Angelic Nondeterminism and UTP

Ana Cavalcanti (University of York, England)

RefineNet meeting, January 2005

Contents

- Angelic Nondeterminism
- *Circus*
- Unifying Theories of Programming (UTP)
- The problem: no angelic nondeterminism
- Set-based model for UTP
- Predicate transformers model for UTP
- Relational model for angelic and demonic nondeterminism
- Binary multirelations as predicates
- Conclusions

Angelic Nondeterminism

- Program development techniques:
  - Demonic choice: abstraction

$$x := -1 \sqcap x := 1$$

  - Angelic choice: guarantees success

$$(\, x := -1 \sqcup x := 1 \,) \;;\;\; (\, x > 0 \vdash x' = x + 1)$$

- Semantics: least upper bound in the lattice of monotonic predicate transformers
- Programming: backtracking in concurrent constraint programming

Angelic Nondeterminism

- Morgan's refinement calculus: logical constants
  - Initial variables

$$x : [\, true, x = x_0 + 1 \,]$$

$$[\![\mathbf{con}\ X \bullet x : [x = X, x = X + 1]]\!]$$

  - Important for development of sequences
  - Important for certain loop invariants

Angelic Nondeterminism

- Calculational data refinement rules

$$b : [pre, post] \preceq [\![\mathbf{con}\ a, b \bullet c : [\, CI \wedge pre, (\exists\, b \bullet AI \wedge post)\,]\,]\!]$$

- Back's work
  - System-user interactions
  - Game-like situations

Circus

- Combination of Z and CSP
- ZRC: refinement calculus for Z in the style of Morgan
- Semantic model: unifying theories of programming
  - Integrated model of state and reactive behaviour
  - No logical constants

Unifying Theories of Programming (UTP)

- Alphabetised relational model
- Relations are defined as pairs

$$(\alpha P, P)$$

- αP: alphabet of observational variables
- P: predicate over observational variables
- Example: $(\{\, x, x', y, y' \,\}, x' = x + 1 \wedge y' = y)$

Relations in the UTP

- Assignment: $x := e \mathrel{\widehat{=}} (x' = e \wedge y' = y \wedge \ldots \wedge z' = z)$
- Skip: $I\!I \mathrel{\widehat{=}} (v' = v)$
- Sequence: $P(v');\ Q(v) \mathrel{\widehat{=}} \exists\, v_0 \bullet P(v_0) \wedge Q(v_0)$
  provided $out\alpha P = in\alpha'(Q) = \{v'\}$
- Nondeterminism (demonic): $P \sqcap Q \mathrel{\widehat{=}} P \vee Q$

The set of relations is a complete lattice

- Ordering: $\Leftarrow$
- Least Upper Bound: $[P \Leftarrow \sqcap S]$ **iff** ($[P \Leftarrow X]$ for all X in S)
- Abort: $\bot \mathrel{\widehat{=}} \textbf{true}$
- Recursion $\mu X \bullet F(X)$: least fixed point
- Infelicity: $((\mu X \bullet X);\ x' = 3) \ = \ (x' = 3)$

Designs

- Extra observational variables: ok and ok'.
- $(P \vdash Q) \mathrel{\widehat{=}} (ok \wedge P) \Rightarrow (ok' \wedge Q)$

