

A Simplex variant:

Transform the satisfiability problem into the form

$$\begin{aligned} A\vec{x} &= \vec{0} \\ \vec{l} &\leq \vec{x} \leq \vec{u} \end{aligned}$$

(where  $l_i$  may be  $-\infty$  and  $u_i$  may be  $+\infty$ ).

Relation to optimization problem is obscured.

But: More efficient if one needs an incremental decision procedure, where inequations may be added and retracted (Dutertre and de Moura 2006).

## 1.5 Non-linear Real Arithmetic

Tarski (1951): Quantifier elimination is possible for *non-linear* real arithmetic (or more generally, for real-closed fields). His algorithm had non-elementary complexity, however.

An improved algorithm by Collins (1975) (with further improvements by Hong) has doubly exponential complexity: Cylindrical algebraic decomposition (CAD).

Implementation: QEPCAD.

### Cylindrical Algebraic Decomposition

Given: First-order formula over atoms of the form  $f_i(\vec{x}) \sim 0$ , where the  $f_i$  are polynomials over variables  $\vec{x}$ .

Goal: Decompose  $\mathbb{R}^n$  into a finite number of regions such that all polynomials have invariant sign on every region  $X$ :

$$\begin{aligned} \forall i \ ( \forall \vec{x} \in X. f_i(\vec{x}) < 0 \\ \vee \forall \vec{x} \in X. f_i(\vec{x}) = 0 \\ \vee \forall \vec{x} \in X. f_i(\vec{x}) > 0 ) \end{aligned}$$

Note: Implementation needs exact arithmetic using algebraic numbers (i.e., zeroes of univariate polynomials with integer coefficients).

## 1.6 Real Arithmetic incl. Transcendental Functions

Real arithmetic with exp/log: decidability unknown.

Real arithmetic with trigonometric functions: undecidable

The following formula holds exactly if  $x \in \mathbb{Z}$ :

$$\exists y (\sin(y) = 0 \wedge 3 < y \wedge y < 4 \wedge \sin(x \cdot y) = 0)$$

(note that necessarily  $y = \pi$ ).

Consequence: Peano arithmetic (which is undecidable) can be encoded in real arithmetic with trigonometric functions.

However, real arithmetic with transcendental functions is decidable for formulas that are *stable under perturbations*, i. e., whose truth value does not change if numeric constants are modified by some sufficiently small  $\varepsilon$ .

Example:

Stable under perturbations:  $\exists x x^2 \leq 5$

Not stable under perturbations:  $\exists x x^2 \leq 0$

(Formula is true, but if we subtract an arbitrarily small  $\varepsilon > 0$  from the right-hand side, it becomes false.)

Unsatisfactory from a mathematical point of view, but sufficient for engineering applications (where stability under perturbations is necessary anyhow).

Approach:

Interval arithmetic + interval bisection if necessary (Ratschan).

Sound for general formulas; complete for formulas that are stable under perturbations; may loop forever if the formula is not stable under perturbations.

## 1.7 Linear Integer Arithmetic

Linear integer arithmetic = Presburger arithmetic.

Decidable (Presburger, 1929), but quantifier elimination is only possible if additional divisibility operators are present:

$\exists x (y = 2x)$  is equivalent to  $\text{divides}(2, y)$  but not to any quantifier-free formula over the base signature.

Cooper (1972): Quantifier elimination procedure, triple exponential for arbitrarily quantified formulas.

## The Omega Test

Omega test (Pugh, 1991): variant of Fourier–Motzkin for conjunctions of (in-)equations in linear integer arithmetic.

Idea:

- Perform easy transformations, e. g.:  
 $3x + 6y \leq 8 \mapsto 3x + 6y \leq 6 \mapsto x + 2y \leq 2$   
 $3x + 6y = 8 \mapsto \perp$   
(since  $3x + 6y$  must be divisible by 3).
- Eliminate equations  
(easy, if one coefficient is 1; tricky otherwise).
- If only inequations are left:  
no real solutions  $\rightarrow$  unsatisfiable for  $\mathbb{Z}$   
“sufficiently many” real solutions  $\rightarrow$  satisfiable for  $\mathbb{Z}$   
otherwise: branch

What does “sufficiently many” mean?

