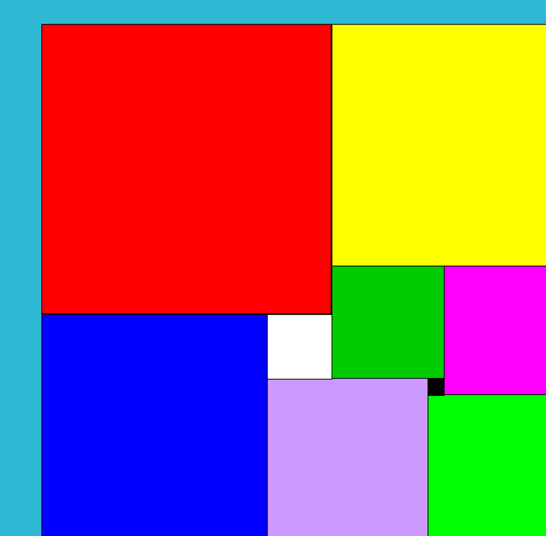
Arithmetic and First-Order Theorem Proving

Marek Kosta

Motivation: ubiquity of arithmetical constraints

- numerous applications of reasoning in the context of (some) arithmetic: compiler optimization, verification of complex real-time systems and many other areas
- great potencial for completely new applications
- expressivity of this combination can be used to model geometry, motion and other physical processes



Different approaches

- Satisfiability Modulo Theories: $a^2 < 0$ is unsatisfiable (in reals)
- Quantifier Elimination: $(\exists x)(ax + b = 0) \leftrightarrow a \neq 0 \vee b = 0$
- Superposition Modulo Arithmetic
- Hierarchical Theorem Proving

Practical tools

- there are efficient first-order refutational theorem provers (SPASS, Vampire, E)
- there are efficient arithmetic solvers, i.e. (non-)linear programming tools, etc.
- to our knowledge SPASS is the only implementation that combines some arithmetical fragments and first-order logic in a complete way
- space for different improvements and further combination of both “worlds” - logic and arithmetic

Theoretical issues

- Superposition, its variants and adjustments are broadly used
- Presburger Arithmetic, its variants and generalizations
- rational, real and complex arithmetic
- interpreted vs. uninterpreted symbols – first-order theorem proving works on syntactic (uninterpreted) side but with arithmetic we usually work in some particular model (or model class)

Goals

- develop new theoretical tools – redundancy criteria in specific fragments of arithmetic
- combine integer, rational (real), linear and non-linear arithmetic in such a way that the fragments obtained would be decidable and effective
- implementation of developed theoretical concepts

MAX-PLANCK-GESELLSCHAFT

max planck institut informatik