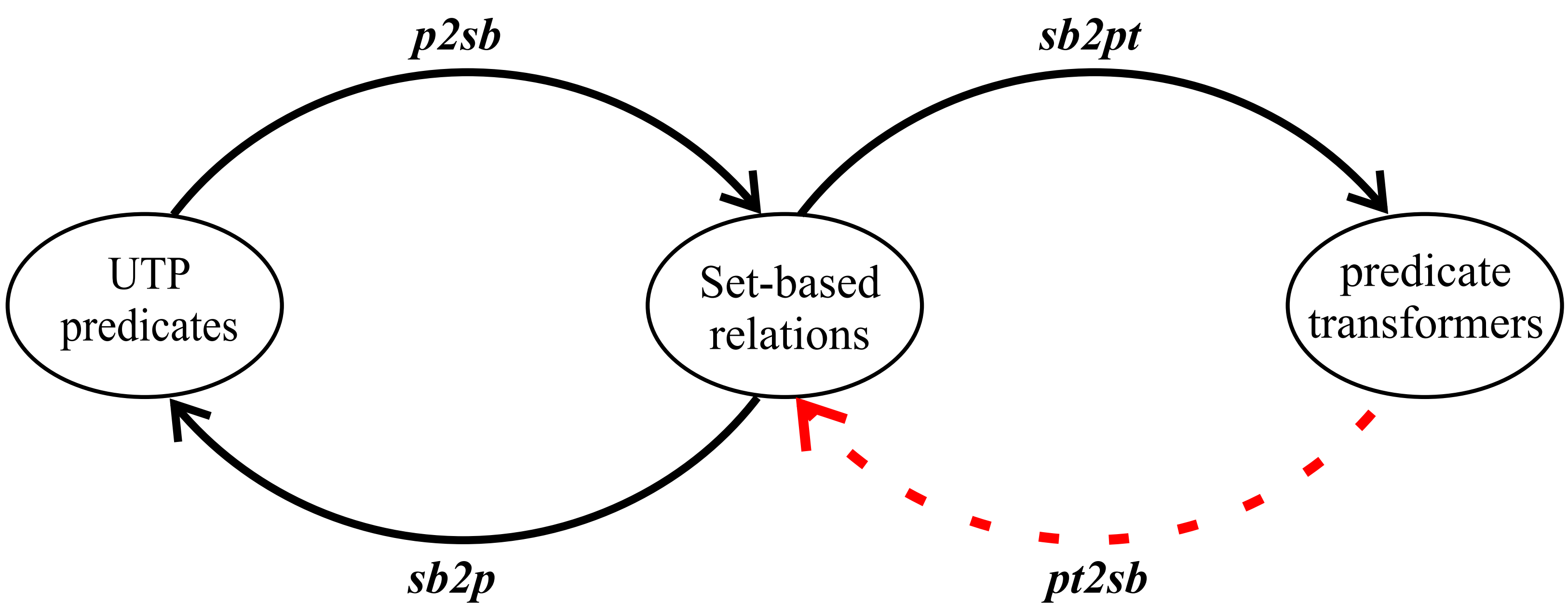
$$(x > 0 \vdash x' = x + 1) = (ok \wedge x > 0 \Rightarrow ok' \wedge x' = x + 1)$$

- Assignment and skip are redefined as designs.
- All predicates expressible as programs are designs.

Healthiness conditions

H1	$R = (ok \Rightarrow R)$	No predictions before startup
H2	$[R[false/ok'] \Rightarrow R[true/ok']]$	Non-termination is not required
H3	$R = R;\ \mathit{\Pi}$	Preconditions do not use dashes
H4	$R;\ \mathbf{true} = \mathbf{true}$	Feasibility

The problem: no angelic nondeterminism



Set-based model for UTP

State

- Record that assigns a value to each observational variable
- For an alphabet A

  S_A: set of records with a component for variable in A.

Set-based relation

Pair

$$(\alpha R, R)$$

where

- αR is the alphabet
- $R : S_{in\alpha R} \leftrightarrow S_{out\alpha R}$

Set-based relation

- Example: $x := 3$ with alphabet $\{\, x, y, x', y' \,\}$

$$\{\, s : S_{\{\, x, y \,\}};\ s' : S_{\{\, x', y' \,\}} \mid s'.x' = 3 \wedge s'.y' = s.y \,\}$$

- Partiality: miracle
- Non-termination is not captured

Isomorphism between UTP and set-based relations

$$p2sb.P \mathrel{\widehat{=}} \{s : S_{in\alpha P};\ s' : S_{out\alpha P} \mid P[s, s'/in\alpha P, out\alpha P]\})$$

$$sb2p.R \mathrel{\widehat{=}}$$
$$\exists\, s_1, s_2 \bullet (s_1, s_2) \in R \wedge (\bigwedge x : in\alpha R \bullet x = s_1.x) \wedge (\bigwedge x : out\alpha R \bullet x = s_2.x)$$

Conclusion: relations cannot handle non-termination properly.

Paradox?

