Modélisation et résolutions numérique et symbolique

via les logiciels MAPLE et MATLAB (MODEL)

Jérémy Berthomieu Mohab Safey El Din Stef Graillat

jeremy.berthomieu@lip6.fr

Reminder

Previously

1. Lagrange interpolation is a special case of CRT in $\mathbb{K}[X]$.

$$\begin{cases} P(x_0) = a_0 \\ \quad \vdots \\ P(x_d) = a_d \end{cases} \iff \begin{cases} P = a_0 \bmod (X - x_0) \\ \quad \vdots \\ P = a_d \bmod (X - x_d). \end{cases}$$

   $\rightarrow$ Complexity in $O(d^2)$.

2. Computation of the characteristic polynomial of a $d \times d$ matrix A by Lagrange interpolation.
   $\rightarrow$ Computation of $d + 1$ determinants $A - \lambda_i \mathrm{Id}$.
   $\rightarrow$ Complexity in $O(d^4)$.

Roadmap

1. Sylvester matrix
2. Eulide algorithm: from the linear algebra point of view
3. Sturm problem: the number of real roots
4. Bivariate polynomial system solving

Sylvester Matrix

Definition

Let P and Q be two polynomials of $\mathbb{K}[X]$ of degree m and n.

$$P = p_m X^m + \cdots + p_0$$
$$Q = q_n X^n + \cdots + q_0.$$

The Sylvester matrix associated to P and Q is the $(m+n)$ matrix

$$S_{P,Q} = \begin{pmatrix}
p_m & 0 & \cdots & 0 & q_n & 0 & \cdots & 0 \\
 & & & \vdots & & & & \vdots \\
p_{m-1} & p_m & & \vdots & q_{n-1} & q_n & & \vdots \\
\vdots & & \ddots & \vdots & \vdots & & \ddots & \vdots \\
 & p_{m-1} & \ddots & \vdots & \vdots & q_{n-1} & \ddots & \\
 & \vdots & & & & \vdots & & \\
p_1 & \vdots & & 0 & q_1 & \vdots & & 0 \\
p_0 & p_1 & & p_m & q_0 & q_1 & & q_m \\
0 & p_0 & & p_{m-1} & 0 & q_0 & & q_{m-1} \\
\vdots & & & \vdots & \vdots & & & \vdots \\
\vdots & 0 & & \vdots & \vdots & 0 & & \vdots \\
\vdots & \vdots & \ddots & & \vdots & \vdots & \ddots & \\
\vdots & \vdots & \ddots & p_1 & \vdots & \vdots & \ddots & q_1 \\
0 & 0 & \cdots & p_0 & 0 & 0 & \cdots & q_0
\end{pmatrix}.$$

Sylvester Matrix

Example

If $P = x^2 + 2x + 3$ and $Q = 9x^5 + 8x^4 + 7x^3 + 6x^2 + 5x + 4$, then their Sylvester is

$$S_{P,Q} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 9 & 0 \\ 2 & 1 & 0 & 0 & 0 & 8 & 9 \\ 3 & 2 & 1 & 0 & 0 & 7 & 8 \\ 0 & 3 & 2 & 1 & 0 & 6 & 7 \\ 0 & 0 & 3 & 2 & 1 & 5 & 6 \\ 0 & 0 & 0 & 3 & 2 & 4 & 5 \\ 0 & 0 & 0 & 0 & 3 & 0 & 4 \end{pmatrix}.$$

Bézout's problem

Problem

Given $P, Q \in \mathbb{K}[X]$, is there any $A, B \in \mathbb{K}[X]$ such that $\deg A < \deg Q = n$, $\deg B < \deg P = m$ and $AP + BQ = 0$?

Answer

Let A, B be as above, then $AP + BQ = 0$ if, and only if,

$$\begin{pmatrix}
p_m & 0 & \cdots & 0 & q_n & 0 & \cdots & 0 \\
 & & & \vdots & & & & \vdots \\
p_{m-1} & p_m & & \vdots & q_{n-1} & q_n & & \vdots \\
\vdots & & \ddots & \vdots & \vdots & & \ddots & \vdots \\
 & p_{m-1} & \ddots & \vdots & & q_{n-1} & \ddots & \\
 & \vdots & & & & \vdots & & \\
p_1 & \vdots & & 0 & q_1 & \vdots & & 0 \\
p_0 & p_1 & & p_m & q_0 & q_1 & & q_m \\
0 & p_0 & & p_{m-1} & 0 & q_0 & & q_{m-1} \\
\vdots & & & \vdots & \vdots & & & \vdots \\
\vdots & 0 & & \vdots & \vdots & 0 & & \vdots \\
\vdots & \vdots & \ddots & & \vdots & \vdots & \ddots & \\
\vdots & \vdots & \ddots & p_1 & \vdots & \vdots & \ddots & q_1 \\
0 & 0 & \cdots & p_0 & 0 & 0 & \cdots & q_0
\end{pmatrix}
\begin{pmatrix}
a_{n-1} \\
\vdots \\
a_0 \\
b_{m-1} \\
\vdots \\
b_0
\end{pmatrix} = 0.$$

