WS 2023

Computer Algebra
(selected slides)

Carsten Schneider

Research Institute for Symbolic Computation (RISC)
Johannes Kepler University Linz

Lecture 2: October 13, 2022

Algorithm (Normalized) extended Euclidean algorithm
Input: $f, g \in R$ with R Euclidean domain.
Output: $\rho_i, r_i, s_i, t_i \in R$ for $0 \le i \le l+1$ and q_i for $0 \le i \le l$

1. $\rho_0 = \mathrm{lu}(f),\ r_0 = \mathrm{normal}(f)(= f/\rho_0),\ s_0 = \rho_0^{-1},\ t_0 = 0$
   $\rho_1 = \mathrm{lu}(g),\ r_1 = \mathrm{normal}(g)(= g/\rho_1),\ s_1 = 0,\ t_1 = \rho_1^{-1}$
2. i=1
   while $r_i \neq 0$ do
   - $q_i = r_{i-1} \,\mathrm{quot}\, r_i$
   - $r_{i+1} = r_{i-1} \mathrm{rem} r_i (= r_{i-1} - q_i\, r_i))$
   - $\rho_{i+1} = \mathrm{lu}(r_{i+1})$
   - $r_{i+1} = \mathrm{normal}(r_{i+1})(= r_{i+1}/\rho_{i+1})$
   - $s_{i+1} = (s_{i-1} - q_i\, s_i)/\rho_{i+1}$
   - $t_{i+1} = (t_{i-1} - q_i\, t_i)/\rho_{i+1}$
   - $i = i + 1$

   od
3. $l = i - 1$
   return ρ_i, r_i, s_i, t_i for $0 \le i \le l+1$, q_i for $0 \le i \le l$

Define

$$R_0 = \begin{pmatrix} s_0 & t_0 \\ s_1 & t_1 \end{pmatrix}$$

$$Q_i = \begin{pmatrix} 0 & 1 \\ \rho_{i+1}^{-1} & -q_i \rho_{i+1}^{-1} \end{pmatrix}, \qquad R_i = Q_i \ldots Q_1 R_0 \qquad 0 \le i \le l$$

EEA-Lemma. For $0 \le i \le l$:

(i) $R_i \begin{pmatrix} f \\ g \end{pmatrix} = \begin{pmatrix} r_i \\ r_{i+1} \end{pmatrix}$

(ii) $R_i = \begin{pmatrix} s_i & t_i \\ s_{i+1} & t_{i+1} \end{pmatrix}$

(iii) r_i, r_{i+1} and f, g have gcds, in particular: $\gcd(f, g) = \gcd(r_i, r_{i+1}) = r_l$

(iv) $s_i\, f + t_i\, g = r_i$ (also $i = l + 1$)

(v) $s_i\, t_{i+1} - t_i\, s_{i+1} = (-1)^i (\rho_0 \ldots \rho_{i+1})^{-1}$ and $\gcd(s_i, t_i) = 1$

(vi) $\gcd(r_i, t_i) = \gcd(f, t_i)$

(vii) $f = (-1)^i \rho_0 \ldots \rho_{i+1} (t_{i+1}\, r_i - t_i\, r_{i+1})$ and
$g = (-1)^{i+1} \rho_0 \ldots \rho_{i+1} (s_{i+1}\, r_i - s_i\, r_{i+1})$

(viii) If $R = \mathbb{F}[x]$ then $\deg(t_i) + \deg(r_{i-1}) = \deg(f)$ for $i \ge 1$,
$\deg(s_i) + \deg(r_{i-1}) = \deg(g)$ for $i > 1$.

Lecture 4: November 9, 2023

Algorithm CRA (Chinese Remainder Algorithm)

Input: $m_0, \ldots, m_{r-1} \in R^* \setminus R^+$ pairwise coprime,
$v_0, \ldots, v_{r-1} \in R$ with R ED.