- With alphabet $\{ x, x' \}$, $(\mu X \bullet X);\ x := 3 \ = \ x := 3$
- Question: is this really a problem?
  - We have a model of terminating programs
  - $\bot$ is **choose**.
- Strongest fixed point: a red herring
- Studying the set-based model can be illuminating

Healthy set-based relations

$$\{ok, ok'\} \subseteq \alpha R$$

SBH1 $\forall\, s, s' \mid s.ok = \mathit{false} \bullet (s, s') \in R$

SBH2 $\forall\, s, s' \mid s'.ok' = \mathit{false} \land (s, s') \in R \bullet (s, s' \oplus \{ok' \mapsto \mathit{true}\}) \in R$

SBH3 $\forall\, s \mid (\exists\, s' \bullet s'.ok' = \mathit{false} \land (s, s') \in R) \bullet (\forall\, s' \bullet (s, s') \in R)$

Healthiness conditions (continued)

For every UTP relation $(\alpha P, P)$ that satisfies **Hi**, $p2sb.(\alpha P, P)$ satisfies **SBHi**.

Conversely, for every set-based relation $(\alpha R, R)$ that satisfies **SBHi**, $sb2p.(\alpha R, R)$ satisfies **Hi**.

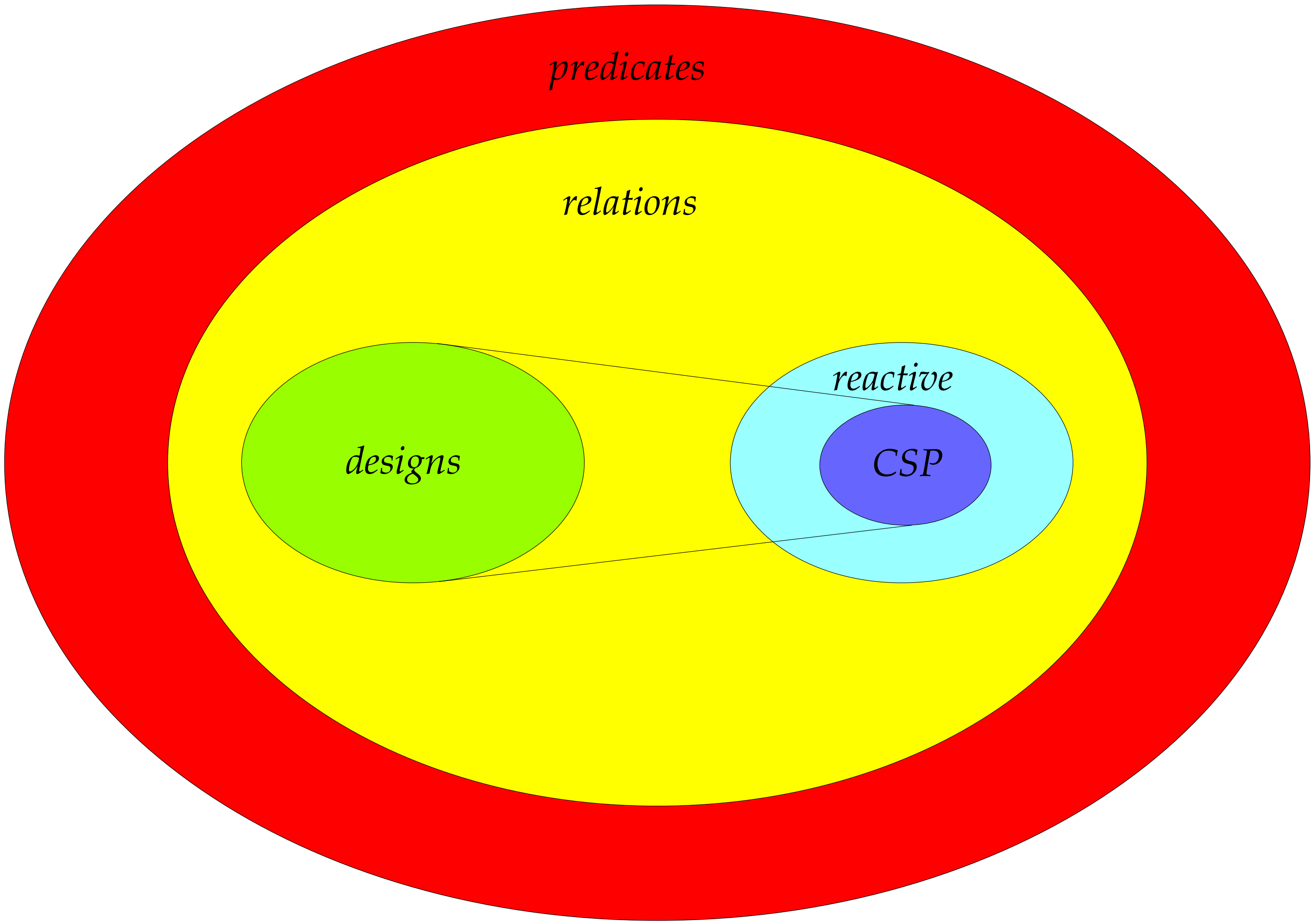
Healthiness conditions (continued)

