Gcd and Resultant

Alin Bostan

Specfun, Inria

MPRI C-2-22

October 12, 2020

GCD and Extended GCD

GCD

If $A, B \in \mathbb{K}[x]$, then $G \in \mathbb{K}[x]$ is a gcd of A and B if

- G divides both A and B,
- any common divisor of A and B divides G.

▷ It is a generator of the ideal of $K[x]$ generated by A and B, i.e.,

$$\left\{ U \cdot A + V \cdot B \;\middle|\; U, V \in \mathbb{K}[x] \right\} = \left\{ W \cdot G \;\middle|\; W \in \mathbb{K}[x] \right\}$$

▷ It is unique up to a constant: the gcd, after normalization (G monic)

▷ It is useful for:

- normalization (simplification) of rational functions
- squarefree factorization of univariate polynomials

▷ Computation: Euclidean algorithm

Euclidean algorithm

Euclid(A, B)

Input A and B in $\mathbb{K}[x]$.

Output A gcd G of A and B.

1. $R_0 := A$; $R_1 := B$; $i := 1$.
2. While R_i is non-zero, do:

   $R_{i+1} := R_{i-1} \bmod R_i$

   $i := i + 1$.
3. Return R_{i-1}.

▷ Correctness: $\gcd(F, G) = \gcd(G, F \bmod G)$

▷ Termination: $\deg(B) > \deg(R_2) > \deg(R_1) > \cdots$

▷ Quadratic complexity: $O\big(\deg(A)\deg(B)\big)$ operations in $\mathbb{K}$

Extended GCD

If $A, B \in \mathbb{K}[x]$, then $G = \gcd(A, B)$ satisfies (Bézout relation)

$$G = U \cdot A + V \cdot B, \quad \text{with } U, V \in \mathbb{K}[x]$$

▷ The co-factors U and V are unique if one further asks

$$\deg(U) < \deg(B) - \deg(G) \quad \text{and} \quad \deg(V) < \deg(A) - \deg(G)$$

Then one calls (G, U, V) is the extended gcd of A and B.

▷ Example: for $A = a + bx$ with $a \neq 0$ and $B = 1 + x^2$,

$$G = 1 \quad \text{and} \quad \frac{a - bx}{a^2 + b^2} \cdot A + \frac{b^2}{a^2 + b^2} \cdot B = 1$$

Extended GCD

Usefulness of Bézout coefficients:

- Recall the proof of "Any algebraic function is D-finite"
- modular inversion and division in a quotient ring $Q = K[x]/(B(x))$:
  A is invertible in Q if and only if $\gcd(A, B) = 1$. In this case:
  the inverse of A in Q is equal to U, where $U \cdot A + V \cdot B = 1$.

▷ Example: For $A = a + bx, B = 1 + x^2$, the inverse of A mod B is

$$U = \frac{a - bx}{a^2 + b^2}.$$

▷ Computation: Extended Euclidean algorithm

Extended Euclidean algorithm

ExtendedEuclid(A, B)

Input A and B in $\mathbb{K}[x]$.

Output A gcd G of A and B, and cofactors U and V.

1. $R_0 := A$; $U_0 := 1$; $V_0 := 0$; $R_1 := B$; $U_1 := 0$; $V_1 := 1$; $i := 1$.
2. While R_i is non-zero, do:
   (a) $(Q_i, R_{i+1}) := \text{QuotRem}(R_{i-1}, R_i)$ $\qquad$ $\# R_{i-1} = Q_i R_i + R_{i+1}$
   (b) $U_{i+1} := U_{i-1} - Q_i U_i$; $V_{i+1} := V_{i-1} - Q_i V_i$.
   (c) $i := i + 1$.
3. Return $\big(R_{i-1}, U_{i-1}, V_{i-1}\big)$.

▷ Correctness: $R_i = U_i A + V_i B$ (by induction):

$$R_{i+1} = R_{i-1} - Q_i R_i = U_{i-1} A + V_{i-1} B - Q_i (U_i A + V_i B) = U_{i+1} A + V_{i+1} B$$

