Chapter 6 The resultant and gcd computation

6.1 Coefficient growth in the Euclidean Algorithm

Q1. How big do we have to choose the modulus p so that we can recover the gcd from its image modulo p?

Q2. How do we find the denominators of the monic gcd?

Q3. Does the approach work for any prime, or are there primes where the degree of the modular gcd is too large?

6.2 Gauss's lemma

Definition 1. *The content of* $f = f_n x^n + \cdots + f_1 x + f_0 \in R[x]$ *with* $f_0, \ldots, f_n \in R$ *and* R *a UFD is defined as cont*$(f) = \gcd(f_0, f_1, \ldots, f_n \in R$. f *is primitive if cont*$(f) = 1$. *We define the primitive partpp*(f) *by* $f =$ *cont*$(f) \cdot$ *pp*(f).

Theorem 1. *Gauss lemma For a Unique Factorization Domain* R, *the product of two primitive polynomials in* $R[x]$ *is primitive.*

Corollary 1. *For* $f, g \in R[x]$, *cont*$(fg) =$ *cont*(f)*cont*(g) *and pp*$(fg) =$ *pp*(f)*pp*(g).

Theorem 2. *Causs If* R *is UFD then* $R[x]$ *is a UFD.*

Corollary 2. *Let* R *be a UFD with field of fractions* K, $f, g \in R[x]$ *and* h *the normalized gcd of* f *and* g *in* $R[x]$.

1. *The primes of* $R[x]$ *are the primes of* R *plus the primitive polynomials in* $R[x]$ *that are irreducible in* $k[x]$.

2. *cont*$(h) = \gcd($*cont*$(f),$ *cont*$(g))$ *in* R *and pp*$(h) = \gcd($*pp*$(f),$ *pp*$(g))$ *in* $R[x]$. *In particular,* $h = \gcd($*cont*$(f),$ *cont*$(g)) \cdot \gcd($*pp*$(f),$ *pp*$(g))$*, and* h *is primitive if one of* f *and* g *is.*

3. $h/$*lc*$(h) \in K[x]$ *is the monic gcd of* f *and* g *in* $K[x]$.

6.3 The resultant

Lemma 1. *Let* $f, g \in F[x]$ *be nonzero. Then* $\gcd(f, g) \neq 1$ *if and only if there exist* $s, t \in F[x]\{0\}$ *such that* $s \cdot f + t \cdot g = 0$, $\deg s < \deg g$, *and* $\deg t < \deg f$.

Given nonzero $f, g \in F[x]$ of degree n, m, we let

$$\begin{array}{rcl} \phi : P_m \times P_n & \longrightarrow & P_{n+m} \\ (s, t) & \longmapsto & sf + tg \end{array}$$

where $P_d = \{a \in F[x] : \deg a < d\}$, $P_0 = \{0\}$.

$$s = \sum_{0 \le j < m} y_j x^j,\ t = \sum_{0 \le j < n} z_j x^j,\ s \cdot f + t \cdot g = \sum_{0 \le j < n+m} u_j x^j$$

Then

$$S \cdot \begin{pmatrix} y_{m-1} \\ \vdots \\ y_0 \\ z_{n-1} \\ \vdots \\ z_0 \end{pmatrix} = \begin{pmatrix} u_{n+m-1} \\ \vdots \\ \vdots \\ \vdots \\ u_1 \\ u_0 \end{pmatrix}$$

where $S = \mathrm{Syl}(\mathrm{f}, \mathrm{g})$ is their Sylvester matrix and res$(f, g) = \det S$ their resultant.

$$
S = \begin{pmatrix}
f_n & & & & g_m & & & & & \\
f_{n-1} & f_n & & & g_{m-1} & g_m & & & & \\
\vdots & \vdots & \ddots & & \vdots & \vdots & \ddots & & & \\
\vdots & \vdots & & f_n & g_1 & \vdots & & \ddots & & \\
\vdots & \vdots & & f_{n-1} & g_0 & \vdots & & & \ddots & \\
\vdots & \vdots & & \vdots & & g_0 & & & & g_m \\
f_0 & \vdots & & & & & \ddots & & & \vdots \\
 & f_0 & & \vdots & & & & \ddots & & \vdots \\
 & & & f_0 & & & & & & g_0
\end{pmatrix}
$$

with m columns of $f_j's$ and n columns of $g_j's$, and all entries outside the two parallelograms equal to zero.

