Decision procedures for Linear Arithmetic

Christophe Ringeissen

LORIA

Lecture 2

Outline

Outline

Uninterpreted Functions + Arithmetic: An Example

$$x+1 \neq 1+y, x = f(c), y = f(d), c \leq d, d+a \leq c, a+b = 1, b = 1+a$$

It is possible to get rid of f by adding the instances of the congruence axiom (Ackermann expansion): the above formula can be equivalently transformed into

$$x+1 \neq 1+y, c = d \Rightarrow x = y, c \leq d, d+a \leq c, a+b = 1, b = 1+a$$

How to solve/satisfy this Linear Arithmetic formula?

Outline

Linear Arithmetic (LA)

- A signature $\Sigma_{LA} = (\{0, 1, +\}, \{\leq\})$
- A single Σ_{LA}-structure, say $LA(X)$, defined by the domain X and the standard interpretation of Σ_{LA}-symbols over X
  - ▷ if X is the set of naturals, then we speak of LA over the naturals
  - ▷ if X is the set of integers, then we speak of LA over the integers
  - ▷ if X is the set of rationals/reals, then we speak of LA over the rational/reals
- $T_{LA(X)}$ is the set of sentences φ such that $LA(X) \models \varphi$
- Why is it important to consider different domains*?*
  - ▷ Satisfiability of formulae may change... Exercise: find an example*!*
- Why have we put together the case rationals and reals?

Theory of Linear Arithmetic (Rationals)

Signature:

$$
\begin{aligned}
&+ : \mathit{rat} \times \mathit{rat} \to \mathit{rat}\\
&0 : \mathit{rat}\\
&1 : \mathit{rat}\\
&<: \mathit{rat} \times \mathit{rat}
\end{aligned}
$$

Some true sentences

$$
\begin{aligned}
&\forall x.\ x + 0 = 0 + x\\
&\forall x, y, z.\ x + (y + z) = (x + y) + z\\
&\forall x, y.\ x + y = y + x\\
&\forall x.\ x + \cdots + x = 0 \Rightarrow x = 0\\
&\forall x \exists y.\ y + \cdots + y = x\\
&0 \neq 1\\
&\forall x.\ \neg(x < x)\\
&\forall x, y, z.\ (x < y \wedge y < z) \Rightarrow x < z\\
&\forall x, y.\ x < y \vee y < x \vee x = y\\
&0 < 1
\end{aligned}
$$

Is there a finite axiomatization? (what about the ...?)

Architecture of a Dec Proc for LA(Rationals)

Literals in LA are equalities ($s = t$), disequalities ($s \neq t$), and inequalities ($s \leq t$)

- Gauss elimination solves conjunctions of equalities
- Fourier-Motzkin checks satisfiability of conjunctions of inequalities and derives entailed equalities
- The disequality handler checks the satisfiability of disequalities

Gauss elimination

Standard algorithm in linear algebra

$$
\begin{array}{ccccccc}
a_{11}x_1 & + & a_{12}x_2 & +\cdots+ & a_{1n}x_n & = & b_1 \\
a_{21}x_1 & + & a_{22}x_2 & +\cdots+ & a_{2n}x_n & = & b_2 \\
\vdots & & \vdots & & \vdots & & \vdots \\
a_{m1}x_1 & + & a_{m2}x_2 & +\cdots+ & a_{mn}x_n & = & b_m
\end{array}
$$

Successive elimination of variables (choose j and replace ℓ_i by $\ell_i + c_j\ell_j$ for $i \neq j$):

$$
\begin{array}{ccccccc}
a_{11}x_1 & + & a_{12}x_2 & +\cdots+ & a_{1n}x_n & = & b_1 \\
 & & a'_{22}x_2 & +\cdots+ & a'_{2n}x_n & = & b'_2 \\
 & & \vdots & & \vdots & & \vdots \\
 & & a'_{m2}x_2 & +\cdots+ & a'_{mn}x_n & = & b'_m
\end{array}
$$

Gauss elimination (cont'd)

After Gauss elimination, we get a triangular matrix
$Ax = b$ is unsatisfiable iff there $n = 0$ in the matrix, where n is rational different from 0
If $Ax = b$ is satisfiable, then Gauss elimination leads to a solved form

$$\bigwedge_{i=1}^{n} x_i = t_i$$

obtained by "back-substitution" from the triangular matrix

Gauss Elimination: Satisfiable Example

$$\left\{ \begin{array}{l} x + y + z = 10 \\ 2x + y + 3z = 20 \end{array} \right| \times(-2)$$

Elimination of x:

$$\left\{ \begin{array}{l} x + y + z = 10 \\ -y + z = 0 \end{array} \right.$$

Back-substitution:

$$\left\{ \begin{array}{l} x = 10 - 2z \\ y = z \end{array} \right.$$

Gauss Elimination: Unsatisfiable Example

$$\begin{cases} x + y = 2 \\ x + 2y = 3 \\ 2x + 3y = 4 \end{cases}$$

After pivoting:

$$\begin{cases} x + y = 2 \\ y = 1 \\ y = 0 \end{cases}$$

and so $0 = 1$: *UNSAT*.