▷ Quadratic complexity: $O\big(\deg(A)\deg(B)\big)$ operations in $\mathbb{K}$

Resultants

Definition

The Sylvester matrix of $A = a_m x^m + \cdots + a_0 \in \mathbb{K}[x]$, $(a_m \neq 0)$, and of $B = b_n x^n + \cdots + b_0 \in \mathbb{K}[x]$, $(b_n \neq 0)$, is the square matrix of size $m+n$

$$\mathsf{Syl}(A,B) = \begin{bmatrix} a_m & a_{m-1} & \dots & a_0 & & & & \\ & a_m & a_{m-1} & \dots & a_0 & & & \\ & & \ddots & \ddots & & & \ddots & \\ & & & a_m & a_{m-1} & \dots & a_0 & \\ b_n & b_{n-1} & \dots & b_0 & & & & \\ & b_n & b_{n-1} & \dots & b_0 & & & \\ & & \ddots & \ddots & & & \ddots & \\ & & & b_n & b_{n-1} & \dots & b_0 & \end{bmatrix}$$

The resultant $\mathsf{Res}(A,B)$ of A and B is the determinant of $\mathsf{Syl}(A,B)$.

▷ Definition extends to polynomials over any commutative ring R.

Key observation

If $\quad A = a_m x^m + \cdots + a_0 \quad$ and $\quad B = b_n x^n + \cdots + b_0, \quad$ then

$$\begin{bmatrix} a_m & a_{m-1} & \dots & a_0 & & \\ & \ddots & \ddots & & \ddots & \\ & & a_m & a_{m-1} & \dots & a_0 \\ b_n & b_{n-1} & \dots & b_0 & & \\ & \ddots & \ddots & & \ddots & \\ & & b_n & b_{n-1} & \dots & b_0 \end{bmatrix} \times \begin{bmatrix} \alpha^{m+n-1} \\ \vdots \\ \alpha \\ 1 \end{bmatrix} = \begin{bmatrix} \alpha^{n-1}A(\alpha) \\ \vdots \\ A(\alpha) \\ \alpha^{m-1}B(\alpha) \\ \vdots \\ B(\alpha) \end{bmatrix}$$

Corollary: If $A(\alpha) = B(\alpha) = 0$, then $\mathsf{Res}\,(A, B) = 0$.

Example: the discriminant

The discriminant of A is the resultant of A and of its derivative A'.

E.g. for $A = ax^2 + bx + c$,

$$\mathsf{Disc}(A) = \mathsf{Res}\,(A, A') = \det \begin{bmatrix} a & b & c \\ 2a & b & \\ & 2a & b \end{bmatrix} = -a(b^2 - 4ac).$$

E.g. for $A = ax^3 + bx + c$,

$$\mathsf{Disc}(A) = \mathsf{Res}\,(A, A') = \det \begin{bmatrix} a & 0 & b & c & \\ & a & 0 & b & c \\ 3a & 0 & b & & \\ & 3a & 0 & b & \\ & & 3a & 0 & b \end{bmatrix} = a^2(4b^3 + 27ac^2).$$

$\triangleright$ The discriminant vanishes when A and A' have a common root, that is when A has a multiple root.

Main properties

- Link with gcd $\mathsf{Res}\,(A,B) = 0$ if and only if $\gcd(A,B)$ is non-constant.

- Elimination property

  There exist $U, V \in \mathbb{K}[x]$ not both zero, with $\deg(U) < n$, $\deg(V) < m$ and such that the following Bézout identity holds in $\mathbb{K} \cap (A, B)$:

$$\mathsf{Res}\,(A,B) = UA + VB.$$

- Poisson formula

  If $A = a(x-\alpha_1)\cdots(x-\alpha_m)$ and $B = b(x-\beta_1)\cdots(x-\beta_n)$, then

$$\mathsf{Res}\,(A,B) \; = \; a^n b^m \prod_{i,j}(\alpha_i - \beta_j) \; = \; a^n \prod_{1\le i\le m} B(\alpha_i).$$

- Multiplicativity

$$\mathsf{Res}\,(A{\cdot}B, C) = \mathsf{Res}\,(A,C){\cdot}\mathsf{Res}\,(B,C), \quad \mathsf{Res}\,(A, B{\cdot}C) = \mathsf{Res}\,(A,B){\cdot}\mathsf{Res}\,(A,C).$$

Proof of Poisson's formula

▷ Direct consequence of the key observation:

If $A = (x-\alpha_1)\cdots(x-\alpha_m)$ and $B = (x-\beta_1)\cdots(x-\beta_n)$ then

$$\mathsf{Syl}(A,B) \times \begin{bmatrix} \beta_1^{m+n-1} & \dots & \beta_n^{m+n-1} & \alpha_1^{m+n-1} & \dots & \alpha_m^{m+n-1} \\ \vdots & & \vdots & \vdots & & \vdots \\ \beta_1 & \dots & \beta_n & \alpha_1 & \dots & \alpha_m \\ 1 & \dots & 1 & 1 & \dots & 1 \end{bmatrix} =$$

$$= \begin{bmatrix} \beta_1^{n-1}A(\beta_1) & \dots & \beta_n^{n-1}A(\beta_n) & 0 & \dots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ A(\beta_1) & \dots & A(\beta_n) & 0 & \dots & 0 \\ 0 & \dots & 0 & \alpha_1^{m-1}B(\alpha_1) & \dots & \alpha_m^{m-1}B(\alpha_m) \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \dots & 0 & B(\alpha_1) & \dots & B(\alpha_m) \end{bmatrix}$$

