The *Rich Model Toolkit*
EU COST Action IC0901

Paul Jackson

University of Edinburgh

AI4FM Kick-Off Meeting
Newcastle
21st May 2010

What is COST?

EU program providing funding for research networking

$$\textit{COST} \quad = \quad \textit{European Cooperation in the field of Scientific and Technical Research}$$

- Targets academic research of industrial relevance
- COST funds *Actions* in 9 research areas. ICT is one area.
- 5 Actions in ICT started per year
- Each Action lasts 4 years, receives EUR 90k/year

What is COST? (continued)

- An Action funds
  - Scientific meetings
  - Short term scientific missions (1 week - 3 months) for early stage researchers
  - Training schools
- Participation open
  - Scientific meetings open
  - Funding provided for researchers from *participating institutions*
  - Institutions can join after Action start

The *Rich Model Toolkit* Action

Objective:

> *making automated reasoning techniques and tools easier to use and applicable to a wider range of problems*

Central approach is to develop infrastructure for supporting communication between tools

- Action started in October 2009
- Countries:

  Austria, Czech Republic, Denmark, France, Finland, Germany, Israel, Italy, Poland, Romania, Serbia, Spain, Sweden, Switzerland, United Kingdom
- Action led by Victor Kuncak (EPFL, Switzerland)
- Management Committee includes:

  Armin Biere, Stefan Ratschan, Peter Sestoft, Ilkka Niemela, Keijo Heljanko, Tayssir Touili, Barbara Jobstmann, Tobias Nipkow, Andrey Rybalchenko, Alexander Rabinovich, Maria Paola Bonacina, Leszek Pacholski, Gabriel Istrate, Maius Minea, Silvia Ghilezan, Predrag Janicic, Enric Rodriguez Carbonell, Cesar Sanchez, Reiner Hahnle, Natasha Sharygina, Victor Kuncak, Paul Jackson, Ian Horrocks

Action Concepts

- *Rich Models*
  - Standard formats for specification and description of software, hardware, embedded, and distributed systems
  - Aim to support modeling at a wide range of abstraction levels
- *The Toolkit*
  - Supports both verification and synthesis
  - Enables communication via data in Rich Model formats

Working Groups

1. Rich Model Language: design and benchmark Suite
   - Translators to/from Isabelle/HOL, SMTLIB, TPTP, OWL
   - Formats for proofs and counter-examples.
2. Decision procedures for Rich Model Language fragments
   - sets, collections with cardinality bounds, relations, arrays, bit vectors, transitive closure logics, non-linear arithmetic, description logics.
   - Integration into SMT and FOL frameworks.
   - Encoding of problems into base theories.

Working Groups (continued)

3. Analysis of executable Rich Models
   - *Executable* means modelled by a transition system.
   - Properties of interest include safety, liveness, functional correctness, timing and performance.
   - Sub-problems considered include
     - refinement of data types such as lists, trees, and their combination with arithmetic.
     - predicate abstraction and abstraction refinement
     - Synthesis and invariant/ranking function generation
     - Extraction of rich models from software source code, bytecode and hardware desgns.
   - Applications include analysis of: functional programs, linked and concurrent data structure implementations, correct resource use and finite-state protocols.
4. Synthesis from Rich Model Language descriptions.
   - synthesis algorithms for more expressive logics
   - Efficient implementations of synthesis algorithms
   - Quantitative generalization of synthesis
   - Simplified synthesis problems of practical interest

Upcoming events

- SVARM Workshop at FLoC 2010 in Edinburgh
  - July 20-21
  - Shankar from SRI speaking on Evidential Tool-Bus

My research of relevance to AI4FM

- Victor: a verification condition translator and prover driver
  - Works on VCs extracted from annotated SPARK-Ada programs
  - Currently translates into Isabelle/HOL and SMT languages
  - In collaboration with Praxis, developer of SPARK analysis toolkit
  - Aim is to learn about verification challenges faced by SPARK users
  - SPARK users would be very interested in AI4FM results.
  - While SPARK verification not top-down, many users also work with Z specifications and refinement of those specifications
- Proof procedures for non-linear arithmetic problems
  - PhD project of Grant Passmore
  - EPSRC proposal joint with Larry Paulson under review
- Have extensive past experience with Nuprl and PVS theorem provers

Generally am very interested in AI4FM project and possibly collaborating with participants