Bézout's problem

Theorem

The kernel of $S_{P,Q}$ gives all the solutions of $AP + BQ = 0$ with $\deg P < n$, $\deg Q < m$.

Proposition

P and Q are coprime, if, and only if, $\det S_{P,Q} \neq 0$.

Proof

If P and Q are coprime, then from $AP + BQ = 0 \iff AP = -BQ$, one deduces that $Q|A$ and $P|B$. But $\deg A < \deg Q$ and $\deg B < \deg P$, so that $A = B = 0$ and $\det S_{P,Q} \neq 0$.
If they are not coprime, $A = Q/\gcd(P, Q)$ and $B = -P/\gcd(P, Q)$ are nontrivial solutions of the problem, so that $\det S_{P,Q} = 0$.

Resultant and discriminant

Definition

The resultant of two polynomials in $\mathbb{K}[X]$ is the determinant of their Sylvester matrix.
It is 0 if, and only if, they have a common root.

Definition

The discriminant of a polynomial is the resultant of this polynomial and its derivative.
It is 0 if, and only if, the polynomial has a multiple root.

Complexity

The resultant of P and Q can be computed in $O\left((m+n)^3\right) = O\left(\max(m,n)^3\right)$.
The discriminant of P can be computed in $O\left(m^3\right)$.

Resultant

Example

1. If $P = X^2 + 2X + 3$ and $Q = 9X^5 + 8X^4 + 7X^3 + 6X^2 + 5X + 4$, then their resultant is

$$\begin{vmatrix} 1 & 0 & 0 & 0 & 0 & 9 & 0 \\ 2 & 1 & 0 & 0 & 0 & 8 & 9 \\ 3 & 2 & 1 & 0 & 0 & 7 & 8 \\ 0 & 3 & 2 & 1 & 0 & 6 & 7 \\ 0 & 0 & 3 & 2 & 1 & 5 & 6 \\ 0 & 0 & 0 & 3 & 2 & 4 & 5 \\ 0 & 0 & 0 & 0 & 3 & 0 & 4 \end{vmatrix} = 10347.$$

2. If $P = 2X^2 - 2$ and $Q = X + 1$, then their resultant is

$$\begin{vmatrix} 2 & 1 & 0 \\ 0 & 1 & 1 \\ -2 & 0 & 1 \end{vmatrix} = 0.$$

Discriminant

Example

If $P = X^3 + 2X^2 + X$, then $P' = 3X^2 + 4X + 1$ and its discriminant is

$$\begin{vmatrix} 1 & 0 & 3 & 0 & 0 \\ 2 & 1 & 4 & 3 & 0 \\ 1 & 2 & 1 & 4 & 3 \\ 0 & 1 & 0 & 1 & 4 \\ 0 & 0 & 0 & 0 & 1 \end{vmatrix} = 0.$$

Discriminant

Example

If $P = X^3 + 2X^2 + X$, then $P' = 3X^2 + 4X + 1$ and its discriminant is

$$\begin{vmatrix} 1 & 0 & 3 & 0 & 0 \\ 2 & 1 & 4 & 3 & 0 \\ 1 & 2 & 1 & 4 & 3 \\ 0 & 1 & 0 & 1 & 4 \\ 0 & 0 & 0 & 0 & 1 \end{vmatrix} = 0.$$

Indeed, -1 is a double root of P and so, is a root of P'.

Sylvester matrix

Proposition

The rank of $S_{P,Q}$ is $m + n - \deg \gcd(P, Q)$.

Proof

By induction, it is clear that $\dim \ker S_{P,Q} \leq \deg \gcd(P, Q)$.
Let $A_0 = Q / \gcd(P, Q)$ and $B_0 = -P / \gcd(P, Q)$. Pairs $A_i = x^i A_0$, $B_i = x^i B_0$ with $i \in \{0, \ldots, \deg \gcd(P, Q)\}$ are solutions of Bézout's problem and they are all linearly independant. Therefore $\dim \ker S_{P,Q} \geq \deg \gcd(P, Q)$.

