TARSKI - SEIDENBERG

Theorem 1.9 (Tarski-Seidenberg – first form) *There exists an algorithm which, given a system of polynomial equations and inequalities in the variables $T = (T_1, \ldots, T_p)$ and X with coefficients in $\mathbb{R}$*

$$\mathcal{S}(T, X) \ : \quad \begin{cases} S_1(T, X) \rhd_1 0 \\ S_2(T, X) \rhd_2 0 \\ \cdots \\ S_\ell(T, X) \rhd_\ell 0 \end{cases}$$

(where the $\rhd_i$ are either $=$ or $\neq$ or $>$ or $\geq$), produces a finite list $\mathcal{C}_1(T)$, ..., $\mathcal{C}_k(T)$ of systems of polynomial equations and inequalities in T with coefficients in $\mathbb{R}$ such that, for every $t \in \mathbb{R}^p$, the system $\mathcal{S}(t, X)$ has a real solution if and only if one of the $\mathcal{C}_j(t)$ is satisfied.

Theorem 2.3 (Tarski-Seidenberg – second form) *Let A be a semialgebraic subset of $\mathbb{R}^{n+1}$ and $\pi : \mathbb{R}^{n+1} \to \mathbb{R}^n$, the projection on the first n coordinates. Then $\pi(A)$ is a semialgebraic subset of $\mathbb{R}^n$.*

Theorem 2.6 (Tarski-Seidenberg – third form) *If $\Phi(X_1, \ldots, X_n)$ is a first-order formula, the set of $(x_1, \ldots, x_n) \in \mathbb{R}^n$ which satisfy $\Phi(x_1, \ldots, x_n)$ is semialgebraic.*

Oddly enough Seidenberg replace elimination of quantifiers with elimination on "non-equalities"

$p > q \quad \exists z, t$

$p - q = z^2$

$p \neq q \quad t(p-q) = 1.$

$\Sigma \neq \emptyset \iff \hat{\Sigma} \neq \emptyset.$

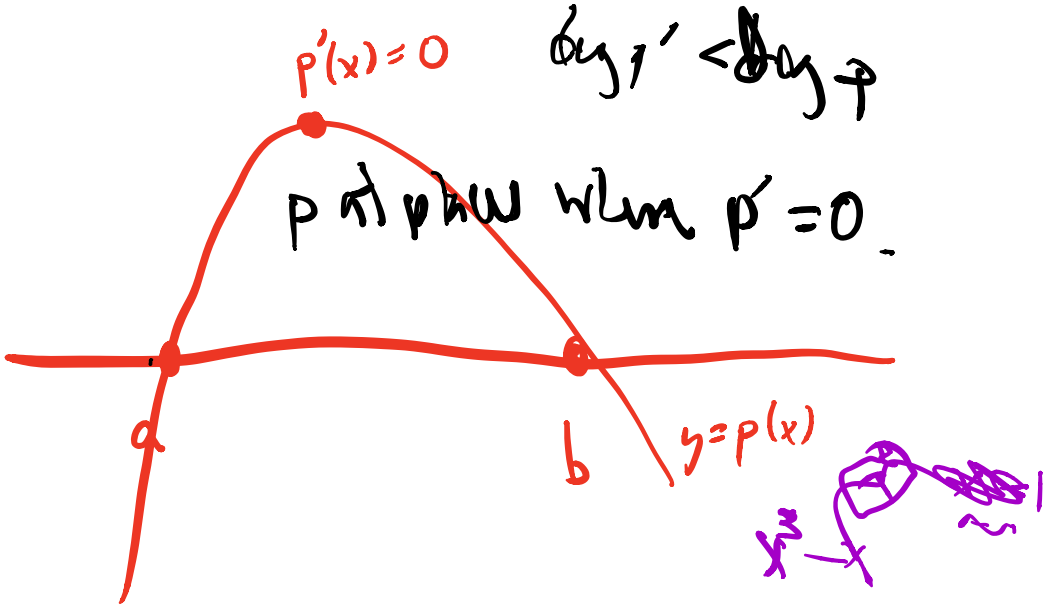
$f = 0 \text{ or } g = 0$

$\iff f \cdot g = 0$

$f = 0 \wedge g = 0$

$\iff f^2 + g^2 = 0.$

① Remember Rolle's theorem



So e.g. $p(x)$ has a ! root (at most) if $p'(x)$ has no roots.

Remark: # of real roots can be bounded by # of monomials (Khovanskii)

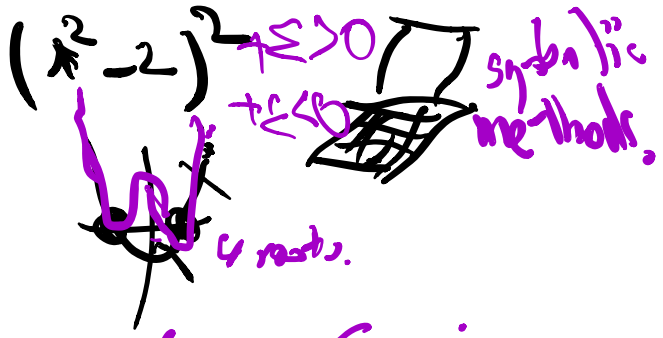
Exercise (Descartes): $\sum_{i=0} a_i x^i$ has at most the number of alternations of signs in the coefficients positive roots.

② Multiple roots are harder to see.

If p has a root, so does p^2

but "small perturbation" $p^2 + \{\varepsilon\}$

might not.



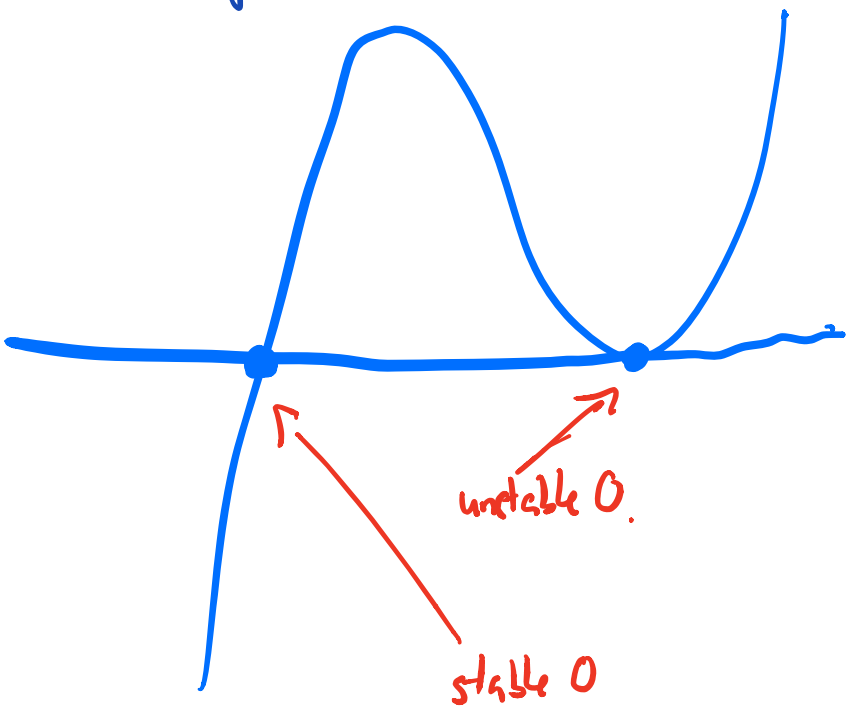
Remark: $\mathbb{R}$ differs from $\mathbb{C}$ in terms of instability of roots.

This is a serious "practical" problem.

↘ Modulo? Coefficients.

up to equiv. if coeff. not as important as degrees

$y = x^3 - 2x^2 + x = x(x-1)^2$



Is the zero at $x = 1$ an experimental error?

$\text{sign}(f) > 0$

for $x > 0$ a.e. unlike a stable case.

(2') $p(x)$ has a double root iff

$\gcd(p, p') \neq 1$.

gcd can be determined alg. by Euclidean algorithm.

③ Resultant

$$\gcd(f, g) = 1$$

$\Leftrightarrow$

$$\exists\, a, b \in \mathbb{F}[x] \quad .$$

$\Leftrightarrow \exists\, a, b$ of low degree with $af + bg = 0$.

$(f, g) \to (\text{rem}_g f, g)$. $af + bg = 1$

$\Leftarrow$

and $\deg a < \deg g = q$

and $\deg b < \deg f = p$.

Make a matrix

$\text{Deg} < p + \text{Deg} < q \to \text{Deg} < p+q$

$(a, b) \longrightarrow af + bg$

and check if $\det = 0$ or not.

Example

ax^2+bx+c

vs

$dx+e$

$$\begin{vmatrix} a & b & c \\ 0 & d & e \\ d & e & 0 \end{vmatrix} = 0 \quad \#(dx+e) \mid ax^2+bx+c.$$

$\gcd(ax^2+bx+c,\ dx+e) \neq \text{const.}$

$(x^2+1)^2$

④ Sturm's theorem. $\gcd(p(x), p'(x)) = \prod (x-\rho)^{d-1}$

In case $f(x)$ has no multiple roots. $p(x)$

(So all roots are between the roots of $f'(x)$)

INFORMALLY look for whether

∞

$f(\rho_1')f(\rho_2') < 0$ or not.

