Parametric Euclidean Algorithm

Ali Ayad

Discrete Mathematics - EDST - Lebanese University

Dimacos – November 14, 2012

The problem

Let $f_1, f_2 \in \mathbb{Q}[u_1, \ldots, u_t][X]$ be parametric univariate polynomials where $u_1, \ldots, u_t$ are the parameters.

- $\mathcal{P} = \overline{\mathbb{Q}}^t$: the parameters space
- For a polynomial $g \in \mathbb{Q}(u_1, \ldots, u_t)[X]$ and a value $a = (a_1, \ldots, a_t) \in \mathcal{P}$, we denote by G the polynomial $G = g(a_1, \ldots, a_t, X) \in \overline{\mathbb{Q}}[X]$.

The Goal

Calculate GCD of F_1 and F_2 in $\overline{\mathbb{Q}}[X]$ in a uniform way for $a \in \mathcal{P}$, i.e., find constructible subsets $W_1, \ldots, W_N$ of $\mathcal{P}$ verifying :

- Each W_i is equipped with a parametric polynomial $g_i \in \mathbb{Q}[u_1, \ldots, u_t][X]$ such that the polynomial G_i is a gcd of F_1 and F_2 in $\overline{\mathbb{Q}}[X]$ for all $a \in W_i$.
- $W_1, \ldots, W_N$ form a partition of $\mathcal{P}$.

Example

Let $f_1 = X^3 + uX^2 + vX + 1$ and $f_2 = X^2 - uX - 1$. Then

$$\mathcal{P} = W_1 \cup W_2 \cup W_3 \cup W_4,$$

$$\begin{cases} W_1 = \{2u^2 + v + 1 \neq 0, g_1 \neq 0\}, \\ g_1 = 2u^3 - 2u^2 v + 2u^2 - v^2 + uv + 5u - 2v, \end{cases}$$

$$\begin{cases} W_2 = \{2u^2 + v + 1 \neq 0, g_1 = 0\}, \\ g_2 = (2u^2 + v + 1)X + 2u + 1, \end{cases}$$

$$\begin{cases} W_3 = \{2u^2 + v + 1 = 0, 2u + 1 \neq 0\}, \\ g_3 = 2u + 1, \end{cases}$$

$$\begin{cases} W_4 = \{2u^2 + v + 1 = 0, 2u + 1 = 0\}, \\ g_4 = f_2. \end{cases}$$

The problem

The Euclidean algorithm

- Consider $f_1, f_2 \in \mathbb{Q}(u_1, \ldots, u_t)[X]$
- Compute the sequence

$$\{r_0, r_1, \ldots, r_s, r_{s+1} = 0\} \subset \mathbb{Q}(u_1, \ldots, u_t)[X]$$

  of remainders by successive euclidean divisions of the polynomials $r_0 = f_1$ and $r_1 = f_2$ in $\mathbb{Q}(u_1, \ldots, u_t)[X]$.
- r_s is a gcd of f_1 and f_2 in $\mathbb{Q}(u_1, \ldots, u_t)[X]$.

Two problems

Problem 1

Zeros of the denominators of the coefficients of $r_0, r_1, \ldots, r_s$ in $\mathbb{Q}(u_1, \ldots, u_t)$ are not covered.

Problem 2

Even for a value $a \in \mathcal{P}$ which does not vanish any denominator of the coefficients of $r_2, \ldots, r_s$, the polynomial $R_s \in \overline{\mathbb{Q}}[X]$ is not necessarily a gcd of F_1 and F_2.

Let

$$r_0 = f_1 = uX^2 + X - 1 \quad \text{and} \quad r_1 = f_2 = vX + 1,$$

where u and v are parameters. Then

$$r_2 = -\frac{1}{v}\left(1 - \frac{u}{v}\right) - 1 \quad \text{and} \quad r_3 = 0$$

1. For arbitrary value of u and for $v = 0$, R_2 is not defined (**Problem 1**).
2. For $(u, v) = (2, 1)$, then $R_2 = 0$ and $F_2 = X + 1$ is a gcd of $F_1 = 2X^2 + X - 1$ and F_2 (**Problem 2**).