Fourier-Motzkin Elimination

- Principle: eliminate a variable x thanks to transitivity

$$x \leq \alpha, \beta \leq x \leadsto \beta \leq \alpha$$

$\beta \leq \alpha$ is UNSAT if β, α are numbers such that $\beta > \alpha$.

- How to deduce the implicit equalities?

Implicit equalities come from the inequalities involved in the derivation of $0 \leq 0$.
Example: $x \leq y, y \leq x$ leads to $0 \leq 0$ and the two inequalities are indeed implicit equalities $x = y, y = x$

Fourier-Motzkin Elimination: An Example

$$\left\{ \begin{array}{l} 3x \leq 2y \\ 3y \leq 4 \\ 3 \leq 2x \end{array} \right. \left| \begin{array}{l} \times 2 \\ \\ \times 3 \end{array} \right.$$

By eliminating x, we generate

$$\left\{ \begin{array}{l} 3y \leq 4 \\ 9 \leq 4y \end{array} \right. \left| \begin{array}{l} \times 4 \\ \times 3 \end{array} \right.$$

By eliminating y, we get $27 \leq 16$: UNSAT

Derive entailed inequalities

Theorem

(Farkas) The set of consequences of a given set of inequalities is closed under non-negative linear combinations

Using the following definitions:

- A non-negative (positive) linear combination of $C_1, ..., C_m$ is an inequality of the form $\sum_{i=1}^{m} \alpha_k C_k$ where each $\alpha_k \geq 0$ ($\alpha_k > 0$, resp) for $k = 1, ..., m$
- αC_k denotes the expression $\sum_{j=1}^{n} \alpha a_{k,j} x_j \leq \alpha b_k$
- $C_1 + C_2$ denotes the expression $\sum_{j=1}^{n} (a_{1,j} + a_{2,j}) x_j \leq (b_1 + b_2)$
- C_k (for $k = 1, ..., m$) denotes the inequality

$$\sum_{j=1}^{n} a_{k,j} x_j \leq b_k$$

Derive entailed implicit equalities

Proposition

If $\alpha_k > 0$ for $k = 1, ..., m$ and $\sum_{k=1}^{m} \alpha_k C_k = 0 \leq 0$ then C_j is an implicit equality for $j = 1, ..., m$

Obtain Implicit equalities: Proof

Proof.

$$\sum_{k=1}^{m} \alpha_k C_k = \alpha_1 C_1 + \cdots + \alpha_j C_j + \cdots \alpha_m C_m = 0,$$

$$-1 C_j = \sum_{k=1, k \neq j}^{m} \frac{\alpha_k}{\alpha_j} C_j \quad \text{for } j = 1, ..., m$$

Since the set of consequence of $P := \{C_1, ..., C_m\}$ is closed under non-negative combinations, we have that $P \models -1 C_j$. On the other hand, we have that $P \models C_j$ (since $C_j \in P$). □

Fourier-Motzkin Elimination

Aim: Elimination of a variable thanks to transitivity

- Consider a set of inequalities φ and a variable x occurring in φ with coefficients of different signs
- Partition φ into
  - $x \leq \alpha$ (x of positive sign): $\{x \leq \alpha_i \mid x \leq \alpha_i \in \varphi\}$
  - $\beta \leq x$ (x of negative sign): $\{\beta_i \leq x \mid \beta_i \leq x \in \varphi\}$
  - γ (x not in γ)
- Consider $(\beta \leq \alpha) \cup \gamma$ where
  $\beta \leq \alpha = \{\beta_i \leq \alpha_i \mid \beta_i \leq x \in (\beta \leq x), x \leq \alpha_i \in (x \leq \alpha)\}$

Proposition

φ and $(\beta \leq \alpha) \cup \gamma$ are equisatisfiable.