But then you'd need to find the

$\rho_1' < \rho < \rho_2'$ where $f(\rho) = 0$.

to continue to do the next degree.

This can be done algorithmically.

(elegantly?)

STURM'S THEOREM

Better approach:

Start $(P, P', P_3 = qP' - P, P_4$ etc$)$

$v(a)$ = number of alternations of signs at a

$v(b)$ " " " " " at b.

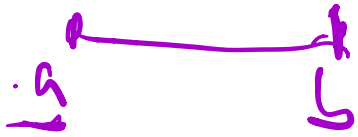
$a<b$; # of roots in $[a,b]$ is $v(a)-v(b)$.

Example. $p(x) = x^3 - x$

$p'(x) = 3x^2 - 1$

$P_3 = \frac{4}{3}x$

$P_4 = 1.$



gives $\left(x^3 - x,\ 3x^2 - 1,\ \frac{4}{3}x,\ 1\right)$

$v(-\infty) = (-, +, -, +) = 3$

$v(.5) \quad (-, -, +, +) = 1$

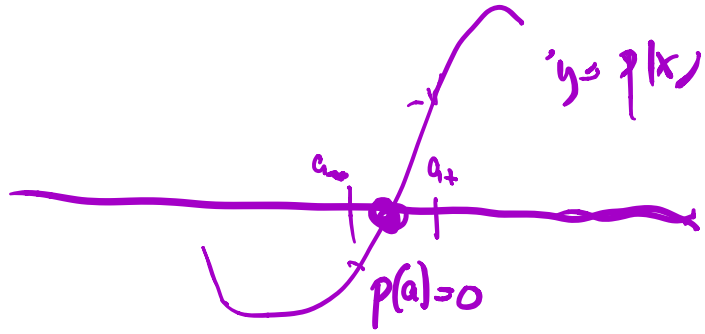
$v(2) = (+, +, +, +) = 0$

Idea of proof: look at what happens to this as you pass a root of $p(x)$ if all zeroes are simple.

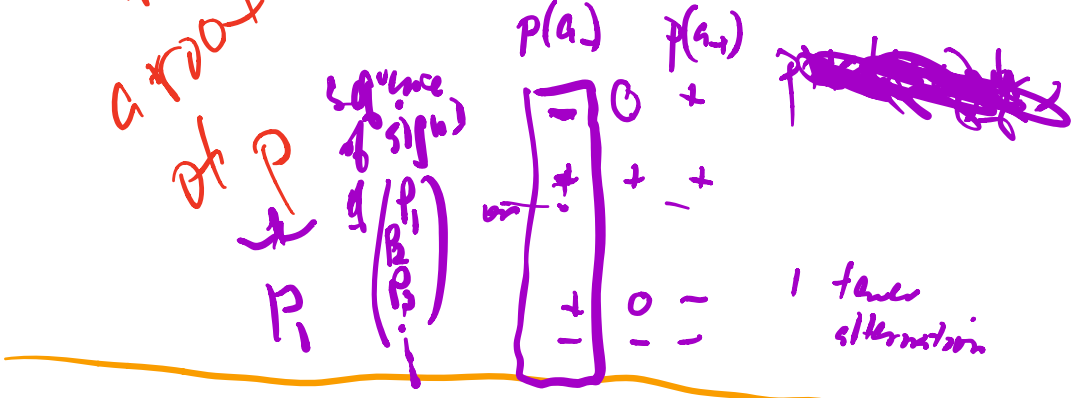
Or a root of some p_i $i>1$.

$p(x) = \prod (x - p_i)$

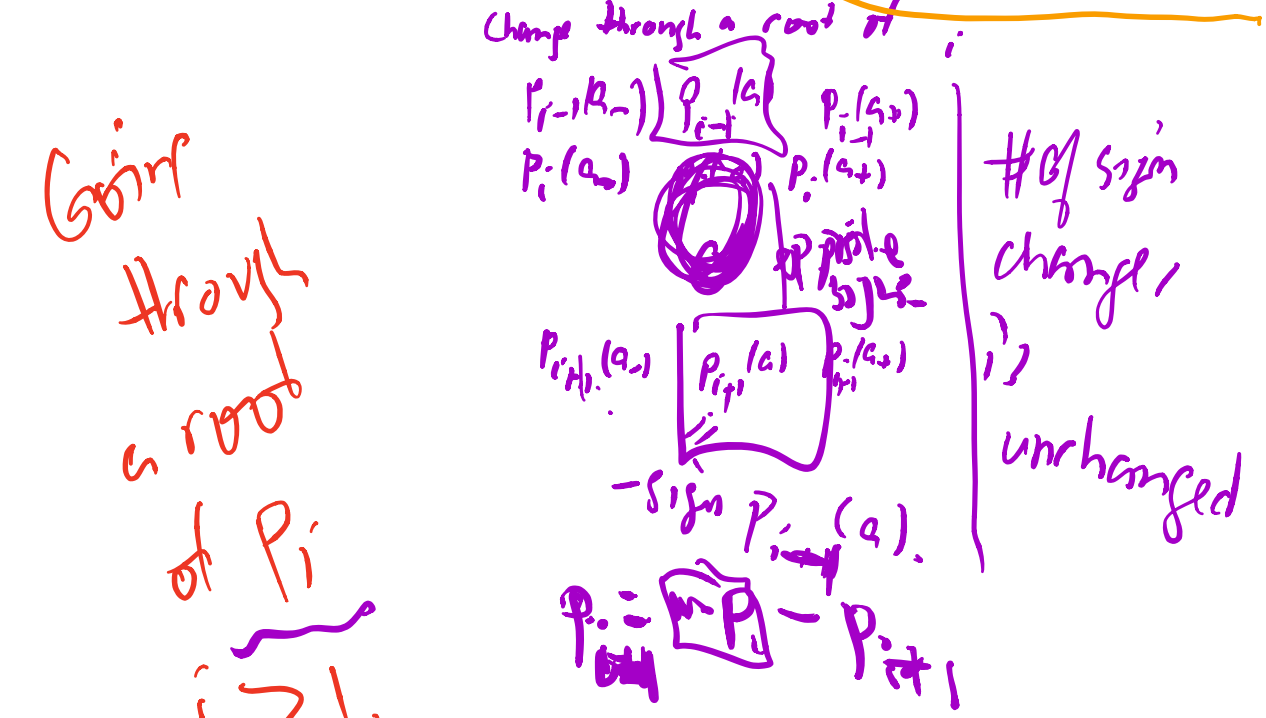
Quest. 20



Going thru a root of P at P_i



Going through a root of P_i, $i \geq 1$.



KEY PROPERTIES:

1. $P = P_0$, and P_K is a nonzero constant.
2. If c is a root of P_0, the product $P_0 P_1$ is negative on some interval $(c-\varepsilon, c)$ and positive on some interval $(c, c+\varepsilon)$.
3. If c is a root of P_i, $0 < i < K$, then $P_{i-1}(c) P_{i+1}(c) < 0$.

So do the same for P with multiple roots -

$$P_1\ P_2\ P_3 \cdots P_r = GCD(P_1, P_2).$$

P_2 : q^2

GCD(PP') has the same # of alternations of signs as

$$P_1/P_r,\ P_2/P_r \cdots P_{r-1}/P_r,\ 1.$$

when dividing at any a not a root of P.

∴ Sturm works even if P has multiple roots.

SYLVESTER'S THEOREM

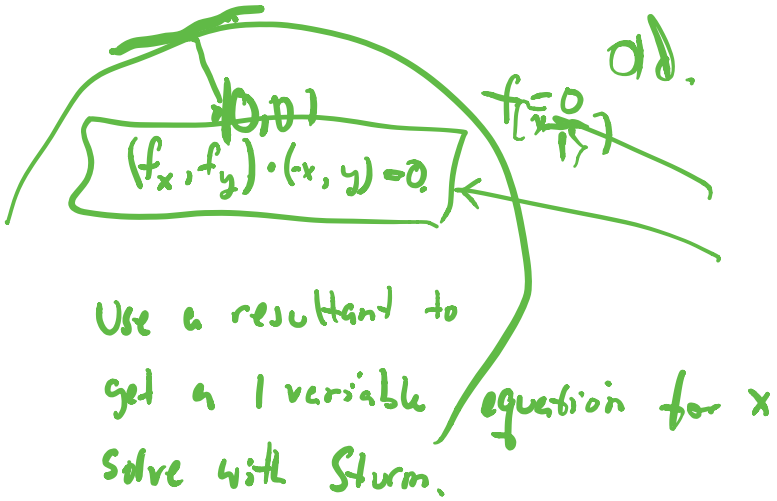
Definition 1.2.8. *Let R be a real closed field, and let f and g be in $R[X]$. The* Sturm sequence *of f and g is the sequence of polynomials $(f_0, \ldots, f_k)$ defined as follows:*

$f_0 = f\,, \quad f_1 = f'g\,,$
$f_i = f_{i-1}q_i - f_{i-2}$ *with* $q_i \in R[X]$ *and* $\deg(f_i) < \deg(f_{i-1})$ *for* $i = 2, \ldots, k\,,$
f_k *is a greatest common divisor of* f *and* $f'g\,.$