Pseudo-division

Let $f_1, f_2 \in \mathbb{Q}[u_1, \ldots, u_t][X]$, $m_1 = \deg_X(f_1)$ and $m_2 = \deg_X(f_2)$. There exist unique polynomials $q, r \in \mathbb{Q}[u_1, \ldots, u_t][X]$ such that

$$lc(f_2)^{m_1 - m_2 + 1} f_1 = q f_2 + r$$

with

$$r = 0 \quad \text{or} \quad \deg_X(r) < \deg_X(f_2),$$

q is called the pseudo-quotient and r is the pseudo-remainder (denoted by $Prem(f_1, f_2)$) of the pseudo-division of f_1 by f_2.

Avoiding Problem 1 : Pseudo-division

Sequence of pseudo-remainders

The sequence of pseudo-remainders of successive pseudo-divisions applicated to $\tilde{r}_0 = f_1$ and $\tilde{r}_1 = f_2$ is the sequence

$$\{\tilde{r}_0, \tilde{r}_1, \ldots, \tilde{r}_s, \tilde{r}_{s+1} = 0\} \subset \mathbb{Q}[u_1, \ldots, u_t][X]$$

where $\tilde{r}_i = Prem(\tilde{r}_{i-2}, \tilde{r}_{i-1})$

Pseudo-remainders

- $\tilde{r}_s$ is a gcd of f_1 and f_2 in $\mathbb{Q}[u_1, \ldots, u_t][X]$.
- For any $a \in \mathcal{P}$ which does not vanish any leading coefficient of the polynomials in the sequence, the polynomial $\tilde{R}_s \in \overline{\mathbb{Q}}[X]$ is a gcd of F_1 and F_2.

Avoiding Problem 1 : Example

Let

$$\tilde{r}_0 = f_1 = X^3 + uX^2 + vX + 1 \quad \text{and} \quad \tilde{r}_1 = f_2 = X^2 - uX - 1.$$

Then

$$\begin{cases} \tilde{r}_2 = (2u^2 + v + 1)X + (2u + 1), \\ \tilde{r}_3 = 2u^3 - 2u^2 v + 2u^2 - v^2 + uv + 5u - 2v, \\ \tilde{r}_4 = 0. \end{cases}$$

- $\tilde{r}_3$ is a gcd of f_1 and f_2 in $\mathbb{Q}[u, v][X]$.
- For $(u, v) = (0, 0)$, $\tilde{R}_3 = 0$ and $\tilde{R}_2 = X + 1$ is a gcd of $F_1 = X^3 + 1$ and $F_2 = X^2 - 1$ (**Problem 2**).

Let $g = g_m X^m + \cdots + g_1 X + g_0 \in \mathbb{Q}[u_1, \ldots, u_t][X]$.

- For any $0 \leq i \leq m$, the truncation of g at i is

$$Tru_i(g) = g_i X^i + \cdots + g_1 X + g_0 \in \mathbb{Q}[u_1, \ldots, u_t][X].$$

- The set of truncations of g, is the finite subset of $\mathbb{Q}[u_1, \ldots, u_t][X]$:

$$Tru\,(g) = \begin{cases} \{g\} & \text{if} \quad g_m = lc(g) \in \mathbb{Q}, \\ \{g\} \cup Tru\,(Tru_{m-1}(g)) & \text{else.} \end{cases}$$

If $g_i \notin \mathbb{Q}$ for all $0 \leq i \leq m$, then we add 0 to $Tru\,(g)$.

