Presburger arithmetic and verification of infinite state systems

Jérôme Leroux
LaBRI/CNRS, Bordeaux, France

The automatic verification of reactive systems is a major field of research. These systems are usually modeled with variables taking values in some infinite domains. Popular approaches for analyzing these models are based on decision procedures adapted to the variables domains. For integral variables the Presburger arithmetic $\mathrm{FO}(Z, +, <)$ provides a natural logic to express linear constraints between integral variables. This logic has positive aspects: it is decidable and actually many solvers implement decision procedures for the full logic.

Some of these solvers like LASH, LIRA and MONA are based on automata packages. Intuitively, mappings from words to integer vectors are used to associate to automata potentially infinite sets of integer vectors (one vector per accepted word). Usually, the minimal deterministic automata are proved canonically associated to the represented sets and not on the way they have been computed. In particular these solvers are well adapted to sets obtained after long chains of operations like in symbolic model checking. However, extracting geometrical properties (for instance linear constraints) from automata is a challenging problem. From a theoretical point of view, this problem has been solved in 2005 with a polynomial time algorithm that computes Presburger formulas from automata representing Presburger sets. The algorithm first extracts the "necessary" linear constraints from the automaton. Then, it computes an unquantified Presburger formula using only these constraints, Boolean operations, translations by integer vectors, and scaling by integer values. Note that the algorithm that computes automata from Presburger formulas and the converse one that produces Presburger formulas from automata provide together the very first algorithm that normalizes Presburger formulas into unique canonical forms that only depend on the denoted sets. Intuitively in this normalization process, the minimization procedure for automata acts like a simplification procedure for the Presburger arithmetic.

In this presentation, we recall the classical algorithms that produce automata from Presburger formulas. We also recall some theoretical results like the Muchnik criterion that provides a simple way for deciding if an automaton represents a Presburger formula, the Cobham/Semenov theorem that characterizes the sets that can be represented by automata with two multiplicatively independent basis of decomposition. We also provide some hints on the construction of Presburger formulas from automata. Finally, we show some experiments and we provide applications of the Presburger arithmetic on the verification of infinite state systems.

References

[1] Jérôme Leroux. A polynomial time Presburger criterion and synthesis for number decision diagrams. In *20th IEEE Symposium on Logic in Computer Science (LICS 2005), Proceedings*, pages 147–156. IEEE Computer Society, 2005.

[2] Jérôme Leroux and Gérald Point. Tapas : The Talence Presburger Arithmetic Suite. In *Tools and Algorithms for the Construction and Analysis of Systems, 15th International Conference, TACAS 2009, Proceedings*, volume 5505 of *Lecture Notes in Computer Science*, pages 182–185. Springer, 2009.

[3] Jérôme Leroux and Grégoire Sutre. Flat counter automata almost everywhere! In *Automated Technology for Verification and Analysis, Third International Symposium, ATVA 2005, Proceedings*, volume 3707 of *Lecture Notes in Computer Science*, pages 489–503. Springer, 2005.