EFFECTIVE QUANTIFIER ELIMINATION OVER REAL CLOSED FIELDS

N. Vorobjov

Tarski (1931, 1951):
Elementary algebra and geometry is decidable. More generally, there is an algorithm for quantifier elimination in the first order theory of the reals.

Boolean formula $F(\mathbf{x}_1, \ldots, \mathbf{x}_\nu)$ with atoms of the kind $f > 0$, where $f \in \mathbb{R}[\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_\nu]$,
$\mathbf{x}_i = (x_{i,1}, \ldots, x_{i,n_i})$.

$\Phi(\mathbf{x}_0) := Q_1\mathbf{x}_1 Q_2\mathbf{x}_2 \cdots Q_\nu\mathbf{x}_\nu F(\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_\nu)$,
where $Q_i \in \{\exists, \forall\}$, $Q_i \neq Q_{i+1}$.

Theorem 1. *There is a quantifier-free formula* $\Psi(\mathbf{x}_0)$ *such that* $\Psi(\mathbf{x}_0) \Leftrightarrow \Phi(\mathbf{x}_0)$ *over* $\mathbb{R}$,
i.e., $\{\mathbf{x}_0 \in \mathbb{R}^{n_0} |\, \Psi(\mathbf{x}_0)\} = \{\mathbf{x}_0 \in \mathbb{R}^{n_0} |\, \Phi(\mathbf{x}_0)\}$.

Theorem remains true if $\mathbb{R}$ is replaced by any *real closed field* R, e.g., real algebraic numbers, Puiseux series over $\mathbb{R}$ in an infinitesimal.

Theorem 2. *If atoms $f \in \mathbb{Z}[\mathrm{x}_0, \mathrm{x}_1, \ldots, \mathrm{x}_\nu]$, then there is an algorithm which eliminates quantifiers from $\Phi(\mathrm{x}_0)$, i.e., for a given $\Phi(\mathrm{x}_0)$ produces $\Psi(\mathrm{x}_0)$.*

Corollary 3. *The first order theory of the reals is decidable, i.e., there is an algorithm which for a given* closed *formula*

$$Q_1\mathrm{x}_1 Q_2\mathrm{x}_2 \cdots Q_\nu\mathrm{x}_\nu F(\mathrm{x}_1, \ldots, \mathrm{x}_\nu)$$

decides whether it's true or false.

Integer coefficients are mentioned here to be able to handle the problem on a Turing machine. If we are less picky about the model of computation, for example allow exact arithmetic operations and comparisons in a real closed field R, then Theorem **??** and Corollary **??** are also true for formulae over R. In what follows we will use exactly this approach.

Let R be a real closed field.

Definition 4. A set $X \subset R^n$ is called *semialgebraic* if X is representable in a form $X = \{\mathbf{x} \in R^n | F(\mathbf{x})\}$, where $F(\mathbf{x})$ is a quantifier-free formula.

Corollary 5. *Let* $X = \{\mathbf{x}_0 \in R^{n_0} | \Phi(\mathbf{x}_0)\}$, *where* $\Phi(\mathbf{x}_0) := Q_1\mathbf{x}_1 Q_2\mathbf{x}_2 \cdots Q_\nu \mathbf{x}_\nu F(\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_\nu)$. *Then* X *is semialgebraic.*

Examples:

- Feasibility of a system of polynomial equations and inequalities
(= is a semialgebraic set empty?)

- Representation of the closure (or interior, or singular locus,
or tubular neighbourhood, etc.) of a semialgebraic set by a Boolean combination of polynomial inequalities

- Polynomial optimization: find the set of points of local minima of a polynomial function on a semialgebraic set.

There is no need to explain to logicians the usefulness of quantifier elimination. Instead I list a few straightforward examples of how it can be used in "ordinary" mathematics.

Semialgebraic set in all the examples initially can be naturally represented by prenex formulae with quantifiers (sometimes involving ε/δ language.

