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 $T = (T_1, \dots, T_p)$ and X with coefficients in $\mathbb{R}$*

$$\mathcal{S}(T, X) \ : \ \begin{cases} S_1(T, X) \triangleright_1 0 \\ S_2(T, X) \triangleright_2 0 \\ \cdots \\ S_\ell(T, X) \triangleright_\ell 0 \end{cases}$$

(where the $\triangleright_i$ 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 $\Phi(X_1, \dots, X_n)$ is a first-order formula, the set of $(x_1, \dots, x_n) \in \mathbb{R}^n$ which satisfy $\Phi(x_1, \dots, x_n)$ is semialgebraic.*

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

$$\begin{tikzcd} \hat{\Sigma} \arrow[d] & \subset & \mathbb{R}^m \arrow[d, "\pi"] \\ \Sigma := \pi(\hat{\Sigma}) & \subset & \mathbb{R}^n \end{tikzcd}$$

semialg set

$p > q \quad \exists z, t \quad p - q = z^2$

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

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

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

$\iff fg = 0$

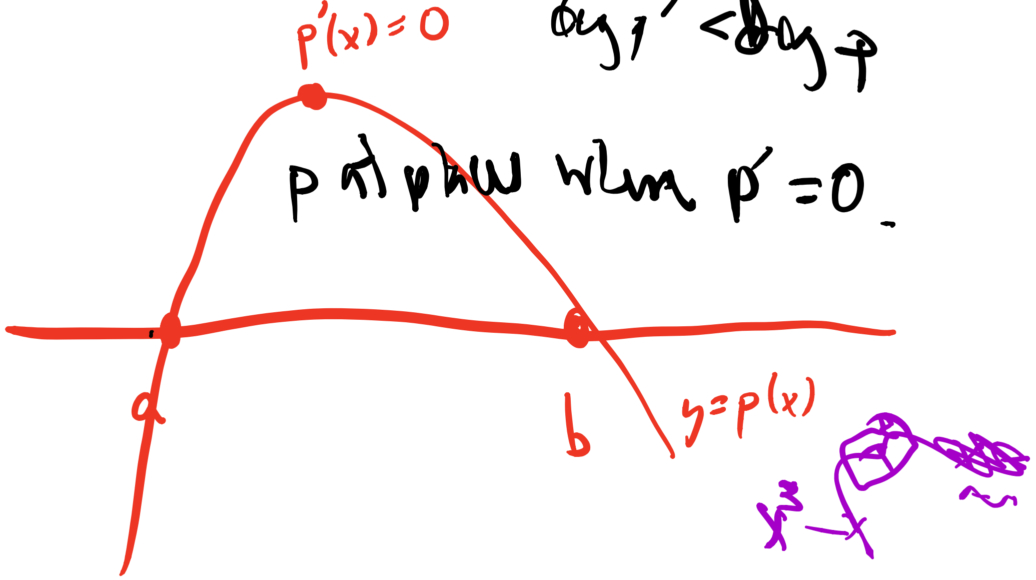
$f = 0 \wedge g = 0$

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

① Remember Rolle's theorem

$\deg p' < \deg p$

p attains max when $p' = 0$.



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)

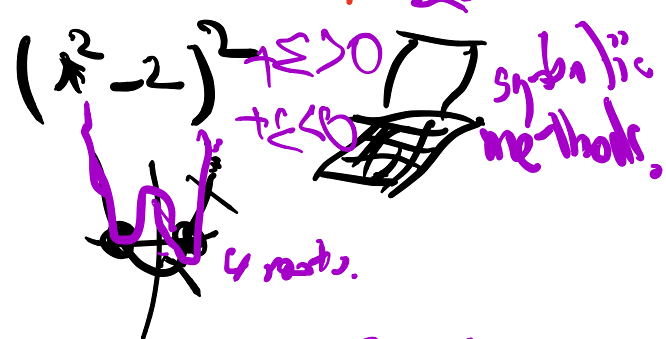
Exercise (Descartes): $\sum_{i=0} a_i x^i$ has at most the number of alternations of signs in the coefficients positive roots.

