4

Applications of quantifier elimination

In this chapter we prove significant theorems in real algebraic geometry as easy consequences of the quantifier elimination theorem. This includes Tarski's transfer principle which is frequently useful in proving the solvability of polynomial systems non-constructively. We also solve Hilbert's 17^{th} problem by showing that every non-negative polynomial is a sum of squares of rational functions.

4.1 Tarski's transfer principle

As discussed in Corollary 3.5, because every first-order sentence is equivalent to a quantifier-free sentence modulo the theory of real-closed fields, its truth over real-closed $\mathbb{F}$ does not actually depend on $\mathbb{F}$ and its elements — because there are no quantifiers that interact with $\mathbb{F}$. Thus the sentences that are true over some real-closed field are exactly those sentences true over every real-closed field. A technical refinement of this statement is known as:

Tarski's transfer principle. Let $\mathbb{F}$ be real-closed, $\mathbb{F}'/\mathbb{F}$ a real-closed extension and K definable over $\mathbb{F}$. Then K is non-empty over $\mathbb{F}$ if and only if it is non-empty over $\mathbb{F}'$.

Proof. Let $K = \{\, x \in \mathbb{F}^n : \mathbb{F} \models \phi(x, b) \,\}$ for some parameters $b \in \mathbb{F}^m$. Denote by K' the set defined in $\mathbb{F}'$ using the same formula ϕ and parameters $b \in \mathbb{F}^m \subseteq \mathbb{F}'^m$. By inclusion of fields, if K is non-empty, then so is K'. Now suppose the converse: that there exists $\overline{x} \in K'$, which means $\mathbb{F}' \models \exists x : \phi(x, b)$. Now by Theorem 3.1, $\exists x : \phi(x, y)$ is equivalent over *every* real-closed field to a quantifier-free formula $\psi(y)$. We know that $\psi(b)$ is true over $\mathbb{F}'$. But it involves no quantifiers, so it must be true over $\mathbb{F}$ as well, and this finally shows that $\mathbb{F} \models \exists x : \phi(x, b)$, i.e., K is non-empty. □

Corollary 4.1. A system of polynomial equations and inequalities with integer coefficients has a solution in some real-closed field if and only if it has a solution in $\mathsf{rcl}(\mathbb{Q})$ and hence in every real-closed field. In particular, if a $\mathbb{Z}$-defined polynomial system has a solution, it has a real algebraic solution.

Example 4.2. There are huge real-closed fields containing $\mathbb{R}$ such as the real closure of a multivariate function field over $\mathbb{R}$ in infinitesimal variables $0 \ll \varepsilon_1 \ll \cdots \ll \varepsilon_p$. Such fields offer greater modeling flexibility in constructing solutions to polynomial systems. Consider the following problem which is of a type that appears in *algebraic*

statistics [Boe22, Lemma 4.63]: does there exist a real symmetric matrix

$$\Sigma = \begin{pmatrix} p & a & b & c \\ a & q & d & e \\ b & d & r & f \\ c & e & f & s \end{pmatrix} \quad \text{such that}$$

$$\Sigma \text{ is positive definite, } \det(\Sigma_{1,2}) = \det(\Sigma_{2,1}) = a = 0,$$
$$\det(\Sigma_{134,234}) = \det(\Sigma_{234,124}) = cdf + bef - af^2 - cer - bds + ars = 0,$$
$$\text{and no other minor of } \Sigma \text{ vanishes?}$$

Instead of attaching existential quantifiers to all variables and invoking a costly elimination algorithm, we observe that, using $a = 0$, the second equation can be solved for

$$b = \frac{cdf - cer}{ds - ef}.$$

We now view Σ as a matrix in an ordered function field over $\mathbb{R}$, as follows. Setting the diagonals $p = q = r = s = 1$ and all other free variables $0 \ll c \ll d \ll e \ll f$ infinitesimally small makes all principal minors positive in the ordered field $\mathbb{R}(c, d, e, f)$, since all off-diagonal entries are infinitesimal. It is a cheap symbolic computation to evalute the minors of the matrix

$$\begin{pmatrix} 1 & 0 & \frac{cdf-ce}{d-ef} & c \\ 0 & 1 & d & e \\ \frac{cdf-ce}{d-ef} & d & 1 & f \\ c & e & f & 1 \end{pmatrix} \text{ over } \mathbb{R}(c, d, e, f)$$

