Formalizing Simplex within Isabelle/HOL

Mirko Spasić Filip Marić
{mirko|filip}@matf.bg.ac.rs

Department of Computer Science
Faculty of Mathematics
University of Belgrade

Formal and Automated Theorem Proving and Applications, 2011

Outline

Outline

Outline

Outline

Linear Arithmetic

1. Linear arithmetic over reals (LRA)
2. Linear arithmetic over integers (LIA)

Formula

- Quantifier-free linear arithmetic formula

$$a_1 x_1 + \cdots + a_n x_n \bowtie b,$$

$a_1, \ldots, a_n, b \in \mathbb{Q}, x_1, \ldots, x_n \in \mathbb{Q}(\mathbb{N})$

Decision Procedure

- Linear arithmetic is decidable
- Decision procedure, returning *sat* if and only if an input linear arithmetic formula is satisfiable, and returning *unsat*, otherwise

Two Methods

1. Fourier-Motzkin procedure
2. Simplex method

Simplex Method

- Originally constructed to solve linear programming optimization problem
- Decision procedure for linear arithmetic does not have to maximize anything, but have to find a single feasible solution of input constraints

One Variant of Simplex Method

- Dual Simplex algorithm

DPLL(T)

- SMT solvers, in the DPLL(T) framework, use Simplex-based linear arithmetic solver
- Procedure is capable of deciding the satisfiability of conjunctions of linear constraints

Outline

Reliability

- SMT solvers are quite complex software
- Result of SMT solving is *sat* or *unsat*

Main Question

Can we be so sure that solver give us right answer?

- If the answer is sat, we simply can check if the calculated model is realy model for input formula, otherwise, there is no simple checking
- Real problems require a high level of reliability

Outline

Isabelle

Our Goal

Prove correctness for Simplex method, within the Isabelle/HOL theorem proving system

- Isar (Intelligible semiautomated reasoning) language
- Primitive recursion
- Isabelle's built-in theory of Lists, theory of Sets, of Functions, Mappings, Rationals
- Effective executable code (without bugs) in functional programming languages can be generated

Outline

linear_poly

Theory of multivariate linear polynomials

- Vector space
- Associativity, commutativity, neutral element, ...
- Effectively executable operations (addition, subtraction, multiplication by constant, valuation)

Outline

Small Example

Find solution for conjunctions of linear constraints:

$$[x \geq 1, \quad y \leq -1, \quad x \leq 2, \quad y + 2x + z \geq 4, \quad x + z = 5]$$

$$\Downarrow$$

Small Example

Tableau

$s_1 = y + 2x + z$
$s_2 = x + z$

Constraints

$[x \geq 1, y \leq -1, x \leq 2, s_1 \geq 4, s_2 = 5]$

Bound and Valuation

Variable	LBound	Valuation	UBound
x	$-\infty$	0	∞
y	$-\infty$	0	∞
z	$-\infty$	0	∞
s_1	$-\infty$	0	∞
s_2	$-\infty$	0	∞

Small Example

Tableau

$s_1 = y + 2x + z$
$s_2 = x + z$

Constraints

$[x \geq 1, y \leq -1, x \leq 2, s_1 \geq 4, s_2 = 5]$

Bound and Valuation

Variable	LBound	Valuation	UBound
x	1	0	∞
y	$-\infty$	0	∞
z	$-\infty$	0	∞
s_1	$-\infty$	0	∞
s_2	$-\infty$	0	∞

Small Example

Tableau

$s_1 = y + 2x + z$
$s_2 = x + z$

Constraints

$[x \geq 1, y \leq -1, x \leq 2, s_1 \geq 4, s_2 = 5]$

Bound and Valuation

Variable	LBound	Valuation	UBound
x	1	1	∞
y	$-\infty$	0	∞
z	$-\infty$	0	∞
s_1	$-\infty$	2	∞
s_2	$-\infty$	1	∞

Small Example

Tableau

$s_1 = y + 2x + z$
$s_2 = x + z$

Constraints

$[x \geq 1, y \leq -1, x \leq 2, s_1 \geq 4, s_2 = 5]$

Bound and Valuation

Variable	LBound	Valuation	UBound
x	1	1	∞
y	$-\infty$	0	-1
z	$-\infty$	0	∞
s_1	$-\infty$	2	∞
s_2	$-\infty$	1	∞

Small Example

Tableau

$s_1 = y + 2x + z$
$s_2 = x + z$

Constraints

$[x \geq 1, y \leq -1, x \leq 2, s_1 \geq 4, s_2 = 5]$

Bound and Valuation

Variable	LBound	Valuation	UBound
x	1	1	∞
y	$-\infty$	-1	-1
z	$-\infty$	0	∞
s_1	$-\infty$	1	∞
s_2	$-\infty$	1	∞

Small Example

Tableau

$s_1 = y + 2x + z$
$s_2 = x + z$

Constraints

$[x \geq 1, y \leq -1, x \leq 2, s_1 \geq 4, s_2 = 5]$

Bound and Valuation

Variable	LBound	Valuation	UBound
x	1	1	2
y	$-\infty$	-1	-1
z	$-\infty$	0	∞
s_1	$-\infty$	1	∞
s_2	$-\infty$	1	∞