Complexity:

Tarski's quantifier elimination algorithm: "non-elementary" (can't be bounded from above by any tower of exponentials of a finite height).

Problem: construct an efficient algorithm

Possible approach: cylindrical (algebraic) cell decomposition (mid-70s, Wüthrich, Collins)

Definition 6. *Cylindrical cell* is defined by induction as follows.

1. Cylindrical 0-cell in R^n is an isolated point. Cylindrical 1-cell in R is an open interval $(a, b) \subset R$.

2. For $n \geq 2$ and $0 \leq k < n$ a cylindrical $(k+1)$-cell B in R^n is either a graph of a continuous bounded function $f : C \to R$, where C is a cylindrical a cylindrical $(k+1)$-cell in R^{n-1}, or else a set of the form

   $$\{(x_1, \ldots, x_n) \in R^n |\, (x_1, \ldots, x_{n-1}) \in C$$

   and $f(x_1, \ldots, x_{n-1}) < x_n < g(x_1, \ldots, x_{n-1})\}$,

   where C is a cylindrical k-cell in R^{n-1}, and $f, g : C \to R$ are continuous bounded functions such that

   $$f(x_1, \ldots, x_{n-1}) < g(x_1, \ldots, x_{n-1})$$

   for all points $(x_1, \ldots, x_{n-1}) \in C$.

Cylindrical cell decomposition is a very useful tool when we study o-minimal structures. Since I'll need this concept also in my other lecture, let me give a definition. We first define a cylindrical cell. One can notice that any cylindrical cell is homeomorphic to an open ball of the matching dimension (semialgebraically homeomorphic in the case of an arbitrary R).

We will give the definition only for the bounded case.

Definition 7. *Cylindrical cell decomposition* $\mathcal{D}$ of a subset $A \subset R^n$ is defined by induction as follows.

1. If $n = 1$, then $\mathcal{D}$ is a finite family of pairwise disjoint cylindrical cells (i.e., isolated points and intervals) whose union is A.

2. If $n \geq 2$, then $\mathcal{D}$ is a finite family of pairwise disjoint cylindrical cells in R^n whose union is A and there is a cylindrical cell decomposition $\mathcal{D}'$ of $\pi(A)$ such that $\pi(C)$ is its cell for each $C \in \mathcal{D}$, where $\pi : R^n \to R^{n-1}$ is the projection map onto the coordinate subspace of $x_1, \ldots, x_{n-1}$. We say that $\mathcal{D}'$ is *induced* by $\mathcal{D}$.

Definition 8. Let $B \subset A \subset R^n$ and $\mathcal{D}$ be a CCD of A. Then $\mathcal{D}$ is *compatible* with B if for any $C \in \mathcal{D}$ we have either $C \subset B$ or $C \cap B = \emptyset$ (i.e., some subset $\mathcal{D}' \subset \mathcal{D}$ is a CCD of B).

Example:

Theorem 9. (Collins, Wüthrich). *If $X \subset R^n$ is a semialgebraic set, then there is an algorithm for computing CCD of R^n compatible with X. Moreover, CCD is* semialgebraic, *i.e., each cell is described by a system of polynomial equations and inequalities.*

Technical tools: *resultants and sub-resultants*.

Compare with classical *elimination theory* (van-der-Waerden, Modern Algebra) and Chevalley's Theorem.

Corollary 10. *There is an algorithm for quantifier elimination.*

The corollary is almost obvious from the definition of the CCD. One reasons by induction on quantifiers starting from Q_ν and moving outward. On each step we use the relation (described in the definition) between the decomposition of the space of all current variables and the decomposition of the subspace of current free variables.

Complexity:

Let $\Phi(\mathbf{x}_0)$ involve s atoms of the kind $f > 0$, where $f \in R[\mathbf{x}_0, \dots, \mathbf{x}_\nu]$, $n := n_0 + \cdots + n_\nu$, and $\deg(f) < d$.