Theorem 1.2.9 (Sylvester's Theorem). *Let R be a real closed field and let f and g be two polynomials in $R[X]$. Let $a, b \in R$ be such that $a < b$ and neither a nor b are roots of f. Then the difference between the number of roots of f in the interval $]a, b[$ for which g is positive and the number of roots of f in the interval $]a, b[$ for which g is negative, is equal to $v(f, g; a) - v(f, g; b)$.*

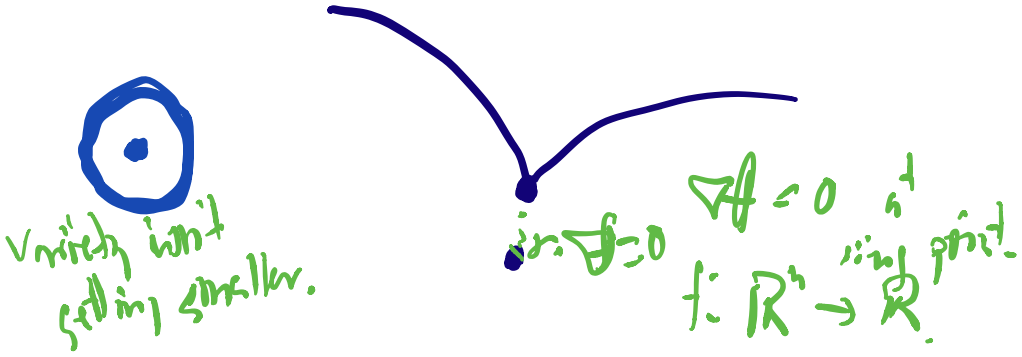
SEIDENBERG'S METHOD.

Reduce to existence of real points on varieties. Generalize the following method from plane curves.



What Can Go Wrong?

WHAT CAN GO WRONG?



THIS IS HIGHLY NON-GENERIC

Annals of Math. 1954.

6. Additional remarks

(a) Originally we had an idea for a proof which is practically immediate if K is the field of real numbers and which in any event makes the reason for the truth of the decision method especially clear. Instead of asking whether a hypersurface $f(x_1, \cdots, x_n) = 0$ carries a real point, we ask whether a variety V given by $f_1(x_1, \cdots, x_n) = 0, \cdots, f_s(x_1, \cdots, x_n) = 0$ carries one. It does, obviously in the case K is the field of real numbers, if and only if there is on V a real point nearest the origin. Arranging matters so that the origin is not the center of any sphere containing a component of V of positive dimension, the minimum condition stated determines a subvariety V_0 of V, of dimension less than the dimension of V if V is of positive dimension, such that V carries a real point if and only if V_0 does. In this way it comes to deciding whether a 0-dimensional variety contains a real point: after appropriate projections one has that the ambient space is 1-dimensional, and then Sturm's Theorem is applicable.

TARSKI - SEIDENBERG PROOF (c.f. Bochnak, Coste, Roy)

PREAMBLE.

Notation 1.4.3. *Let $f_1, \ldots, f_s$ be a sequence of polynomials in $R[X]$ and let $x_1 < \ldots < x_N$ be the roots in R of all f_i that are not identically zero. By convention we define $x_0 = -\infty$, $x_{N+1} = +\infty$. If $I_k =]x_k, x_{k+1}[$, $\operatorname{sign}(f_i(x))$ is constant for $x \in I_k$, and is denoted $\operatorname{sign}(f_i(I_k))$.*

The matrix with s rows and $2N+1$ columns whose i^{th} row is

---

$$\operatorname{sign}(f_i(I_0)), \operatorname{sign}(f_i(x_1)), \operatorname{sign}(f_i(I_1)), \ldots, \operatorname{sign}(f_i(x_N)), \operatorname{sign}(f_i(I_N))$$

is denoted $\operatorname{SIGN}_R(f_1, \ldots, f_s)$. Note that $\operatorname{SIGN}_R(f_1, \ldots, f_s)$ is a matrix with entries in $\{-1, 0, 1\}$.

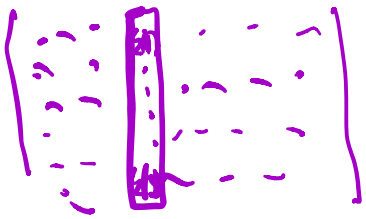
If $m = \max(\{\deg(f_i) \mid i = 1, \ldots, s\})$ then $N \leq sm$. The disjoint union of the sets of matrices with entries in $\{-1, 0, 1\}$ having s rows and $2\ell + 1$ columns, for $\ell = 0, \ldots, sm$, is denoted $W_{s,m}$.

Lemma 1.4.4. *Let ϵ be a function from $\{1, \ldots, s\}$ to $\{-1, 0, +1\}$. Then there exists a subset $W(\epsilon)$ of $W_{s,m}$ such that for every real closed field R and every sequence $f_1, \ldots, f_s$ of polynomials in $R[X]$ of degrees $\leq m$, the system*

$$\begin{cases} \operatorname{sign}(f_1(X)) = \epsilon(1) \\ \qquad \vdots \\ \operatorname{sign}(f_s(X)) = \epsilon(s) \end{cases}$$

has a solution x in R if and only if $\operatorname{SIGN}_R(f_1, \ldots, f_s) \in W(\epsilon)$.

Proof. $W(\epsilon)$ is the subset of $W_{s,m}$ whose elements are matrices having one of their columns coinciding with the sequence $\epsilon(1), \ldots, \epsilon(s)$. □



The importance of the concept of "SIGN$_R$" is that the "SIGN$_R$" of a sequence of polynomials $f_1, \ldots, f_s$ is completely determined by the "SIGN$_R$" of a new and simpler sequence.

The importance of the concept of "SIGN_R" is that the "SIGN_R" of a sequence of polynomials $f_1, \ldots, f_s$ is completely determined by the "SIGN_R" of a new and simpler sequence.

Lemma 1.4.5. *There exists a mapping φ from $W_{2s,m}$ to $W_{s,m}$ such that for every real closed field R and every sequence $f_1, \ldots, f_s$ of polynomials in $R[X]$ of degrees $\leq m$, with f_s nonconstant and none of the $f_1, \ldots, f_{s-1}$ identically zero, we have:*

$$\mathrm{SIGN}_R(f_1, \ldots, f_s) = \varphi(\mathrm{SIGN}_R(f_1, \ldots, f_{s-1}, f_s', g_1, \ldots, g_s)) ,$$

where f_s' is the derivative of f_s, and $g_1, \ldots, g_s$ are the remainders of the euclidean division of f_s by $f_1, \ldots, f_{s-1}, f_s'$, respectively.

Proof. Let $x_1 < \ldots < x_N$, with $N \leq 2sm$, be the roots in R of those polynomials among $f_1, \ldots, f_{s-1}, f_s', g_1, \ldots, g_s$ that are not identically zero. Extract from these roots the subsequence $x_{i_1} < \ldots < x_{i_M}$ of the roots of the polynomials $f_1, \ldots, f_{s-1}, f_s'$. The sequence $i_1, \ldots, i_M$ depends only on $w = \mathrm{SIGN}_R(f_1, \ldots, f_{s-1}, f_s', g_1, \ldots, g_s)$. By convention, let $i_0 = 0$ with $x_0 = -\infty$ and let $i_{M+1} = N+1$ with $x_{N+1} = +\infty$. For $k = 1, \ldots, M$ one of the polynomials $f_1, \ldots, f_{s-1}, f_s'$ vanishes at x_{i_k}. It is enough to know w in order to choose a function $\theta : \{1, \ldots, M\} \to \{1, \ldots, s\}$ such that $f_s(x_{i_k}) = g_{\theta(k)}(x_{i_k})$. We show that the existence of a root of f_s in an interval $]x_{i_k}, x_{i_{k+1}}[$, for $k = 0, \ldots, M$, depends only on w. The polynomial f_s has a root

– in $]x_{i_k}, x_{i_{k+1}}[$, for $k = 1, \ldots, M-1$, if and only if

$$\mathrm{sign}(g_{\theta(k)}(x_{i_k}))\,\mathrm{sign}(g_{\theta(k+1)}(x_{i_{k+1}})) = -1 ,$$

– in $]-\infty, x_{i_1}[$ (if $M \neq 0$) if and only if

$$\mathrm{sign}(f_s'(]-\infty, x_1[))\,\mathrm{sign}(g_{\theta(1)}(x_{i_1})) = 1 ,$$

– in $]x_{i_M}, +\infty[$ (if $M \neq 0$) if and only if

$$\mathrm{sign}(f_s'(]x_N, +\infty[))\,\mathrm{sign}(g_{\theta(M)}(x_{i_M})) = -1 ,$$

– in $]-\infty, +\infty[$ always if $M = 0$.