Corollary 3. *Let R be a UFD and $f, g \in R[x]$ not both zero. Then $\gcd(f, g)$ is nonconstant in $R[x]$ if and only if res$(f, g) = 0$ in R.*

Theorem 3. *Let $f, g \in Z[x]$, and $n = \deg f \geq m = \deg g \geq 1$. Then*

$$|\textit{res}(f, g)| \leq \|f\|_2^m \|g\|_2^n \leq (n+1)^{m/2}(m+1)^{n/2}||f||_\infty^m ||g||_\infty^n$$

Theorem 4. *Let $f, g \in F[x, y]$, and $n = \deg_x f \geq m = \deg_x g$ and $\deg_y f, \deg_y g \leq d$. Then*

$$\deg_y \textit{res}_x(f, g) \leq (n+m)d$$

6.4 Modular gcd algorithms

Lemma 2. *We let R be a ring (commutative, with 1), $f, g \in R[x]$ nonzero, $r =$ res$(f, g) \in R$, $I \subseteq R$ an ideal, denote by a bar the reduction modulo I, and assume that* lc$(f) \neq 0$.

1. $\bar{r} = 0 \Longleftrightarrow$ *res*$(\bar{f}, \bar{g}) = 0$.

2. *If R/I is a UFD, then $\bar{r} = 0$ if and only if $\gcd(\bar{f}, \bar{g})$ is nonconstant.*

Theorem 5. *Let R be a Eculidean domain, $p \in R$ prime, and $f, g \in R[x]$ nonzero. Furthermore, let $h = \gcd(f, g) \in R[x]$, and assume that p does not divide $b = \gcd(lc(f), lc(g)) \in R$. A bar denotes reduction modulo p. Then*

1. $lc(h)$ divides b

2. $\deg \gcd(\bar{f}, \bar{g}) = \deg h \Longleftrightarrow p \nmid res(f/h, g/h)$ in R.

Probabilistic algorithms: Monte Carlo algorithm, Las Vegas algorithm

6.5 Modular gcd algorithms in $F[x, y]$

Algorithm 6.36 Modular bivariate gcd

Input: Primitive polynomials $f, g \in F[x, y]$ with $\deg_x f = n \geq \deg_x g \geq 1$ and $\deg_y f, \deg_y g \leq d$, $R = F[y]$ with at least $(4n + 2)d + 2$ elements.

Output: $h = \gcd(f, g) \in F[x, y]$.

1. $b \longleftarrow \gcd(\mathrm{lc}_x(f), \mathrm{lc}_x(g))$, $l \longleftarrow d + 1 + \deg_y b$

2. repeat

3. choose a set $S \subseteq F$ of evaluation points $b(u) \neq 0$

4. for $u \in S$, compute monic $v_u = \gcd(f(x,u), g(x,u)) \in F[x]$

5. $e \longleftarrow \min \deg v_u, u \in S,\ S \longleftarrow \{u \in S : \deg v_u = e\}$
   if $\sharp S \geq l$ then remove $\sharp S - l$ elements from S else goto 3

6. compute by interpolation each coefficient in $F[y]$ of the polynomials $w, f^*, g^* \in R[x]$ of degrees in y less than l such that

$$w(x,u) = b(u)v_u$$

$$f^*(x,u)w(x,u) = b(u)f(x,u), g^*(x,u)w(x,u) = b(u)g(x,u)$$

7. until $\deg_y(f^*w) = \deg_y(bf)$ and $\deg_y(g^*w) = \deg_y(bg)$

8. return $\mathrm{pp}_x(w)$

Theorem 6. *Mignotte's bound Suppose that* $f, g, h \in Z[x]$ *have degrees* $\deg f = n \geq 1, \deg g = m, \deg h = k$ *and* gh *divides* f *in* $Z[x]$. *Then*

1. $||g||_\infty ||h||_\infty \leq ||g||_2 ||h||_2 \leq ||g||_1 ||h||_1 \leq 2^{m+k} ||f||_2 \leq (n+1)^{1/2} 2^{m+k} ||f||_\infty$

2. $||h||_\infty \leq ||h||_2 \leq 2^k ||f||_2 \leq 2^k ||f||_1$ *and* $||h||_\infty \leq ||h||_2 \leq (n+1)^{1/2} 2^k ||f||_\infty$

Algorithm 6.38 Modular gcd in $Z[x]$: small primes version

Input: Primitive polynomials $f, g \in Z[x]$ with $\deg f = n \geq \deg g \geq 1$ and $||f||_\infty, ||g||_\infty \leq A$.