Then the complexity of constructing CCD and the corresponding quantifier elimination has an upper bound

$$(sd)^{O(1)^n}.$$

Similar upper bound on the number of cells, degrees and quantities of polynomials describing CCD and quantifier-free formula equivalent to Φ.

If coefficients of polynomials f are integer of bit-sizes less than M, then the (Turing machine) complexity does not exceed

$$M^{O(1)}(sd)^{O(1)^n}.$$

Davenport & Heintz (1988) (similar results by Weispfenning (1988)) found a (parametric) example of Φ of degrees ≤ 4, with two free variables and

$$n_1 \leq 2, \ldots, n_\nu \leq 2$$

(i.e., each quantifier is responsible for at most two variables) defining in R^2 a semialgebraic set consisting of

$$2^{2^n}$$

isolated points.

$\Rightarrow$ Any CCD for Φ can't contain lesser number of cells.

$\Rightarrow$ Lower complexity bound for any CCD-based algorithm is doubly exponential.

Fisher & Rabin (1974): lower bound for *decision* methods is exponential in the number of quantifier alternations.

Simplest case:

$$\exists x \in R\,(f(x) = 0),$$

where $f \in R[x]$, $\deg(f) < d$.

Sturm's Theorem (1835):

Euclidean algorithm for the division of f by its derivative f'.

Let $g_1 = f, g_2 = f'$, and $g_3, \ldots, g_t$ be the sequence of the negatives of the remainders in the Euclidean algorithm. For any $x \in R$ let $V(x)$ be the number of *sign changes* in
$g_1(x), g_2(x), \ldots, g_t(x)$.

Theorem 11. *The number of distinct real roots of f in $[a, b] \subset R$ is*

$$S(f, f') := V(a) - V(b).$$

Note:
sign($f(\infty)$) =sign(leading coefficient a_0 of f)
sign($f(-\infty)$) =sign($a_0 x^d$ at -1).

Note that over an algebraically closed field the answer is always “Yes”.

Sturm’s theorem provides an algorithm to decide the existential formula over any real closed field.

Now we want to generalize this algorithm to be able to handle systems of many equations and inequalities (in one variable, for time being).

Ben-Or/Kozen/Reif algorithm (1986):

Definition 12. Let $f_1, \dots, f_k \in R[x]$, deg(f_i) $< d$. *Consistent sign assignment* is a string $\sigma = (\sigma_1, \dots, \sigma_k)$ where $\sigma_i \in \{>, <, =\}$, such that the system

$$f_1\sigma_1 0, \dots, f_k\sigma_k 0$$

has a solution in R.

Input:
$f_1, \dots, f_k \in R[x]$.
Output:
The list of all consistent sign assignments.

Prepare the input:
Make all f_i squarefree and relatively prime. Then sets of roots of polynomials f_i are disjoint, in particular any consistent sign assignment has *at most one* $=$. Moreover, we can add a new polynomial f so that all consistent assignments for $f_1, \dots, f_k$ can be reconstructed from all consistent assignments of $<$ and $>$ for $f_1, \dots, f_k$ at roots of f.

Case $k = 0$: $f = 0$ Sturm's Theorem.

Case $k = 1$: f, f_1

$$C_1 := \{x |\ f = 0 \wedge f_1 > 0\}$$

$$\overline{C_1} := \{x |\ f = 0 \wedge f_1 < 0\}$$

Obviously, the total number of roots of f is $S(f, f') = |C_1| + |\overline{C_1}|$.
(Here and in the sequel S corresponds to the interval $[-\infty, \infty]$.)

Lemma 13. $S(f, f'f_1) = |C_1| - |\overline{C_1}|$.