Now let $y_1 < \ldots < y_L$ (with $L \leq sm$) be the roots in R of the polynomials $f_1, \ldots, f_s$. As before, let $y_0 = -\infty$, $y_{L+1} = +\infty$. Define the function

$$\begin{array}{rccl} \rho : & \{0, \ldots, L+1\} & \longrightarrow & \{0, \ldots, M+1\} \cup \{(k, k+1) \mid k = 0, \ldots, M\} \\ & \ell & \longmapsto & \begin{cases} k & \text{if } y_\ell = x_{i_k} , \\ (k, k+1) & \text{if } y_\ell \in]x_{i_k}, x_{i_{k+1}}[. \end{cases} \end{array}$$

From what we have seen before, the number L and the function ρ depend only on w. We are now ready to verify that $\mathrm{SIGN}_R(f_1, \ldots, f_s)$ depends only on w.

For $j = 1, \ldots, s-1$, we have

– if $\rho(\ell) = k$ $\quad \mathrm{sign}(f_j(y_\ell)) = \mathrm{sign}(f_j(x_{i_k}))$,

– if $\rho(\ell) = (k, k+1)$ $\quad \mathrm{sign}(f_j(y_\ell)) = \mathrm{sign}(f_j(]x_{i_k}, x_{i_{k+1}}[))$.

We also have

– if $\rho(\ell) = k$ or $(k, k+1)$ $\quad \mathrm{sign}(f_j(]y_\ell, y_{\ell+1}[)) = \mathrm{sign}(f_j(]x_{i_k}, x_{i_{k+1}}[))$.

We now deal with the case $j = s$. We have

– if $\rho(\ell) = k$ $\quad \mathrm{sign}(f_s(y_\ell)) = \mathrm{sign}(g_{\theta(k)}(x_{i_k}))$,

– if $\rho(\ell) = (k, k+1)$ $\quad \mathrm{sign}(f_s(y_\ell)) = 0$.

The most delicate case concerns $\mathrm{sign}(f_s(]y_\ell, y_{\ell+1}[))$:

– if $\ell \neq 0$, $\rho(\ell) = k$ $\quad \mathrm{sign}(f_s(]y_\ell, y_{\ell+1}[)) = \mathrm{sign}(g_{\theta(k)}(x_{i_k}))$ if this is nonzero, $\mathrm{sign}(f_s(]y_\ell, y_{\ell+1}[)) = \mathrm{sign}(f_s'(]x_{i_k}, x_{i_{k+1}}[))$ otherwise,

– if $\ell \neq 0$, $\rho(\ell) = (k, k+1)$ $\quad \mathrm{sign}(f_s(]y_\ell, y_{\ell+1}[)) = \mathrm{sign}(f_s'(]x_{i_k}, x_{i_{k+1}}[))$,

– if $\ell = 0$ $\quad \mathrm{sign}(f_s(]-\infty, y_1[)) = -\mathrm{sign}(f_s'(]-\infty, x_1[))$.

□

Proposition 1.4.6. *Let* $f_i(X,Y) = h_{i,m_i}(Y)X^{m_i} + \cdots + h_{i,0}(Y)$, *for* $i = 1,\ldots,s$, *be a sequence of polynomials in* $n+1$ *variables with coefficients in* $\mathbb{Z}$, *where* $Y = (Y_1,\ldots,Y_n)$, *and let* $m = \max(\{m_i \mid i = 1,\ldots,s\})$. *Let* W' *be a subset of* $W_{s,m}$. *Then there exists a boolean combination* $\mathcal{B}(Y)$ *of polynomial equations and inequalities in the variables* Y *with coefficients in* $\mathbb{Z}$, *such that, for every real closed field* R *and every* $y \in R^n$, *one has*

$$\mathrm{SIGN}_R(f_1(X,y),\ldots,f_s(X,y)) \in W' \Leftrightarrow \mathcal{B}(y) \text{ is satisfied in } R\,.$$

THIS ENABLES ELIMINATING VARIABLES ONE AT A TIME.

WORTH PAUSING TO THINK ABOUT THE COMPLEXITY OF THIS ALGORITHM.

JUST IN CASE.

Proof. Without loss of generality, we may assume that none of the polynomials $f_1, \ldots, f_s$ is identically zero and that $h_{i,m_i}(Y)$ is not identically zero for $i = 1, \ldots, s$. We associate to the sequence of polynomials $(f_1, \ldots, f_s)$ the sequence $(m_1, \ldots, m_s)$ of their degrees in X. To compare these finite sequences of integers, define a strict order as follows:

$$\sigma = (m'_1, \ldots, m'_t) \prec \tau = (m_1, \ldots, m_s)$$

if there exists $p \in \mathbb{N}$ such that, for every $q > p$, the number of times q appears in σ is equal to the number of times q appears in τ, and the number of times p appears in σ is smaller than the number of times p appears in τ. This gives a well-ordering of the set of sequences of integers: there is no infinite chain $\sigma_1 \succ \sigma_2 \succ \sigma_3 \succ \ldots$. We proceed now by induction with respect to the order $\prec$.

Let $m = \max(\{m_1, \ldots, m_s\})$. If $m = 0$, then the result is straightforward, since $\mathrm{SIGN}_R(f_1(X,y), \ldots, f_s(X,y))$ is the list of signs of "constant terms" $h_{1,0}(y), \ldots, h_{s,0}(y)$.

Suppose that $m \geq 1$ and $m_s = m$. Let $W'' \subset W_{2s,m}$ be the inverse image of $W' \subset W_{s,m}$ under the mapping φ defined in Lemma 1.4.5. By this lemma, for every real closed field R and for every $y \in R^n$ such that $h_{i,m_i}(y) \neq 0$ for $i = 1, \ldots, s$, the property

$$\mathrm{SIGN}_R(f_1(X,y), \ldots, f_s(X,y)) \in W'$$

is equivalent to the property

$$\mathrm{SIGN}_R(f_1(X,y), \ldots, f_{s-1}(X,y), f'_s(X,y), g_1(X,y), \ldots, g_s(X,y)) \in W'' \,,$$

where f'_s is the derivative of f_s with respect to X and $g_1, \ldots, g_s$ are the remainders in the euclidean division (with respect to X) of f_s by $f_1, \cdots, f_{s-1}, f'_s$, respectively, multiplied by appropriate even powers of $h_{1,m_1}, \ldots, h_{s,m_s}$, respectively, in order to clear the denominators. Now, the sequence of degrees in X of $f_1, \ldots, f_{s-1}, f'_s, g_1, \cdots, g_s$ is smaller than $(m_1, \ldots, m_s)$ with respect to the order $\prec$. On the other hand, if at least one among the $h_{i,m_i}(y)$ is zero, we can truncate the corresponding polynomial f_i and obtain a sequence of polynomials, whose sequence of degrees in X is smaller than $(m_1, \ldots, m_s)$ with respect to the order $\prec$. This completes the proof of Proposition 1.4.6 and proves the Tarski-Seidenberg principle as well. □ □

PAUL COHEN (CPAM)

DEFINITION. A real-valued function $f(x_1, \cdots, x_n)$ is *effective* if there is a primitive recursive procedure which to every polynomial relation $A(y, t_1, \cdots, t_m)$ assigns a polynomial relation $B(x_1, \cdots, x_n, t_1, \cdots, t_m)$ such that

$$A(f(x), t_1, \cdots, t_m) \Leftrightarrow B(x_1, \cdots, x_n, t_1, \cdots, t_m).$$

We observe some simple facts about effective functions. The effective functions are closed under composition. The functions $x + y$, $x \cdot y$, sgn x are effective. If $f(x)$ takes only finitely many values, all of which are integers, then f is effective if and only if for each k the relation $f(x) = k$ is equivalent to a

Example $f(x) = \sqrt{x^2+1}$.

polynomial relation $B(x)$. If f is effective and takes only the values 0 and 1, and if g_1 and g_2 are effective, and if $h \equiv g_1$ if $f = 0$, $h \equiv g_2$ if $f = 1$, then h is effective.

LEMMA. 1.1. *$f(x_1, \cdots, x_n)$ is effective if there is a primitive recursive function which assigns to every d a polynomial relation $A(c_0, \cdots, c_d, x_1, \cdots, x_n, \lambda)$ such that*

$$A(c, x, \lambda) \Leftrightarrow \lambda = \operatorname{sgn}(c_0 f^d + \cdots + c_d).$$

Proof: This is just a simple consequence of the fact that all polynomial relations are constructed from inequalities $p(x) > 0$. A rigorous proof proceeds by induction on the number of terms in the polynomial relation.

DEFINITION. Let $p(x)$ be a polynomial in one variable. By a *graph* for $p(x)$ we mean a k-tuple $t_1 < t_2 < \cdots < t_k$ such that, in each interval of the form $(-\infty, t_1)$, (t_i, t_{i+1}), (t_k, ∞), p is monotonic. By the data of the graph we mean the k-tuple $\langle t_1, \cdots, t_k \rangle$, $\operatorname{sgn} p(t_i)$ for $1 \leqq i \leqq k$, $\operatorname{sgn} p(t_1 - 1)$, and $\operatorname{sgn} p(t_k + 1)$.

We shall now prove the following two theorems by induction on n.