② Multiple roots are harder to see.

If p has a root, so does p^2

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

might not.



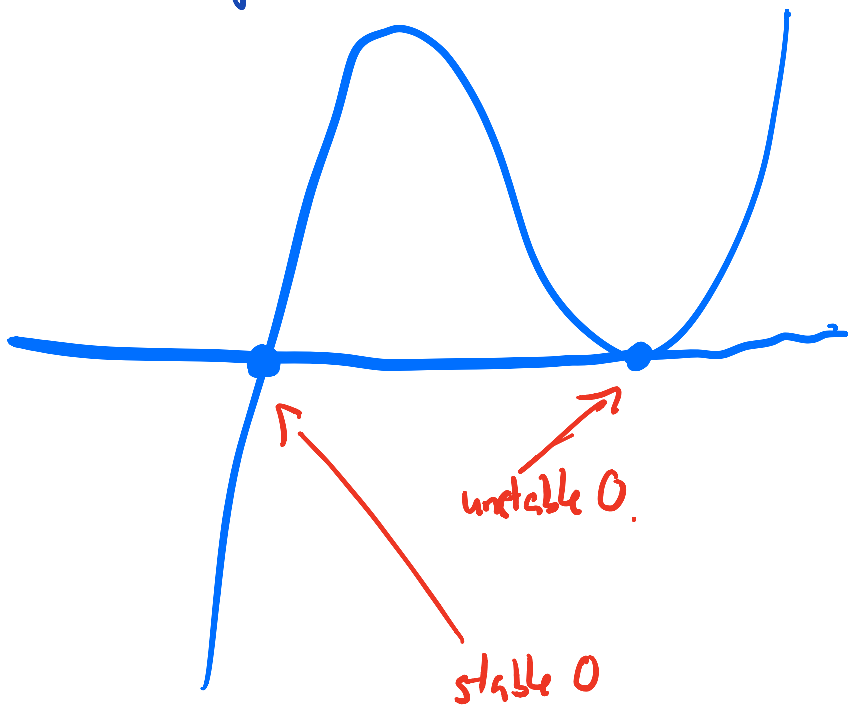
Remark: $\mathbb{R}$ differs from $\mathbb{C}$ in terms of instability of roots.

This is a serious "practical" problem.

Moduli? Coefficients.

$\boxed{\text{Up to equiv. the coeff. not as important as the degrees.}}$

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



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

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

for $x > 0$ <u>a.e.</u> 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

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

$\iff \exists a, b \in \mathbb{F}[x]$ $\iff \exists a, b$ of low degree with $af + bg = 0$.

$\exists (f, g)$ $\exists (\text{rand } f, g)$. $a\boxed{f_p} + b\,g_q$ gcd $= 1$

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

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

Make a matrix

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

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

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

Example

$$ax^2+bx+c$$

vs

$$dx+e$$

$$\begin{array}{c|ccc|} & a & b & c \\ 1 & 0 & d & e \\ x & d & e & 0 \end{array} = 0 \quad \text{iff } (dx+e) \mid ax^2+bx+c.$$

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

$$(x^2+1)^2$$

④ Sturm's theorem.

$GCD(p(x), p'(x)) = \prod_{p} (x-p)^{d-1}$

In case $f(x)$ [$p(x) \Rightarrow$] has no multiple roots.

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

INFORMALLY look for whether

$f(p_1')f(p_2') < 0$ or not.

But then you'd need to find the

$p_1' < p < p_2'$ where $f(p) = 0$.

to continue to do the next degree.

This can be done algorithmically.

(elegantly?)

