Superposition Modulo Linear Arithmetic – Sup(LA)

Ernst Althaus, Evgeny Kruglov,
Christoph Weidenbach

Max Planck Institute for Computer Science
Saarbrücken

Overview

- Motivation
  - Building arithmetic into Automated Theorem Proving will constitute a milestone in Automated Reasoning.
  - Verification of linear hybrid systems, program analysis, protocol analysis, etc.
  - New decidability results.
- Task
  - Integrate LA into the SUP calculus in a modular fashion.
  - Extend the technology of redundancy detection in the free first-order theory to the combination of the free theory and Linear Arithmetic.
- Challenge
  - Many theoretical questions have been solved (Hierarchic Theorem Proving by Bachmair, Ganzinger, Waldmann), but there was no answer to redundancy detection in the combination of theories.

Notions

- Clause: $\Lambda \parallel \Gamma \rightarrow \Delta$
  - $\bigcap \Lambda \cap \bigcap \Gamma \Rightarrow \bigcup \Delta$
  - Λ a linear arithmetic constraint (LAC), defined as conjunction of atoms built over the rationals, the theory symbols: $+, <, >, \approx, \leq, \geq$
  - Γ, Δ are sequences of first-order atoms, only containing signature symbols from the free first-order theory.
  - All parts share universally quantified variables.

$$x > y,\ 4x - 3.5y \geq 0 \parallel S_1(x, y) \rightarrow S_2(x, y)$$

Inference rules

- Resolution: $$I\,\frac{\Lambda_1 \,||\, \Gamma_1 \to \Delta_1, E_1 \qquad \Lambda_2 \,||\, \Gamma_2, E_2 \to \Delta_2}{(\Lambda_1, \Lambda_2 \,||\, \Gamma_1, \Gamma_2 \to \Delta_1, \Delta_2)\sigma}$$

  where σ is the unifier of E_1 and E_2 $(E_1\sigma = E_2\sigma)$.

- Factoring: $$I\,\frac{\Lambda \,||\, \Gamma \to \Delta, E_1, E_2}{(\Lambda \,||\, \Gamma \to \Delta, E_1)\sigma}$$

  where σ is the unifier of E_1 and E_2.

Reduction rules

- Tautology Deletion: $R\dfrac{\Lambda \,||\, \Gamma \rightarrow \Delta}{}$

  where $\Gamma \rightarrow \Delta$ is a tautology or $\exists \vec{x} \Lambda$ is unsatisfiable.

- Subsumption Deletion: $R\dfrac{\Lambda_1 \,||\, \Gamma_1 \rightarrow \Delta_1 \qquad \Lambda_2 \,||\, \Gamma_2 \rightarrow \Delta_2}{\Lambda_1 \,||\, \Gamma_1 \rightarrow \Delta_1}$

  where $\Gamma_1\sigma \subseteq \Gamma_2,\ \Delta_1\sigma \subseteq \Delta_2,\ \ \Lambda_2 \Rightarrow \Lambda_1\sigma.$
  The substitution $\sigma = \delta\tau$:
  - δ the standard subsumption matcher between the free parts of the clauses
  - τ a theory matcher mapping the variables solely occurring in first constraint to variables in the second one.