Euclidean Algorithm

Theorem

Let $S_{P,Q}$ be the Sylvester matrix of P and Q. Let $S'_{P,Q}$ be the matrix obtained from a triangularization of $S^T_{P,Q}$. Then, the polynomial corresponding to the nonzero row of lowest degree in $S'_{P,Q}$ is $\gcd(P, Q)$.

Corollary

The gcd of P and Q can be computed in $O((m+n)^3) = O(\max(m, n)^3)$.

Euclidean Algorithm

Example

If $P = X^3 + 1$ and $Q = X^2 - 1$, then their Sylvester matrix is

$$\begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & -1 & 0 & 1 \\ 1 & 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 & -1 \end{pmatrix}$$

After transposition and Gaussian elimination, one has

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & -1 & 0 & 0 \\ 0 & 1 & 0 & -1 & 0 \\ 0 & 0 & 1 & 0 & -1 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & -1 & -1 & 0 \\ 0 & 1 & 0 & -1 & 0 \\ 0 & 0 & 1 & 0 & -1 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & -1 & -1 & 0 \\ 0 & 0 & 0 & -1 & -1 \\ 0 & 0 & 1 & 0 & -1 \end{pmatrix}$$

$$\to \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & -1 & -1 & 0 \\ 0 & 0 & 0 & -1 & -1 \\ 0 & 0 & 0 & -1 & -1 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & -1 & -1 & 0 \\ 0 & 0 & 0 & -1 & -1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & -1 & -1 & 0 \\ 0 & 0 & 0 & -1 & -1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

A gcd of P and Q is $-X - 1$, and thus $X + 1$.

Extended Euclidean Algorithm

Reminder

Let $P, Q \in \mathbb{K}[X]$ and let $G \in \mathbb{K}[X]$ be their gcd. Then, there exist $U, V \in \mathbb{K}[X]$ such that $\deg U < \deg Q = n$, $\deg V < \deg P = m$ and

$$PU + QV = G.$$

Theorem

Let $S_{P,Q}$ be the Sylvester matrix of P and Q. One can determine U and V by solving the following linear system:

$$S_{P,Q} \begin{pmatrix} u_{n-1} \\ \vdots \\ u_0 \\ v_{m-1} \\ \vdots \\ v_0 \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ g_\ell \\ \vdots \\ g_0 \end{pmatrix}, \quad \text{where } \ell = \deg G.$$

Extended Euclidean Algorithm

Example

If $P = X^3 + 1$ and $Q = X^2 - 1$, then their gcd is $X + 1$ and their Sylvester matrix is

$$\begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & -1 & 0 & 1 \\ 1 & 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 & -1 \end{pmatrix}$$

Solving

$$\begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & -1 & 0 & 1 \\ 1 & 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 & -1 \end{pmatrix} \begin{pmatrix} u_1 \\ u_0 \\ v_2 \\ v_1 \\ v_0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}$$

yields $U = -kX + k + 1$ and $V = kX^2 - (k+1)X + k$.

Number of roots of a complex polynomial

D'Alembert – Gauss' Theorem

Let $P \in \mathbb{C}[X]$ be a nonzero polynomial of degree n. Then, P has exactly n roots in $\mathbb{C}$ counted with multiplicities.

Proof sketch

If $\deg P = 0$, it is trivial. Otherwise, by induction, it suffices to prove that P has at least one root.

Number of roots of a complex polynomial

Examples

1. $P = X^2 + 1$ has two distinct roots in $\mathbb{C}$ i and $-i$.
2. $P = X^3(X^2 - 2iX - 1)$ has two roots 0 and i but 0 must be counted thrice and i must be counted twice. Therefore, it has five roots in $\mathbb{C}$.
3. $P = 3$ has no roots in $\mathbb{C}$.

Problem

D'Alembert – Gauss' theorem is only true because $\mathbb{C}$ is algebraically closed.

Number of roots of a real polynomial

Question

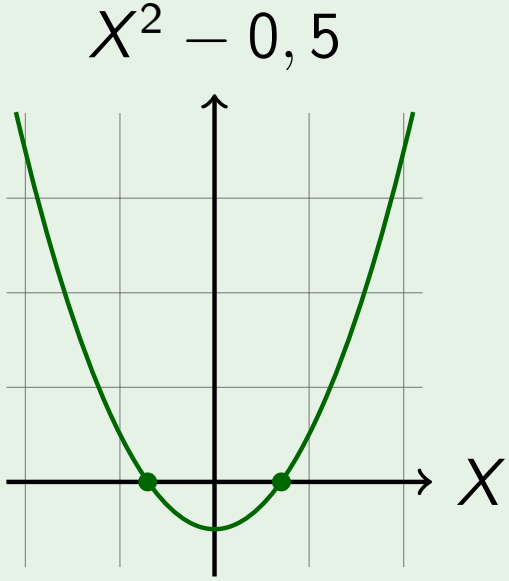
Let $P \in \mathbb{R}[X]$ be a nonzero polynomial of degree n. How many roots of P are in $\mathbb{R}$?

