NP-time variable elimination method.

Souymodip Chakraborty

November 5, 2015

Abstract

1

Consider the ring of polynomials $D[X]$ in the *integral domain* D, where X is the set of indeterminates (or variables). A polynomial $p(x_1,\cdots,x_n)$, with variables $x_1,\cdots,x_n \in X$, is seen as a sum of products with nonzero coefficients in D, where each $x_1^{d_1}\cdots x_n^{d_n}$ is called a *term*; together with its coefficient it is called a *monomial*; the *degree* of the term $x_1^{d_1}\cdots x_n^{d_n}$ is $d_1+\cdots+d_n$; *degree* of a polynomial is the maximum degree of its terms. A polynomial is multivariate if $|X|>1$. The ring of multivariate polynomials $D[X]$ can be viewed as a ring of univariate polynomials $D[X\setminus\{x\}][x]$ with coefficients in the integral domain $D[X\setminus\{x\}]$ ([?] page 63, Theorem 2.). Particularly, the degree of a term of a polynomial in $D[X\setminus\{x\}][x]$ is the power of x in that term.

$E(D[X])$ is the set of (in)equations (e.g $x_1^2-x_2\geq 0.4$) where the left hand side (lhs) is a polynomial (e.g. $x_1^2-x_2$) in $D[X]$ and the right hand side (e.g. 0.4) is in D. A variable x is *independent* of $H\subseteq E(D[X])$ iff $H = H\cap E(D[X\setminus\{x\}])$ else it is *dependent.* The *quotient domain* $\mathcal{Q}(D)$ is the rational form of the type $\frac{f}{g}$ where $f,g\in D$.

A weighted tree T is a triple (V,E,w), where V is the set of vertices, $E\subseteq V\times V$ is the set of edges and w is an injective weight function from $E\to\mathcal{V}$, where $\mathcal{V}$ is a set of variables. Let $X=\mathsf{img}(w)$. Define relations next and parent as follows; for $x,y\in X$, $v,v',v_1,v_2\in V$, with $w^{-1}(x)=(v_1,v)$ and $w^{-1}(y)=(v',v_2)$, $(x,y)\in\mathsf{next}$ iff $v=v'$, and $(x,y)\in\mathsf{parent}$ iff $v_1=v'$. next^+ is the transitive closure of next. Consider a term $\sigma=x_1\cdots x_k$ such that for every $1\leq i<k$, $(x_i,x_{i+1})\in\mathsf{next}$. Define $\mathsf{head}(\sigma)=x_1$, $\mathsf{tail}(\sigma)=x_k$ and $x_i\cdots x_k$ as a suffix of σ, for $1\leq i\leq k$. Let $H\subseteq E(\mathbb{Q}[X])$ be a set of (in)equations with the following properties. For each $\xi\in H$:

P1. For all $x\in X$, $\mathsf{lhs}(\xi)\in\mathbb{Q}[X\setminus\{x\}][x]\to\mathsf{degree}(\xi)\leq 1$

P2. For each term $\sigma=x_1\cdots x_k$ in ξ, $(x_i,x_{i+1})\in\mathsf{next}$.

P3. If $\mathsf{lhs}(\xi)=a_1\sigma_1+\cdots+a_k\sigma_k$, where $a_i\in\mathbb{Q}$ and σ_i are terms, then for all $1\leq i,j\leq k$, $(\mathsf{head}(\sigma_i),\mathsf{head}(\sigma_j))\in\mathsf{parent}$.

Suppose $H\subseteq E(\mathbb{Q}[X])$ satisfies properties *P1, P2* and *P3* and let n be the number of variables and m be the number of (in)equations in H. We only consider positive variable valuations. Thus for every variable x we have the in-equation $x > 0$ in H. We present a non-deterministic algorithm to decide whether H is satisfiable. We begin by setting $H_0 = H$ and at each iteration i, we eliminate a (particular) variable, say x and transform the set of equations from $H_i \subseteq E(\mathbb{Q}[X])$ to $H_{i+1} \subseteq E(\mathbb{Q}[X \setminus \{x\}])$. We consider comparisons $\bowtie$ to be of the type $\{\geq, =, \leq\}$. (Strict inequalities can be removed by adding very small positive quantity ϵ. For example $f < g$ can be transformed to $f + \epsilon \leq g$.) The algorithm proceeds in the following steps:

1. If H_i is independent of all variables, then each (in)equation, involves only rational numbers (and $\epsilon \to^{+} 0$)[1]. Return true iff each (in)equality in H_i is true.

2. Choose a variable x such that every variable y with $(x, y) \in \mathsf{next}^{+}$, is independent of H_i.

3. H_x is the largest subset of H_i such that every formula in H_x is dependent on x. If H_x is empty then $H_{i+1} = H_i$. Suppose H_x is not empty, every inequation $\xi \in H_x$ can be transformed to a form $(\sigma x \bowtie a_0 + a_1\sigma_1 + \cdots + a_k\sigma_k)$, where $\sigma, \sigma_1, \cdots, \sigma_k$ are terms in $\mathbb{Q}[X \setminus \{x\}]$ and $a_0, \cdots, a_k \in \mathbb{Q}$. We will denote this form by $f \cdot x \bowtie g$. Set $H_{i+1} = H_i \setminus H_x$.