- Surprise: **H3** implies **H2**.
- Feasibility should not be of paramount concern
- Non-**H3** designs, however, can be as follows.

$$(x' \neq 2 \vdash \mathbf{true}) = (ok \Rightarrow x' = 2 \vee ok')$$

- Are these designs relevant for the modelling of other paradigms???

Healthiness conditions (continued)



Predicate transformers model for UTP

Pair

$$(\alpha PT, PT)$$

where

- αPT is the alphabet
- PT: monotonic total function from $\mathbb{P}\, S_{out\alpha PT}$ to $\mathbb{P}\, S_{in\alpha PT}$

Theorem There is an isomorphism between universally conjunctive predicate transformers and set-based relations.

Isomorphism between predicate transformers and set-based relations

$$sb2pt.R.\psi \mathrel{\widehat{=}} \overline{\mathrm{dom}(R \rhd \psi)}$$

$$pt2sb.PT \mathrel{\widehat{=}} \{s : S_{in\alpha PT};\ s' : S_{out\alpha PT} \mid s \in \overline{PT.\overline{\{s'\}}}\}$$

Theorem *sb2pt* and *pt2sb* establish an isomorphism between universally conjunctive predicate transformers and set-based relations.

Angelic nondeterminism out!

Angelic nondeterminism, as modelled in the lattice of monotonic predicate transformers, cannot be modelled in our space of universally conjunctive predicate transformers, as joins are not preserved. (Back and von Wright, 1992)

Universal conjunctivity

- Standard predicate transformers: universal conjunctivity implies termination

$$PT.true = true$$

- In the framework of designs
  - Postcondition *true* is $S_{out\alpha PT}$: stop or not, and do anything.
  - Precondition *true* is $S_{in\alpha PT}$: it is not even needed to start.
- Conjunctivity is still an issue

Relational model for angelic and demonic nondeterminism

- Binary multirelations: I. Rewtizky, 2003
- Similar to Back's choice semantics

Pair

$$(\alpha BM, BM)$$

where

- αR is the alphabet
- $R : S_{in\alpha BM} \leftrightarrow \mathbb{P}\, S_{out\alpha BM}$

Binary multirelations: Nondeterminism

- Range: sets of demonic choices (postconditions)
- Different sets: angelic choices of demonic choices

Healthiness condition

BMH $\quad \forall\, s, \psi_1, \psi_2 \mid (s, \psi_1) \in BM \wedge \psi_1 \subseteq \psi_2 \bullet (s, \psi_2) \in BM$

Examples

- Abort

$$\emptyset$$

- Miracle

$$S_{in\alpha BM} \leftrightarrow \mathbb{P}\, S_{out\alpha BM}$$

- $x := e$

$$\{\, s, ss' \mid \{\, [s]' \oplus \{x' \mapsto e\} \,\} \subseteq ss' \,\}$$

Examples

- $x := 0 \sqcup x := 1$

$$\{\, s, \psi \mid \{\, (x' \mapsto 0) \,\} \subseteq \psi \vee \{\, (x' \mapsto 1) \,\} \subseteq \psi \,\}$$