Sturm + Lemma $\Rightarrow$

$$\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} |C_1| \\ |\overline{C_1}| \end{pmatrix} = \begin{pmatrix} S(f, f') \\ S(f, f'f_1) \end{pmatrix}$$

Case $k = 2$: $\quad f, f_1, f_2$

$$C_2 := \{x | f = 0 \wedge f_2 > 0\}$$

$$\overline{C_2} := \{x | f = 0 \wedge f_2 < 0\}$$

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \begin{pmatrix} |C_1 \cap C_2| \\ |\overline{C_1} \cap C_2| \\ |C_1 \cap \overline{C_2}| \\ |\overline{C_1} \cap \overline{C_2}| \end{pmatrix} =$$

$$= \begin{pmatrix} S(f, f') \\ S(f, f' f_1) \\ S(f, f' f_2) \\ S(f, f' f_1 f_2) \end{pmatrix}$$

In case k we get a matrix A_k which is a tensor product of k copies of A_1 and is non-singular. Its unique solution describes all consistent sign assignments for $f = 0, f_1, \ldots, f_k$. Solving the system by any standard method (e.g., Gaussian elimination), we list all consistent assignments. However this naive approach leads to the complexity exponential in k.

Polynomial-time algorithm:

deg(f_i) $< d \Rightarrow$ the number of all roots in all f_i is $O(kd) \Rightarrow$ the number of all consistent sign assignments is $O(kd)$.

"Divide-and-conquer" then leads to complexity polynomial in kd.

PLAN:

$X = \{\mathbf{x}_0 \in R^{n_0} | \, \Phi(\mathbf{x}_0)\}$, where
$\Phi(\mathbf{x}_0) := Q_1\mathbf{x}_1 Q_2\mathbf{x}_2 \cdots Q_\nu \mathbf{x}_\nu F(\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_\nu)$.

1. The algorithm eliminates quantifiers by induction starting from Q_ν outwards.

2. It's sufficient to consider just the case of

   $$\Phi(\mathbf{y}) := \exists \mathbf{x}\, F(\mathbf{x}, \mathbf{y}),$$

   where $\mathbf{x} \in R^n$, $\mathbf{y} \in R^m$.

3. We will first construct an algorithm for the *decidability* problem

   $$\exists \mathbf{x} F(\mathbf{x})$$

   and then "parameterize" the algorithm with vector $\mathbf{y}$.

(3) → (2) → (1)

$\exists \mathbf{x} F(\mathbf{x})$, $\mathbf{x} \in R^n$, $F(\mathbf{x})$ is a Boolean formula with s atoms of the kind $f * 0$, $f \in R[\mathbf{x}]$, $* \in \{=, >, <, \geq, \leq\}$, deg$(f) < d$.

In case $n = 1$: Ben-Or/Kozen/Reif applied to the set of all atomic polynomials. The list of all consistent sign assignments allows to decide whether $\exists x F(x)$ is true.

Arbitrary n: Similar strategy: list all consistent sign assignments.

How: Find a finite set $\Lambda \subset R^n$ such that any consistent assignment defines a system of equations and strict inequalities having a solution in this set. Knowing Λ it's easy to find the list of consistent assignments.

Points from Λ are (isolated) solutions of systems of polynomials equations based on atoms of $F(\mathbf{x})$.

Solving systems of equations:
Let a system of polynomial equations have at most finite number of solutions over algebraic closure $\bar{R}$.

Possible approaches:

- Gröbner bases
- Effective Hilbert's Nullstellensatz
- u-resultants

We will use u-resultants.

Homogeneous polynomials:
A polynomial in n variables is an expression:

$$\sum_{(i_1,\ldots,i_n)} a_{i_1,\ldots,i_n} x_1^{i_1} \cdots x_n^{i_n}.$$

A polynomial is *homogeneous* or a *form* if $i_1 + \cdots + i_n$ =const for all $(i_1, \ldots, i_n)$ with $a_{i_1,\ldots,i_n} \neq 0$.

Examples:
Homogeneous: $x^2 + xy$
Non-homogeneous: $x^2 - 1$

0 is a root of any non-constant homogeneous polynomial.