Complexity of Fourier-Motzkin Algorithm

When eliminating a variable, a quadratic number of inequalities may be introduced:

$$m \xrightarrow{x_1} m^2 \xrightarrow{x_2} (m^2)^2 \cdots \xrightarrow{x_n} m^{2^n}$$

Fourier-Motzkin is doubly exponential...
➽ Interest of considering special cases of inequalities

Modified Fourier-Motzkin Algorithm

- The algorithm can be modified also to derive implicit equalities
  - ▷ each inequality C_k in the initial set is given a label (say k) and is augmented with a set containing its label, i.e. $C_k : \{k\}$
  - ▷ when performing a Fourier step, we propagate labels as follows:

$$c_i C_j + c_j C_i : L_i \cup L_j$$

where L_i is the set of labels associated to C_i and L_j that associated to C_j

- whenever an inequality of the form $0 \leq 0 : L$ is derived, all inequalities whose labels are in L are implicit equalities

Handling Disequalities in Convex Theories

Definition

A theory T is said to be *convex* if for any T-satisfiable set of equalities P, we have $T \models (P \Rightarrow \bigvee_{i=1}^{n} s_i = t_i)$ implies there exists some $k \in [1, n]$ such that $T \models (P \Rightarrow s_k = t_k)$.

This definition can be reworded in terms of satisfiability:

Definition

A theory T is said to be *convex* if for any T-satisfiable set of equalities P, we have $\neg(P \Rightarrow \bigvee_{i=1}^{n} s_i = t_i)$ is T-unsatisfiable implies there exists some $k \in [1, n]$ such that $\neg(P \Rightarrow s_k = t_k)$ is T-unsatisfiable.

Since $\neg(P \Rightarrow Q)$ corresponds to $P \wedge \neg Q$, we get:

Definition

A theory T is said to be *convex* if for any T-satisfiable set of equalities P, we have $P \wedge \bigwedge_{i=1}^{n} s_i \neq t_i$ is T-unsatisfiable implies there exists some $k \in [1, n]$ such that $P \wedge s_k \neq t_k$ is T-unsatisfiable.

Convex Theories: Examples and Counter-Examples

Examples of **convex** theories:

Theory of equality
LA(Rationals)

Some **non-convex** theories:

LA(Naturals):

$$x + y = 1 \Rightarrow x = 1 \vee y = 1$$

but $x + y = 1 \not\Rightarrow x = 1$ and $x + y = 1 \not\Rightarrow y = 1$
Theory of Arrays:

$$e = rd(wr(a, i, d), j) \Rightarrow e = d \vee e = rd(a, j)$$

but $e = rd(wr(a, i, d), j) \not\Rightarrow e = d$ and
$e = rd(wr(a, i, d), j) \not\Rightarrow e = rd(a, j)$

Disequality Handler

- Independence of disequalities:

➽ **convexity**: LA(Rationals) is convex

- So, the disequality handler only needs to consider the solved equalities (derived by Gauss elimination) and perform the substitutions in each disequality separately

  ▷ unsatisfiability is reported as soon as a disequality of the form $s \neq s$ is obtained by performing such substitutions

Disequality Handler: Example

$$\begin{cases} x + y + z = 10 \\ 2x + y + 3z = 20 \\ 3x + 6y \neq 30 \end{cases}$$

Solving the set of equalities leads to the solved form:

$$\begin{cases} x = 10 - 2z \\ y = z \end{cases}$$

Substituting x and y in the disequality:

$$(3x + 6y \neq 30)\{x \mapsto 10 - 2z, y \mapsto z\}$$

$$30 - 6z + 6z \neq 30$$

$$30 \neq 30$$

UNSAT

A Decision Procedure for LA(Rationals)

- Equalities/Inequalities/Disequalities sent to the related module GE/FME/DH
- Each module applies a certain set of rules to make it trivial to check the unsatisfiability (cf. deriving $\perp$)
- Entailed equalities of the form $x = t$ (where x is a variable which does not occur in t) derived by GE are sent
  - to FME to eliminate one variable
  - to DH to simplify the disequalities so to make it trivial to check the unsatisfiability (cf. deriving $t \neq t$)
- Implicit equalities derived by FME are sent to GE to furtherly simplify equalities

Satisfiability Problem in LA(Rationals)

$$\begin{cases} 2x + y + 3z = 20 \\ x + y + z \leq 10 \\ 10 + 2x - 2y \leq 4x + 2z - 10 \\ 3x + 6y \neq 30 \end{cases}$$

Satisfiable?
Is there any implicit equality?

Outline

Difference Constraints (Pratt)

A special case of linear arithmetic, where constraints are of the form: $x_i - x_j \leq c$, or $x_i - 0 \leq c$, or $0 - x_j \leq c$.

A common form of constraint (in verification problems)

Construction of a **directed** graph with a vertex 0 and a vertex per variable: $x_i - x_j \leq c$ represented by an edge $x_i \rightarrow x_j$ of weight c.

Theorem

A set of difference constraints is satisfiable iff there is no negative weight cycle in the graph.

Complexity: $O(n^3)$ thanks to the Bellman-Ford algorithm to solve the "single-source shortest-path problem"