

Designing a *Proof* tool for *Engineering* use

Farhad Mehta
ETH Zurich

Dagstuhl Seminar -
Rigorous methods for Software
Construction and Analysis
11th May 2006

ETH

Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Rodin

The (inevitable) Pain of doing Formal Proof

Farhad Mehta
ETH Zurich

Dagstuhl Seminar -
Rigorous methods for Software
Construction and Analysis
11th May 2006

ETH

Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Rodin

Formal Proof ?

The act of discharging a *proof obligation* expressed in *formal mathematical notation*

Contrast with push-button techniques:
Model checking, Abstract interpretation, Testing...

Some bitter truths :

- The alternatives have their limitations.
- *Formal proofs* are here to stay.
- Automated provers have their limitations.
- *Interactive proofs* are here to stay.

The *Pains* of an Engineer
doing Formal Proof...

... and some possible
alleviations

Something new to learn

Pain :

Esoteric mathematical notation

Alleviation :

Build on existing knowledge and intuition

Light formal language with simple constructs

Nature of POs

For engineering applications typically:

- Simple but large in number
- Shallow but look daunting

Nature of POs

Pain :

900 POs to discharge before lunch
(but they all look so trivial?)

Alleviation :

Use powerful automated provers and an
aggressive proving strategy

Nature of POs

Pain :

How did that strange PO come about?

What am I proving?

Alleviation :

Provide hints and relevant info for a PO

Structure the PO

Pain of interactive proof

Pain :

What was that proof command again?

Alleviation :

Use Click'n'Proove ...

Changing POs

POs change often in the course of a development due to changes or overseights in the source model.

Pain of changing POs

Pain :

My proofs just broke #!%

Alleviation :

Allow multiple ways to keep proofs valid
(reuse, replay, refactor...)

And once everything
is over...

Pain of convincing others

Pain :

No-one trusts my proofs!

Alleviation :

Document each reasoning step

Allow proof checking

Conclusion

- No silver bullet !
- Many small incremental improvements can still be made...

