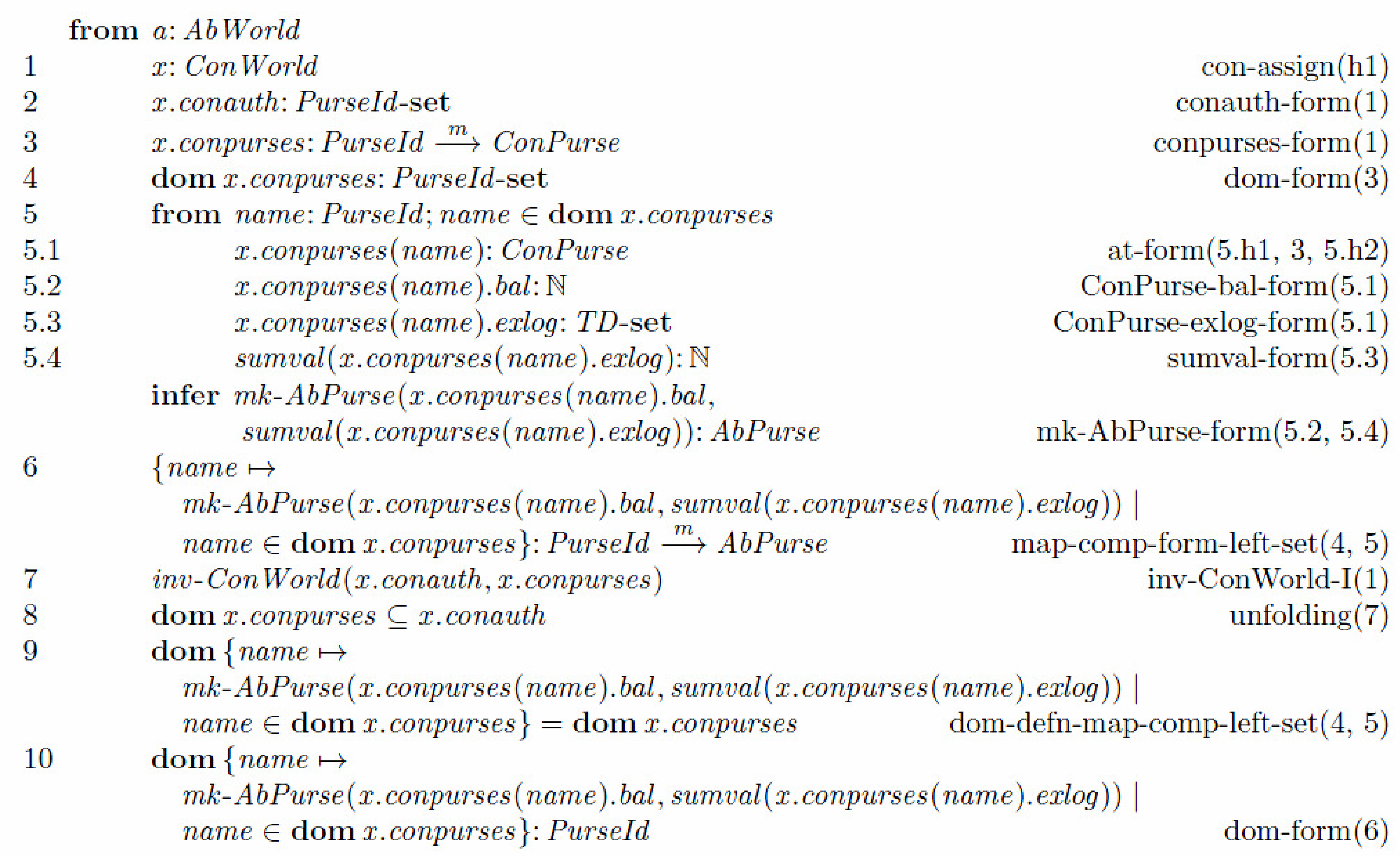
Counterpoint: Towards a Proof-Support Tool for VDM