Output: $f \in R$ with $d(f) < d(m_0) + \ldots d(m_{r-1})$ such that for $0 \leq i < r$:

$$m_i \mid f - v_i \quad \Leftrightarrow \quad f \equiv v_i \mod m_i$$

1. $m = m_0 \ldots m_{r-1} \in R$
2. for $0 \leq i < r$ do
3. $\quad f_i = m/m_i \in R$
4. $\quad$ call the EEA and compute $s_i, t_i \in R$ such that $s_i\, f_i + t_i\, m_i = 1$
5. $\quad c_i = v_i\, s_i \,\mathrm{rem}\, m_i \in R \qquad$ [note:$d(c_i) < d(m_i)$]
6. od
7. return $f = \sum_{i=0}^{r-1} c_i\, f_i$

Remark 1: $l_i = s_i\, f_i$ and $c_i\, f_i = v_i\, l_i \,\mathrm{rem}\, m$.

Remark 2: If $d(v_i) < d(m_i)$ then $f \,\mathrm{rem}\, m_i = v_i$.

Remark 3: The computation of t_i in the EEA can be skipped.

Lecture 5: November 16, 2023

Theorem (Rational function reconstruction) Let $h, f \in \mathbb{F}[x]$ with $\deg(f) < \deg(h) =: n$ and $k \in \{1, \ldots, n\}$. Let $\{(r_j, s_j, t_j)\}$ be the ERS of h and f and let $j \in \mathbb{N}$ be minimal such that $\deg(r_j) < k$. Then:

1. There exist $r, t \in \mathbb{Z}$ with

$$r \equiv t\, f \mod m \quad \text{where } \deg(r_j) < k \text{ and } \deg(t_j) \leq n - k,$$

   namely $(r, t) = (r_j, t_j)$.

   If $\gcd(r_j, t_j) = 1$ then $\gcd(t_j, h) = 1$.

Theorem (Rational function reconstruction) Let $h, f \in \mathbb{F}[x]$ with $\deg(f) < \deg(h) =: n$ and $k \in \{1, \ldots, n\}$. Let $\{(r_j, s_j, t_j)\}$ be the ERS of h and f and let $j \in \mathbb{N}$ be minimal such that $\deg(r_j) < k$. Then:

1. There exist $r, t \in \mathbb{Z}$ with

$$r \equiv t\, f \mod m \quad \text{where } \deg(r_j) < k \text{ and } \deg(t_j) \leq n - k,$$

   namely $(r, t) = (r_j, t_j)$.
   If $\gcd(r_j, t_j) = 1$ then $\gcd(t_j, h) = 1$.

2. If $\frac{r}{t} \in \mathbb{F}(x)$ is a canonical form solution to

$$r \equiv t\, f \mod h \quad \Leftrightarrow \quad r\, t^{-1} \equiv f \mod h$$

   with $\deg(t) \leq n - k$, $\deg(r) < k$ and $\gcd(t, h) = 1$, then

$$(r, t) = \frac{1}{\mathrm{lc}(t_j)} \Big(r_j, t_j \Big).$$

Theorem (Rational function reconstruction) Let $h, f \in \mathbb{F}[x]$ with $\deg(f) < \deg(h) =: n$ and $k \in \{1, \ldots, n\}$. Let $\{(r_j, s_j, t_j)\}$ be the ERS of h and f and let $j \in \mathbb{N}$ be minimal such that $\deg(r_j) < k$. Then:

1. There exist $r, t \in \mathbb{Z}$ with

$$r \equiv t\, f \mod m \quad \text{where } \deg(r_j) < k \text{ and } \deg(t_j) \leq n - k,$$

   namely $(r, t) = (r_j, t_j)$.
   If $\gcd(r_j, t_j) = 1$ then $\gcd(t_j, h) = 1$.