If $\mathbf{x} = (x_1, \ldots, x_n) \in \bar{R}^n$ is a root of a homogeneous polynomial h, then for any $a \in \bar{R}$ the point $a\mathbf{x} = (ax_1, \ldots, ax_n)$ is also a root of h.

$\Rightarrow$ If $\mathbf{x} \neq 0$, then there is a straight line of roots of h passing through 0 and $\mathbf{x}$. We can say that *the line itself is a root of* h.

Projective space:
The space of all straight lines through the origin is called $(n-1)$-*dimensional projective space* $\mathbb{P}^{n-1}(\bar{R})$.

An element of $\mathbb{P}^{n-1}(\bar{R})$, which is a line passing through 0 and $\mathbf{x} = (x_1, \ldots, x_n) \neq 0$, is denoted by $(x_1 : x_2 : \cdots : x_n)$.

Any polynomial $h \in \bar{R}[\mathbf{x}]$ can be *homogenized*: Let deg$(h) = d$. Introduce a new variable x_0 and a homogeneous polynomial
hom$(h) := x_0^d h(x_1/x_0, \ldots, x_n/x_0)$.

If $(x_1, \ldots, x_n)$ is a root of h, then $(1 : x_1 : \cdots : x_n)$ is a root of hom(h). If $(y_0 : y_1 : \cdots : y_n) \in \mathbb{P}^{n-1}(\bar{R})$ is a root of hom(h) and $y_0 \neq 0$, then $(y_1/y_0, \ldots, y_n/y_0)$ is a root of h.
Of course, hom(h) can have a root of the form $(0 : z_1 : \cdots : z_n)$ which does not correspond in this sense to any root of h, it's called a "root at infinity".

Similar relation is true for *systems* of polynomial equations: *homogenized system has not less solutions than the original system*.

Example:

original system: $x_1 - x_2 = x_1 - x_2 + 1 = 0$

homogenization: $x_1 - x_2 = x_1 - x_2 + x_0 = 0$.

Original is inconsistent, the homogenized has a unique solution $(0 : 1 : 1)$ (at infinity).

u-**resultant:**

Consider a system of n homogeneous equations in $n+1$ variables: $h_1 = \cdots = h_n = 0$.

The system is always consistent in $\mathbb{P}^n(\bar{R})$.
It can have either finite or infinite number of solutions.

Introduce new variables $u_0, u_1, \ldots, u_n$.

Proposition 14. *There is a homogeneous polynomial* $R_{h_1,\ldots,h_n} \in \bar{R}[u_0, \ldots, u_n]$, called u-resultant, *such that* $R_{h_1,\ldots,h_n} \not\equiv 0$ *iff the system has finite number of solutions.*
If $R_{h_1,\ldots,h_n} \not\equiv 0$, *then*

$$R_{h_1,\ldots,h_n} = \prod_{1 \le i \le r} (\chi_0^{(i)} u_0 + \cdots + \chi_n^{(i)} u_n),$$

where $(\chi_0^{(i)} : \cdots : \chi_n^{(i)})$, $1 \le i \le r$ *are all solutions in* $\mathbb{P}^n(\bar{R})$ *of the system.*

Assume that in $\exists \mathbf{x} F(\mathbf{x})$ formula $F(\mathbf{x})$ is just a system of inequalities

$$f_1 \geq 0 \wedge \cdots \wedge f_s \geq 0,$$

and that $\{\mathbf{x} |\ F(\mathbf{x})\} \subset R^n$ is bounded.

Let $\deg(f_i) < d$ for all $1 \leq i \leq s$ and D be minimal even integer $\geq sd + 1$.