Consider inequations  $ax \leq s$  and  $bx \geq t$  with  $a, b \in \mathbb{N}^{>0}$  and polynomials  $s, t$ .

If these inequations have real solutions, the interval of solutions ranges from  $\frac{1}{b}t$  to  $\frac{1}{a}s$ .

The longest possible interval of this kind that does not contain any integer number ranges from  $i + \frac{1}{b}$  to  $i + 1 - \frac{1}{a}$  for some  $i \in \mathbb{Z}$ ; it has the length  $1 - \frac{1}{a} - \frac{1}{b}$ .

Consequence:

If  $\frac{1}{a}s > \frac{1}{b}t + (1 - \frac{1}{a} - \frac{1}{b})$ , or equivalently,  $bs \geq at + ab - a - b + 1$  is satisfiable, then the original problem must have integer solutions.

It remains to consider the case that  $bs \geq at$  is satisfiable (hence there are real solutions) but  $bs \geq at + ab - a - b + 1$  is not (hence the interval of real solutions need not contain an integer).

In the latter case,  $bs \leq at + ab - a - b$  holds, hence for every solution of the original problem:

$$t \leq bx \leq \frac{b}{a}s \leq t + (b - 1 - \frac{b}{a})$$

$$\text{and if } x \text{ is an integer, } t \leq bx \leq t + \lfloor b - 1 - \frac{b}{a} \rfloor$$

$\Rightarrow$  Branch non-deterministically:

$$\text{Add one of the equations } bx = t + i \text{ for } i \in \{0, \dots, \lfloor b - 1 - \frac{b}{a} \rfloor\}.$$

Alternatively, if  $b > a$ :

$$\text{Add one of the equations } ax = s - i \text{ for } i \in \{0, \dots, \lfloor a - 1 - \frac{a}{b} \rfloor\}.$$

Note: Efficiency depends highly on the size of coefficients. In applications from program verification, there is almost always some variable with a very small coefficient. If all coefficients are large, the branching step gets expensive.

## Branch-and-Cut

Alternative approach: Reduce satisfiability problem to optimization problem (like Simplex). ILP, MILP: (mixed) integer linear programming.

Two basic approaches:

Branching: If the simplex algorithm finds a solution with  $x = 2.7$ , add the inequation  $x \leq 2$  or the inequation  $x \geq 3$ .

Cutting planes: Derive an inequation that holds for all real solutions, then round it to obtain an inequation that holds for all integer solutions, but not for the real solution found previously.

Example:

$$\begin{aligned} \text{Given: } \quad 2x - 3y &\leq 1 \\ \quad \quad 2x + 3y &\leq 5 \\ \quad \quad -5x - 4y &\leq -7 \end{aligned}$$

Simplex finds an extremal solution  $x = \frac{3}{2}$ ,  $y = \frac{2}{3}$ .

From the first two inequations, we see that  $4x \leq 6$ , hence  $x \leq \frac{3}{2}$ . If  $x \in \mathbb{Z}$ , we conclude  $x = \lfloor x \rfloor \leq \lfloor \frac{3}{2} \rfloor = 1$ .

$\Rightarrow$  Add the inequation  $x \leq 1$ , which holds for all integer solutions, but cuts off the solution  $(\frac{3}{2}, \frac{2}{3})$ .

In practice:

Use both: Alternate between branching and cutting steps.  
Better performance than the individual approaches.

## 1.8 Difference Logic

Difference Logic (DL):

Fragment of linear rational or integer arithmetic.

Formulas: conjunctions of atoms  $x - y < c$  or  $x - y \leq c$ ,

$x, y \in X$ ,

$c \in \mathbb{Q}$  (or  $c \in \mathbb{Z}$ ).