Answer

If $n = 0$ or $n = 1$, trivially P has n roots. Otherwise...

Number of roots of a real polynomial

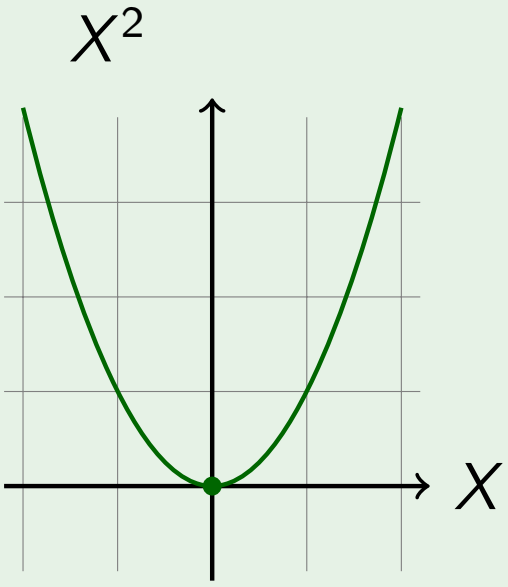
Example



2 simple roots.

Number of roots of a real polynomial

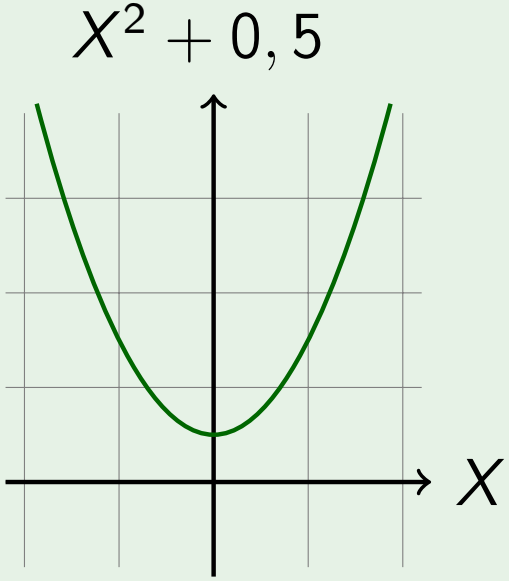
Example



1 double root.

Number of roots of a real polynomial

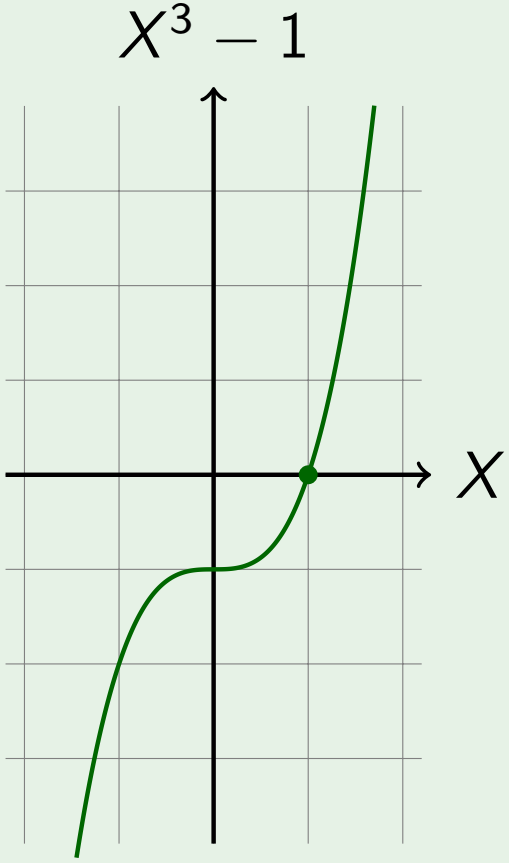
Example



0 roots.