Output: $h = \gcd(f, g) \in Z[x]$.

1. $b \longleftarrow \gcd(\mathsf{lc}(f), \mathsf{lc}(g)), k \longleftarrow \lceil 2\log_2((n+1)^n bA^{2n}) \rceil$
   $B \longleftarrow (n+1)^{1/2} 2^n Ab$, $i \longleftarrow \lceil \log_2(2B+1) \rceil$

2. repeat

3. choose a set S of $2l$ primes, each less than $2k \ln k$

4. $S \longleftarrow \{p \in S : p \nmid b\}$ for each $p \in S$ compute $v_p = \gcd(\bar{f}, \bar{g}) \in Z_p[x]$

5. $e \longleftarrow \min\{\deg v_p : p \in S\}$, $S \longleftarrow \{p \in S : \deg v_p = e\}$
   if $\sharp S \geq l$ then remove remove $\sharp S - l$ elements from S else goto 3

6. call CRA to compute unique polynomials $w, f^*, g^* \in Z[x]$

$$w \equiv bv_p \mod p,\ f^*w \equiv bf \mod p,\ g^*w \equiv bg \mod p$$

7. until $||f^*||_1||w||_1 \leq B$ and $||g^*||_1||w||_1 \leq B$

8. return pp(w)

Theorem 7. *The algorithm 6.38 can be performed with* $O(n(n^2+log^2 A)(\log n+\log\log A)^2)$ *word operations.*

6.9 Nonzero preservation and the gcd of several polynomials

Lemma 3. *Let R be an integral domain, $n \in \mathbb{N}, S \subseteq R$ finite with $s = \sharp S$ elements, and $r \in R[x_1, \ldots, x_n]$ a polynomial of total degree at most $d \in \mathbb{N}$.*

1. If r is not the zero polynomial, the r has at most ds^{n-1} zeroes in S^n.

2. If $s > d$ and r vanishes on S^n, then $r = 0$.

Algorithm 6.45 Gcd of many polynomials

Input: $f_1, \ldots, f_n \in F[x]$, where F is a field.

Output: $h \in F[x]$ monic, so that $h = \gcd(f_1, \ldots, f_n)$ is probably true.

1. choose $a_3, \ldots, a_n \in S$ independently at random

2. $g \longleftarrow f_2 + \sum_{3 \leq i \leq n} a_i f_i$

3. return $\gcd(f_1, g)$

Theorem 8. *Suppose that* $\deg f_i \leq d$ *for each* i, *and* $h^* = \gcd(f_1, \ldots, f_n$. *Then the algorithm uses at most* $2(n-2)(d+1) + \frac{5}{2}d^2 + O(d)$ *operations in* F, h^* *divides* h, *and* $\mathrm{prob}\{h \neq h^*\} \leq d/\sharp S$.

6.10 Subresultants

Theorem 9. *Let $0 \le k \le m \le n$. Then k does not appear in the degree sequence if and only if there exist $s, t \in F[x]$ satisfying*

$$t \neq 0, \deg s < m - k, \deg t < n - k, \deg(sf + tg) < k.$$

Given nonzero $f, g \in F[x]$ of degree n, m, we let

$$\begin{array}{rcl} \phi_k : P_{m-k} \times P_{n-k} & \longrightarrow & P_{n+m-2k} \\ (s,t) & \longmapsto & sf + tg \,\mathsf{quo}\, x^k. \end{array}$$

where $P_d = \{a \in F[x] : \deg a < d\}$, $P_0 = \{0\}$.

