Report on TACAS 19

State of the art of Program Verification and Analysis

Joshua Dawes

CERN

MANCHESTER 1824
The University of Manchester

TACAS 19

- *Tools and Algorithms for the Construction and Analysis of Systems*.

- Part of the *European Joint Conferences on Theory and Practice of Software*.

- Held in Prague, Czech Republic.

- Featured talks on mostly theoretical developments in verification and synthesis of various systems.

Highlights

- Fault Localisation - Christakis et al.
  - Given an error trace, can we find fixes that *prune* the rest of the trace?
  - Considering multiple traces together, can we find fixes that, when applies to all, can prune all possible future trace suffixes?
  - **Very nice idea, and clearly useful in software engineering!**
  - But only tested in a “toy” setup… **needs industrial application.**

Highlights

- Model Checking with mCRL2 - Bunte et al.
  - **Tool for model checking with a wealth of industrial applications in its history - including at CERN!**
  - Model Checking - build an abstract model of a system and check wrt some specification. Very old and well-established area of Computer Science.
  - Downsides? Widespread application hasn't been adopted maybe because there must exist some *model* to be checked…
  - If a model satisfies a specification, how do we know that the system reflects the model?

Highlights

- Phasar Static Analysis tool for C/C++ - Schubert et al.
  - Powerful open-source static analysis framework for C/C++.
  - Focuses on gathering statistics about a program such as call graphs, class hierarchies, dataflow, etc.
  - **Used by people!**
  - Same approach as us with VyPR2 - advertising the intention to work with groups wanting to apply the tool.

Tools, tools and more tools…

- There's a theme in formal methods of every research group having its own tool for what they specialise in.
  - Model checkers (usually mature and actually usable outside the experimental data presented in the introductory paper)
  - Runtime Verifiers (niche field, so not common to have a general RV tool…)
- Refreshing approach from Bisping et al. on *Coupled Similarity* for transition systems - publishing theory, encouraging other groups to use it in tools.

Runtime Verification

- Small part of TACAS - RV is still a bit niche.
    - Difficulty working with industry
- **Strong theoretical development.**
- **But use cases are scarce.**
- Experimental results are with either

  (1)Toy examples - synthesised traces to display certain characteristics.

  (2)Open source projects - better, but the experiments are still done in a sandbox without communication with the project maintainer about the environment in which things would work in production.

Presentation of the VyPR2 Prototype

- Presented as a joint effort between CERN and Manchester, with major input from AICa for VyPR's first application.

- **The talk presented RV from a pragmatic point of view.**

- "We have some theory… but how do we actually use it?"

- Highlighted the engineering effort.

- This was a nice contrast from the theoretical focus of other talks.

Main Points

- Instrumentation is usually not considered - I presented an instrumentation method for CFTL.

- Verification of a service deployed in production - I gave an overview of the pipeline.
  - Deployment to a machine, instrumentation, monitoring, offline analysis.

- I presented an overview of the VyPR2 prototype's application to the uploader, and how it helped us to find performance drops.

Conclusions

- Strong theoretical development in verification and RV.
- Not a lot of work on application.
- VyPR2 - good start - still a lot to do.
  - Explanation based on path reconstruction (partly implemented + subject of next paper).
  - Optimising instrumentation (probably subject of another paper).

Schedule

- Purely theoretical paper on explanation by path reconstruction soon - just started writing - 3rd paper.

- Talk in CERN IT - end of May - finding more use cases.

- Instrumentation optimisation - loop unrolling (I gave a talk before Christmas) - 4th paper.

- Then either 1) publish a technical report to arxiv with theoretical “glue” for thesis, or 2) just leave that stuff for the thesis.

CERN

MANCHESTER 1824
The University of Manchester