▷ To conclude, take determinants and use Vandermonde's formula

Application: computation with algebraic numbers

Let $A = \prod_i (x - \alpha_i)$ and $B = \prod_j (x - \beta_j)$ be polynomials of $\mathbb{K}[x]$. Then

$$\prod_{i,j} (t - (\alpha_i + \beta_j)) = \mathrm{Res}_x(A(x), B(t - x)),$$

$$\prod_{i,j} (t - (\beta_j - \alpha_i)) = \mathrm{Res}_x(A(x), B(t + x)),$$

$$\prod_{i,j} (t - \alpha_i \beta_j) = \mathrm{Res}_x(A(x), x^{\deg B} B(t/x)),$$

$$\prod_{i} (t - B(\alpha_i)) = \mathrm{Res}_x(A(x), t - B(x)).$$

In particular, the set $\overline{\mathbb{Q}}$ of algebraic numbers is a field.

Proof: Poisson's formula. E.g., first one: $\displaystyle\prod_i B(t - \alpha_i) = \prod_{i,j} (t - \alpha_i - \beta_j)$.

▷ The same formulas apply mutatis mutandis to algebraic power series.

A beautiful identity of Ramanujan's

$$\frac{\sin\frac{2\pi}{7}}{\sin^2\frac{3\pi}{7}} - \frac{\sin\frac{\pi}{7}}{\sin^2\frac{2\pi}{7}} + \frac{\sin\frac{3\pi}{7}}{\sin^2\frac{\pi}{7}} = 2\sqrt{7}.$$

- If $a = \pi/7$ and $x = e^{ia}$, then $x^7 = -1$ and $\sin(ka) = (x^k - x^{-k})/(2\,i)$
- Since $x \in \overline{\mathbb{Q}}$, any rational expression in the $\sin(ka)$ is in $\mathbb{Q}(x)$, thus in $\overline{\mathbb{Q}}$
- In particular our LHS, $F(x) = \frac{N(x)}{D(x)}$, is an algebraic number

```
> f:=sin(2*a)/sin(3*a)^2-sin(a)/sin(2*a)^2+sin(3*a)/sin(a)^2:
> expand(convert(f,exp)):
> F:=normal(subs(exp(I*a)=x,%)):
```

$$\frac{2\,i\,(x^{16} + 5\,x^{14} + 12\,x^{12} + x^{11} + 20\,x^{10} + 3\,x^9 + 23\,x^8 + 3\,x^7 + 20\,x^6 + x^5 + 12\,x^4 + 5\,x^2 + 1)}{x\,(x^2 - 1)\,(x^2 + 1)^2\,(x^4 + x^2 + 1)^2}$$

- Get R in $\mathbb{Q}[t]$ with root $F(x)$, via resultant $\operatorname{Res}_x(x^7 + 1, t \cdot D(x) - N(x))$

```
> R:=factor(resultant(x^7+1,t*denom(F)-numer(F),x));
```

$$-1274\,i\,(t^2 - 28)^3$$

Shanks' 1974 identities

$$\sqrt{11+2\sqrt{29}}+\sqrt{16-2\sqrt{29}+2\sqrt{55-10\sqrt{29}}}=\sqrt{5}+\sqrt{22+2\sqrt{5}}$$

$$\sqrt{\sqrt{m+n}+\sqrt{n}}+\sqrt{\sqrt{m+n}+m-\sqrt{n}+2\sqrt{m\left(\sqrt{m+n}-\sqrt{n}\right)}}$$
$$=\sqrt{m}+\sqrt{2\sqrt{m+n}+2\sqrt{m}}$$

Two exercises for next time

(1) Let $P, Q \in \mathbb{K}[x]$ be two polynomials, and let $N \in \mathbb{N} \setminus \{0\}$.

(a) Show that the unique monic polynomial in $\mathbb{K}[x]$ whose roots are the N-th powers of the roots of P can be obtained by a resultant computation.

