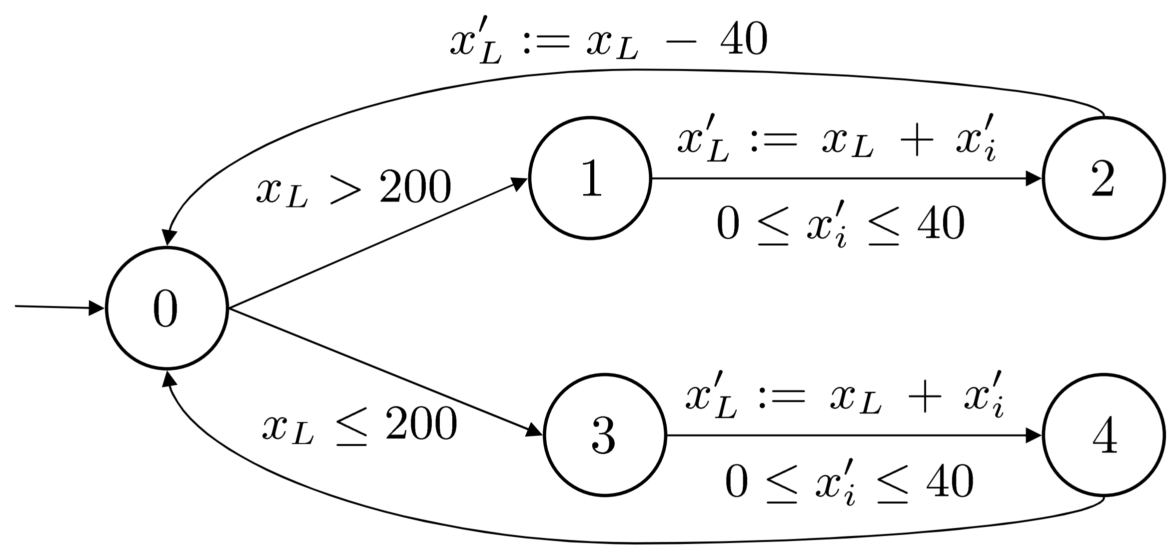
max planck institut
informatik

Superposition Modulo Linear Arithmetic
SUP(LA)

Ernst Althaus & Evgeny Kruglov & Christoph Weidenbach

Trento, September 17th, 2009

Example: Watertank Controller



$$x_L > 200 \parallel S_0(x_L, x_i) \rightarrow S_1(x_L, x_i)$$

$$x'_i \leq 40, x'_i \geq 0, x'_L = x_L + x'_i \parallel S_1(x_L, x_i) \rightarrow S_2(x'_L, x'_i)$$

$$x'_L = x_L - 40 \parallel S_2(x_L, x_i) \rightarrow S_0(x'_L, x_i)$$

$$[\forall x, y\ (x \leq 240 \wedge S_0(x, y))] \rightarrow [\exists x', y'\ (S_0(x', y') \wedge x' > 240)]$$

Motivation for LA Combination

- linear arithmetic is an important ingredient of many problems from practice
- linear arithmetic can not be handled in first-order logic

Goal

Integrate linear arithmetic (LA) over the rationals into first-order theorem proving such that

- the calculus is sound and complete
- LA-reasoning can be done in a modular way
- the result is useful

In general, a complete calculus cannot be achieved without restrictions.

State of the Art

Current Approaches:

- DPLL(LA) : boolean combinations of ground LA (dis)equations, sound, complete
- Nelson-Oppen: LA + equational theory, complete for ground settings
- DPLL(Γ) : complete for some ground cases
- Locality: sound, complete, polynomial decidability for ground local settings
- Building LA directly into the superposition calculus: no completeness, no technique for finite saturation
- Others: restrict LA and/or first-order part to finite domain

Summary:

- Completeness only for ground case

SUP(LA)

Hierarchic Combination of Superposition and Linear Arithmetic:

- sound
- complete if crucial free first-order functions are sufficiently complete
- LA reasoning is handled modular, build on existing LA solvers
- generalizes superposition and DPLL(LA)

- does not a priori generalize the ground completeness results
- hierarchic combinations are not trivially extended to several theories

- implemented in SPASS(LA) based on QSOpt, Z3

DPLL(LA)

$$u + v \geq 5 \lor v \leq 0$$

$$u + w = 4 \lor w \geq 3$$

SUP(LA)

$$c_u + c_v < 5,\ c_v > 0 \parallel \square$$

$$c_u + c_w \neq 4,\ c_w < 3 \parallel \square$$

$$x - 3z > 0,\ c_v + y > 0 \parallel P(x), Q(x,y) \rightarrow f(y) \approx y, P(y)$$

Semantics

$$\begin{aligned} &\exists u, v, w.\ [\neg(u + v < 5 \land v > 0) \quad \land \\ &\quad \neg(u + w \neq 4 \land w < 3) \quad \land \\ &\quad \forall x, y, z.\ (x - 3z > 0 \land v + y > 0 \land P(x) \land Q(x,y) \rightarrow f(y) \approx y \lor P(y))] \end{aligned}$$

SUP(LA) Calculus

Constraint Refutation:

$$\mathcal{I}\,\frac{\Lambda_1 \parallel \Box \quad \ldots \quad \Lambda_n \parallel \Box}{\Box}$$