2. If $\frac{r}{t} \in \mathbb{F}(x)$ is a canonical form solution to

$$r \equiv t\, f \mod h \quad \Leftrightarrow \quad r\, t^{-1} \equiv f \mod h$$

   with $\deg(t) \leq n - k$, $\deg(r) < k$ and $\gcd(t, h) = 1$, then

$$(r, t) = \frac{1}{\mathrm{lc}(t_j)}\Big(r_j, t_j\Big).$$

3. There is a solution as in 2 iff $\gcd(r_j, t_j) = 1$.

Theorem (Rational number reconstruction) Let $m, f \in \mathbb{N}$ with $f < m$ and $k \in \{1, \ldots, m\}$. Let $\{(r_j, s_j, t_j)\}$ be the ERS of m and f and let $j \in \mathbb{N}$ be minimal such that $r_j < k$.

1. There exist $r, t \in \mathbb{Z}$ with
$$r \equiv t\,f \mod m \quad \text{where } |m| < k \text{ and } 0 \leq t \leq \frac{m}{k},$$
namely $(r, t) = \mathsf{sgn}(t_j)(r_j, t_j)$. If $\gcd(r_j, t_j) = 1$ then $\gcd(t_j, m) = 1$.
2. If $\frac{r}{t} \in \mathbb{Z}$ is a canonical form solution to
$$r \equiv t\,f \mod m \quad \Leftrightarrow \quad r\,t^{-1} \equiv f \mod m$$
with $\deg(t) \leq \frac{m}{k}$, $\deg(r) < k$ and $\gcd(t, m) = 1$, then
$$(r, t) = \mathsf{sgn}(t_j)\Big(r_j, t_j\Big)$$
3. There is a solution as in 2 iff $\gcd(r_j, t_j) = 1$

Theorem (Rational number reconstruction) Let $m, f \in \mathbb{N}$ with $f < m$ and $k \in \{1, \ldots, m\}$. Let $\{(r_j, s_j, t_j)\}$ be the ERS of m and f and let $j \in \mathbb{N}$ be minimal such that $r_j < k$.

Define $q \in \mathbb{N}^*$ with

$$r_{j-1} - q\, r_j < k \leq r_{j-1} - (q-1) r_j \quad [q = 0 \text{ if } j = l+1]$$

Set $$r_j^* = r_{j-1} - q\, r_j, \quad t_j^* = t_{j-1} - q\, t_j.$$

1. There exist $r, t \in \mathbb{Z}$ with
$$r \equiv t\, f \mod m \quad \text{where } |m| < k \text{ and } 0 \leq t \leq \frac{m}{k},$$
namely $(r,t) = \mathrm{sgn}(t_j)(r_j, t_j)$. If $\gcd(r_j, t_j) = 1$ then $\gcd(t_j, m) = 1$.
2. If $\frac{r}{t} \in \mathbb{Z}$ is a canonical form solution to
$$r \equiv t\, f \mod m \quad \Leftrightarrow \quad r\, t^{-1} \equiv f \mod m$$
with $\deg(t) \leq \frac{m}{k}$, $\deg(r) < k$ and $\gcd(t, m) = 1$, then
$$(r, t) = \mathrm{sgn}(t_j)\Big(r_j, t_j\Big)$$
3. There is a solution as in 2 iff $\gcd(r_j, t_j) = 1$

Theorem (Rational number reconstruction) Let $m, f \in \mathbb{N}$ with $f < m$ and $k \in \{1, \ldots, m\}$. Let $\{(r_j, s_j, t_j)\}$ be the ERS of m and f and let $j \in \mathbb{N}$ be minimal such that $r_j < k$.
Define $q \in \mathbb{N}^*$ with

$$r_{j-1} - q\, r_j < k \leq r_{j-1} - (q-1) r_j \quad [q = 0 \text{ if } j = l+1]$$

