of Communicating Sequential Processes. In: Barkaoui, K., Cavalcanti, A., Cerone, A. (eds.) ICTAC 2006. LNCS, vol. 4281, pp. 123–137. Springer, Heidelberg (2006)
20. Roscoe, A.W.: Understanding concurrent systems. Springer (2010)