Number of roots of a real polynomial

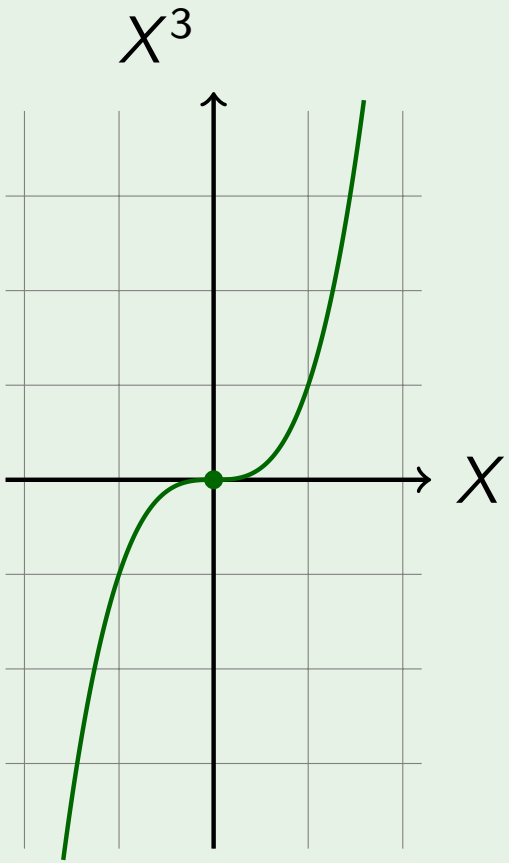
Example



1 simple root.

Number of roots of a real polynomial

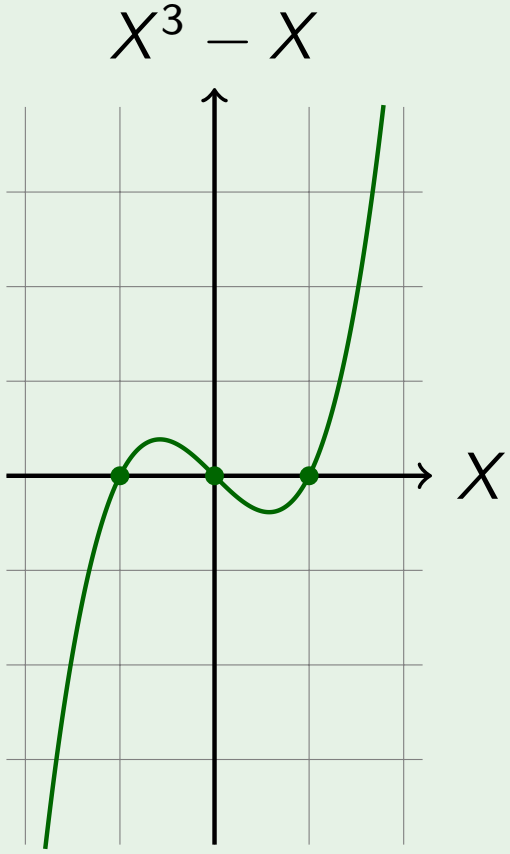
Example



1 triple root.

Number of roots of a real polynomial

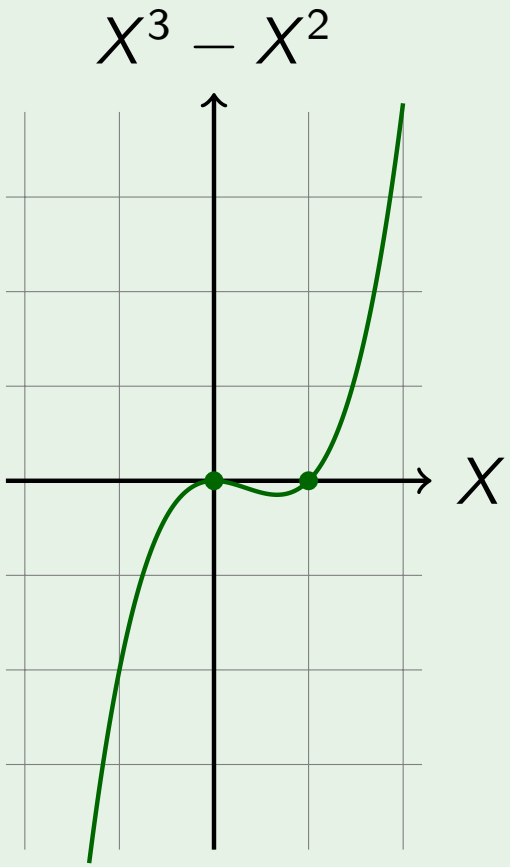
Example



3 simple roots.

Number of roots of a real polynomial

Example



1 double root and 1 simple root.