THEOREM A_n. *There are effective functions of $a_0, \cdots, a_n$ which give the data for a graph of $p(x) \equiv a_n x^n + \cdots + a_0$. More precisely, there are $2n$ effective functions of $a_0, \cdots, a_n$, namely, $t_i(a)$, $\operatorname{sgn} p(t_i(a))$, where $1 \leqq i \leqq n - 1$, $\operatorname{sgn} p(t_1(a) - 1)$ and $\operatorname{sgn} p(t_{n-1}(a) + 1)$, such that $t_1(a) < \cdots < t_{n-1}(a)$ form a graph for $p(x)$.*

THEOREM B_n. *Let $p(x) \equiv a_n x^n + \cdots + a_0$. There are $n + 1$ effective functions of $a_0, \cdots, a_n$, namely $k(a)$ and $\xi_1(a) < \xi_2(a) \cdots < \xi_n(a)$, such that $\xi_1(a), \cdots, \xi_{k(a)}(a)$ are all the roots of $p(x)$.*

In the proofs of these theorems we shall use without proving it the fact that certain simple functions we encounter are indeed effective. The case $n = 0$ of the theorem being trivial, assume both theorems have been proved for all values less than a given n. We now prove Theorem A_n as follows: Consider the polynomial $p'(x)$. Its coefficients are effective functions of those of p. By Theorem B_{n-1}, its zeros lie among $\xi_1, \cdots, \xi_{n-1}$, where ξ_i are effective. These ξ_i can be taken as defining a graph for p and since ξ_i are effective, so are $\operatorname{sgn} p(\xi_i)$, $\operatorname{sgn} p(\xi_1 - 1)$, $\operatorname{sgn} p(\xi_{n-1} + 1)$.

To prove Theorem B_n, let $t_1 < \cdots < t_{n-1}$ define an effective graph for p, which is possible by virtue of Theorem A_n. By examining $\operatorname{sgn} p(t_i)$, $\operatorname{sgn} p(t_1 - 1)$, $\operatorname{sgn} p(t_{n-1} + 1)$, we can determine the number of roots of p effectively. In each interval $(-\infty, t_1)$, (t_i, t_{i+1}), (t_{n-1}, ∞) there is at most one root of p, and there is also the possibility that some of the t_i are roots of p. To show that the roots of p are effective, we consider for example the case of a possible root ξ between t_i and t_{i+1}. The other cases are handled quite similarly. By virtue of Lemma 1.1, it is sufficient to show that if $q(x) \equiv c_0 x^m + \cdots + c_m$, $\operatorname{sgn} q(\xi)$ is an effective function of c_i and the coefficients of p. Let $\tilde{q}(x)$ be the remainder obtained by dividing $p(x)$ into $q(x)$. Its coefficients are effective functions of the coefficients of p and the c_i. Also $\deg \tilde{q} < n$, and $\tilde{q}(\xi) = q(\xi)$. This means that by replacing q by $\tilde{q}$ we can assume that $\deg q < n$. Let $u_1 < u_2 < \cdots < u_n$ define an effective graph for q. We now claim that there is an effective function of the coefficients of p and q which gives us the position of ξ relative to the u_i, i.e., tells us, for which i, $u_i > \xi$ or whether $u_i = \xi$. This, of course, will in turn determine $\operatorname{sgn} q(\xi)$ and prove the theorem. Suppose, for definiteness, $t_1 < \xi < t_2$. There are two cases to distinguish:

(i) no u_i is in $[t_1, t_2]$,

(ii) only $u_\alpha, u_{\alpha+1}, \cdots, u_{\alpha+l}$ are in $[t_1, t_2]$.

Since the u_i and t_j are given effectively, these cases can be distinguished effectively. In the first case, the position of ξ relative to u_i is determined by the position of t_1 and t_2 relative to u_i. In the second case, by examining $\operatorname{sgn} p(u_\alpha), \cdots, \operatorname{sgn} p(u_{\alpha+l})$, $\operatorname{sgn} p(t_1)$ and $\operatorname{sgn} p(t_2)$ we can determine the position of ξ relative to the u_i. Thus, Theorem B_n is proved.

We can now prove Tarski's theorem. Let $A(x_1, \cdots, x_n)$ be a polynomial relation. Then A is a Boolean function of finitely many relations $p_i(x_1) > 0$, where each p_i is a polynomial whose coefficients are polynomials in $x_2, \cdots, x_n$. Since the roots of p_i are effective functions of $x_2, \cdots, x_n$, and there exist graphs for p_i which are effective functions of $x_2, \cdots, x_n$, it is clear that by examining the relative position of these various points one can easily determine what the various possibilities are for the sequence $\{\operatorname{sgn} p_i(x)\}$ for arbitrary x. This in turn means that we can find a polynomial relation $B(x_2, \cdots, x_n)$ such that $\exists x_1 A(x_1, \cdots, x_n) \equiv B(x_2, \cdots, x_n)$.

* Sylvester theorem.

(Thanks to a talk of Coste at IPAM :)

QE via counting roots (Tarski)

- Algorithmic reduction to an equivalent prenex form

$$Q_1 X_1 \; Q_2 X_2 \ldots Q_\ell X_\ell \; \Psi(Y_1, \ldots, Y_k, X_1, \ldots, X_\ell) \; ,$$

  where Q_i are quantifiers and Ψ is quantifier-free.
- It suffices to eliminate one quantifier at a time, and to deal with an existential quantifier.
- $\exists X \, \mathcal{S}(Y_1, \ldots, Y_k, X)$ where $\mathcal{S}$ is a system of polynomial equations and inequalities.
- Case of $P(\underline{Y}, X) = 0, Q_1(\underline{Y}, X) > 0, \ldots, Q_r(\underline{Y}, X) > 0$: variants of Sturm to produce Boolean combinations $\mathcal{T}_c$ of sign conditions on the coefficients (depending on $\underline{Y}$) satisfied iff the number of solutions in X is c.
- Primitive recursive complexity.

QE via CAD (Cylindrical Algebraic Decomposition - Collins)

- Starting with $Q_1 X_1 \; Q_2 X_2 \ldots Q_\ell X_\ell \; \Psi(Y_1, \ldots, Y_k, X_1, \ldots, X_\ell)$, where Ψ is a Boolean combination of sign conditions on polynomials in a finite family $\mathcal{P}$.
- Construct a CAD of $R^{k+\ell}$ adapted to $\mathcal{P}$. The formula describes a union of cells in R^k. Already OK for decision algorithm.
- For quantifier elimination, a quantifier-free description of cells is needed. This is provided by Thom's lemma: if $\mathcal{Q} \subset R[X]$ is a finite family of polynomials closed under derivation, $\bigcap_{Q \in \mathcal{Q}} \{x \in R \mid Q(x) \; ?_Q \; 0\}$ (where $?_Q$ is either $>$, $=$, $<$) is empty, or a point or an open interval.
- Better complexity: doubly exponential in the number of variables (free and bound).

QE via critical points

- Instead of eliminating one quantifier after the other, eliminate one block of existential quantifiers at a time using a parametric version of critical point method.
- Complexity: doubly exponential in the number of alternations of quantifiers (Grigoriev-Vorobjov, Renegar, Basu-Pollack-Roy).

Back To Real Ordered Fields.

- $(F, 0, 1, \cdot, +, <)$.

$P \subset F$ = positive cone.

$F = P \cup \{0\} \cup N, \quad N = -P$

all three disjoint.

Theorem: (Artin)

① F is orderable $\Leftrightarrow -1$ is not $\sum f_i^2$

② The order can be chosen so that

if $e \neq \sum f_i^2$

we can make e negative.

Proof.

(trotting Zorn's lemma)

Order Positive cones and take a maximal one....

Theorem $(F, >)$ can always be embedded in a real closed field.

Note: Can't be picked out of $\overline{F}$.

Examples of orderings of

$\mathbb{E}$
|
$\mathbb{Q}$

$\mathbb{Q}(x)$

$\mathbb{R}(x)$

$x = 0^+ \quad y = 0^+$

$\mathbb{Q}(x,y)$ vs $\mathbb{Q}(x)(y)$.

$\mathbb{R}(x,y)$,

[Worth recalling the classical idea of a generic point]

A basic idea in the classical theory is the following:

(1.3) **Definition.** *Let $k \subset \mathbb{C}$ be a subfield, and let $\mathfrak{P}$ be a prime ideal. A k-generic point $x \in V(\mathfrak{P})$ is a point such that every polynomial $f(X_1,\ldots,X_n)$ with coefficients in k that vanishes at x is in the ideal $\mathfrak{P}$, hence vanishes on all of X.*

Example: In example (b) above if the coefficients of the g_i are in $\mathbb{Q}$, the point $(\pi, g_2(\pi),\ldots,g_n(\pi))$ is a $\mathbb{Q}$-generic point of this rational curve.