Introduce a new variable ε and consider

$$g(\varepsilon) := \prod_{1 \leq i \leq s} (f_i + \varepsilon) - \varepsilon^{s+1} \sum_{1 \leq j \leq n} x_j^D.$$

Lemma 15. *If the system $f_1 \geq 0 \wedge \cdots \wedge f_s \geq 0$ is consistent, then there is a solution which is a limit of a solution of*

$$\frac{\partial g(\varepsilon)}{\partial x_1} = \cdots = \frac{\partial g(\varepsilon)}{\partial x_n} = 0$$

as $\varepsilon \to 0$.

We consider just the case of a system of inequalities to simplify the explanations. The case of an arbitrary formula is slightly more geometrically complicated, but very similar in spirit.

If $\{\mathbf{x}|\ F(\mathbf{x})\}$ is *not* bounded, then it can be reduced to the bounded cased by intersecting this set with a ball of sufficiently large radius.

Picture:

Lemma 16. *For all sufficiently small $\varepsilon > 0$, if*

$$f_1 \geq 0 \wedge \cdots \wedge f_s \geq 0$$

is consistent, then the homogenization of

$$\frac{\partial g(\varepsilon)}{\partial x_1} = \cdots = \frac{\partial g(\varepsilon)}{\partial x_n} = 0$$

has a finite number of solutions.

Proof. Gröbner basis or u-resultant techniques. □

Denote the homogenization by

$$G_1(\varepsilon) = \cdots = G_n(\varepsilon) = 0.$$

By Proposition, every solution of this system is a coefficient vector in a divisor of the u-resultant $R_{G_1(\varepsilon),\ldots,G_n(\varepsilon)}$.

The lemma of course means that the system itself also has a finite number of solutions, since the homogenization always has more solutions.

Represent $R_{G_1(\varepsilon),\ldots,G_n(\varepsilon)}$ in the form

$$R_{G_1(\varepsilon),\ldots,G_n(\varepsilon)} = R_m\varepsilon^m + \sum_{j>m} R_j\varepsilon^j,$$

where m is the lowerst degree w.r.t. ε.

Lemma 17.

$$R_m = \prod_{1\le i\le r} (\eta_0^{(i)}u_0 + \cdots + \eta_n^{(i)}u_n),$$

where $(\eta_0^{(i)}, \ldots, \eta_n^{(i)})$ *is the limit of* $(\chi_0^{(i)}, \ldots, \chi_n^{(i)})$ *as* $\varepsilon \to 0$*.*

Corollary 18. *If* $f_1 \ge 0 \wedge \cdots \wedge f_s \ge 0$ *is consistent, then its solution is*

$$(\eta_1^{(i)}/\eta_0^{(i)}, \ldots, \eta_n^{(i)}/\eta_0^{(i)}),$$

where $\eta_0^{(i)} \ne 0$ *and* $(\eta_0^{(i)}u_0 + \cdots + \eta_n^{(i)}u_n)$ *is a divisor of* R_m*.*

If we were able to factorize R_m over $\bar{R}$, then the algorithm for consistency of $f_1 \geq 0 \wedge \cdots \wedge f_s \geq 0$ could be roughly as follows:

- Construct the u-resultant $R_{G_1(\varepsilon),\ldots,G_n(\varepsilon)}$;
- Find the lowest term R_m w.r.t. ε in $R_{G_1(\varepsilon),\ldots,G_n(\varepsilon)}$;
- Factorize R_m finding the limits $(\eta_0^{(i)}, \ldots, \eta_n^{(i)})$ (when $\varepsilon \to 0$);
- Check whether
$$(\eta_1^{(i)}/\eta_0^{(i)}, \ldots, \eta_n^{(i)}/\eta_0^{(i)})$$
satisfies $f_1 \geq 0 \wedge \cdots \wedge f_s \geq 0$.
If yes, then this system is is consistent, else it's inconsistent.

Unfortunately, we are unable to factorize a polynomial in general case. Even in special cases, when effective multivariate factorization algorithms are known, they are very involved.

Therefore, our scheme will be different.

