Mondex in Z/Eves

Leo Freitas and Jim Woodcock
University of York
May 2006

Introduction

- *formalising Mondex in Z/Eves*
- *suggesting improvements*
- *Z/Eves idioms and specification patterns*
- *how to drive Z/Eves, fast!*
- *problems found in Mondex models*
- *benchmarks*
- *conclusions and future work*

How faithful is it?

- *carbon copy of Oxford PRG-126*
- *implicit finiteness information made explicit*
  - $AuxWorld$ *elements (Chapter 5)*
  - $chosenLost$ *components (Chapter 10)*
- *theorems to discharge such choice are included*

How faithful is it?

Auxiliary toolkit (Appendix D)

- *inappropriate for mechanisation*
- *proposed alternative using sequences and induction*
  - *avoids finiteness problems*
  - *avoids specificity of instantiation*
  - *can rely on toolkit theorems for sequences*

$$
\begin{array}{|l}
totalAbBalance : (NAME \pfun AbPurse) \rightarrow \mathbb{N} \\
\hline
totalAbBalance\,\emptyset = 0 \\
\forall w : (NAME \pfun AbPurse);\ n : NAME;\ AbPurse \mid \\
\qquad n \notin \operatorname{dom} w \bullet totalAbBalance\,(\{ n \mapsto \theta AbPurse \} \cup w) \\
\qquad\qquad\qquad = balance + totalAbBalance\,w
\end{array}
$$

How faithful is it?

Suggestion: inductive update over sequences

$$update : \operatorname{seq} \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \rightarrow \operatorname{seq} \mathbb{Z}$$

$$\begin{aligned}
&\forall\, i, n : \mathbb{Z} \bullet update(\langle\rangle, i, n) = \langle\rangle \\
&\forall\, i, x, n : \mathbb{Z} \bullet update(\langle x \rangle, i, n) = \mathbf{if}\ i = 1\ \mathbf{then}\ \langle n \rangle\ \mathbf{else}\ \langle x \rangle \\
&\forall\, s, t : \operatorname{seq} \mathbb{Z};\ i, n : \mathbb{Z} \bullet update((s \frown t), i, n) = \\
&\qquad \mathbf{if}\ i \in \operatorname{dom} s\ \mathbf{then}\ update(s, i, n) \frown t \\
&\qquad \mathbf{else\ if}\ i - \#s \in \operatorname{dom} t\ \mathbf{then}\ s \frown update(t, (i - \#s), n) \\
&\qquad \mathbf{else}\ s \frown t
\end{aligned}$$

How faithful is it?

Suggestion: inductive summation of sequences

$$sum : \operatorname{seq} \mathbb{Z} \rightarrow \mathbb{Z}$$

$$sum\ \langle\rangle = 0$$
$$\forall\, n : \mathbb{Z} \bullet sum\ \langle n \rangle = n$$
$$\forall\, s, t : \operatorname{seq} \mathbb{Z} \bullet sum\ (s \frown t) = sum\ s + sum\ t$$

theorem tSumUpdate

$$\forall\, s : \operatorname{seq} \mathbb{Z};\ i, n : \mathbb{Z} \mid i \in \operatorname{dom} s \bullet$$
$$sum(update(s, i, n)) = sum\ s - s\ i + n$$

theorem rule rSumPos

$$\forall\, s : \operatorname{seq} \mathbb{N} \bullet sum\ s \in \mathbb{N}$$

How complete is it?

Models

- $\mathcal{A}$ *model (Chapter* 3*)*
- $\mathcal{B}$ *model: purse, world, init., final. (Chapters* 4, 5, 6*)*
- $\mathcal{C}$ *model (Chapter* 7*)*
- *applicability proofs (Chapter* 8*)*

How complete is it?

Refinement: $\mathcal{A}$ to $\mathcal{B}$

- *retrieve definitions (Chapter 10)*
- *$\mathcal{A}$ to $\mathcal{B}$ initialisation (Chapter 11)*
- *$\mathcal{A}$ to $\mathcal{B}$ finalisation (Chapter 12)*
- *$\mathcal{A}$ to $\mathcal{B}$ applicability (Chapter 13)*

How complete is it?