Set $$r_j^* = r_{j-1} - q\, r_j, \quad t_j^* = t_{j-1} - q\, t_j.$$

1. There exist $r, t \in \mathbb{Z}$ with
$$r \equiv t\, f \mod m \quad \text{where } |m| < k \text{ and } 0 \leq t \leq \frac{m}{k},$$
namely $(r, t) = \mathrm{sgn}(t_j)(r_j, t_j)$. If $\gcd(r_j, t_j) = 1$ then $\gcd(t_j, m) = 1$.
2. If $\frac{r}{t} \in \mathbb{Z}$ is a canonical form solution to
$$r \equiv t\, f \mod m \quad \Leftrightarrow \quad r\, t^{-1} \equiv f \mod m$$
with $\deg(t) \leq \frac{m}{k}$, $\deg(r) < k$ and $\gcd(t, m) = 1$, then
$$(r, t) = \mathrm{sgn}(t_j)\Big(r_j, t_j\Big) \quad \text{or} \quad (r, t) = \mathrm{sgn}(t_j^*)\Big(r_j^*, t_j^*\Big).$$
3. There is a solution as in 2 iff $\gcd(r_j, t_j) = 1$

Theorem (Rational number reconstruction) Let $m, f \in \mathbb{N}$ with $f < m$ and $k \in \{1, \ldots, m\}$. Let $\{(r_j, s_j, t_j)\}$ be the ERS of m and f and let $j \in \mathbb{N}$ be minimal such that $r_j < k$.

Define $q \in \mathbb{N}^*$ with

$$r_{j-1} - q\, r_j < k \leq r_{j-1} - (q-1)r_j \quad [q = 0 \text{ if } j = l+1]$$

Set $$r_j^* = r_{j-1} - q\, r_j, \quad t_j^* = t_{j-1} - q\, t_j.$$

1. There exist $r, t \in \mathbb{Z}$ with
$$r \equiv t\, f \mod m \quad \text{where } |m| < k \text{ and } 0 \leq t \leq \frac{m}{k},$$
namely $(r, t) = \mathrm{sgn}(t_j)(r_j, t_j)$. If $\gcd(r_j, t_j) = 1$ then $\gcd(t_j, m) = 1$.
2. If $\frac{r}{t} \in \mathbb{Z}$ is a canonical form solution to
$$r \equiv t\, f \mod m \quad \Leftrightarrow \quad r\, t^{-1} \equiv f \mod m$$
with $\deg(t) \leq \frac{m}{k}$, $\deg(r) < k$ and $\gcd(t, m) = 1$, then
$$(r, t) = \mathrm{sgn}(t_j)\Big(r_j, t_j\Big) \quad \text{or} \quad (r, t) = \mathrm{sgn}(t_j^*)\Big(r_j^*, t_j^*\Big).$$
3. There is a solution as in 2 iff $\gcd(r_j, t_j) = 1$
or $\left(\gcd(r_j^*, t_j^*) = 1 \text{ and } |t_j^*| \leq \frac{m}{k}\right)$

Theorem (Rational number reconstruction) Let $m, f \in \mathbb{N}$ with $f < m$ and $k \in \{1, \ldots, m\}$. Let $\{(r_j, s_j, t_j)\}$ be the ERS of m and f and let $j \in \mathbb{N}$ be minimal such that $r_j < k$.

Define $q \in \mathbb{N}^*$ with

$$r_{j-1} - q\, r_j < k \le r_{j-1} - (q-1) r_j \quad [q = 0 \text{ if } j = l+1]$$