Number of roots of a real polynomial

Proposition

1. Let $P \in \mathbb{R}[X]$ be a nonzero polynomial of degree n. If $z \in \mathbb{C}$ is a root of P, then so is $\overline{z}$.
2. The number of roots of P in $\mathbb{C} \setminus \mathbb{R}$ is even.
   Therefore $n = r + 2s$, where r is the number of roots of P in $\mathbb{R}$, and s is the number of roots of P in $\mathbb{C}$.

Proof

$$\overline{P(z)} = \overline{p_n z^n + \cdots + p_0} = p_n \overline{z}^n + \cdots + p_0 = 0.$$

Squarefree polynomial

Definition

A polynomial P is squarefree if $\gcd(P, P') = 1$. That is, P has no multiple roots.

Example

1. $P = X^2 - 2$ is squarefree ;
2. $Q = (X - 1)^2$ is not squarefree ;
3. $R = X^3 - X^2 = X^2(X - 1)$ is not squarefree.

Squarefree polynomial

Theorem

Let P be a polynomial such that $P = P_1^{r_1} \cdots P_n^{r_n}$, $\gcd(P_i, P_j) = 1$ if $i \neq j$. Then, $Q = P_1 \cdots P_n$ is squarefree and

$$Q = \frac{P}{\gcd(P, P')}.$$

Squarefree polynomial

Theorem

Let P be a polynomial such that $P = P_1^{r_1} \cdots P_n^{r_n}$, $\gcd(P_i, P_j) = 1$ if $i \neq j$. Then, $Q = P_1 \cdots P_n$ is squarefree and

$$Q = \frac{P}{\gcd(P, P')}.$$

Proof

Assuming $r_i \geq 1$ for all i, $P' = P_1^{r_1 - 1} \cdots P_n^{r_n - 1} R$, with $\gcd(R, P_i) = 1$ for all i. Then, $\gcd(P, P') = P_1^{r_1 - 1} \cdots P_n^{r_n - 1}$ and

$$Q = \frac{P}{\gcd(P, P')} = P_1 \cdots P_n.$$

Sturm's theorem

Sturm's theorem

Let $P \in \mathbb{R}[X]$ be a nonzero squarefree polynomial of degree n. Let $a, b \in \mathbb{R}$, $a < b$. One can determine how many roots of P are in $]a, b[$.

Algorithm

Sturm's sequence is

$$\begin{aligned} P_0 &= P \\ P_1 &= P' \\ P_2 &= -\operatorname{rem}(P_0, P_1) \\ P_3 &= -\operatorname{rem}(P_1, P_2) \\ &\vdots \\ 0 &= -\operatorname{rem}(P_{m-1}, P_m). \end{aligned}$$

Sturm's theorem

Sturm's theorem

Let $P = P_0, P' = P_1, P_2, \ldots, P_m$ be a Sturm's sequence. Let $\sigma(x)$ be the number of sign changes in the sequence $P_0(x), \ldots, P_m(x)$. The number of roots of P in $]a, b[$ is

$$\sigma(a) - \sigma(b).$$

The number of roots of P in $\mathbb{R}$ is

$$\sigma(-\infty) - \sigma(+\infty),$$

where $P_i(\pm\infty) = \lim_{x \to \pm\infty} P(x)$.

Proof

Skipped.

Sturm's theorem: complexity

Proposition

The STURM's sequence can be computed by twisting the Euclidean algorithm applied to P and P'.
Then, one has to evaluate all the polynomials in a and b.

Sturm's theorem: complexity

Proposition

The Sturm's sequence can be computed by twisting the Euclidean algorithm applied to P and P'.
Then, one has to evaluate all the polynomials in a and b.

Complexity

Assuming P has degree d.
The computation of Sturm's sequance can be computed in $O(d^2)$.
The sequences $P_0(-\infty), \ldots, P_m(-\infty)$ and $P_0(+\infty), \ldots, P_m(+\infty)$ can be easily determined by looking at the signs and the degrees of the leading terms of the P_i.
Therefore, the number of real roots of P can be computed in $O(d^2)$.

Sturm's theorem

Example

1. $P = P_0 = X^4 + 1$.

Sturm's theorem

Example

1. $P = P_0 = X^4 + 1$, $P' = P_1 = 4X^3$, $P_2 = -1$.

Sturm's theorem

Example

1. $P = P_0 = X^4 + 1$, $P' = P_1 = 4X^3$, $P_2 = -1$.
2. $P_0(-5) = 626$, $P_1(-5) = -500$, $P_2(-5) = -1$, so $\sigma(-5) = 1$.

