Thesis Topic – Attacks on Hard Grammar Problems

Maximilian Schlund

March 10, 2015

1 Project Tasks

Given a procedural program (e.g. modeled as a pushdown system) and a specification (e.g. as a context-free grammar, cf. [BAA15]) it is a well-known **undecidable problem** to check inclusion (or even equivalence) between the two. Also the versatile framework by Podelski et al. [HHP13] reduces several verification tasks to checking inclusion between various automata models.

A promising attack on such problems is **approximation** as we have shown lately (e.g. approximation via regular languages [BLS15, LCMM12] or commutative approximation [ELS14]. Our current tool is based on the FPSOLVE library and is merely a prototype and much remains to be done to turn the approach into a practical checker. Very recently, the tool COVENANT was presented for the intersection non-emptiness problem [GNS+15].

In particular the following avenues of research seem promising:

- Investigate refinement strategies for the commutative abstraction. For example one can use the matrix-semiring over a commutative semiring to capture some features of non-commutative multiplication and still make the analysis terminate in finite time.
- Use simple semirings (e.g. the tropical semiring) to find counterexamples to equivalence quickly.
- Combine several language-based approximation methods, like the sub/superword-closure and the Mohri-Nederhof approximation [MN01].
- For equivalence and inclusion it would be particularly interesting to devise (necessary incomplete) methods to **prove** equivalence/inclusion between grammars.

2 Steps

- Familiarize yourself with FPSOLVE (or similar) and the techniques used (semirings, Newton's method,...).
- Develop (semi-)algorithms for grammar problems (intersection non-emptsiness, inclusion, equivalence) and (optionally) also try to devise methods that can prove that an instance has no solution.

- Implement a checking tool for grammar problems (preferably using FPSOLVE).
- Evaluate the tool on several benchmarks and compare it to other approaches (like cfganalyzer or COVENANT).
- (optional) Investigate how practical verification problems can be reduced to the questions above and implement the approach using static analysis tools.

This topic can be pursued as a Bachelor's thesis, Master's thesis, or as a guided research project, depending on your interests and level of expertise.

3 Contact

If you are interested, please write an email to Maximilian Schlund (schlund@model.in.tum.de) or just drop by at my office (Room 03.11.055).

References

[BAA15] Osbert Bastani, Saswat Anand, and Alex Aiken. Specification inference using context-free language reachability. In *Proceedings of the 42Nd Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, POPL '15, pages 553–566, New York, NY, USA, 2015. ACM.

[BLS15] Georg Bachmeier, Michael Luttenberger, and Maximilian Schlund. Finite Automata for the Sub- and Superword Closure of CFLs: Descriptional and Computational Complexity. In *Proceedings of LATA*, Lecture Notes in Computer Science, March 2015.

[ELS14] Javier Esparza, Michael Luttenberger, and Maximilian Schlund. FPsolve: A Generic Solver for Fixpoint Equations over Semirings. In *Proceedings of CIAA 2014*, pages 1–15, 2014.

[GNS+15] Graeme Gange, Jorge A Navas, Peter Schachte, Harald Søndergaard, and Peter J Stuckey. A Tool for Intersecting Context-Free Grammars and Its Applications. In *Proceedings of NASA Formal Methods*, 2015.

[HHP13] Matthias Heizmann, Jochen Hoenicke, and Andreas Podelski. Software model checking for people who love automata. In *Computer Aided Verification*, volume 8044 of *Lecture Notes in Computer Science*, pages 36–52. Springer Berlin Heidelberg, 2013.

[LCMM12] Zhenyue Long, Georgel Calin, Rupak Majumdar, and Roland Meyer. Language-theoretic abstraction refinement. In Juan de Lara and Andrea Zisman, editors, *Fundamental Approaches to Software Engineering*, volume 7212 of *Lecture Notes in Computer Science*, pages 362–376. Springer Berlin Heidelberg, 2012.

[MN01] Mehryar Mohri and Mark-Jan Nederhof. Regular approximation of context-free grammars through transformation. In Jean-Claude Junqua and Gertjan van Noord, editors, *Robustness in Language and Speech Technology*, volume 17 of *Text, Speech and Language Technology*, pages 153–163. Springer Netherlands, 2001.