Security properties (Chapter 2)

- *all definitions (but Section 2.4)*
- *proofs in Section* 2.4 *contain informal arguments*
- $totalAbBalance$ *(Appendix* D*) is inadequate for mechanisation*
- *mechanisable using suggested model of sequences*

Retrieve definitions (Chapter 10)

- *steps for existential proof is unclear*
- *end up requiring that at least one payment has been made*

$$RabCl \Rightarrow (\exists\, pdThis : PayDetails \bullet true)$$

Suggestions of improvement

Auxiliary lemmas from Chapter 8

- *several lemmas needed for precondition proofs*
  - *promoted operations*
  - *appropriate instantiations*
- *textual proofs avoids promoted operations via* $Ignore$
- *other lemmas are stated but not used (yet)*
- *no explanation is given for harder proofs*

Suggestions of improvement

Well explained proofs are worthwhile (so far)

- *later chapters proofs are thoroughly explained*
- *the mechanised proofs are mostly the same as the explanation*

Suggestions of improvement

Z idioms: one-point-mu!

- *inadequacy of some θ and μ expressions used*
- *θ equivalence for Mondex μ expressions*
- *function application equivalence for θ expressions*
- *extra housekeeping rules for free types, and schema*
  - *partial injectivity and/or functionality*
  - *relational property and/or maximal types*
  - *trivial repetition of schema component types as theorems*

Suggestions of improvement

e.g., precondition proofs for $StartFromPurseEafromOkay$ *use*

$$PayDetails \mathrel{\widehat=} [\, TransferDetails;\ fromSeqNo, toSeqNo : \mathbb{N} \mid from \neq to \,]$$
$$CounterPartyDetails \mathrel{\widehat=} [\, name : NAME;\ value : \mathbb{N};\ nextSeqNo : \mathbb{N} \,]$$

$$\begin{array}{l}
\textbf{theorem}\ \text{rule rStartFromMuPayDetailsValue} \\
\quad \forall\, name : NAME;\ nextSeqNo : \mathbb{N};\ cpd : CounterPartyDetails \\
\qquad \mid name \neq cpd.name \bullet (\mu\, PayDetails \mid from = name \land \\
\qquad\quad to = cpd.name \land value = cpd.value \land \\
\qquad\quad fromSeqNo = nextSeqNo \land \\
\qquad\quad toSeqNo = cpd.nextSeqNo) \\
\qquad = \theta PayDetails[from := name, to := cpd.name, \\
\qquad\quad value := cpd.value, fromSeqNo := nextSeqNo, \\
\qquad\quad toSeqNo := cpd.nextSeqNo]
\end{array}$$

Suggestions of improvement

- *minor LaTeX mistakes on strokes (Chapters* 7 *and* 10*)*
- *more explicit applicability theorems and proofs (Chapter* 8*)*
- *misleading name of operation given in proof on p.* 63 *(Chapter* 8*)*
- *more explicit referencing to used lemmas in proofs (Chapter* 10*)*
- *explicit state finiteness properties*
  - $AuxWorld$ *invariant (Chapter* 5*)*
  - $chosenLost$ *components (Chapter* 10*)*

Driving Z/Eves

- *extra type rules for free types and bindings*
- *extra type rules for schema components*
- *encoding of finiteness as predicates*
- *expansion lemmas for complex schemas (e.g., $BetweenWorld$)*
- *additional lemmas for promoted schemas precondition*

Extending Z/Eves

Theory for functional overriding (Chapter 8)

theorem rule rPFunElement $[X, Y]$
$\forall f : X \pfun Y;\ x : X;\ y : Y \mid x \in \operatorname{dom} f \land y = f\,x \bullet (x, y) \in f$

theorem rule rPFunSubsetOplusRel $[X, Y]$
$\forall f, g : X \pfun Y \mid g \subseteq f \bullet f \oplus g = f \oplus (\operatorname{dom} g \lhd f)$

theorem lPFunSubsetOplusUnitRel $[X, Y]$
$\forall f : X \pfun Y;\ x : X;\ y : Y \mid x \in \operatorname{dom} f \land y = f\,x \bullet$
$\quad f = f \oplus \{(x \mapsto y)\}$

Problem: are after purses authentic?

- $abAuthPurse'$ *is not authentic in* $AbTransferOkayTD$ *and* $AbTransferLostTD$ *(p.*$20, 21$*)*
  - *necessity proof that* $\Delta Authentic$ *is needed*
  - *it should give a counter example*
  - *requires complex* μ *expression equivalence*

$$
\begin{array}{|l}
\hline
\textit{AbTransferOkayTD} \\
\textit{AbWorldSecureOp} \\
\hline
\textit{Authentic}[\textit{from?}/\textit{name?}] \land \textit{Authentic}[\textit{to?}/\textit{name?}] \land \cdots \\
\hline
\end{array}
$$

$$
\begin{array}{l}
\forall\, x, y : NAME;\ xP, yP : AbPurse \mid x \neq y \land (\forall\, n : NAME \bullet n \in \{\, x, y \,\}) \\
\quad \bullet \forall\, AbWorldSecureOp \mid Authentic[from?/name?] \land \\
\qquad abAuthPurse' = \{(x, xP), (y, yP)\} \bullet from? \in \operatorname{dom} abAuthPurse'
\end{array}
$$