Ken Pierce

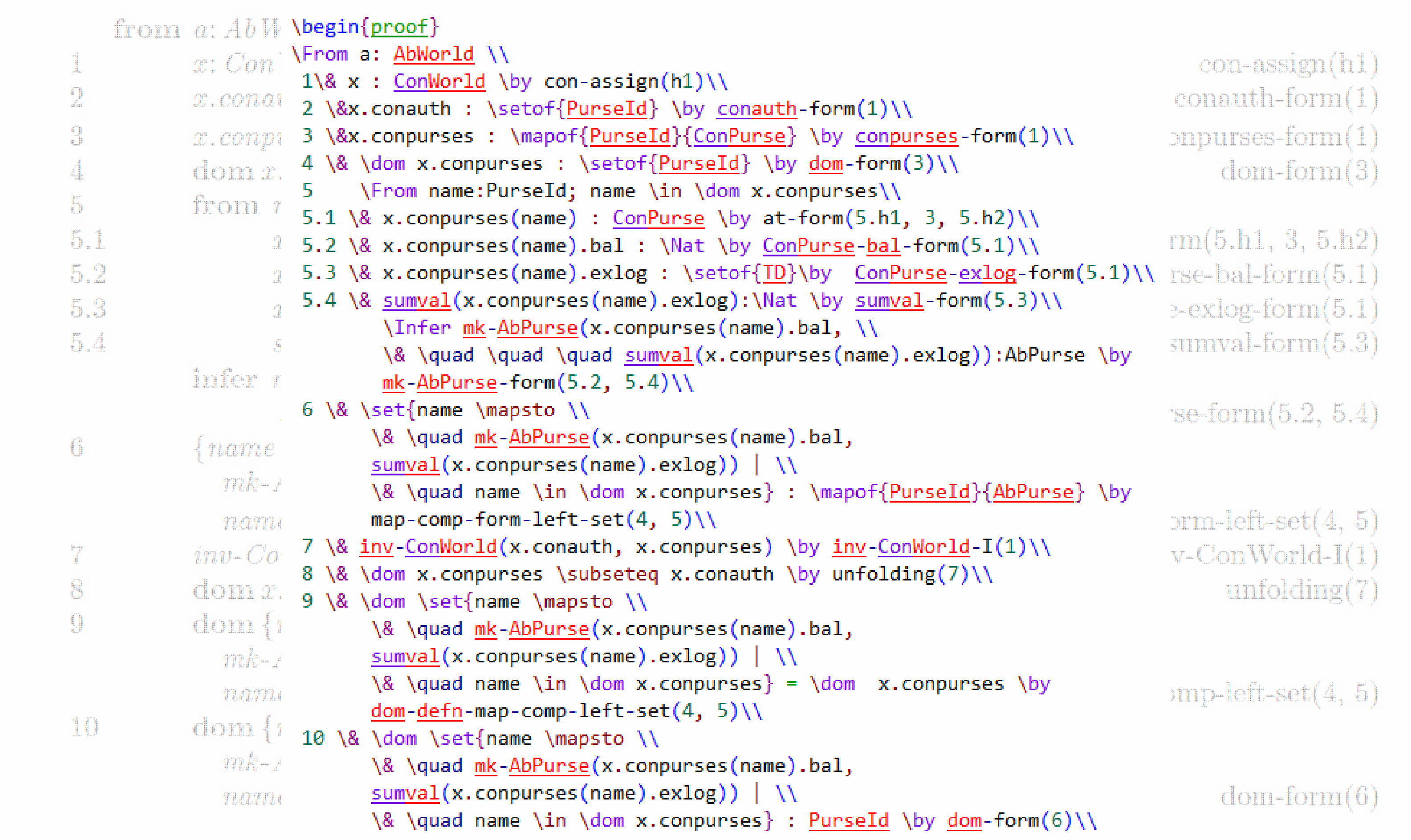
Newcastle University, UK

Motivation (1)