Avoiding Problem 2 : Truncations

Example

For

$$g = uX^4 + uvX^3 + 3X^2 - u^4X + 1$$

$$\begin{cases} Tru(g) = \{g, Tru_3(g), Tru_2(g)\}, \text{ where} \\ Tru_3(g) = uvX^3 + 3X^2 - u^4X + 1, \\ Tru_2(g) = 3X^2 - u^4X + 1, \end{cases}$$

and for

$$h = u^3X^2 + uv^2X + v^2 + 1$$

$$\begin{cases} Tru(h) = \{h, Tru_1(h), Tru_0(h), 0\}, \text{ where} \\ Tru_1(h) = uv^2X + v^2 + 1, \\ Tru_0(h) = v^2 + 1. \end{cases}$$

Tree of pseudo-remainders

For each nonzero polynomial $\tilde{r}_0 \in Tru\,(f_1)$, we associate a tree of pseudo-remainders of $\tilde{r}_0$ by f_2, denoted by $TPrems(\tilde{r}_0, f_2)$.

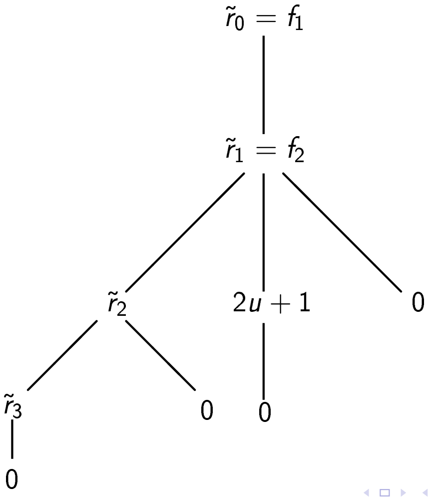
- The root of this tree contains $\tilde{r}_0$.
- The sons of $\tilde{r}_0$ contain the elements of $Tru(f_2)$.
- Each node N contains a polynomial $Pol(N) \in \mathbb{Q}[u_1, \ldots, u_t][X]$.
- A node N is a leaf of the tree if $Pol(N) = 0$.
- If N is not a leaf, the sons of N contain the elements of the set of truncations of $Prem(Pol(p(N)), Pol(N))$ where $p(N)$ is the parent of N.

Forest of pseudo-remainders

The set of all the trees associated to the nonzero elements of $Tru\,(f_1)$ is called the forest of pseudo-remainders of f_1 by f_2, it is denoted by $T(f_1, f_2)$.

Example of forest of pseudo-remainders

Let $f_1 = X^3 + uX^2 + vX + 1$ and $f_2 = X^2 - uX - 1$



Let $\tilde{r}_0 \in Tru\,(f_1) \setminus \{0\}$ and $TPrems(\tilde{r}_0, f_2)$ the tree with root contains $\tilde{r}_0$. For each leaf L of $TPrems(\tilde{r}_0, f_2)$, we consider the unique path

$$P_L = \{\tilde{r}_0, \tilde{r}_1, \ldots, \tilde{r}_s, \tilde{r}_{s+1} = Pol(L) = 0\}$$

We associate to L a constructible subset W_L of $\mathcal{P}$ defined by :

$$\bigwedge_{2 \leq i \leq s+1} \Big[\deg_X(\tilde{r}_i) = \deg_X \big(Prem(\tilde{r}_{i-2}, \tilde{r}_{i-1}) \big) \Big].$$

Partition of the parameters space

1. The constructible sets W_L where L are the leaves of the forest $T(f_1, f_2)$ form a partition of $\mathcal{P}$.
2. For every leaf L of $T(f_1, f_2)$, the path P_L is a parametric pseudo-remainder sequence of f_1 and f_2, i.e., for any $a \in W_L$, the set

$$\{\tilde{R}_0, \tilde{R}_1, \ldots, \tilde{R}_s, \tilde{R}_{s+1} = Pol(L) = 0\} \subset \overline{\mathbb{Q}}[X]$$

is the sequence of pseudo-remainders of F_1 and F_2. In particular, $0 \neq \tilde{R}_s \in \overline{\mathbb{Q}}[X]$ is a gcd of F_1 and F_2.