(b) If P is the minimal polynomial of an algebraic number α, show that one can determine an annihilating polynomial of $Q(\alpha)$ using a resultant.

(2) The aim of this exercise is to prove algorithmically the following identity:

$$\sqrt[3]{\sqrt[3]{2} - 1} = \sqrt[3]{\frac{1}{9}} - \sqrt[3]{\frac{2}{9}} + \sqrt[3]{\frac{4}{9}}. \tag{1}$$

Let $a = \sqrt[3]{2}$ and $b = \sqrt[3]{\frac{1}{9}}$.

(a) Determine $P_c \in \mathbb{Q}[x]$ annihilating $c = 1 - a + a^2$, using a resultant.

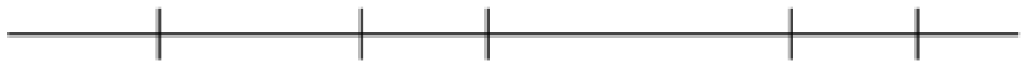
(b) Deduce $P_R \in \mathbb{Q}[x]$ annihilating the RHS of (1), by another resultant.

(c) Show that the polynomial computed in (b) also annihilates the LHS of (1).

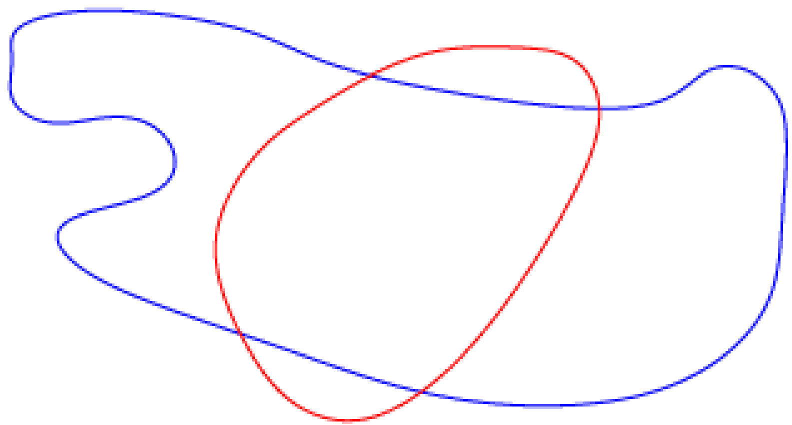
(d) Conclude.

Systems of two equations and two unknowns

Geometrically, roots of a polynomial $f \in \mathbb{Q}[x]$ correspond to points on a line.



Roots of polynomials $A \in \mathbb{Q}[x, y]$ correspond to plane curves $A = 0$.