- if $\exists\vec{v}.\forall\vec{x}.[\Lambda_1 \rightarrow \Box \wedge \ldots \wedge \Lambda_n \rightarrow \Box]$ is inconsistent in LA

Example:

$$\mathcal{I}\,\frac{x \geq 150 \parallel \Box}{\Box} \qquad \mathcal{I}\,\frac{c_v \geq 0 \parallel \Box \quad c_v < 0 \parallel \Box}{\Box}$$

Example

DPLL(LA) Problem: $(c_u > 5 \vee c_u < 2) \wedge c_u < 4 \wedge c_u > 3$

SUP(LA) Problem:

$$c_u \leq 5, c_u \geq 2 \| \square$$
$$c_u \geq 4 \| \square$$
$$c_u \leq 3 \| \square$$

Constraint Refutation: $\square$ solved by call to SMT solver (Z3)

SUP(LA) Calculus

Reflexivity Resolution:

$$\mathcal{I}\frac{\Lambda \parallel \Gamma, t \approx s \rightarrow \Delta}{(\Lambda \parallel \Gamma \rightarrow \Delta)\sigma}$$

- if $t\sigma = s\sigma$ for the mgu σ
- If the ordering restrictions apply
- if σ is simple

Example:

$$\mathcal{I}\frac{x < 0 \parallel z \approx x \rightarrow}{x < 0 \parallel \square} \quad \sigma = \{z \mapsto x\}$$

SUP(LA) Calculus

Superposition Left:

$$\mathcal{I}\,\frac{\Lambda_1 \parallel \Gamma_1 \rightarrow \Delta_1, l \approx r \qquad \Lambda_2 \parallel s[l'] \approx t, \Gamma_2 \rightarrow \Delta_2}{(\Lambda_1, \Lambda_2 \parallel s[r] \approx t, \Gamma_1, \Gamma_2 \rightarrow \Delta_1, \Delta_2)\sigma}$$

- if $l\sigma = l'\sigma$ for the mgu σ
- if l' is not a variable and the ordering restrictions apply
- if σ is simple

Example:

$$\mathcal{I}\,\frac{x < 0 \parallel f(y) \approx x \rightarrow \qquad \parallel \rightarrow f(z) \approx z}{x < 0 \parallel z \approx x \rightarrow}$$

$$x < 0 \parallel \square$$

$$\square$$

SUP(LA) Completeness

- a clause set is *sufficient complete* if all terms of free function head symbols ranging into the LA sort can be eventually reduced to LA terms

$$x < 0 \parallel f(y) \approx x \rightarrow \qquad \parallel \rightarrow f(z) \approx z$$

$$x' \geq 0 \parallel f(y') \approx x' \rightarrow$$

- SUP(LA) is complete for sufficiently complete clause sets

SUP(LA) Redundancy

- a clause is redundant if all its simple ground instances are implied by simple ground instances of smaller clauses

Subsumption Deletion:

$$\mathcal{R}\frac{\Lambda_1 \parallel \Gamma_1 \rightarrow \Delta_1 \qquad \Lambda_2 \parallel \Gamma_2 \rightarrow \Delta_2}{\Lambda_1 \parallel \Gamma_1 \rightarrow \Delta_1}$$

- if $\Gamma_1\sigma \subseteq \Gamma_2, \Delta_1\sigma \subseteq \Delta_2$
- if σ is simple
- if $\forall\vec{x}\,\exists\vec{y}\,[\Lambda_2 \rightarrow \Lambda_1\sigma]$ where $\vec{y} = vars(\Lambda_1\sigma) \setminus vars(\Lambda_2)$

Example: $x \leq 240 \parallel\rightarrow S_0(x, y)$

subsumes

$$z \leq 240, z \geq 200, y \geq 0, y \leq 40, x - y - z = -40 \parallel\rightarrow S_0(x, y)$$

LA Reasoning Tasks

Redundancy: $\forall \vec{x}.\, \exists \vec{y}.\, [\Lambda_2 \longrightarrow \Lambda_1]$

Tautology: $\exists \vec{y}.\, \Lambda$

Refutation: $\exists \vec{y}. \forall \vec{x}. [\Lambda_1 \longrightarrow \Box \wedge \ldots \wedge \Lambda_n \longrightarrow \Box]$

LA Reasoning Mapped to LP Solving

Tautology: $\exists\vec{y}.\,\Lambda$

standard LP problem if no strict inequalities

$3x < 5$ is mapped to $3(x+y) \leq 5$ and $y \neq 0$

Redundancy: $\forall\vec{x}.\,\exists\vec{y}.\,[\Lambda_2 \rightarrow \Lambda_1]$

if $\vec{y} = \{\}$ check whether all solutions of Λ_2 are contained in Λ_1

y_i is mapped to $p_1x_1 + \ldots + p_nx_n$ where $\vec{x} = \{x_1, \ldots, x_n\}$

Refutation: $\exists\vec{y}.\forall\vec{x}.[\Lambda_1 \rightarrow \Box \wedge \ldots \wedge \Lambda_n \rightarrow \Box]$

standard LP problem if $\vec{y} = \{\}$

no LP solution if $\vec{y} \neq \{\}$: use LA decision procedure

Future Work

- Mature architecture & implementation
- aim at decidability results
- study ground case
- study (several) theory combinations

Thank you for your attention