Corollary 4. *Let $0 \leq k \leq m \leq n$ and $0 \leq i \leq l+1$.*

1. *k appears in the degree sequence $\iff$ ϕ_k is an isomorphism.*

2. *If $k = n_i$, then the linear coefficients s_i, t_i computed in the EEA are the unique solution of $\phi_k(s_i, t_i) = 1$.*

Let $f = \sum_{0 \le j \le n} f_j x^j$ and $g = \sum_{0 \le j \le m} g_j x^j$ with $f_j, g_j \in F$. If

$$s = \sum_{0 \le j < m-k} y_j x^j,\ t = \sum_{0 \le j < n-k} z_j x^j,\ sf + tg = \sum_{0 \le j < n+m-k} u_j x^j \in F[x]$$

then

$$S_k \cdot (y_{m-k-1}, \ldots, y_0, z_{n-k-1}, \ldots, z_0)^T = (u_{n+m-k-1}, \ldots, u_k)^T,$$

$$
S_k = \begin{pmatrix}
f_n & & & & g_m & & & & & \\
f_{n-1} & f_n & & & g_{m-1} & g_m & & & & \\
\vdots & & \ddots & & \vdots & & \ddots & & & \\
f_{n-m+k+1} & \cdots & \cdots & f_n & g_{k+1} & \cdots & \cdots & g_m & & \\
\vdots & & & \vdots & \vdots & & & & \ddots & \\
f_{k+1} & \cdots & \cdots & f_m & g_{m-n+k+1} & \cdots & \cdots & \cdots & \cdots & g_m \\
\vdots & & & \vdots & \vdots & & & & & \vdots \\
f_{2k-m+1} & \cdots & \cdots & f_k & g_{2k-n+1} & \cdots & \cdots & \cdots & \cdots & g_k
\end{pmatrix}
$$

$\theta_k = \det S_k \in R$ for $0 \leq k \leq \deg g$ are the subresultants.

Corollary 5. *Let $0 \le k \le m \le n$, and $0 \le i \le k+1$.*

1. *k appears in the degree sequence $\iff \det S_k \neq 0$.*

2. *If $k = n_i$, and $y_0, \ldots y_{m-k-1}, z_0, \ldots, z_{n-k-1} \in F$ form the unique solution to*

$$S_k \cdot (y_{m-k-1}, \ldots, y_0, z_{n-k-1}, \ldots, z_0)^T = (0, \ldots, 0, 1)^T,$$

   then

$$s_i = \sum_{0 \le j < m-k} y_j x^j, \ t_i = \sum_{0 \le j < n-k} z_j x^j.$$

Theorem 10. *Let* $f, g \in \mathbb{Z}[x]$, $n = \deg f \geq m$. *Then*

$$|\sigma_k| = |\det S_k| \leq ||f||_2^{m-k}||g||_2^{n-k} \leq (n+1)^{n-k}||f||_\infty^{m-k}||g||_\infty^{n-k}$$

Theorem 11. *Let* $f, g \in F[x, y], n = \deg_x f \geq m = \deg_x g \geq 1, \deg_y f, \deg_y g \leq d$, *and* $0 \leq k \leq m$. *Then* $\deg_y \sigma_k \leq (n + m - 2k)d$.

6.11 Modular Extended Euclidean Algorithms

6.12 Pseudo-division and primitive Euclidean Algorithms

Pseudo division computing $q, r \in \mathbb{Z}[x]$ from $a, b \in \mathbb{Z}[x]$ with

$$\mathsf{lc}(b)^{1+\deg a-\deg b} a = qb + r,\ \deg r < \deg b$$

Algorithm 6.61 Primitive Euclidean Algorithm

Input: Primitive polynomials $f, g \in R[x]$, where R is a UFD, of degrees $n \geq m$.

Output: $h = \gcd(f, g) \in R[x]$.

1. $r_0 \longleftarrow f, r_1 \longleftarrow, n_0 \longleftarrow n, n_1 \longleftarrow m$

2. $i \longleftarrow 1$
   while $r_i \neq 0$ do
   $a_{i-1} \longleftarrow \mathsf{lc}(r_i)^{1+n_{i-1}-n_i} r_{i-1}, q_i \longleftarrow a_{i-1}\mathsf{quo} r_i$
   $r_{i+1} \longleftarrow pp(a_{i-1}\mathsf{rem} r_i), n_{i+1} \longleftarrow \deg r_{i+1}$
   $i \longleftarrow i + 1$

3. $l \longleftarrow i - 1$, return $\mathrm{normal}(r_l)$