Set $$r_j^* = r_{j-1} - q\, r_j, \quad t_j^* = t_{j-1} - q\, t_j.$$

1. There exist $r, t \in \mathbb{Z}$ with
$$r \equiv t\, f \mod m \quad \text{where } |m| < k \text{ and } 0 \le t \le \frac{m}{k},$$
namely $(r, t) = \operatorname{sgn}(t_j)(r_j, t_j)$. If $\gcd(r_j, t_j) = 1$ then $\gcd(t_j, m) = 1$.
2. If $\frac{r}{t} \in \mathbb{Z}$ is a canonical form solution to
$$r \equiv t\, f \mod m \quad \Leftrightarrow \quad r\, t^{-1} \equiv f \mod m$$
with $\deg(t) \le \frac{m}{k}$, $\deg(r) < k$ and $\gcd(t, m) = 1$, then
$$(r, t) = \operatorname{sgn}(t_j)\Big(r_j, t_j\Big) \quad \text{or} \quad (r, t) = \operatorname{sgn}(t_j^*)\Big(r_j^*, t_j^*\Big).$$
3. There is a solution as in 2 iff $\gcd(r_j, t_j) = 1$
or $(\gcd(r_j^*, t_j^*) = 1$ and $|t_j^*| \le \frac{m}{k})$
4. There is at most one solution as in 2 with $|r| < \frac{k}{2}$.

Lecture 6: November 23, 2022

Corollary PP-Cont Let R be an UFD and let $f, g \in R[x]$. Then:

1. $\mathrm{pp}(f\,g) = \mathrm{pp}(f)\,\mathrm{pp}(g)$
2. $\mathrm{cont}(f\,g) = \mathrm{cont}(f)\,\mathrm{cont}(g)$

Corollary PP-Cont Let R be an UFD and let $f, g \in R[x]$. Then:

1. $\mathsf{pp}(f\, g) = \mathsf{pp}(f)\, \mathsf{pp}(g)$
2. $\mathsf{cont}(f\, g) = \mathsf{cont}(f)\, \mathsf{cont}(g)$

Corollary UFD-GCD Let R be an UFD. Let $f, g \in R[x]$ and define $h = \gcd_{R[x]}(f, g)$. Then:

1. We can split gcd-calculation problem by

$$h = \gcd_R(\mathsf{cont}(f), \mathsf{cont}(g)) \cdot \gcd_{R[x]}(\mathsf{pp}(f), \mathsf{pp}(g))$$

   In particular, h is primitive if f or g are primitive.

2. We have

$$\frac{h}{\mathrm{lc}(h)} = \gcd_{\mathbb{K}[x]}(f, g)$$

   in the quotient field $\mathbb{K} = Q(R)$.

Algorithm GCD for $R[x]$
Input: $f, g \in R[x]^*$ with UFD R and its quotient field $\mathbb{K} = Q(R)$
where one can compute gcds in R and $\mathbb{K}$ is computable.
Output: $\gcd(f, g) \in R[x]$

1. $\tilde{f} = \mathrm{pp}(f)$, $\tilde{c} = \mathrm{cont}(f)$
   $\tilde{g} = \mathrm{pp}(g)$, $\tilde{d} = \mathrm{cont}(g)$
2. Compute the following gcds in R:
   $a = \gcd_R(\tilde{c}, \tilde{d}) \in R$
   $b = \gcd_R(\mathrm{lc}(\tilde{f}), \mathrm{lc}(\tilde{g})) \in R$
3. Call the Euclidean algorithm in $\mathbb{K}[x]$ to get the monic polynomial
   $v = \gcd_{\mathbb{K}[x]}(\tilde{f}, \tilde{g}) \in \mathbb{K}[x]$
4. return $a\,\mathrm{pp}(b\,v)$

Remark: In step 1 (and most probably in step 3) we also utilize gcd computations in R.

As a consequence one obtains the following general statement.

Corollary Let $\mathbb{E} = G[x_1, \ldots, x_n]$ be a polynomial ring over a UFD G. Suppose that one can compute gcds in G and that the quotient field $Q(G)$ is computable. Then one can compute gcds in $\mathbb{E}$ and can carry out the field operations in $Q(\mathbb{E})$.

As a consequence one obtains the following general statement.

Corollary Let $\mathbb{E} = G[x_1, \dots, x_n]$ be a polynomial ring over a UFD G. Suppose that one can compute gcds in G and that the quotient field $Q(G)$ is computable. Then one can compute gcds in $\mathbb{E}$ and can carry out the field operations in $Q(\mathbb{E})$.