- $x := 0 \sqcap x := 1$

$$\{\, s, \psi \mid \{\, (x' \mapsto 0), (x' \mapsto 1) \,\} \subseteq \psi \,\}$$

- $x := 0 \sqcap (x := 1 \sqcup x := 2)$

$$\{\, s, \psi \mid \{\, (x' \mapsto 0), (x' \mapsto 1) \,\} \subseteq \psi \vee \{\, (x' \mapsto 0), (x' \mapsto 2) \,\} \subseteq \psi \,\}$$

Isomorphism

$$bm2pt.BM.\psi = \{\, s \mid (s,\psi) \in BM \,\}$$

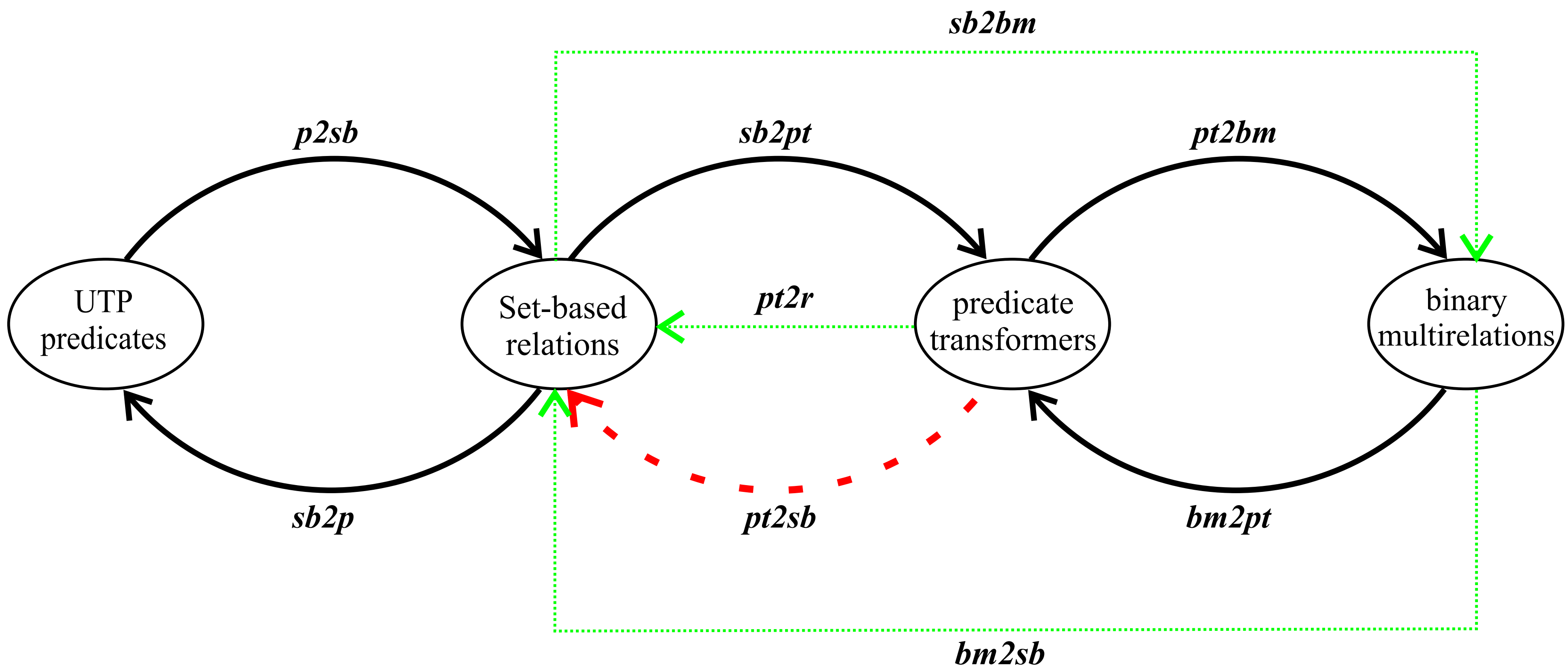
$$pt2bm.PT = \{\, (s,\psi) \mid s \in PT.\psi \,\}$$

- Correspondence between predicate transformers and binary multirelations
- Monotonic predicate transformers correspond to healthy binary multirelations