STURM'S THEOREM

Better approach:

Start $(P_1, P', P_3 = aP' - P, P_4 \text{ etc})$

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

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

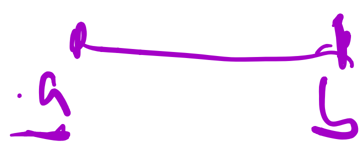
$a<b$; # of roots in $[a,b]$ is $v(a)-v(b)$.

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

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

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

$P_4 = 1.$

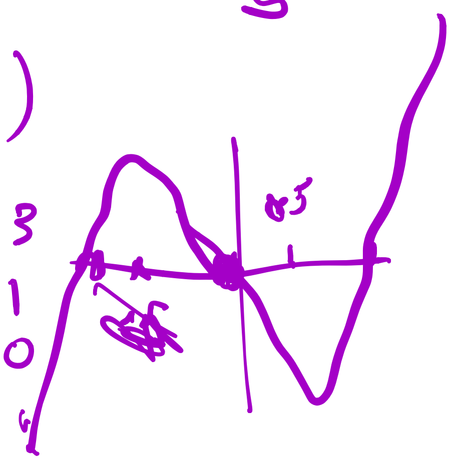


gives $\left(x^3 - x,\ 3x^2 - 1,\ \frac{4}{3}x,\ 1\right)$

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

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

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

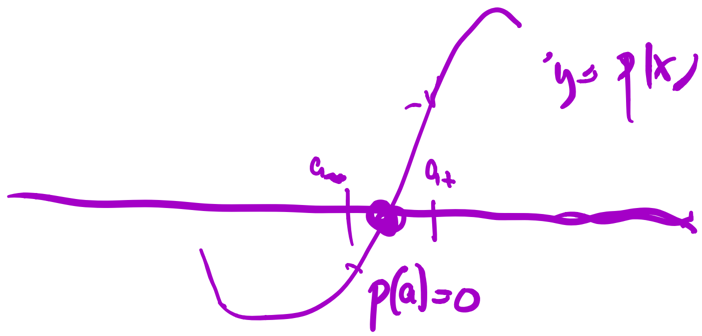


Idea of proof: look at what happens to this as you pass a root of $p(x)$ if all zeroes are simple.

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

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

Quad. ≥ 0



Going thru a root of p

sequence of signs of

	$p(a_-)$		$p(a_+)$
p	$-$	0	$+$
p_1	$+$	$+$	$+$
p_2			
p_3	$+$	0	$-$
$\vdots$	$-$	$-$	$-$

1 fewer alternation

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

Change through a root of p_i

$p_{i-1}(a_-)$ $\quad$ $p_{i-1}(a)$ $\quad$ $p_{i-1}(a_+)$

$p_i(a_-)$ $\quad$ 0 $\quad$ $p_i(a_+)$ $\quad$ opposite signs

$p_{i+1}(a_-)$ $\quad$ $p_{i+1}(a)$ $\quad$ $p_{i+1}(a_+)$

$-\text{sign } p_{i+1}(a)$.

$p_{i-1} = q\, p_i - p_{i+1}$

# of sign change, i.e., unchanged

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 -

$$P_1 \quad \underset{q}{P_2} \quad P_3 \cdots P_r = GCD(P_1, P_2).$$

$\frac{P}{GCD(P,P')} = q$

has the same # of alternations of signs as

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

when evaluating at any a not a root of P.

$\therefore$ Sturm works even if P has multiple roots.