Proof. By induction on the number n of variables.

- If $n = 0$, the corollary holds.
- Suppose that one can compute gcds in the UFD $R = G[x_1, \dots, x_{n-1}]$ and that the field operations in $Q(R)$ can be executed.
  Then one can execute the algorithm above to compute gcds in $\mathbb{E} = R[x_n]$. In addition, one can carry out the field operations in $Q(R[x_n]) = Q(\mathbb{E})$; note that one can even calculate reduced representations in $Q(\mathbb{E})$, i.e., the numerators and denominators in $G[x_1, \dots, x_{n-1}, x_n]$ are co-prime.

As a consequence one obtains the following general statement.

Corollary Let $\mathbb{E} = G[x_1, \ldots, x_n]$ be a polynomial ring over a UFD G. Suppose that one can compute gcds in G and that the quotient field $Q(G)$ is computable. Then one can compute gcds in $\mathbb{E}$ and can carry out the field operations in $Q(\mathbb{E})$.

Proof. By induction on the number n of variables.

- If $n = 0$, the corollary holds.
- Suppose that one can compute gcds in the UFD $R = G[x_1, \ldots, x_{n-1}]$ and that the field operations in $Q(R)$ can be executed.
  Then one can execute the algorithm above to compute gcds in $\mathbb{E} = R[x_n]$. In addition, one can carry out the field operations in $Q(R[x_n]) = Q(\mathbb{E})$; note that one can even calculate reduced representations in $Q(\mathbb{E})$, i.e., the numerators and denominators in $G[x_1, \ldots, x_{n-1}, x_n]$ are co-prime.

Remark: If G is a field, one obtains much more efficient algorithms; soon we will consider, e.g., $R = G[x, y]$ for a field G.

Lecture 7: November 30, 2023

Thm. Let $f, g \in \mathbb{F}[x]^*$ with $n = \deg(f)$, $m = \deg(g)$. Then:

1. $\gcd(f, g) = 1$ iff ϕ is an isomorphism.
2. If $\gcd(f, g) = 1$, then the output

   $$s_l \qquad \text{and} \qquad t_l$$

   of the EEA is the unique solution in $\mathbb{F}[x]_{<m} \times \mathbb{F}[x]_{<n}$ of $\phi(s_l, t_l) = 1$.

$$\begin{bmatrix} f_n \\ f_{n-1} \\ \vdots \\ f_0 \\ \\ \\ \end{bmatrix}$$

$$
\begin{bmatrix}
f_n & 0 & & & \\
f_{n-1} & f_n & & & \\
\vdots & \vdots & & & \\
f_0 & \vdots & & & \\
 & f_0 & & & \\
 & & & &
\end{bmatrix}
$$

$$
\begin{array}{r c}
 & \overbrace{\qquad\qquad\qquad\qquad}^{m} \\
\begin{array}{r} m\left\{\begin{array}{c} \\ \\ \\ \\ \end{array}\right. \\ n\left\{\begin{array}{c} \\ \\ \\ \\ \\ \end{array}\right. \end{array} &
\left[\begin{array}{cccccccc}
f_n & 0 & & & & & & \\
f_{n-1} & f_n & & & & & & \\
\vdots & \vdots & \ddots & & & & & \\
 & & & f_n & & & & \\
\vdots & \vdots & & \vdots & & & & \\
f_0 & \vdots & & \vdots & & & & \\
 & f_0 & & \vdots & & & & \\
 & & \ddots & \vdots & & & & \\
 & & & f_0 & & & &
\end{array}\right]
\end{array}
$$