Small Example

Tableau

$s_1 = y + 2x + z$
$s_2 = x + z$

Constraints

$[x \geq 1, y \leq -1, x \leq 2, s_1 \geq 4, s_2 = 5]$

Bound and Valuation

Variable	LBound	Valuation	UBound
x	1	1	2
y	$-\infty$	-1	-1
z	$-\infty$	0	∞
s_1	4	1	∞
s_2	$-\infty$	1	∞

Small Example

Tableau

$$x = 0.5s_1 - 0.5y - 0.5z$$
$$s_2 = 0.5s_1 - 0.5y + 0.5z$$

Constraints

$$[x \geq 1, y \leq -1, x \leq 2, s_1 \geq 4, s_2 = 5]$$

Bound and Valuation

Variable	LBound	Valuation	UBound
x	1	1	2
y	$-\infty$	-1	-1
z	$-\infty$	0	∞
s_1	4	1	∞
s_2	$-\infty$	1	∞

Small Example

Tableau

$$x = 0.5s_1 - 0.5y - 0.5z$$
$$s_2 = 0.5s_1 - 0.5y + 0.5z$$

Constraints

$$[x \geq 1, y \leq -1, x \leq 2, s_1 \geq 4, s_2 = 5]$$

Bound and Valuation

Variable	LBound	Valuation	UBound
x	1	2.5	2
y	$-\infty$	-1	-1
z	$-\infty$	0	∞
s_1	4	4	∞
s_2	$-\infty$	2.5	∞

Small Example

Tableau

$z = s_1 - y - 2x$

$s_2 = s_1 - y - x$

Constraints

$[x \geq 1, y \leq -1, x \leq 2, s_1 \geq 4, s_2 = 5]$

Bound and Valuation

Variable	LBound	Valuation	UBound
x	1	2.5	2
y	$-\infty$	-1	-1
z	$-\infty$	0	∞
s_1	4	4	∞
s_2	$-\infty$	2.5	∞

Small Example

Tableau

$z = s_1 - y - 2x$

$s_2 = s_1 - y - x$

Constraints

$[x \geq 1, y \leq -1, x \leq 2, s_1 \geq 4, s_2 = 5]$

Bound and Valuation

Variable	LBound	Valuation	UBound
x	1	2	2
y	$-\infty$	-1	-1
z	$-\infty$	1	∞
s_1	4	4	∞
s_2	$-\infty$	3	∞

Small Example

Tableau

$z = s_1 - y - 2x$

$s_2 = s_1 - y - x$

Constraints

$[x \geq 1, y \leq -1, x \leq 2, s_1 \geq 4, s_2 = 5]$

Bound and Valuation

Variable	LBound	Valuation	UBound
x	1	2	2
y	$-\infty$	-1	-1
z	$-\infty$	1	∞
s_1	4	4	∞
s_2	5	3	5

Small Example

Tableau

$z = s_2 - x$

$s_1 = s_2 + y + x$

Constraints

$[x \geq 1, y \leq -1, x \leq 2, s_1 \geq 4, s_2 = 5]$

Bound and Valuation

Variable	LBound	Valuation	UBound
x	1	2	2
y	$-\infty$	-1	-1
z	$-\infty$	1	∞
s_1	4	4	∞
s_2	5	3	5

Small Example

Tableau

$z = s_2 - x$

$s_1 = s_2 + y + x$

Constraints

$[x \geq 1, y \leq -1, x \leq 2, s_1 \geq 4, s_2 = 5]$

Bound and Valuation

Variable	LBound	Valuation	UBound
x	1	2	2
y	$-\infty$	-1	-1
z	$-\infty$	3	∞
s_1	4	6	∞
s_2	5	5	5

Small Example

Tableau

$z = s_2 - x$

$s_1 = s_2 + y + x$

Constraints

$[x \geq 1, y \leq -1, x \leq 2, s_1 \geq 4, s_2 = 5]$

Bound and Valuation

Variable	LBound	Valuation	UBound
x	1	2	2
y	$-\infty$	-1	-1
z	$-\infty$	3	∞
s_1	4	6	∞
s_2	5	5	5

Algorithm

Step of Algorithm

$$\frac{\text{Input list of constraints} \quad \Longrightarrow \quad \text{List of basic constraints}}{\text{l} \quad \dashrightarrow \quad \text{init1 (l)}}$$

$$\frac{\text{List of basic constraints} \quad \Longrightarrow \quad \text{state } *}{\text{init1 (l)} \quad \dashrightarrow \quad \text{init2 (init1 (l))}}$$

$$\frac{\text{state} \quad \Longrightarrow \quad \text{state}}{\text{s} \quad \dashrightarrow \quad \text{check (assert\_next (s))}}$$

$$^{*}state \equiv (tableau \times constraints \times LBound \times Valuation \times UBound)$$

Outline

Main Lemmas and Theorem

Lemmas

- $satisfiable(l) \iff satisfiable(init1(l))$
- $satisfiable(init1(l)) \iff satisfiable(init2(init1(l)))$
- $satisfiable(s) \iff satisfiable(check(assert\_next(s)))$

Theorem

$$satisfiable(l) \iff simplex(l)$$

Future work

Doubtless

- Finallize this proof

Perhaps

- Formalize whole SMT solver for linear arithmetic, using formalized SAT solver

The End

Thanks for your attention!