	from $a\colon AbWorld$	
1	$x\colon ConWorld$	con-assign(h1)
2	$x.conauth\colon PurseId\text{-}\mathbf{set}$	conauth-form(1)
3	$x.conpurses\colon PurseId \xrightarrow{m} ConPurse$	conpurses-form(1)
4	$\mathbf{dom}\, x.conpurses\colon PurseId\text{-}\mathbf{set}$	dom-form(3)
5	**from** $name\colon PurseId;\ name \in \mathbf{dom}\, x.conpurses$	
5.1	$x.conpurses(name)\colon ConPurse$	at-form(5.h1, 3, 5.h2)
5.2	$x.conpurses(name).bal\colon \mathbb{N}$	ConPurse-bal-form(5.1)
5.3	$x.conpurses(name).exlog\colon TD\text{-}\mathbf{set}$	ConPurse-exlog-form(5.1)
5.4	$sumval(x.conpurses(name).exlog)\colon \mathbb{N}$	sumval-form(5.3)
	infer $mk\text{-}AbPurse(x.conpurses(name).bal,$ $sumval(x.conpurses(name).exlog))\colon AbPurse$	mk-AbPurse-form(5.2, 5.4)
6	$\{name \mapsto$ $mk\text{-}AbPurse(x.conpurses(name).bal, sumval(x.conpurses(name).exlog)) \mid$ $name \in \mathbf{dom}\, x.conpurses\}\colon PurseId \xrightarrow{m} AbPurse$	map-comp-form-left-set(4, 5)
7	$inv\text{-}ConWorld(x.conauth, x.conpurses)$	inv-ConWorld-I(1)
8	$\mathbf{dom}\, x.conpurses \subseteq x.conauth$	unfolding(7)
9	$\mathbf{dom}\,\{name \mapsto$ $mk\text{-}AbPurse(x.conpurses(name).bal, sumval(x.conpurses(name).exlog)) \mid$ $name \in \mathbf{dom}\, x.conpurses\} = \mathbf{dom}\, x.conpurses$	dom-defn-map-comp-left-set(4, 5)
10	$\mathbf{dom}\,\{name \mapsto$ $mk\text{-}AbPurse(x.conpurses(name).bal, sumval(x.conpurses(name).exlog)) \mid$ $name \in \mathbf{dom}\, x.conpurses\}\colon PurseId$	dom-form(6)

Motivation (2)



```
\begin{proof}
\From a: AbWorld \\
 1\& x : ConWorld \by con-assign(h1)\\
 2 \&x.conauth : \setof{PurseId} \by conauth-form(1)\\
 3 \&x.conpurses : \mapof{PurseId}{ConPurse} \by conpurses-form(1)\\
 4 \& \dom x.conpurses : \setof{PurseId} \by dom-form(3)\\
 5    \From name:PurseId; name \in \dom x.conpurses\\
 5.1 \& x.conpurses(name) : ConPurse \by at-form(5.h1, 3, 5.h2)\\
 5.2 \& x.conpurses(name).bal : \Nat \by ConPurse-bal-form(5.1)\\
 5.3 \& x.conpurses(name).exlog : \setof{TD}\by  ConPurse-exlog-form(5.1)\\
 5.4 \& sumval(x.conpurses(name).exlog):\Nat \by sumval-form(5.3)\\
       \Infer mk-AbPurse(x.conpurses(name).bal, \\
       \& \quad \quad \quad sumval(x.conpurses(name).exlog)):AbPurse \by
       mk-AbPurse-form(5.2, 5.4)\\
 6 \& \set{name \mapsto \\
      \& \quad mk-AbPurse(x.conpurses(name).bal,
      sumval(x.conpurses(name).exlog)) | \\
      \& \quad name \in \dom x.conpurses} : \mapof{PurseId}{AbPurse} \by
      map-comp-form-left-set(4, 5)\\
 7 \& inv-ConWorld(x.conauth, x.conpurses) \by inv-ConWorld-I(1)\\
 8 \& \dom x.conpurses \subseteq x.conauth \by unfolding(7)\\
 9 \& \dom \set{name \mapsto \\
      \& \quad mk-AbPurse(x.conpurses(name).bal,
      sumval(x.conpurses(name).exlog)) | \\
      \& \quad name \in \dom x.conpurses} = \dom  x.conpurses \by
      dom-defn-map-comp-left-set(4, 5)\\
 10 \& \dom \set{name \mapsto \\
      \& \quad mk-AbPurse(x.conpurses(name).bal,
      sumval(x.conpurses(name).exlog)) | \\
      \& \quad name \in \dom x.conpurses} : PurseId \by dom-form(6)\\
```

Counterpoint

- Overture extension
  - *Proof* perspective
- Proof obligation manager
  - on top of the current PO generator
  - incl. refinement / reification proofs
    - manage multiple specifications and relations
- Proof artifacts
- Visual mnemonics

Proof Artifacts: Automated Proof

- Supported by plug-ins for external provers
- Define extension points
  - for look & feel, AST access
- Feedback in VDM syntax preferable
- Brute force
  - plus automated retry upon specification change