$$
\begin{array}{cc}
 & \overbrace{\hphantom{f_{n-1} \quad f_n \quad \cdots \quad f_n}}^{m} \\
\begin{array}{c} m\left\{\begin{array}{c} \\ \\ \\ \\ \end{array}\right. \\ n\left\{\begin{array}{c} \\ \\ \\ \\ \\ \end{array}\right. \end{array} &
\left[\begin{array}{cccccc}
f_n & 0 & & g_m & & \\
f_{n-1} & f_n & & g_{m-1} & & \\
\vdots & \vdots & \ddots & & & \\
\vdots & \vdots & f_n & g_1 & & \\
\vdots & \vdots & \vdots & g_0 & & \\
f_0 & \vdots & \vdots & & & \\
 & f_0 & \vdots & & & \\
 & & \ddots & & & \\
 & & f_0 & & &
\end{array}\right]
\end{array}
$$

$$
\begin{array}{cc}
 & \overbrace{\hphantom{f_{n-1} \quad f_n \quad\quad f_n}}^{m} \\
\begin{array}{c}
m\left\{\begin{array}{c} \\ \\ \\ \\ \end{array}\right. \\
n\left\{\begin{array}{c} \\ \\ \\ \\ \\ \end{array}\right.
\end{array}
&
\left[\begin{array}{cccccccc}
f_n & 0 & & g_m & & & & \\
f_{n-1} & f_n & & g_{m-1} & g_m & & & \\
\vdots & \vdots & \ddots & & \vdots & & & \\
\vdots & \vdots & f_n & g_1 & \vdots & & & \\
\vdots & \vdots & \vdots & g_0 & g_1 & & & \\
\vdots & \vdots & \vdots & & g_0 & & & \\
f_0 & \vdots & \vdots & & & & & \\
 & f_0 & \vdots & & & & & \\
 & & \ddots\; f_0 & & & & &
\end{array}\right]
\end{array}
$$

$$
\begin{array}{r l}
 & \begin{array}{cc} \overbrace{\hspace{3.5cm}}^{m} & \overbrace{\hspace{5cm}}^{n} \end{array} \\
\begin{array}{r} m\left\{\vphantom{\begin{array}{c}a\\a\\a\\a\end{array}}\right. \\ n\left\{\vphantom{\begin{array}{c}a\\a\\a\\a\\a\end{array}}\right. \end{array} &
\begin{bmatrix}
f_n & 0 & & g_m & & \\
f_{n-1} & f_n & & g_{m-1} & g_m & \\
\vdots & \vdots & \ddots & \vdots & \vdots & \ddots \\
\vdots & \vdots & f_n & g_1 & \vdots & \\
\vdots & \vdots & \vdots & g_0 & g_1 & \\
\vdots & \vdots & \vdots & & g_0 & g_m \\
f_0 & \vdots & \vdots & & \ddots & \vdots \\
 & f_0 & \vdots & & & \vdots \\
 & & f_0 & & & g_0
\end{bmatrix}
\end{array}
$$

Let $s = \sum_{k=0}^{m-1} a_k x^k$, $t = \sum_{k=0}^{n-1} b_k x^k$, $f = \sum_{k=0}^{n} f_k x^k$, $g = \sum_{k=0}^{m} f_k x^k$. Then

$$\boxed{s\,f + t\,g = h = \sum_{k=0}^{n+m-1} h_k\, x^k}$$

$$\Updownarrow$$

$$
\begin{array}{c c}
 & \overbrace{\hphantom{f_n \quad 0 \quad \cdots \quad f_n}}^{m} \quad \overbrace{\hphantom{g_m \quad g_m \quad \cdots \quad \cdots \quad g_m}}^{n} \\
\begin{array}{c} m\left\{\vphantom{\begin{array}{c}1\\1\\1\\1\end{array}}\right. \\ n\left\{\vphantom{\begin{array}{c}1\\1\\1\\1\\1\\1\end{array}}\right. \end{array}
&
\begin{bmatrix}
f_n & 0 & & g_m & & & \\
f_{n-1} & f_n & & g_{m-1} & g_m & & \\
\vdots & \vdots & \ddots & & \vdots & & \\
\vdots & \vdots & f_n & g_1 & \vdots & & \\
\vdots & \vdots & \vdots & g_0 & g_1 & & \\
\vdots & \vdots & \vdots & & g_0 & & g_m \\
f_0 & \vdots & \vdots & & & \ddots & \\
 & f_0 & \vdots & & & & \\
 & & \ddots & & & & \\
 & & f_0 & & & & g_0
\end{bmatrix}
\begin{bmatrix}
a_{m-1} \\ a_{m-2} \\ \vdots \\ a_0 \\ b_{n-1} \\ b_{n-2} \\ \vdots \\ b_0
\end{bmatrix}
=
\begin{bmatrix}
 \\ \\ \\ \\ \\ \\ \\ \\
\end{bmatrix}
\end{array}
$$