to see that up to symmetry there are precisely two minors which are zero in $\mathbb{R}(c, d, e, f)$, namely those we designed for. This matrix satisfies all our requirements over the ordered field $\mathbb{R}(c, d, e, f)$. This field is embedded in its real closure which is first-order equivalent to $\mathbb{R}$. It follows by Tarski's transfer principle that we can find a real symmetric matrix satisfying our requirements as well. In fact, almost any matrix as above with $c, d, e, f \in \mathbb{R}$ *sufficiently small* will do. In this case, one of the equations could be solved for b as a rational function in the other variables. More complicated algebraic equations may require the use of formal power or even Puiseux series but the same idea applies in these cases. △

Another consequence of the fact that the first-order theories of all real-closed fields coincide is that we may use analytic techniques over $\mathbb{R}$ (as $\mathbb{R}^n$ is a Hilbert space) to derive theorems in other real-closed fields. Any theorem which can be formulated in the language of ordered rings and proved over $\mathbb{R}$ by any means gives rise to a theorem in all real-closed fields. Example 2.8 contained an example of a discontinuous semialgebraic function. Over $\mathbb{R}$ we can prove that every semialgebraic function is piecewise continuous. This statement subsequently transfers to all real-closed fields.

Lemma 4.3. Let $f : \mathbb{R} \to \mathbb{R}$ be a semialgebraic function and $U \subseteq \mathbb{R}$ an open interval. Then there is $x \in U$ such that f is continuous at x.

Proof. If there is an open subset $V \subseteq U$ such that $f(V)$ is finite, we may pick $b \in f(V)$ such that $f^{-1}(b) \subseteq \mathbb{R}$ is infinite and semialgebraic and therefore (by Exercise 2.2) contains an interval on which f is constant and of course continuous.

Otherwise we set $V_0 = U$ and construct inductively for every integer $n \in \mathbb{N}$ an open set V_{n+1} such that $\overline{V_{n+1}} \subseteq V_n$. By assumption $X = f(V_n)$ is infinite and semialgebraic and hence contains an interval (a, b) which we may constrain to have length at most $1/n$. Its inverse image $Y = V_n \cap f^{-1}(a, b)$ is semialgebraic and infinite and therefore contains an interval which we may assume to be finite and we name it V_{n+1}. Its closure is closed and bounded and therefore compact in $\mathbb{R}$ by the Heine–Borel theorem. By Cantor's intersection theorem, $\bigcap_{n=0}^{\infty} V_n = \bigcap_{n=0}^{\infty} \overline{V_n}$ is non-empty. Since $\mathbb{R}$ is archimedean, the choice of Y and X above guarantees that f is continuous at every point in this set: namely, for any $\varepsilon > 0$ there exists $n \in \mathbb{N}$ such that $1/n < \varepsilon$ and for every $x, y \in V_{n+1}$ we have $|f(x) - f(y)| < 1/n < \varepsilon$. The length of the interval V_{n+1} is the δ in the ε-δ definition of continuity. □

Theorem 4.4. Let $\mathbb{F}$ be real-closed and $f : \mathbb{F} \to \mathbb{F}$ semialgebraic. Then there is a partition $\mathbb{F} = I_1 \cup \cdots \cup I_k \cup X$ such that X is finite and each I_j is an open interval on which f is continuous.

Proof. The set of discontinuities of f,

$$X = \{\, x \in \mathbb{F} : \mathbb{F} \models \exists \varepsilon > 0 \, \forall \delta > 0 \, \exists y : |x - y| < \delta \wedge |f(x) - f(y)| > \varepsilon \,\},$$

is definable but it contains no intervals by Lemma 4.3. Thus it is finite by Exercise 2.2 and f is continuous on the semialgebraic set $\mathbb{F} \setminus X$ which is a union of intervals. □

4.2 Hilbert's 17th problem

The 17th problem on Hilbert's famous list of problems for 20th century Mathematics was resolved by Emil Artin in 1927 who, together with Otto Schreier, developed the theory of real-closed fields. The theorem is an easy consequence of quantifier elimination, which was only proved a decade later.

Theorem 4.5. Let $\mathbb{F}$ be real-closed and $f \in \mathbb{F}[x_1, \ldots, x_n]$ be non-negative on $\mathbb{F}^n$. Then f can be written as a sum of squares of rational functions over $\mathbb{F}$.