Sturm's theorem

Example

1. $P = P_0 = X^4 + 1$, $P' = P_1 = 4X^3$, $P_2 = -1$.
2. $P_0(-5) = 626$, $P_1(-5) = -500$, $P_2(-5) = -1$, so $\sigma(-5) = 1$.
3. $P_0(5) = 626$, $P_1(5) = 500$, $P_2(5) = -1$, so $\sigma(5) = 1$.

Sturm's theorem

Example

1. $P = P_0 = X^4 + 1$, $P' = P_1 = 4X^3$, $P_2 = -1$.
2. $P_0(-5) = 626$, $P_1(-5) = -500$, $P_2(-5) = -1$, so $\sigma(-5) = 1$.
3. $P_0(5) = 626$, $P_1(5) = 500$, $P_2(5) = -1$, so $\sigma(5) = 1$.
4. So P has $\sigma(-5) - \sigma(5) = 1 - 1 = 0$ roots in $]-5, 5[$.

Sturm's theorem

Example

1. $P = P_0 = X^3 - X$.

Sturm's theorem

Example

1. $P = P_0 = X^3 - X$, $P' = P_1 = 3X^2 - 1$, $P_2 = \frac{2}{3}X$, $P_3 = 1$.

Sturm's theorem

Example

1. $P = P_0 = X^3 - X$, $P' = P_1 = 3X^2 - 1$, $P_2 = \frac{2}{3}X$, $P_3 = 1$.
2. $P_0(-2) = -6$, $P_1(-2) = 11$, $P_2(-2) = -\frac{4}{3}$, $P_3(-2) = 1$, so $\sigma(-2) = 3$.

Sturm's theorem

Example

1. $P = P_0 = X^3 - X$, $P' = P_1 = 3X^2 - 1$, $P_2 = \frac{2}{3}X$, $P_3 = 1$.
2. $P_0(-2) = -6$, $P_1(-2) = 11$, $P_2(-2) = -\frac{4}{3}$, $P_3(-2) = 1$, so $\sigma(-2) = 3$.
3. $P_0(2) = 6$, $P_1(2) = 11$, $P_2(2) = \frac{4}{3}$, $P_3(2) = 1$, so $\sigma(2) = 0$.

Sturm's theorem

Example

1. $P = P_0 = X^3 - X$, $P' = P_1 = 3X^2 - 1$, $P_2 = \frac{2}{3}X$, $P_3 = 1$.
2. $P_0(-2) = -6$, $P_1(-2) = 11$, $P_2(-2) = -\frac{4}{3}$, $P_3(-2) = 1$, so $\sigma(-2) = 3$.
3. $P_0(2) = 6$, $P_1(2) = 11$, $P_2(2) = \frac{4}{3}$, $P_3(2) = 1$, so $\sigma(2) = 0$.
4. So P has $\sigma(-2) - \sigma(2) = 3 - 0 = 3$ roots in $]-2, 2[$.

Sturm's theorem

Example

1. $P = P_0 = X^3 - X$, $P' = P_1 = 3X^2 - 1$, $P_2 = \frac{2}{3}X$, $P_3 = 1$.
2. $P_0\left(\frac{1}{2}\right) = -\frac{3}{8}$, $P_1\left(\frac{1}{2}\right) = -\frac{1}{4}$, $P_2\left(\frac{1}{2}\right) = \frac{1}{3}$, $P_3\left(\frac{1}{2}\right) = 1$, so $\sigma\left(\frac{1}{2}\right) = 1$.
3. $P_0(2) = 6$, $P_1(2) = 11$, $P_2(2) = \frac{4}{3}$, $P_3(2) = 1$, so $\sigma(2) = 0$.
4. So P has $\sigma\left(\frac{1}{2}\right) - \sigma(2) = 1 - 0 = 1$ root in $\left]\frac{1}{2}, 2\right[$.

Sturm's theorem

Example

1. $P = P_0 = X^4 - X$, $P' = P_1 = 4X^3 - 1$, $P_2 = \frac{3}{4}X$, $P_3 = 1$.
2. $P_0(-\infty) = +\infty$, $P_1(-\infty) = -\infty$, $P_2(-\infty) = -\infty$, $P_3(-\infty) = 1$, so $\sigma(-\infty) = 2$.
3. $P_0(+\infty) = +\infty$, $P_1(+\infty) = +\infty$, $P_2(+\infty) = +\infty$, $P_3(+\infty) = 1$, so $\sigma(+\infty) = 0$.
4. So P has $\sigma(-\infty) - \sigma(+\infty) = 2 - 0 = 2$ roots in $\mathbb{R}$.