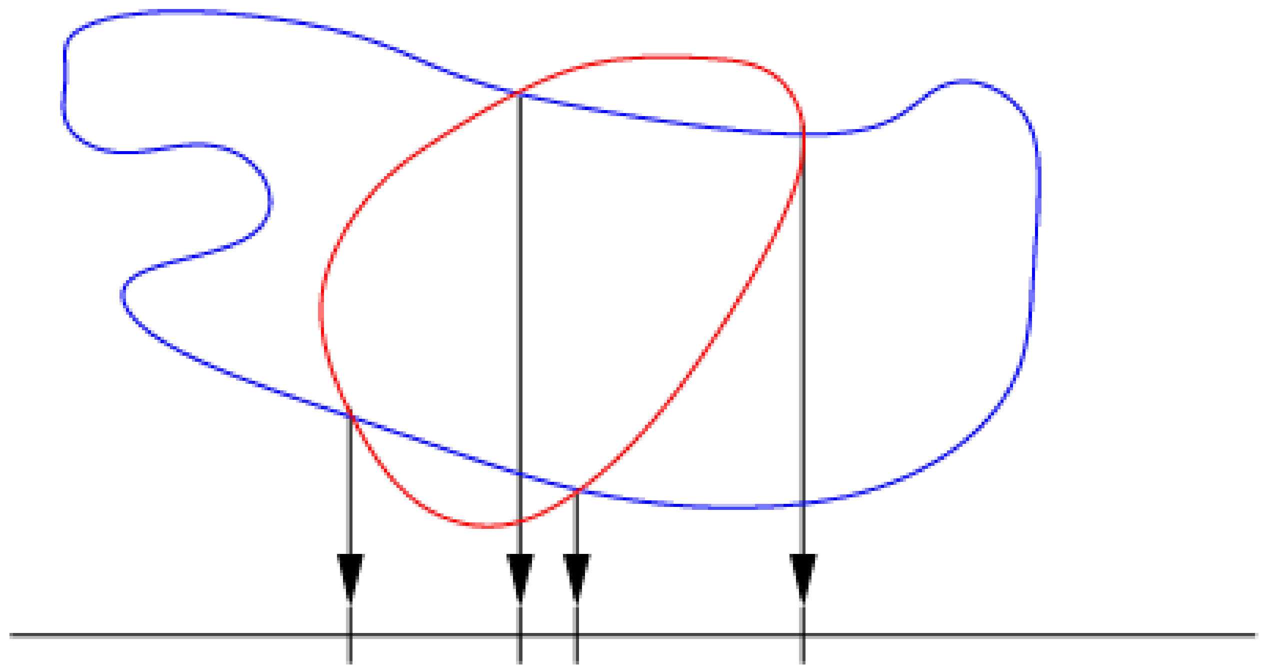


Let now A and B be in $\mathbb{Q}[x, y]$. Then:

- either the curves $A = 0$ and $B = 0$ have a common component,
- or they intersect in a finite number of points.

Application: Resultants compute projections

Theorem. Let $A = a_m y^m + \cdots$ and $B = b_n y^n + \cdots$ be polynomials in $\mathbb{Q}[x][y]$. The roots of $\mathsf{Res}_y(A, B) \in \mathbb{Q}[x]$ are either the abscissas of points in the intersection $A = B = 0$, or common roots of a_m and b_n.



Proof. Elimination property: $\mathsf{Res}\,(A, B) = UA + VB$, for $U, V \in \mathbb{Q}[x, y]$.

Thus $A(\alpha, \beta) = B(\alpha, \beta) = 0$ implies $\mathsf{Res}_y(A, B)(\alpha) = 0$

Application: implicitization of parametric curves

Task: Given a rational parametrization of a curve

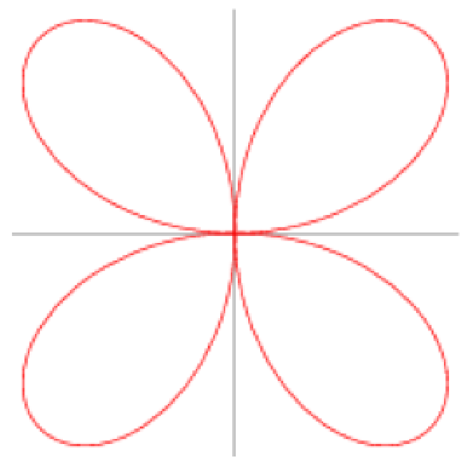
$$x = A(t), \quad y = B(t), \qquad A, B \in \mathbb{K}(t),$$

compute a non-trivial polynomial in x and y vanishing on the curve.

Recipe: take the resultant in t of numerators of $x - A(t)$ and $y - B(t)$.

Example: for the four-leaved clover (a.k.a. quadrifolium) given by

$$x = \frac{4t(1-t^2)^2}{(1+t^2)^3}, \quad y = \frac{8t^2(1-t^2)}{(1+t^2)^3},$$



$$\mathrm{Res}_t((1+t^2)^3x - 4t(1-t^2)^2, (1+t^2)^3y - 8t^2(1-t^2)) = 2^{24}\left((x^2+y^2)^3 - 4x^2y^2\right).$$

Computation of the resultant

An Euclidean-type algorithm for the resultant bases on:

- If $A = QB + R$, and $R \neq 0$, then (by Poisson's formula)

$$\mathsf{Res}\,(A,B) = (-1)^{\deg A \deg B}\,\mathsf{lc}(B)^{\deg A - \deg R}\,\mathsf{Res}\,(B,R).$$

- If B is constant, then $\quad \mathsf{Res}\,(A,B) = B^{\deg A}$.

If $(R_0, \ldots, R_{N-1}, R_N = \gcd(A,B), 0)$ is the remainder sequence produced by the Euclidean algorithm for $R_0 = A$ and $R_1 = B$, then

- either $\deg R_N$ is non-constant, and $\mathsf{Res}\,(A,B) = 0$,
- or $\mathsf{Res}\,(A,B) = R_N^{\deg R_{N-1}} \prod_{i=0}^{N-2} (-1)^{\deg R_i \deg R_{i+1}}\,\mathsf{lc}(R_{i+1})^{\deg R_i - \deg R_{i+2}}$.

▷ This leads to a $O(N^2)$ algorithm for $\mathsf{Res}\,(A,B)$, where $\deg(A), \deg(B) \leq N$.

▷ A divide-and-conquer $O(\mathsf{M}(N) \log N)$ algorithm requires extra-work.