Proof. Suppose otherwise, so that f is not a sum of squares of rational functions. Thus by Lemma 1.10 and Theorem 1.11 we can extend the cone $\sum \mathbb{F}(x_1, \ldots, x_n)^2$ to an ordering on $\mathbb{F}(x_1, \ldots, x_n)$ in which $-f$ is positive. Let $\mathbb{F}'$ be the real closure of $\mathbb{F}(x_1, \ldots, x_n)$ under that ordering. This is a real-closed extension of $\mathbb{F}$.

When viewed as an element in $\mathbb{F}'$, f is negative. But it is still a polynomial and plugging the elements $x_1, \ldots, x_n \in \mathbb{F}'$ into f produces a negative element, namely f itself. This shows $\mathbb{F}' \models \exists x : f(x) < 0$. By Tarski's transfer principle we obtain the contradiction $\mathbb{F} \models \exists x : f(x) < 0$ to the non-negativity of f as a function on $\mathbb{F}^n$. □

This proof illustrates the power of the model-theoretic approach and quantifier elimination. The sentence $\exists x : f(x) < 0$ can be proved in the larger field $\mathbb{F}'$ with its tweaked order relation $<$. By Tarski's transfer principle, the same string of symbols must be a true statement in the other real-closed field $\mathbb{F}$ even though $<$ denotes a slightly different (restricted) order relation there.

Example 4.6. That Theorem 4.5 does not hold with sums of squares of polynomials (instead of rational functions) was already known to Hilbert when he posed this problem. The example commonly given of this phenomenon is due to Motzkin:

$$f = 1 - 3x^2y^2 + x^2y^4 + x^4y^2.$$

Its non-negativity follows from the AGM inequality

$$\frac{a+b+c}{3} \geq \sqrt[3]{abc}$$

invoked with $a = 1$, $b = x^2y^4$ and $c = x^4y^2$ all of which are non-negative. Suppose that it can be written as a sum of squares $\sum_i f_i^2$ for polynomials $f_i \in \mathbb{R}[x, y]$. For degree reasons, the only monomials appearing in the f_i are those of degree at most 3. It is easily seen from the structure of f that x, x^2, x^3, y, y^2, y^3 cannot appear in any of the f_i with a non-zero coefficient. This leaves the general form $f_i = a_i + b_ixy + c_ix^2y + d_ixy^2$. But then $\sum_i b_i^2 = -3$ again by comparison of coefficients between f and $\sum_i f_i^2$ which is impossible. △

4.3 Exercises

Choose exercises to solve from the list below for up to 5 bonus points. Solutions must be submitted on MyCourses by **Thursday, May 25, 12:00**.

4.1 Let $K \subseteq \mathbb{R}^n$ be a $\mathbb{Z}$-defined semialgebraic set. Prove that $K \cap \mathsf{rcl}(\mathbb{Q})^n$ is dense in K in the euclidean topology. 2 points

4.2 Let $\mathbb{F}$ be an ordered field and consider a symmetric $n \times n$-matrix Σ with entries in $\mathbb{F}$. Let us say that this matrix is *positive definite* if all of its principal minors are positive. In $\mathbb{R}$ this is equivalent to all *leading* principal minors being positive. Prove that this equivalence holds over all ordered fields. 2 points

4.3 Let Σ be a symmetric $n \times n$-matrix with entries in an ordered field $\mathbb{F}$. (1) Prove that Σ has n eigenvalues, counted with multiplicity, in $\mathsf{rcl}(\mathbb{F})$. The *signature* of Σ is the triple $(c_+, c_-, c_0) \in \mathbb{N}^3$ counting the positive, negative and zero eigenvalues of Σ in $\mathsf{rcl}(\mathbb{F})$. We have $c_+ + c_- + c_0 = n$. (2) Argue that the signature is well-defined and independent of the real-closed extension of $\mathbb{F}$. (3) Prove *Sylvester's Law of inertia* [Zha05, Theorem 1.5]: the signature of Σ does not change under a congruence transformation $A^\mathsf{T}\Sigma A$ where $A \in \mathbb{F}^{n\times n}$ is invertible. What can you say about the converse? 6 points

4.4 Write the Motzkin polynomial as a sum of squares in $\mathbb{R}(x, y)$. 3 points