Problem: 4 missing properties of $BetweenWorld$ (p.42)

- val purses in the $ether$ refer to authentic $from$ and to purses $(B3)$

$$\forall pd : PayDetails \mid val\ pd \in ether \bullet pd \in authenticTo$$
$$\forall pd : PayDetails \mid val\ pd \in ether \bullet pd \in authenticFrom$$

- ack purses in the $ether$ refer to authentic $from$ and to purses $(B4)$

$$\forall pd : PayDetails \mid ack\ pd \in ether \bullet pd \in authenticTo$$
$$\forall pd : PayDetails \mid ack\ pd \in ether \bullet pd \in authenticFrom$$

- $BetweenWorld$ is inconsistent when val or ack msg. are handled

Benchmarks: Mondex in numbers (so far)

Given sets	*2*
Free types	*4*
Axiomatic definitions	*5*
Schemas	*131*
Total definitions	**142**

Z/Eves rules	*47*
Lemmas	*12*
Theorems	*21*
Proof scripts	*80*
Domain checks	*57*
Total proofs	**137**

- *DC are Z/Eves proof obligations*
- *DC are sufficient conditions for definedness*
- *generates proofs even when definitions are not used*

Benchmarks: Mondex in numbers (so far)

Automation	**grule**	**frule**	**rule**	**Lemmas**	**Total**
Free types	*14*	*0*	*4*	*0*	**18**
Schemas/bindings	*0*	*14*	*5*	*7*	**26**
μ-θ *expressions*	*0*	*0*	*8*	*0*	**8**
Extended overriding	*0*	*0*	*2*	*1*	**3**
Finiteness	*0*	*0*	*0*	**4**	**4**
Total	*14*	*14*	*19*	*12*	**59**

Benchmarks: proof effort explained

- *trivial push button steps*
- *repetitive steps from previous proofs*
- *intermediate steps requiring Z/Eves expertise*
- *creative steps requiring domain knowledge (i.e., instantiations)*
- *hard steps for general (additional/unrelated) theories*
  - *function overriding lemmas*
  - mu-θ *expression equivalences*
- *to do: finiteness proofs (i.e., induction, bijective, etc.)*

Benchmarks: estimated proof effort

Effort	**Steps**
Trivial (push button)	*209*
Intermediate (Z/Eves knowledge)	*421*
Creative (domain knowledge)	*89*
Total steps	**719**

Benchmarks: breakdown of activities (May/2006)

- *typesetting*
  - *manually typing Chapters* 3 *and* 4
  - *PRG*-126 *sources from Chapter* 5
  - *using* `ntheorem.sty` *from* 22^{nd} *of May*
- *proof effort*
  - *most effort on preconditions for Chapter* 8
  - *repeated proofs for Z/Eves automation*
  - *extended theory for overriding and* μ-θ *equivalence*

Benchmarks: how long it took?

Chapter	Hours	Days of May
3—$\mathcal{A}$ *model*	6	3^{rd}
4—$\mathcal{B}$ *purse*	10	3^{rd}, 4^{th}
5—$\mathcal{B}$ *world*	4	5^{th}
6—$\mathcal{B}$ *init/final*	1	5^{th}
7—$\mathcal{C}$ *world*	1	5^{th}
8—*Preconditions*	15	5^{th}, 16^{th}, 17^{th}, 18^{th}
10—*Retrieve state*	7	18^{th}, 22^{nd}
LaTeX document	10	3^{rd}, 4^{th}, 22^{nd}, 23^{nd}
Total	**54**	$\mathbf{3^{rd}}$–$\mathbf{23^{rd}}$

around 7 working days

Benchmarks: how much is left?

- *proof effort pending*
  - *finiteness lemmas*
  - *security properties (Section 2.4) proofs*
  - *equivalence lemma for $\exists$ on Chapter 10*
- *what is next?*
  - *adequate theory/automation for finiteness*
  - *refinement proofs Chapters*

Conclusions

- *unknown bugs: payback for such effort (?)*
  - *missing properties of* $BetweenWorld$ *affects around* 6 *operation*
  - *that means it allows operations over non-authentic purses*
- *what is the point?*
  - *motivated not by the tool, but by the problem*
  - *suitability of Z: did it helped or got in the way?*
- *discussion . . .*

Future work

- *comparing results*
- *different bugs or proofs from different formalisations?*
- *what if no bugs from* $BetweenWorld$ *are found?*
- *how to assess such scenarios?*