(1.4) **Proposition.** *If $\mathbb{C}$ has infinite transcendence degree over k, then every variety $V(\mathfrak{P})$ has a k-generic point.*

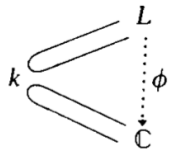
Proof. Let $f_1,\ldots f_m$ be generators of $\mathfrak{P}$. We may enlarge k if we wish by adjoining the coefficients of all the f_i without destroying the hypothesis. Let

$$\mathfrak{P}_0 = \mathfrak{P} \cap k[X_1,\ldots,X_n]$$

and let

$$L = \text{quotient field of } k[X_1,\ldots,X_n]/\mathfrak{P}_0.$$

Then L is an extension field of k of finite transcendence degree. But any such field is isomorphic to a subfield of $\mathbb{C}$: i.e., $\exists$ a monomorphism ϕ



If $\overline{X}_i$ = image of X_i in L and $a_i = \phi(\overline{X}_i)$, I claim $a = (a_1,\ldots,a_n)$ is a k-generic point. In fact, $f_i \in \mathfrak{P}_0$, $1 \leqq i \leqq k$, hence $f_i(\overline{X}_1,\ldots,\overline{X}_n) = 0$ in L. Therefore $f_i(a_1,\ldots,a_n) = 0$ in $\mathbb{C}$ and a is indeed a point of X. But if $f \in k[X_1,\ldots,X_n]$ and $f \notin \mathfrak{P}$, then $f \notin \mathfrak{P}_0$, hence $f(\overline{X}_1,\ldots,\overline{X}_n) \neq 0$ in L. Therefore $f(a_1,\ldots,a_n) = \phi(f(\overline{X}_1,\ldots\overline{X}_n)) \neq 0$ in $\mathbb{C}$. QED

For any subset $S \subset \mathbb{C}^n$, let $I(S)$ be the ideal of polynomials $f \in \mathbb{C}[X_1,\ldots,X_n]$ that vanish at all points of S. Then an immediate corollary of the existence of generic point is:

(1.5) **Hilbert's Nullstellensatz.** *If $\mathfrak{P}$ is a prime ideal, then $\mathfrak{P}$ is precisely the ideal of polynomials $f \in \mathbb{C}[X_1,\ldots,X_n]$ that vanish identically on $V(\mathfrak{P})$, i.e., $\mathfrak{P} = I(V(\mathfrak{P}))$. More generally, if $\mathfrak{A}$ is any ideal, then $\sqrt{\mathfrak{A}} = I(V(\mathfrak{A}))$.*

Proof. Given any $f \in \mathbb{C}[X]$, let k be a finitely generated field over $\mathbb{Q}$ containing the coefficients of f and let $a \in V(\mathfrak{P})$ be a k-generic point. If $f \notin \mathfrak{P}$, then $f(a) \neq 0$ hence f does not vanish identically on $V(\mathfrak{P})$; the 2nd assertion reduces to the 1st by means of (f) on p. 2.

Cohen's version of Robinson's version of Hilbert 17:

Another application is to Hilbert's seventeenth problem which may be found in [6]. We repeat it here. We use the fact about real fields that, if K is a real field and $a \in K$ is not a sum of squares, then in some ordering of K, a is negative. Let $f(x_1, \cdots, x_n)$ be a rational function with real coefficients which is non-negative for all real values of x_i for which the denominator is not zero. Let S be any real-closed field containing the field of real numbers. The decision procedure for real-closed fields may be applied to the statement

$$A \equiv \exists x_1 \cdots x_n (f(x_1, \cdots, x_n) < 0 \text{ and the denominator of } f \text{ is not zero}).$$

This will yield a polynomial relation involving the coefficients of f which is necessary and sufficient for A to hold in S. Since the order relation of the reals is unique and the coefficients of f are real, this polynomial relation holds in S if and only if it holds in the real numbers. Thus we have shown that f is non-negative if the x_i range over any real-closed field S. Since every real field can be extended to a real-closed field, f is non-negative if the x_i range over any real field. Let K be the field of rational functions in $x_1, \cdots, x_n$ with real coefficients. Assume f is not a sum of squares. Then we can order K so that f is negative since K is a real field. This means that if we think of f as an element of $K(t_1, \cdots, t_n)$, then f assumes a negative value when the variables are replaced by the elements x_i lying in the real field K. This is a contradiction, so f must be a sum of squares.

Can we be quantitative?

What is the truth about these algorithmic questions?

Pfister's Theory of Multiplicative QF's.

Corollaries:

① In any field $\left(\sum_{i=1}^{2^k} x_i^2\right)$ is closed under multiplication

② $f \in \mathbb{R}[X_1 \cdots X_n]$ is ≥ 0

iff $f = \sum_{i=1}^{2^n} r_i^2$

(Best lower bound $\geq n+2$ approximately)

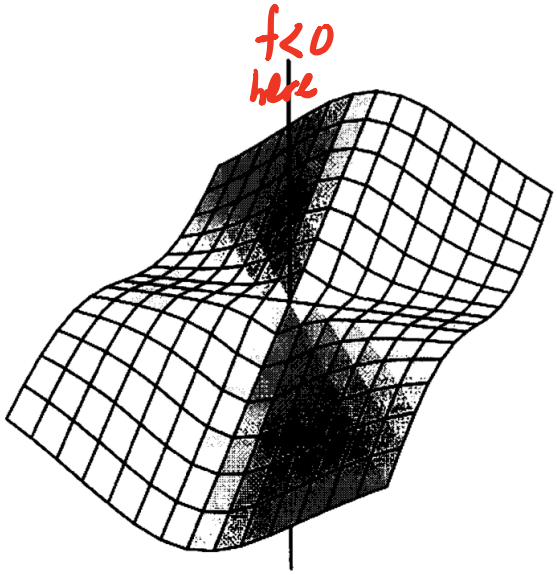
③ Variations for $f \in \mathbb{R}[V]$

for a real variety:

Example:

given by the equation $x^3 = z(x^2 + y^2)$. Then $f = x^2 + y^2 - z^2 \in \mathcal{P}(V)$ is negative on the stick $x = y = 0$ outside the origin. Nevertheless, f is a sum of squares in $K(V)$:

$$f = x^2 + y^2 - \frac{x^6}{(x^2+y^2)^2} = \frac{3x^4y^2 + 3x^2y^4 + y^6}{(x^2+y^2)^2}.$$



PRETTY FREAKY!

CARTAN UMBRELLA

Positive on the cloth

not on the handle.

COROLLARY CONT'D:

- $f > 0$ w reg. points
  $= \sum f_i^2$

[Milnor - Husemoller]

§ 4. Multiplicative Inner Product Spaces

The results in this section are due to Pfister. (Compare [Scharlau, 1969] and [Lorenz].) However for convenience we will modify Pfister's definitions.

If x belongs to an inner product space X, it will be convenient to call $x \cdot x$ the *norm* of x. Thus a field element α is a *norm from* X if $\alpha = x \cdot x$ for some x.

(4.1) Definition. An inner product space X is *multiplicative* if

$$X \cong \langle \alpha \rangle \otimes X$$

for every field element $\alpha \neq 0$ which is a norm from X.

(This is not the usual definition.)

One important property of multiplicative spaces is the following.

(4.2) Lemma. *If X is multiplicative, then the set of all field elements $\alpha \neq 0$ which are norms from X forms a subgroup of $F^\bullet$.*

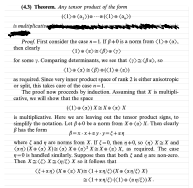
Proof. If $\alpha = x \cdot x \neq 0$ and $\beta = y \cdot y \neq 0$, choose an isomorphism

$$f\colon\ X \to \langle \beta \rangle \otimes X .$$

Setting $f(x) = e \otimes z$, where $e \cdot e = \beta$, we obtain

$$x \cdot x = f(x) \cdot f(x) = \beta\, z \cdot z .$$

Therefore the quotient $\alpha/\beta = z \cdot z$ is also a norm from X, which completes the proof. □



(4.3) **Theorem.** *Any tensor product of the form*

$$(\langle 1 \rangle + \langle a_1 \rangle) \otimes \cdots \otimes (\langle 1 \rangle + \langle a_n \rangle)$$

is multiplicative.

Proof. First consider the case $n = 1$. If $\beta \neq 0$ is a norm from $\langle 1 \rangle \otimes \langle a \rangle$, then clearly

$$\langle 1 \rangle \otimes \langle a \rangle \cong \langle \beta \rangle \otimes \langle \gamma \rangle$$

for some γ. Comparing determinants, we see that $\langle \gamma \rangle \cong \langle \beta a \rangle$, so

$$\langle 1 \rangle \otimes \langle a \rangle \cong \langle \beta \rangle \otimes \langle a \beta \rangle$$

as required. Since very inner product space of rank 2 is either anisotropic or split, this takes care of the case $n = 1$.