Bivariate polynomial system solving

Problem

How to solve a polynomial system

$$(S) = \begin{cases} P(X, Y) = 0 \\ Q(X, Y) = 0? \end{cases}$$

Answer

Let P, Q be in $\mathbb{K}[X, Y]$.
Let (S_X) be the same system as (S), where P, Q are seen in $\mathbb{K}(X)[Y]$.
(S_X) has a solution if, and only if, the resultant of P and Q, which is a polynomial in X, is 0. The roots of this resultant are x_0 candidates. Then, from the x_0 candidates, one can see if there are some y such that (x_0, y) is a solution of (S).

Bivariate polynomial system solving

Example

$$(S) = \begin{cases} P(X,Y) = X^2 + Y^2 - 1 = 0 \\ Q(X,Y) = X \ + Y \ - 1 = 0. \end{cases}$$

The resultant of P and Q seen as polynomials in Y is

$$\begin{vmatrix} 1 & 1 & 0 \\ 0 & X-1 & 1 \\ X^2-1 & 0 & X-1 \end{vmatrix} = (X-1)^2 + (X^2-1) = 2X(X-1).$$

$x = 0$ and $x = 1$ are candidates, they yield both systems

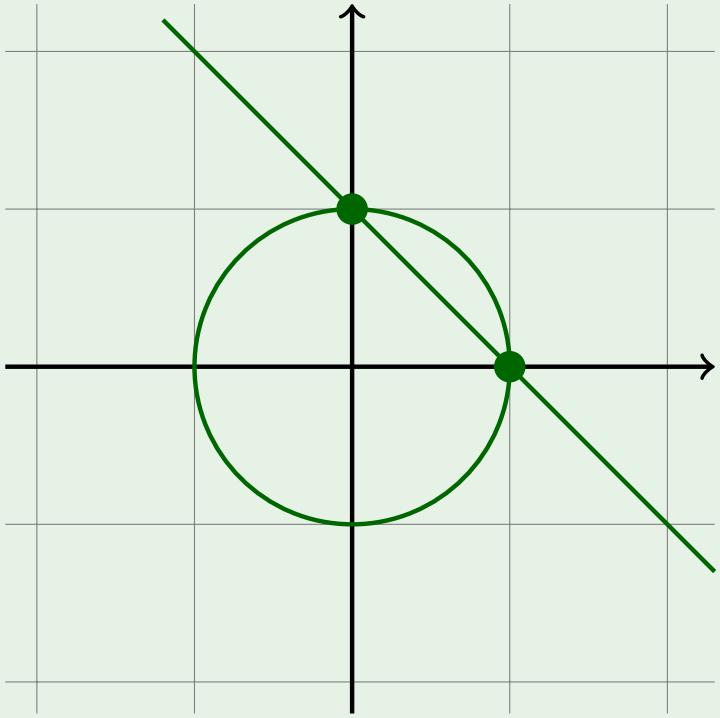
$$(S_0) = \begin{cases} Y^2 - 1 = 0 \\ Y \ - 1 = 0 \end{cases} \Leftrightarrow y = 1, \quad (S_1) = \begin{cases} Y^2 = 0 \\ Y \ = 0 \end{cases} \Leftrightarrow y = 0.$$

The solutions are $(0,1)$ and $(1,0)$.

Bivariate polynomial system solving

Example

$$(S) = \begin{cases} P(X,Y) = X^2 + Y^2 - 1 = 0 \\ Q(X,Y) = X \ + Y \ - 1 = 0. \end{cases}$$



Bivariate polynomial system solving

Example

$$(S) = \begin{cases} P(X,Y) = X^2 + Y^2 - 1 & = 0 \\ Q(X,Y) = X^2 + Y^2 + 4Y + 3 = 0. \end{cases}$$

The resultant of P and Q seen as polynomials in Y is

$$\begin{vmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 4 & 1 \\ X^2-1 & 0 & X^2+3 & 2 \\ 0 & X^2-1 & 0 & X^2+3 \end{vmatrix} = 16X^2.$$

$x = 0$ is the only candidate, it yields system

$$(S_0) = \begin{cases} Y^2 - 1 & = 0 \\ Y^2 + 4Y + 3 = 0 \end{cases} \quad \Leftrightarrow y = -1.$$

The solution is $(0, -1)$.

Bivariate polynomial system solving

Example

$$(S) = \begin{cases} P(X,Y) = X^2 + Y^2 - 1 & = 0 \\ Q(X,Y) = X^2 + Y^2 + 4Y + 3 = 0. \end{cases}$$