LAC Implication Problem

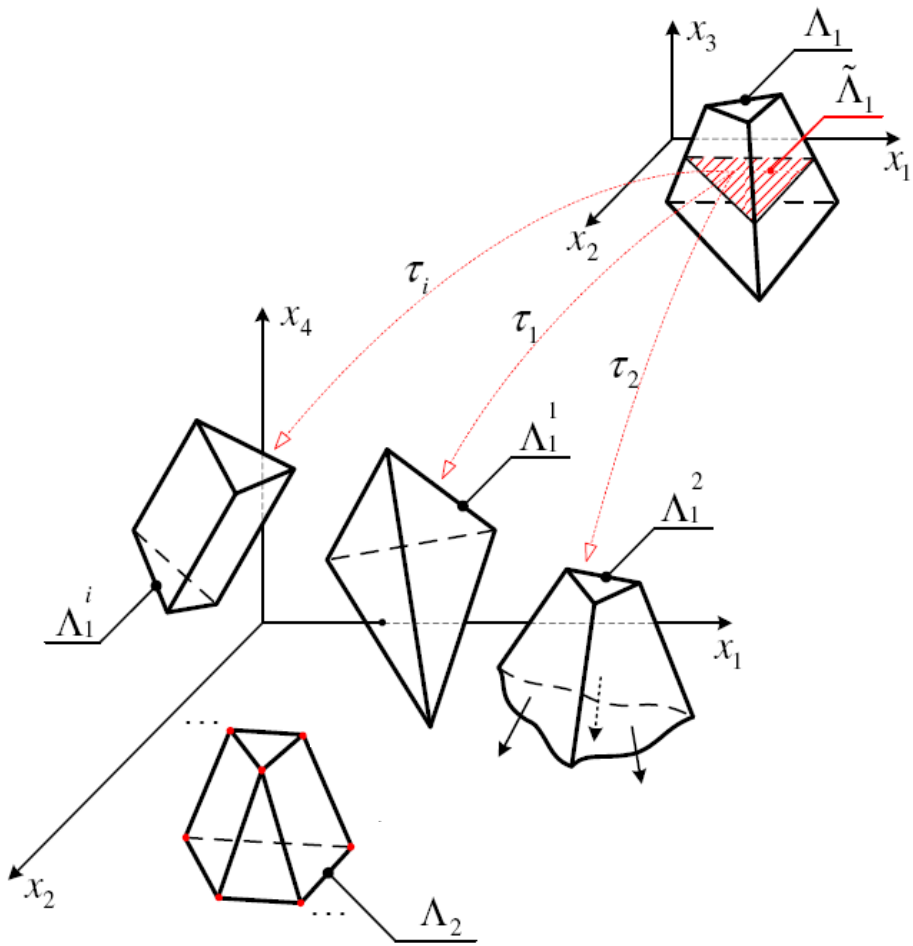
- Recall the problem: $\boxed{\Lambda_2 \Rightarrow \Lambda_1 \delta \tau}$

- τ is an affine transformation: $\boxed{\tau : \vec{y} \mapsto S\vec{x} + T\vec{z} + \vec{\beta}}$

$\vec{x} = vars(\Lambda_2) \cap vars(\Lambda_1 \delta),$	common variables
$\vec{y} = dom(\tau) = vars(\Lambda_1 \delta) \setminus vars(\Lambda_2),$	variables solely occurring in $\Lambda_1 \delta$
$\vec{z} = vars(\Lambda_2) \setminus vars(\Lambda_1 \delta),$	variables solely occurring in Λ_2

- With the substitution τ the constraint $\Lambda_1 \sigma$ contains parameter products (non-linear problem).

LAC Implication Problem



Non-closed Polyhedra Containment

- Decide whether the set

$$\Lambda_1 = \{\vec{x} \mid A'\vec{x} \le \vec{c}',\ \ A''\vec{x} < \vec{c}''\}$$

contains the set

$$\Lambda_1 = \{\vec{x} \mid B'\vec{x} \le \vec{d}',\ \ B''\vec{x} < \vec{d}''\}$$

- **Corollary 2.** *A set* $\{\boldsymbol{x} \in \mathbb{R}^n \mid A'\boldsymbol{x} \le \boldsymbol{c}', A''\boldsymbol{x} < \boldsymbol{c}''\}$ *contains a non-empty set* $\{\boldsymbol{x} \in \mathbb{R}^n \mid B'\boldsymbol{x} \le \boldsymbol{d}', B''\boldsymbol{x} < \boldsymbol{d}''\}$ *if each inequality of the first system can be obtained by a non-negative linear combination of the inequalities of* $B'\boldsymbol{x} \le \boldsymbol{d}'$, $B'' < \boldsymbol{d}''$, *or* $0 < 1$, *where at least one multiplier of a strict inequality has to be different from zero if the inequality of the original system is strict.*

Polyhedra Containment