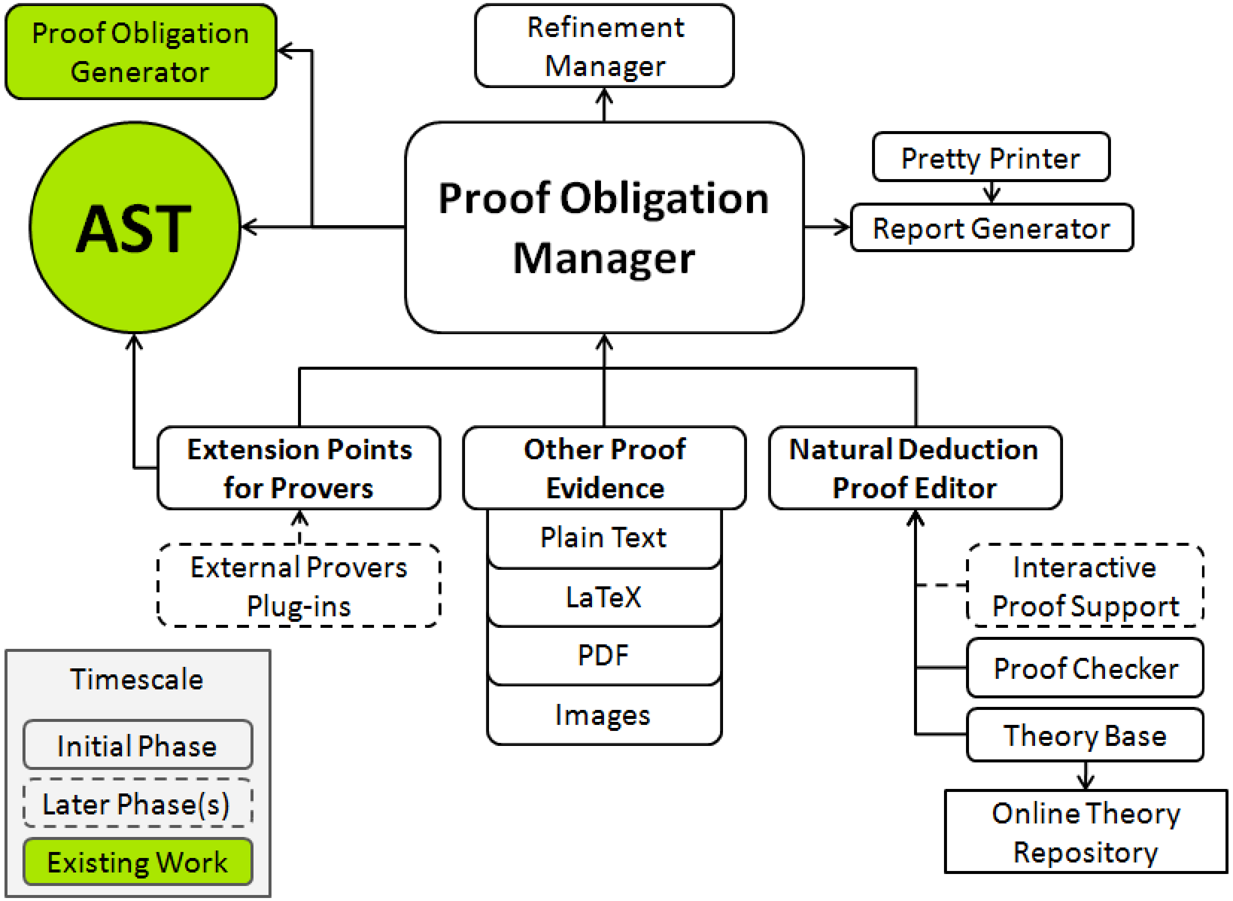
Proof Artifacts: Natural Deduction

- Proof editor
  - file format
  - automated line numbering, syntax highlighting
- Proof checker
  - plus automated rechecking upon specification change
- Directory of theorems
  - plus online repository
- User-guided proof
  - e.g. like mural, AI4FM