The proof now proceeds by induction. Assuming that X is multiplicative, we will show that the space

$$(\langle 1 \rangle + \langle a \rangle) X \cong X \oplus \langle a \rangle\, X$$

is multiplicative. Here we are leaving out the tensor product signs, to simplify the notation. Let $\beta \neq 0$ be a norm from $X \oplus \langle a \rangle\, X$. Then clearly β has the form

$$\beta = x \cdot x + y \cdot y = \zeta + a\eta$$

where ζ and η are norms from X. If $\zeta = 0$, then $\eta \neq 0$, so $\langle \eta \rangle\, X \cong X$ and $\langle a \rangle\, (X \oplus \langle a \rangle\, X) \cong \langle a \rangle^2\, X \cong X \cong \langle a \rangle\, X$, as required. The case $\eta = 0$ is handled similarly. Suppose then that both ζ and η are non-zero. Then $X \cong \langle \zeta \rangle\, X \cong \langle a\eta \rangle\, X$ as it follows that

$$\begin{aligned} (\langle 1 + a\eta \rangle\, (X \oplus \langle a \rangle\, X) &\cong (1 + a\eta)\langle 1 \rangle (X \oplus \langle a\eta \rangle\, X) \\ &\cong (1 + a\eta)\langle 1 \rangle \oplus \langle a\eta \zeta \rangle) X . \end{aligned}$$

But we have already established that the inner product space

$$\langle 1 \rangle \otimes \langle a\eta\zeta \rangle$$

is multiplicative. Since $1 + a\eta\zeta$ is a non-zero norm from this space, we see that the factor $\langle 1 + a\eta\zeta \rangle$ can be cancelled, and we are left with

$$(\langle 1 \rangle \otimes \langle a\eta\zeta \rangle)\, X \cong X \oplus \langle a \rangle\, X ,$$

as required.

FROM JACOBSON BASIC ALGEBRA II.

LEMMA 2. *Let Q be a strongly multiplicative quadratic form, a an element of F^*. Let $Q_a \sim \operatorname{diag}\{1, a\}$. Then $Q_a \otimes Q$ is strongly multiplicative.*

Proof. It is clear that $Q_a \otimes Q$ is equivalent to $Q \oplus aQ$. Hence, it suffices to show that the latter is strongly multiplicative. We now use the notation $\sim$ also for equivalence of quadratic forms and if $Q_1 \sim \operatorname{diag}\{a, b\}$, then we denote $Q_1 \otimes Q_2$ by $\operatorname{diag}\{a, b\} \otimes Q_2 \sim aQ_2 \oplus bQ_2$. Let k be an element of F^* represented by $Q \oplus aQ$, so $k = b + ac$ where b and c are represented by Q (possibly trivially if b or c is 0). We distinguish three cases:

Case I. $c = 0$. Then $k = b$ and $Q \sim bQ$. Hence $Q \oplus aQ \sim bQ \oplus abQ = b(Q \oplus aQ) = k(Q \oplus aQ)$.

Case II. $b = 0$. Then $k = ac$ and $k(Q \oplus aQ) = kQ \oplus kaQ = acQ \oplus a^2cQ \sim aQ \oplus Q$ since $cQ \sim Q$ by hypothesis and $Q \sim a^2Q$ for any $a \in F^*$. Thus $k(Q \oplus aQ) \sim Q \oplus aQ$.

Case III. $bc \neq 0$. We have $Q \oplus aQ \sim bQ \oplus acQ \sim \operatorname{diag}\{b, ac\} \otimes Q$. Since $k = b + ac$ is represented by $bx_1^2 + acx_2^2$ and bac and k^2abc differ by a square, it follows from Lemma 1 that $\operatorname{diag}\{b, ac\} \sim \operatorname{diag}\{k, kabc\}$. Hence $\operatorname{diag}\{b, ac\} \otimes Q \sim \operatorname{diag}\{k, kabc\} \otimes Q \sim k \operatorname{diag}\{1, abc\} \otimes Q \sim kQ \oplus kabcQ \sim kQ \oplus kaQ = k(Q \oplus aQ)$.

In all cases we have that $Q \oplus aQ \sim k(Q \oplus aQ)$, so $Q \oplus aQ$ is strongly multiplicative. □

strong multiplicativity

2×2 Diags are equivalent if
1 diag prediction is represented
by the other where the det / ( )².

Jacobson Basic Algebra II p. 668 - ...

THEOREM 11.11. *Suppose that every Pfister form of dimension 2^n represents every non-zero sum of two squares in F. Then every Pfister form of dimension 2^n represents every non-zero sum of k squares in F for arbitrary k.*

Proof. By induction on k. Since any Pfister form represents 1, the case $k = 1$ is clear and the case $k = 2$ is our hypothesis. Now assume the result for $k \geqslant 2$. It suffices to show that if Q is a Pfister form of dimension 2^n and a is a sum of k squares such that $c = 1 + a \neq 0$, then c is represented by Q. This will follow if we can show that $Q \oplus -cQ$ represents 0 non-trivially. For then we shall have vectors u and v such that $Q(u) = cQ(v)$ where either $u \neq 0$ or $v \neq 0$. If either $Q(u) = 0$ or $Q(v) = 0$, then both are 0 and so Q represents 0 non-trivially. Then Q is universal and hence represents c. If $Q(u) \neq 0$ and $Q(v) \neq 0$, then these are contained in F_Q^* and hence $c = Q(u)Q(v)^{-1} \in F_Q^*$, so c is represented by Q. We now write $Q = x^2 \oplus Q'$. Since Q represents a, we have $a = a_1^2 + a'$ where Q' represents a'. We have $\operatorname{diag}\{1, -c\} \otimes Q \sim Q \oplus (-cQ) \sim x^2 \oplus Q' \oplus (-cQ)$ and $Q' \oplus (-cQ)$ represents $a' - (1 + a_1^2 + a') = -(1 + a_1^2)$. If this is 0, then $c = a'$ is represented by Q. Hence we may assume that $1 + a_1^2 \neq 0$. Then by Theorem 11.10, $\operatorname{diag}\{1, -c\} \otimes Q \sim \operatorname{diag}\{1, -1 - a_1^2\} \otimes Q''$ where Q'' is a Pfister form of dimension 2^n. By the hypothesis, this represents $1 + a_1^2$. It follows that $\operatorname{diag}\{1, -1 - a_1^2\} \otimes Q''$ represents 0 non-trivially. Then $Q \oplus -cQ \sim \operatorname{diag}\{1, -1 - a_1^2\} \otimes Q''$ represents 0 non-trivially. This completes the proof. □

THEOREM 11.12. *Let R be a real closed field and let Q be a Pfister form on a 2^n-dimensional vector space over the field $R(x_1, \ldots, x_n)$. Then Q represents every non-zero sum of two squares in $R(x_1, \ldots, x_n)$.*

Proof. Let Q be a Pfister form on a 2^n-dimensional vector space V over $R(x_1, \ldots, x_n)$. We have to show that if $b = b_1^2 + b_2^2 \neq 0$, $b_i \in R(x_1, \ldots, x_n)$, then b is represented by Q. Since Q represents 1, the result is clear if $b_1 b_2 = 0$.

Hence we assume $b_1 b_2 \neq 0$. Let $C = R(i)$, $i^2 = -1$, and consider the extension field $C(x_1, \ldots, x_n)$ of $R(x_1, \ldots, x_n)$ and the vector space $\tilde{V} = V_{C(x_1, \ldots, x_n)} = C(x_1, \ldots, x_n) \otimes_{R(x_1, \ldots, x_n)} V$. If (e_1, e_2) is a base for C/R, then this is a base for $C(x_1, \ldots, x_n)$ over $R(x_1, \ldots, x_n)$. Moreover, every element of $\tilde{V}$ can be written in one and only one way as $e_1 u_1 + e_2 u_2$, $u_i \in V$ (identified with a subspace of $\tilde{V}$ in the usual way). The quadratic form Q has a unique extension to a quadratic form $\tilde{Q}$ on $\tilde{V}$. Evidently $\tilde{Q}$ is a Pfister form. Now put $q = b_1 + b_2 i$. Then $(1, q)$ is a base for C/R and $q^2 - 2b_1 q + b = q^2 - 2b_1 q + (b_1^2 + b_2^2) = 0$. There exists a vector $\tilde{u} = u_1 + q u_2$, $u_i \in V$, such that $\tilde{Q}(\tilde{u}) = q$. Then $Q(u_1) + 2qQ(u_1, u_2) + q^2 Q(u_2) = q$. Since $(1, q)$ is a base for $C(x_1, \ldots, x_n)/R(x_1, \ldots, x_n)$ and $q^2 - 2b_1 q + b = 0$, this implies that $Q(u_1) = bQ(u_2)$. It follows that b is represented by Q. □

Tsen-Lang theorem

Here is the lovely Tsen-Lang theorem

Let K/F be a field extension of transcendence degree n. The theorem of Tsen-Lang (cf. [G, p. 22]) says that if F is an algebraically closed field then K is a C_n-*field*, i.e., any homogeneous polynomial of degree d over K with more than d^n variables has a non-trivial solution in K. This can be restated

Chevalley-Warning is that Finite fields are C_1.

Chevalley–Warning theorem

In number theory, the **Chevalley–Warning theorem** implies that certain polynomial equations in sufficiently many variables over a finite field have solutions. It was proved by Ewald Warning (1935) and a slightly weaker form of the theorem, known as **Chevalley's theorem**, was proved by Chevalley (1935). Chevalley's theorem implied Artin's and Dickson's conjecture that finite fields are quasi-algebraically closed fields (Artin 1982, page x).

