

The COMPASS Proof Obligation Generator

A Test Case of Overture Extensibility

Luis Diogo Couto Richard Payne

August 28, 2013
11th Overture Workshop

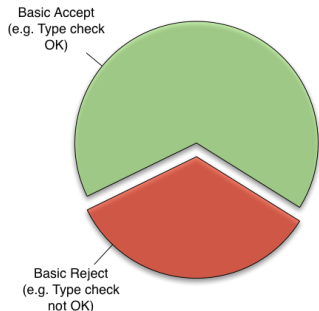
C O M P A S S

www.compass-research.eu



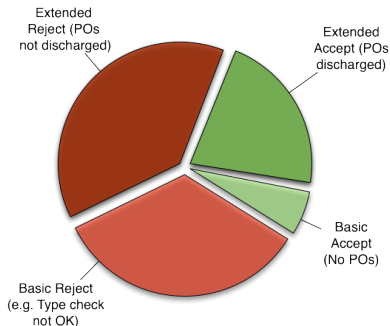
The Overture POG

- ▶ VDM typechecking is statically undecidable
- ▶ Proof Obligation Generator (POG) helps out
- ▶ Overture has a POG plugin
- ▶ Should be **extensible**. Is it?



The Overture POG

- ▶ VDM typechecking is statically undecidable
- ▶ Proof Obligation Generator (POG) helps out
- ▶ Overture has a POG plugin
- ▶ Should be **extensible**. Is it?



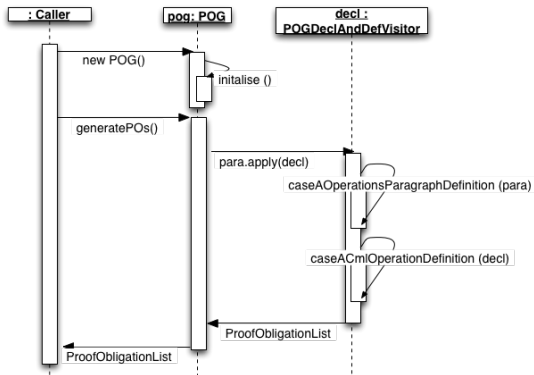
The COMPASS Extension

- ▶ **CML** - a new language for Systems of Systems modelling
- ▶ Based on VDM and CSP
- ▶ COMPASS tool based on Overture
- ▶ CML needs a POG

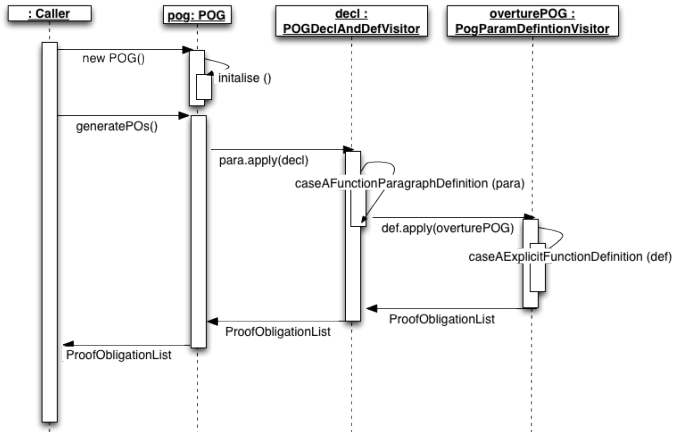
The COMPASS Extension

- ▶ We aim to extend the Overture POG
- ▶ Reuse goals:
 - ▶ directly use Overture to generate **all** VDM POs
 - ▶ minimal code duplication
- ▶ Add support for external analysis
- ▶ COMPASS POG will have to mirror structure and approach of Overture POG

The POG in Action: an example



The POG in Action: an example



Problems

- ▶ Current PO format unsuited for COMPASS (expected)
 - ▶ An AST format would be nice...
- ▶ Difficult to distinguish default nodes (small)
- ▶ Loss of control when Overture POG is called (very big)

Problems

No control in Overture

1. Overture visits an AST Node and takes over
2. Overture visitors end up visiting CML Nodes
3. They can't handle it; the POG crashes



The Fix

- ▶ Alter Overture visitors so they release AST sooner
- ▶ Visitors are parameterized with a *main visitor*
- ▶ `node.apply(this)` becomes `node.apply(main)`
- ▶ Some renaming necessary to keep Overture compatibility
- ▶ A few new Interfaces
- ▶ Very verbose and kind of clunky

The Fix

- ▶ Alter Overture visitors so they release AST sooner

How verbose?

```
PogParamDefinitionVisitor<Q extends IPOContextStack,  
A extends IProofObligationList> extends  
QuestionAnswerAdaptor<IPOContextStack,  
IProofObligationList>
```

The Fix

- ▶ Alter Overture visitors so they release AST sooner
- ▶ Visitors are parameterized with a *main visitor*
- ▶ `node.apply(this)` becomes `node.apply(main)`
- ▶ Some renaming necessary to keep Overture compatibility
- ▶ A few new Interfaces
- ▶ Very verbose and kind of clunky
- ▶ **But it works!**

Assessing Extensibility

- ✓ Able to generate almost all VDM POs with reuse
 - ▶ Volume reduced by aprox. 4.5k (cloned) LOC
- ✓ Updates to the Overture POG ported to COMPASS easily
- ✗ Overture code changes were essential. What if you cannot?

Further Work

Overture

- ▶ AST-based PO expressions (testing)
- ▶ Overhaul POG test suite (planning)

COMPASS

- ▶ POs for the CSP side of CML (early stages)
- ▶ Integration with Isabelle Theorem Prover (ongoing)

Thanks!