4. Define $\Lambda_{\bowtie} \subseteq \mathcal{Q}(\mathbb{Q}[X \setminus \{x\}])$, for $\bowtie \in \{\leq, =, \geq\}$ as follows:

   $$\begin{array}{ll} \Lambda_{\leq} := \{\frac{g}{f} \mid (f \cdot x \leq g) \in H_x\} \cup \{1\}, & \text{quotients that are at least as large as } x \\ \Lambda_{=} := \{\frac{g}{f} \mid (f \cdot x = g) \in H_x\}, & \text{quotients that are equal } x \\ \Lambda_{\geq} := \{\frac{g}{f} \mid (f \cdot x \geq g) \in H_x\} \cup \{\epsilon\} & \text{quotients that are at least as small as } x, \end{array}$$

   where $g = a_0 + a_1\sigma_1 + \cdots + a_k\sigma_k$ and $f = \sigma$.

5. Non-deterministically choose an ordering of elements in $\Lambda_{\leq}$ and $\Lambda_{\geq}$. Then we have the following set of (in)equations:

   $$\frac{g_1}{f_1} \leq \cdots \leq \frac{g_{n_1}}{f_{n_1}} \leq \frac{g_{n_1+1}}{f_{n_1+1}} = \cdots = \frac{g_{n_2}}{h_{n_2}} \leq \frac{g_{n_2+1}}{f_{n_2+1}} \leq \cdots \leq \frac{g_{n_3}}{f_{n_3}} \tag{1}$$

   where, $\dfrac{g_i}{f_i}$ is in $\Lambda_{\leq}$ for $1 \leq i \leq n_1$, in $\Lambda_{=}$ for $n_1 + 1 \leq i \leq n_2$ and in $\Lambda_{\geq}$ for $n_2 + 1 \leq i \leq n_3$.

6. For each $1 \leq j \leq n_3$, we have $\xi_j := (g_j f_{j+1} \bowtie g_{j+1} f_j)$. ξ'_j is obtained from ξ_j by canceling variables that are common divisors of the polynomials in the left hand side and in the right hand side of ξ_j. Add ξ'_j to H_{i+1} for each ξ_j $(1 \leq j \leq n_3)$. Go to step 1.

First we will show that H_{i+1} created in step 6, satisfies *P1*, *P2* and *P3*. Consider,

$$\frac{a_0 + a_1\sigma_1 + \cdots + a_k\sigma_k}{\sigma} \bowtie \frac{b_0 + b_1\sigma'_1 + \cdots + b_l\sigma'_l}{\sigma'} \tag{2}$$

Let $\xi := (\sigma \cdot x \bowtie a_0 + a_1\sigma_1 + \cdots + a_k\sigma_k)$, $\xi' := (\sigma' \cdot x \bowtie b_0 + b_1\sigma'_1 + \cdots + b_l\sigma'_l)$ and $\xi, \xi' \in H_i$ satisfy *P1*, *P2* and *P3*. From the choice of the variable x (step 2), it is evident that either $\sigma | \sigma'$ or $\sigma' | \sigma$ ($a|b$ means a divides b). W.l.o.g let us assumed $\sigma''\sigma' = \sigma$.

[1] ϵ tends to 0 from the positive side.

The crucial observation is that if $\sigma'|\sigma$ then σ' is a suffix of σ, lest there should exist a variable y, such that $(x, y) \in \mathsf{next}$ and y is not independent of H_i.

Therefore, equation (2) can be rewritten as:

$$a_0 + a_1\sigma_1 + \cdots + a_k\sigma_k \ \bowtie\ b_0\sigma'' + b_1\sigma''\sigma'_1 + \cdots + b_l\sigma''\sigma'_l. \tag{3}$$

P3 holds for equation (3), this follows trivially, as $\mathsf{head}(\sigma) = \mathsf{head}(\sigma_i) = \mathsf{head}(\sigma'')$ for $1 \le i \le k$. $(\mathsf{tail}(\sigma''), \mathsf{head}(\sigma')) \in \mathsf{next}$, since $\sigma = \sigma''\sigma'$ and $(\mathsf{head}(\sigma'_i), \mathsf{head}(\sigma'_j)) \in \mathsf{parent}$ for all $1 \le i, j \le l$. Thus, the new equations added to H_{i+1} (after canceling common variables) also satisfy *P1* and *P2* (cancellation is valid since variables can only take positive value).

Correctness of the algorithm is due to the following arguments:

1. Suppose H_i is feasible and let ν be a satisfying valuation of the variables. Then there exists some order among the rational numbers obtained by substituting the values of the variables in the quotients $\{\frac{g(x_1,\cdots,x_n)}{f(x_1,\cdots,x_n)}\}$ present in $\Lambda_\le$ and $\Lambda_\ge$. If we choose this order as the ordering in the equation (1) and obtain H_{i+1} subsequently, then ν is also a satisfying valuation for (in)equations H_{i+1}.

2. If H_{i+1} is satisfiable then the (in)equations (1) are true for some value of $X \smallsetminus \{x\}$. If $\Lambda_=$ is not empty then set $x = \frac{g_{n_2}}{f_{n_2}}$, else choose a value for x such that $\frac{g_{n_1}}{f_{n_1}} \le x \le \frac{g_{n_2+1}}{f_{n_2+1}}$. The value thus chosen is strictly greater than 0, since $\epsilon \in \Lambda_\ge$.(Hence, rational form and cancellation of variables defined in step 5 and step 6, respectively is valid.) This gives us a satisfying valuation of H_i.

Observe that at each iteration i, the size of H_i is $O(|H|)$ and in every iteration we remove one variable and spend $O(mn)$ in obtaining H_{i+1} (modulo division of rational numbers). The maximum number of iteration is n and total time complexity of the non-deterministic algorithm is $O(mn^2)$. Thus satisfiability of a set of polynomial equation with properties *P1*, *P2* and *P3* is in NP.