Consider in the affine space $\bar{R}^{n+1}$ the hypersurface

$$\{(u_0, \ldots, u_n) \in \bar{R}^{n+1} |\, R_m = 0\}.$$

Since R_m factors into linear forms, the hypersurface is a union of hyperplanes passing through 0.

$\eta_0^{(i)} u_0 + \cdots + \eta_n^{(i)} u_n = 0$ is the equation defining hyperplane number i, $1 \leq i \leq r$;
$\Rightarrow$ vector $(\eta_0^{(i)}, \ldots, \eta_n^{(i)})$ is orthogonal to the hyperplane i;
$\Rightarrow$ vector $(\eta_0^{(i)}, \ldots, \eta_n^{(i)})$ is collinear to the *gradient* of R_m at a non-singular point $\mathbf{x}$ of the hyperplane i, i.e., to

$$\Big(\frac{\partial R_m}{\partial u_0}(\mathbf{x}), \ldots, \frac{\partial R_m}{\partial u_n}(\mathbf{x})\Big).$$

To find a finite set of non-singular points on all hyperplanes, intersect $\{R_m = 0\}$ with a "generic" straight line in $\bar{R}^{n+1}$ defined with coefficients from R (actually, from $\mathbb{Z}$).

Algorithm for deciding $\exists \mathbf{x}\, F(\mathbf{x})$:

- Write the homogeneous system $G_1(\varepsilon) = \cdots = G_n(\varepsilon) = 0$.

- Construct u-resultant $R_{G_1(\varepsilon),\dots,G_n(\varepsilon)}$ (how – later).

- Find the lowest term R_m w.r.t. ε in $R_{G_1(\varepsilon),\dots,G_n(\varepsilon)}$.

- Find a generic straight line in the parametric form $\alpha t + \beta$, where $\alpha, \beta \in R^{n+1}$, t is a single variable. The roots of the univariate equation $R_m(\alpha t + \beta) = 0$ correspond to the points of intersection of the line with hyperplanes. If $f_1 \geq 0 \wedge \cdots \wedge f_s \geq 0$ is consistent, then for a root t' of $R_m(\alpha t + \beta) = 0$ the following point is its solution:
$$\left(\frac{\partial R_m/\partial u_1}{\partial R_m/\partial u_0}(\alpha t' + \beta), \dots, \frac{\partial R_m/\partial u_n}{\partial R_m/\partial u_0}(\alpha t' + \beta)\right).$$

- Denoting

$$y_j(\alpha t + \beta) := \frac{\partial R_m/\partial u_j}{\partial R_m/\partial u_0}(\alpha t + \beta),$$

we get:

The system $f_1 \geq 0 \wedge \cdots \wedge f_s \geq 0$ is consistent iff there exists $t' \in R$ such that

$$R_m(\alpha t' + \beta) = 0 \text{ and}$$

$$f_i(y_1(\alpha t' + \beta) \geq 0 \wedge \cdots \wedge y_n(\alpha t' + \beta)) \geq 0$$

for all $1 \leq i \leq s$.

- Check consistency of the latter system of *univariate* polynomials inequalities using Ben-Or/Kozen/Reif.

Technical details we left out:

- Computing u-resultant (polynomial of degree $(sd)^{O(n)}$).

- Finding generic straight line in $\bar{R}^{n+1}$.

- Case of vanishing gradient $\Leftrightarrow$ $\eta_0^{(i)} u_0 + \cdots + \eta_n^{(i)} u_n$ occurs in R_m with power > 1 $\Leftrightarrow$
root t' of $R_m(\alpha t + \beta) = 0$ is multiple.

- Case of an arbitrary Boolean formula as $F(\mathbf{x})$.

Complexity:

Straightforward calculation: $(sd)^{O(n)}$.

Accomplished item (3) of the PLAN ↑: deciding $\exists \mathbf{x} F(\mathbf{x})$.

Now, item (2): quantifier elimination in $\exists \mathbf{x}\, F(\mathbf{x}, \mathbf{y})$.

