Master Sciences Informatiques

Solvers Principles and Architectures (SPA)

Final Exam, Fall 2019

Khalil Ghorbal

1 Combining Theories

A typical SMT solver has several back-ends (one for each supported theory) as well as an underlying SAT solver to handle the Boolean structure of the problem to solve. The solver relies crucially on combining theories, that is the ability to propagate learned results from one backend to another to either prove falsity or find a model.

1. Cite one generic method that allows combining several theories. What restriction does it have?
2. Cite other generic means to combine theories that overcome such restriction? (hint: remember the seminar!)

Consider the formula: $\varphi := x^2 + y^2 \leq 1 \wedge 2x + 2y \geq 3$, and suppose you only have the polyheral abstract domain (the theory of linear inequalities) at your disposal.

3. How would you proceed to prove that φ is UNSAT over the reals? (hint: think of an appropriate logical cut.)

3.$'$ What open goal you will still have to discharge?

4. Is it always possible to find such cuts? Can you slightly edit φ to make it a counter-example?

Bonus .

The satisfiability of the formula φ, and in general any logical combination of polynomial equations and inequalities, is decidable. Indeed, φ is SAT if and only if the sentence $\exists x.\exists y.\quad \varphi$ is true.

5. Perform the Cylindrical Algebraic Decomposition (CAD) of φ and prove it is UNSAT.
6. What are the advantages of combining linear theories (using eventually over-approximations for nonlinear expressions) compared to CAD? Explain.

2 Dantzig's Lexicographic Rule

The simplex algorithm iterates over the bases while decreasing the reduced cost.

1. Explain why the termination is ensured when the decrease is strict at each iteration.

The decrease can however be non-strict leading to degenerate cases for which termination is no longer guaranteed. For instance, consider the following pyramid:

$$P := \{(x, y, z) \in \mathbb{R}^3 \mid y + z \leq 1 \wedge z - y \leq 1 \wedge x + z \leq 1 \wedge z - x \leq 1 \wedge z \geq 0\},$$

and the following optimization problem (see Figure 1)

$$\begin{array}{rl} \min & x - y - 3z \\ \text{s.t.} & (x, y, z) \in P \end{array}$$

The point $s := (0, 0, 1)$ is a (geometric) vertex that corresponds to the top of the pyramid.

2. Rewrite the problem to apply the simplex algorithm.

3. Perform one step of the algorithm assuming the initial point is s (you can use the tableau presentation). What decision the algorithm could make, why?

In general, consider the linear optimization problem ($A \in \mathbb{R}^{m \times n}$):

$$\begin{aligned} \min \quad & c \cdot x \\ \text{s.t.} \quad & Ax \geq b \end{aligned} \qquad (\mathcal{P})$$

and its perturbed version:

$$\begin{aligned} \min \quad & c \cdot x \\ \text{s.t.} \quad & Ax \geq \tilde{b} \qquad \text{where } \tilde{b}_i = b_i - \epsilon^i \end{aligned}$$

for some positive $\epsilon \ll 1$.

4. Does the perturbed problem have degenerate bases? Explain why.

$4'$. Give the geometric intuition for the pyramid P.

Dantzig's idea is to encode a real number r as a polynomial in ϵ of degree at most m:

$$r + r_1\epsilon + r_2\epsilon^2 + \cdots + r_m\epsilon^m,$$

represented as a row: $(r, r_1, \ldots, r_m)$. The usual order over the reals is replaced by the following *lexicographic* order [1]

$$(r, r_1, \ldots, r_m) \geq_{\texttt{lex}} (s, s_1, \ldots, s_m) \iff r + r_1\epsilon + \cdots + r_m\epsilon^m \geq s + s_1\epsilon + \cdots + s_m\epsilon^m, \quad \forall \epsilon.\ 0 < \epsilon \ll 1$$

Now the feasible set $\{x \in \mathbb{R}^n \mid Ax \geq \tilde{b}\}$ can be encoded as:

$$\left\{ y \in \mathbb{R}^{n \times (1+m)} \mid Ay \geq_{\texttt{lex}} \begin{pmatrix} b & -I_m \end{pmatrix} \right\},$$

where $\geq_{\texttt{lex}}$ over $\mathbb{R}^{m \times (1+m)}$ is interpreted row by row.

Consider the following optimization problem ($y \in \mathbb{R}^{n \times (1+m)}$):

$$\begin{aligned} \min \quad & \begin{pmatrix} c & 0 \end{pmatrix} \cdot y \\ \text{s.t.} \quad & Ay \geq_{\texttt{lex}} \begin{pmatrix} b & -I_m \end{pmatrix} \end{aligned} \qquad (\tilde{\mathcal{P}})$$

5. Define the bases (algebraic vertices) for $(\tilde{\mathcal{P}})$. We will call them `lex`-bases.
6. Prove that `lex`-bases of $(\tilde{\mathcal{P}})$ form a subset of the bases of $(\mathcal{P})$. (Observe that the matrix A is left unchanged in $(\tilde{\mathcal{P}})$.)

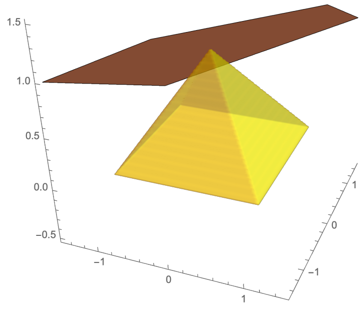

Figure 1: Pyramid P together with the hyperplane defining the objective function at the extreme point.

[1] Check quickly that it is actually an *order*!