Binary multirelations as predicates

- Alphabet: $in\alpha \cup \{\, dc' \}$
- dc'
  - set of demonic choices available
  - set of states on an alphabet $out\alpha$
- Designs: v, ok, and dc', a set of states on v' and ok'

Binary multirelations as predicates



Binary multirelations as predicates

$$bm2sb.BM = \{ s : S_{in\alpha};\ s' : S_{\{dc'\}} \mid (s, s'.dc') \in BM \}$$

$$sb2bm.DCR = \{ s : S_{in\alpha};\ ss : \mathbb{P}\, S_{out\alpha} \mid (s, (dc' \mapsto ss)) \in DCR \}$$

$$pt2r \mathrel{\widehat{=}} bm2sb \circ pt2bm$$

$$pt2r.PT = \{ s : S_{in\alpha};\ s' : S_{\{dc'\}} \mid s \in PT.(s'.dc') \}$$

Binary multirelations as predicates: example

$$\boxed{sb2p.(pt2r.abort) = \mathbf{false}}$$

$$sb2p.(pt2r.abort) \qquad \text{[definition of } pt2r\text{]}$$

$$= sb2p.\{\, s, s' \mid s \in abort.(s'.dc') \,\} \qquad \text{[definition of } abort\text{]}$$

$$= sb2p.\emptyset \qquad \text{[definition of } sb2p\text{]}$$

$$= \exists\, s, s' \bullet (s, s') \in \emptyset \wedge (\bigwedge x : in\alpha \bullet x = s.x) \wedge dc' = s'.dc'$$

$$= false$$

Binary multirelations as predicates: healthiness condition

PBMH $\quad P;\ dc \subseteq dc' = P$

If BM is BMH-healthy, then $sb2p.(bm2sb.BM)$is PBMH-healthy.

If P is a PBMH-healthy predicate, then $sb2bm.(p2sb.P)$ is BMH-healthy.

Binary multirelations as predicates: refinement

$$\boxed{P \sqsubseteq_A Q \mathrel{\widehat{=}} [\, P \Rightarrow Q \,]}$$

$P \sqsubseteq_A Q$ if, and only if, $sb2bm.(p2sb.P) \sqsubseteq_{BM} sb2bm(p2sb.Q)$

Binary multirelations: refinement

$$\boxed{BM_1 \sqsubseteq_{BM} BM_2 \mathrel{\widehat{=}} BM_1 \subseteq BM_2}$$

$BM_1 \sqsubseteq_{BM} BM_2$ if, and only if, $bm2pt.BM_1 \sqsubseteq_{PT} bm2pt.BM_2$

Simplification of

$$\boxed{BM_1 \sqsubseteq_{PO} BM_2 \mathrel{\widehat{=}} \forall\, s, \psi_1 \mid (s, \psi_1) \in BM_1 \bullet \exists\, \psi_2 \bullet (s, \psi_2) \in BM_2 \land \psi_2 \subseteq \psi_1}$$

for healthy multirelations.

Binary multirelations as predicates: operators

Angelic choice

$$sb2p.(pt2r.(P \sqcup Q)) = sb2p.(pt2r.P) \vee sb2p.(prt2.Q)$$

Demonic choice

$$sb2p.(pt2r.(P \sqcap Q)) = sb2p.(pt2r.P) \wedge sb2p.(prt2.Q)$$

Sequence: $P;\ Q^*$

$$\begin{array}{l} Q^* \ \widehat{=}\ \mu X \bullet \mathbf{true} \lhd dc = \emptyset \rhd \mathbf{var}\ s \bullet s' \in dc; \\ \qquad\qquad (v := s.v;\ Q) \sqcup (dc := dc \setminus \{ s \};\ X) \\ \qquad\qquad \mathbf{end} \end{array}$$

Conclusions

- A set-based relational model can be illuminating
  - The need for designs becomes obvious
  - A simpler set of healthiness conditions is promptly revealed
- New relational model: binary multirelations
- Advantages
  - Angelic and demonic nondeterminism
- Price
  - Complex definition for sequence
  - Definition of refinement is changed
- Future: redevelop the model of processes using this extended model