Main idea:
Consider variables $\mathbf{y}$ as *parameters* and try to execute the decidability algorithm for a parametric formula (i.e., with variable coefficients).

Decidability algorithm uses only $+, *$ and comparisons over elements of R.
Arithmetic can be easily performed parametrically, while comparisons require branching.

The parametric algorithm is represented by *algebraic decision tree*.

Picture:

Input of the tree is $\mathbf{y}$. Each vertex of the tree is associated with a polynomial in $\mathbf{y}$, which is the composition of arithmetic operations performed along the branch leading from the root to this vertex.

Upon a *specialization* of input $\mathbf{y}$, the polynomial at the root is evaluated, and the value is compared to zero. Depending on the result of comparison, one of the three branches is chosen, thereby determining the next vertex and the polynomial evaluation to be made, and so on until a leaf is reached.

Each leaf is assigned the value "True" or "False". All specializations of $\mathbf{y}$, arriving at a leaf marked "True", correspond to closed formulae that are true. Similar with "False".

An elimination algorithm:

- Use the decision algorithm parametrically to obtain a decision tree with the variable input $\mathbf{y}$.

- Determine all branches from the root to leaves marked **True**.

- Take conjunction of the inequalities along each such branch:

  $$\bigwedge_{i \in \text{branch}} h_i(\mathbf{y}) \sigma_i 0,$$

  where $\sigma_i \in \{<, >, =\}$.

- $$\exists \mathbf{x}\, F(\mathbf{x}, \mathbf{y}) \Leftrightarrow \bigvee_{\text{branches}} \quad \bigwedge_{i \in \text{branch}} h_i(\mathbf{y}) \sigma_i 0$$

Difficulty:

Too many branches in the tree:

Height = complexity of decidability = $(sd)^{O(n)}$
$\Rightarrow \quad 3^{(sd)^{O(n)}}$ branches (leaves)

But:

Most branches are not followed by any specification of $\mathbf{y}$, i.e., most leaves correspond to Boolean formulae defining $\emptyset$.

Because:

Lemma 19. *Let in the finite set* $g_1, \ldots, g_k \in R[x_1, \ldots, x_n]$ *all degrees* $\deg(g_i) < D$. *Then the number of all consistent sign assignments for this set is less than* $(kD)^{O(n)}$.

Carefully examining the decidability algorithm we see that the number of distinct polynomials h_i in the tree is essentially the same as in one branch, i.e., $(sd)^{O(n)}$. From the complexity estimate we know that their degrees are $(sd)^{O(n)}$. Then, by Lemma, the number of distinct $\neq \emptyset$ sets associated with leaves is $(sd)^{O(n^2)}$.

$\Rightarrow$

Complexity of $\exists$ elimination:

$$(sd)^{O(n^2)}$$

$\forall$ **elimination:**

$$\forall \mathbf{x} F(\mathbf{x}) \Leftrightarrow \neg \exists \mathbf{x} \neg F(\mathbf{x})$$

General case (item (1) of the PLAN ↑):

$$Q_1\mathbf{x}_1 Q_2\mathbf{x}_2 \cdots Q_\nu \mathbf{x}_\nu F(\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_\nu),$$

where $\mathbf{x}_i \in R^{n_i}$, $n := n_0 + \cdots + n_\nu$.

Complexity:

$$(sd)^{n^{O(\nu)}}$$

Compare with CCD algorithm:

$$(sd)^{O(1)^n}$$

Using finer technical tools one can construct quantifier elimination algorithm having complexity

$$(sd)^{\prod_{0 \le i \le \nu} O(n_i)}$$

References:

1. J Renegar, Recent progress on the complexity of the decision problem for the reals, *DIMACS Series in Discrete Maths. and Theoretical Comp. Sci.*, **6**, 1991, 287–308.

2. S Basu, R Pollack, M-F Roy, *Algorithms in Real Algebraic Geometry*, Springer, Berlin-Heidelberg, 2003.