SYLVESTER'S THEOREM

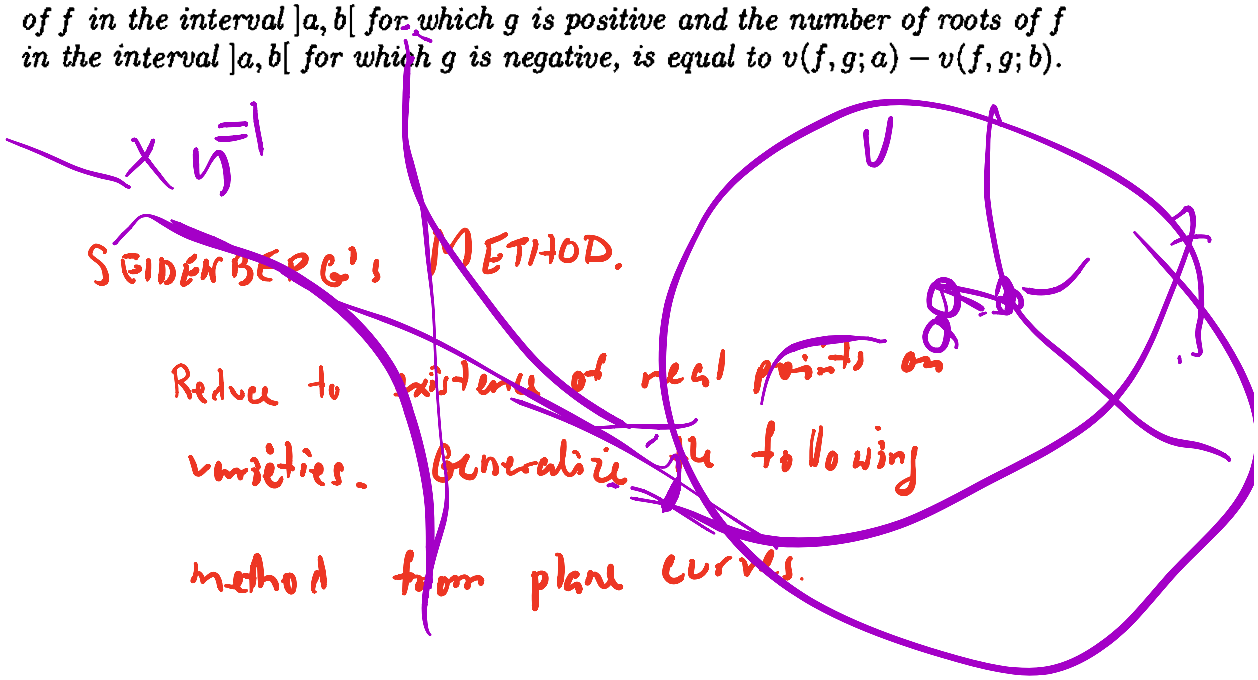
Definition 1.2.8. *Let R be a real closed field, and let f and g be in $R[X]$. The* Sturm sequence *of f and g is the sequence of polynomials $(f_0, \ldots, f_k)$ defined as follows:*

$$f_0 = f\,, \quad f_1 = f'g\,,$$

$$f_i = f_{i-1}q_i - f_{i-2} \text{ with } q_i \in R[X] \text{ and } \deg(f_i) < \deg(f_{i-1}) \text{ for } i = 2, \ldots, k\,,$$

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.

$(0,0)$

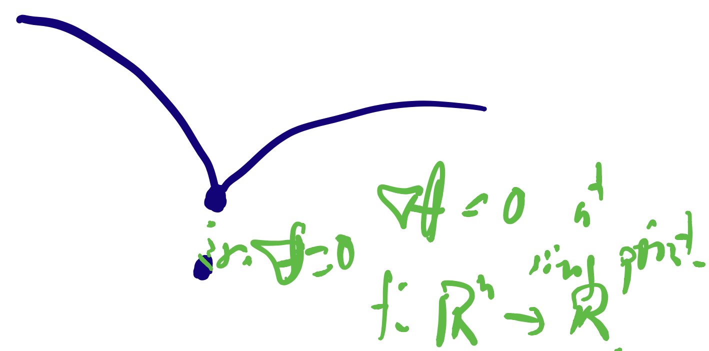
$f = 0$

$$\boxed{(f_x, f_y)\cdot(-x, y) = 0}$$

Use a resultant to get a 1 variable equation for x solve with Sturm.

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.