Lexicographic Variants in Event-B

Laurent Voisin
joint work with Thai Son Hoang (U. Southampton)

2018-11-10

Convergence in Event-B

- Convergence
- Anticipation
- Lexicographic order
- Options

Events can be tagged as convergent

This is proved thanks to a variant, that is a mathematical expression subject to a well-founded order (no infinite descent)

A convergent event must decrease the variant

Two kinds of variants implemented in Rodin:

- Finite sets, $\subset$
- Natural numbers, $<$

Rodin proof obligations for convergence

- Convergence
- Anticipation
- Lexicographic order
- Options

Finite sets:

- FIN FINITE(v)
- cvg_evt/VAR $v' \subset v$

Natural numbers:

- cvg_evt/NAT $v \in \mathbb{N}$
- cvg_evt/VAR $v' < v$

systerel
Safe real-time solutions

Anticipated events

Introducing an event that will eventually converge

The event is tagged as anticipated

It will be tagged convergent in a further refinement

An anticipated event must not increase the variant

Rodin proof obligations for anticipation

Finite sets:

- FIN   FINITE(v)
- ant_evt/VAR $v' \subseteq v$

Natural numbers:

- ant_evt/NAT $v \in \mathbb{N}$
- ant_evt/VAR $v' \leq v$

systerel
Safe real-time solutions

Improved POs for anticipation (bonus)

Prefix PO with $v' \neq v$ (Hallerstede, ABZ2014):

- ant_evt/NAT $v' \neq v \Rightarrow v \in \mathbb{N}$

We can do better for integer variants, using the equivalence with finite set $0..v$, we can drop the NAT PO as the VAR PO is enough:

$$v' \leq v \Rightarrow 0..v' \subseteq 0..v$$

$v' < 0$	$v < 0$	$\ldots \Rightarrow \varnothing \subseteq \varnothing$
$v' < 0$	$v \geq 0$	$\ldots \Rightarrow \varnothing \subseteq 0..v$
$v' \geq 0$	$v < 0$	$\bot \Rightarrow \ldots$
$v' \geq 0$	$v \geq 0$	$v' \leq v \Rightarrow 0..v' \subseteq 0..v$

systerel
Safe real-time solutions

First step towards lexicographic variant

Convergence
Anticipation
Lexicographic order
Options

Example:

M1	evt	(anticipated)	v1
M2	evt	(anticipated)	v2
M3	evt	(convergent)	v3

When flattening, evt is converging on the lexicographic variant

- (v1, v2, v3)

But stronger than needed:

$$\begin{aligned} & v1' \subseteq v1 \\ \land\ & v2' \subseteq v2 \\ \land\ & v3' \subset v3 \end{aligned} \quad \Rightarrow \quad \begin{aligned} & (v1' \subset v1) \\ \lor\ & (v1' = v1 \land v2' \subset v2) \\ \lor\ & (v1' = v1 \land v2' = v2 \land v3' \subset v3) \end{aligned}$$

Lexicographic set variant

Several variants in the same machine: v1, v2, v3

POs for finite sets:

v1/FIN	FINITE(v1)	
v2/FIN	FINITE(v2)	
v3/FIN	FINITE(v3)	
cvg_evt/v1/VAR		$v1' \subseteq v1$
cvg_evt/v2/VAR	$v1' = v1$	$\Rightarrow v2' \subseteq v2$
cvg_evt/v3/VAR	$v1' = v1 \land v2' = v2$	$\Rightarrow v3' \subset v3$
ant_evt/v1/VAR		$v1' \subseteq v1$
ant_evt/v2/VAR	$v1' = v1$	$\Rightarrow v2' \subseteq v2$
ant_evt/v3/VAR	$v1' = v1 \land v2' = v2$	$\Rightarrow v3' \subseteq v3$

Note: POs get simplified when some variant is not modified by the event

Natural lexicographic variant (convergent)

With two variants: v1, v2

Option 1

- cvg_evt/v1/NAT $v1 \in \mathbb{N}$
- cvg_evt/v1/VAR $v1' \leq v1$
- cvg_evt/v2/NAT $v1' = v1 \Rightarrow v2 \in \mathbb{N}$
- cvg_evt/v2/VAR $v1' = v1 \Rightarrow v2' < v2$

Option 2

- cvg_evt/v1/VAR $v1' \leq v1$
- cvg_evt/v2/NAT $v1' = v1 \lor v1'<0 \Rightarrow v2 \in \mathbb{N}$
- cvg_evt/v2/VAR $v1' = v1 \lor v1'<0 \Rightarrow v2' < v2$

Natural lexicographic variant (anticipated)

Option 1

- ant_evt/v1/NAT $v1 \in \mathbb{N}$
- ant_evt/v1/VAR $v1' \leq v1$
- ant_evt/v2/VAR $v1' = v1 \Rightarrow v2' \leq v2$

Option 2

- ant_evt/v1/VAR $v1' \leq v1$
- ant_evt/v2/VAR $v1' = v1 \lor v1' < 0 \Rightarrow v2' \leq v2$

systerel
Safe real-time solutions

Will be available in Rodin 3.5