

ParAlloy: Towards a Framework for Efficient Parallel Analysis of Alloy Models

Nicolás Rosner, Juan P. Galeotti,
Carlos G. Lopez Pombo, and Marcelo F. Frias

Department of Computer Science, FCEyN, Universidad de Buenos Aires,
e-mail: {nrosner, clpombo, jgaleotti, mfrias}@dc.uba.ar

Alloy [Jac02a] is a widely adopted relational modeling language. Its appealing syntax and the support provided by the Alloy Analyzer [Jac02b] tool make model analysis accessible to a public of non-specialists. A model and property are translated to a propositional formula, which is fed to a SAT-solver to search for counterexamples. The translation strongly depends on user-provided bounds for data domains called scopes – the larger the scopes, the more confident the user is about the correctness of the model. Due to the intrinsic complexity of the SAT-solving step, it is often the case that analyses do not scale well enough to remain feasible as scopes grow.

ParAlloy exploits the possibility of splitting the SAT formula, thus allowing for parallel SAT-solving of Alloy models. Three of its important characteristics are:

1. Its core component is a parallel solver for arbitrary propositional formulas –not necessarily in CNF– based on problem decomposition, and making a novel use of BEDs [AH02] for subproblem representation and manipulation, Minisat [ES03] for subproblem analysis, and MPI [SOHL⁺98] for inter-process communication.
2. Its Alloy-specific enhancements further improve (parallel) analyzability by using knowledge obtained from the models to assist splitting decisions.
3. For valid properties (the UNSAT case), the speedups allowed the analysis of Alloy properties (such as some assertions in [Zav06]) that exceed the current capabilities of the Alloy Analyzer. For invalid properties, test case generation or iterative model refinement (the SAT case), parallel analysis of search space paths often leads to much higher speedups, since its exhaustion is unnecessary.

References

- [AH02] Henrik Reif Andersen and Henrik Hulgaard. Boolean expression diagrams. *Information and computation*, 179(2):194–212, 2002.
- [ES03] Niklas Eén and Niklas Sörensson. An extensible sat solver. In Enrico Giunchiglia and Armando Tacchella, editors, *Proceedings of SAT 2003*, volume 2919 of *LNCS*, pages 502–518, 2003. Springer-Verlag.
- [Jac02a] Daniel Jackson. Alloy: a lightweight object modelling notation. *ACM Transactions on Software Engineering and Methodology*, 11(2):256–290, 2002.
- [Jac02b] Daniel Jackson. *A micromodels of software: Lightweight modelling and analysis with Alloy*. Computer Science and Artificial Intelligence Laboratory, MIT, 2002.
- [SOHL⁺98] Marc Snir, Steve Otto, Steven Huss-Lederman, David Walker, and Jack Donarra. *MPI: The complete reference*. MIT Press, 1998.
- [Zav06] Pamela Zave. Compositional binding in network domains. In J. Misra, T. Nipkow, and E. Sekerinski, editors, *Proceedings of the 14th. International FME Symposium*, volume 4085 of *LNCS*, pages 332–347. 2006. Springer-Verlag.