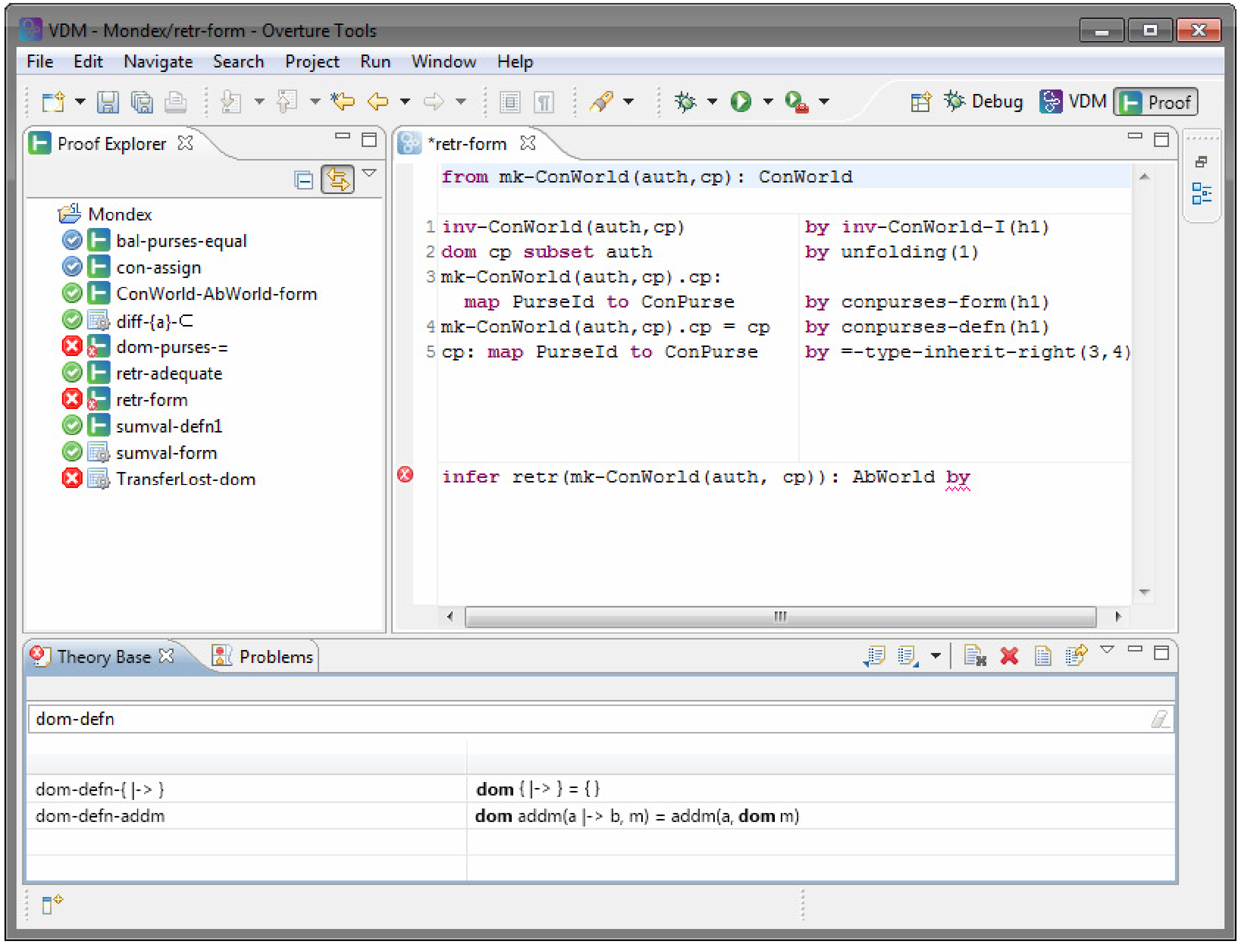
Proof Artifacts: Other Evidence

- E.g. proof by inspection, semi-formal proofs, structured arguments
- Also older proofs in other forms (e.g. scans)
- Plain text, LaTeX, PDF, PNG/JPEG etc.
- “Blue” mnemonic
  - human-checked
  - can warn of changed specification

Proposed Components



Mockup



- Mondex
  - ✓ bal-purses-equal
  - ✓ con-assign
  - ✓ ConWorld-AbWorld-form
  - ✓ diff-{a}-⊂
  - ✗ dom-purses-=
  - ✓ retr-adequate
  - ✗ retr-form
  - ✓ sumval-defn1
  - ✓ sumval-form
  - ✗ TransferLost-dom

```
from mk-ConWorld(auth,cp): ConWorld

1 inv-ConWorld(auth,cp)           by inv-ConWorld-I(h1)
2 dom cp subset auth              by unfolding(1)
3 mk-ConWorld(auth,cp).cp:
    map PurseId to ConPurse       by conpurses-form(h1)
4 mk-ConWorld(auth,cp).cp = cp    by conpurses-defn(h1)
5 cp: map PurseId to ConPurse     by =-type-inherit-right(3,4)

infer retr(mk-ConWorld(auth, cp)): AbWorld by
```

dom-defn

dom-defn-{ |-> }	**dom** { |-> } = { }
dom-defn-addm	**dom** addm(a |-> b, m) = addm(a, **dom** m)

Roadmap

- Requirements document
  - based on community feedback
- Initial proof perspective
  - including ‘other evidence’ artifact support
- Natural deduction file format and editor
- Pilot study for external prover e.g. [Ver&10]

Thanks for Listening

- Any questions?