Contents

Statement of the theorems

Let $\mathbb{F}$ be a finite field and $\{f_j\}_{j=1}^r \subseteq \mathbb{F}[X_1, \ldots, X_n]$ be a set of polynomials such that the number of variables satisfies

$$n > \sum_{j=1}^{r} d_j$$

where d_j is the total degree of f_j. The theorems are statements about the solutions of the following system of polynomial equations

$$f_j(x_1, \ldots, x_n) = 0 \quad \text{for } j = 1, \ldots, r.$$

- *Chevalley–Warning theorem* states that the number of common solutions $(a_1, \ldots, a_n) \in \mathbb{F}^n$ is divisible by the characteristic p of $\mathbb{F}$. Or in other words, the cardinality of the vanishing set of $\{f_j\}_{j=1}^r$ is 0 modulo p.
- *Chevalley's theorem* states that if the system has the trivial solution $(0, \ldots, 0) \in \mathbb{F}^n$, i.e. if the polynomials have no constant terms, then the system also has a non-trivial solution $(a_1, \ldots, a_n) \in \mathbb{F}^n \setminus \{(0, \ldots, 0)\}$.

Chevalley's theorem is an immediate consequence of the Chevalley–Warning theorem since p is at least 2.

Both theorems are best possible in the sense that, given any n, the list $f_j = x_j, j = 1, \ldots, n$ has total degree n and only the trivial solution. Alternatively, using just one polynomial, we can take f_1 to be the degree n polynomial given by the norm of $x_1a_1 + \ldots + x_na_n$ where the elements a form a basis of the finite field of order p^n.

Warning proved another theorem, known as Warning's second theorem, which states that if the system of polynomial equations has the trivial solution, then it has at least q^{n-d} solutions where q is the size of the finite field and $d := d_1 + \cdots + d_r$. Chevalley's theorem also follows directly from this.

Proof of Warning's theorem

Remark: If $i < q - 1$ then

$$\sum_{x \in \mathbb{F}} x^i = 0$$

so the sum over $\mathbb{F}^n$ of any polynomial in $x_1, \ldots, x_n$ of degree less than $n(q - 1)$ also vanishes.

The total number of common solutions modulo p of $f_1, \ldots, f_r = 0$ is equal to

$$\sum_{x \in \mathbb{F}^n} (1 - f_1^{q-1}(x)) \cdot \ldots \cdot (1 - f_r^{q-1}(x))$$

because each term is 1 for a solution and 0 otherwise. If the sum of the degrees of the polynomials f_i is less than n then this vanishes by the remark above.

Artin's conjecture

It is a consequence of Chevalley's theorem that finite fields are quasi-algebraically closed. This had been conjectured by Emil Artin in 1935. The motivation behind Artin's conjecture was his observation that quasi-algebraically closed fields have trivial Brauer group, together with the fact that finite fields have trivial Brauer group by Wedderburn's theorem.

The Ax–Katz theorem

The **Ax–Katz theorem**, named after James Ax and Nicholas Katz, determines more accurately a power q^b of the cardinality q of $\mathbb{F}$ dividing the number of solutions; here, if d is the largest of the d_j, then the exponent b can be taken as the ceiling function of

$$\frac{n - \sum_j d_j}{d}.$$

The Ax–Katz result has an interpretation in étale cohomology as a divisibility result for the (reciprocals of) the zeroes and poles of the local zeta-function. Namely, the same power of q divides each of these algebraic integers.

See also

- Combinatorial Nullstellensatz

References

- Artin, Emil (1982), Lang, Serge.; Tate, John (eds.), *Collected papers*, Berlin, New York: Springer-Verlag, ISBN 978-0-387-90686-7, MR 0671416 (https://www.ams.org/mathscinet-getitem?mr=0671416)
- Ax, James (1964), "Zeros of polynomials over finite fields", *American Journal of Mathematics*, **86**: 255–261, doi:10.2307/2373163 (https://doi.org/10.2307%2F2373163), MR 0160775 (https://www.ams.org/mathscinet-getitem?mr=0160775)
- Chevalley, Claude (1935), "Démonstration d'une hypothèse de M. Artin", *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg* (in French), **11**: 73–75, doi:10.1007/BF02940714 (https://doi.org/10.1007%2FBF02940714), JFM 61.1043.01 (https://zbmath.org/?format=complete&q=an:61.1043.01), Zbl 0011.14504 (https://zbmath.org/?format=complete&q=an:0011.14504)
- Katz, Nicholas M. (1971), "On a theorem of Ax", *Amer. J. Math.*, **93** (2): 485–499, doi:10.2307/2373389 (https://doi.org/10.2307%2F2373389)
- Warning, Ewald (1935), "Bemerkung zur vorstehenden Arbeit von Herrn Chevalley", *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg* (in German), **11**: 76–83, doi:10.1007/BF02940715 (https://doi.org/10.1007%2FBF02940715), JFM 61.1043.02 (https://zbmath.org/?format=complete&q=an:61.1043.02), Zbl 0011.14601 (https://zbmath.org/?format=complete&q=an:0011.14601)
- Serre, Jean-Pierre (1973), *A course in arithmetic* (https://archive.org/details/courseinarithmet00serr/page/5), pp. 5–6 (https://archive.org/details/courseinarithmet00serr/page/5), ISBN 0-387-90040-3

External links

- "Proof's of the Chevalley-Warning theorem" (https://mathoverflow.net/q/178318).

Outline of Artin's proof

- Suppose P is not a sum of squares of rational functions.
- Sums of squares form a proper cone of the field of rational functions, and does not contain P .
- Using Zorn, get a total order on the field of rational functions which does not contain P.
- Taking the real closure of the field of rational functions for this order, get a field in which P takes negative values (when evaluated at the variables, which are elements of the real closure).
- Then P takes negative values over the reals. First instance of a transfer principle in real algebraic geometry. Based on Sturm's theorem, or Hermite quadratic form.

• Our work '14: another constructive proof $\rightsquigarrow$ elementary recursive degree bound:

$$2^{2^{2^{d^{4^k}}}}.$$

Why a tower of five exponentials ?

- outcome of our method ... no other reason ...
- cylindrical decomposition gives univariate polynomials of doubly exponential degrees
- dealing with univariate polynomials of degree d (real root for odd degree, complex root by Laplace) already gives three level of exponentials
- we are lucky enough that all the other steps do not spoil this bound
- long paper (85 pages) ... currently under review.

What can be hoped for ? ?

- Nullstellensatz : single exponential (..., Kollar, Jelonek, ...).
- Nullstellensatz: single exponential lower bounds (...,Philippon , ...).
- Positivstellensatz: single exponential lower bounds [GV]. Grigoriev Vorobjov
- Best lower bound for Hilbert 17th problem : degree linear in k (recent result by [BGP]) ! Blekherman - Gouveia - Pfeiffer
- Deciding emptyness for the reals (critical point method : more sophisticated than cylindrical decomposition) : single exponential [BPR]. Basu - Pollack - Roy

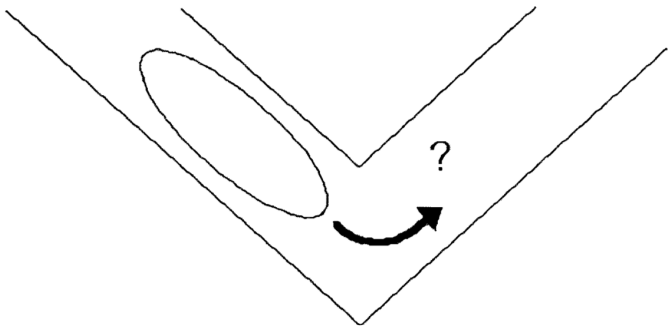
Applications:

① Triangulation of Real Algebraic Sets (and semialgebraic)

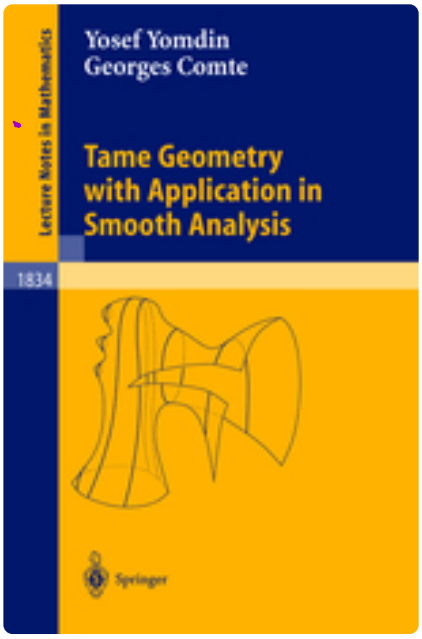
② Łojasiewicz inequality.

③ Piano Mover problem

(iii) Can an ellipse with semiaxes 1 and $\frac{1}{3}$ pass a right angle corner in a corridor with width 1 ?



④ A lot in Real Alg geo and Complexity see.



⑤ "Exotic spheres and bordism of anharmonic manifolds"
(S. Cappell, J. Davis, and SW)

Etc...

References:

① Bochnak, Coste, Roy

② Basu, Pollack, Roy,

③ Coste talk at UCLA

④ Jacobson Basic Algebra I, II

⑤ Milnor - Husemoller, Symm. Bilinear Forms

⑥ Cohen, CPAM

⑦ Seidenberg, Annals

[⑧ Tarski: Rand Corp paper

⑨ Marker, Model theory]