Let $s=\sum_{k=0}^{m-1} a_k x^k$, $t=\sum_{k=0}^{n-1} b_k x^k$, $f=\sum_{k=0}^{n} f_k x^k$, $g=\sum_{k=0}^{m} f_k x^k$.
Then

$$\boxed{s\,f+t\,g=h=\sum_{k=0}^{n+m-1} h_k\,x^k}$$

$$\Updownarrow$$

$$\begin{array}{cc}
 & \begin{array}{cc} \overbrace{\qquad\qquad\qquad\qquad}^{m} & \overbrace{\qquad\qquad\qquad\qquad\qquad\qquad}^{n} \end{array} \\
\begin{array}{c} m\left\{\begin{array}{c} \\ \\ \\ \\ \end{array}\right. \\ n\left\{\begin{array}{c} \\ \\ \\ \\ \\ \\ \end{array}\right. \end{array} &
\begin{bmatrix}
f_n & 0 & & & g_m & & & \\
f_{n-1} & f_n & & & g_{m-1} & g_m & & \\
\vdots & \vdots & \ddots & & & \vdots & & \\
\vdots & \vdots & & f_n & g_1 & \vdots & & \\
\vdots & \vdots & & \vdots & g_0 & g_1 & & \\
\vdots & \vdots & & \vdots & & g_0 & & g_m \\
f_0 & \vdots & & \vdots & & & \ddots & \\
 & f_0 & & \vdots & & & & \\
 & & \ddots & \vdots & & & & \\
 & & & f_0 & & & & g_0
\end{bmatrix}
\begin{bmatrix} a_{m-1} \\ a_{m-2} \\ \vdots \\ a_0 \\ b_{n-1} \\ b_{n-2} \\ \vdots \\ b_0 \end{bmatrix}
=
\begin{bmatrix} h_{m+n-1} \\ \\ \\ \\ \\ \\ \\ \\ \end{bmatrix}
\end{array}$$

Let $s=\sum_{k=0}^{m-1} a_k x^k$, $t=\sum_{k=0}^{n-1} b_k x^k$, $f=\sum_{k=0}^{n} f_k x^k$, $g=\sum_{k=0}^{m} f_k x^k$.
Then

$$\boxed{s\,f+t\,g=h=\sum_{k=0}^{n+m-1} h_k\,x^k}$$

$$\Updownarrow$$

$$
\begin{array}{cc}
 & \overbrace{\hphantom{f_{n-1} \quad f_n \quad \ddots \quad f_n}}^{m} \quad \overbrace{\hphantom{g_{m-1} \quad g_m \quad \ddots \quad g_m}}^{n} \\
\begin{matrix} m\left\{\begin{matrix}\\ \\ \\ \end{matrix}\right. \\ n\left\{\begin{matrix}\\ \\ \\ \\ \\ \end{matrix}\right.\end{matrix} &
\begin{bmatrix}
f_n & 0 & & & g_m & & & \\
f_{n-1} & f_n & \ddots & & g_{m-1} & g_m & & \\
\vdots & \vdots & & f_n & g_1 & \vdots & & \\
\vdots & \vdots & & \vdots & g_0 & g_1 & & \\
\vdots & \vdots & & \vdots & & g_0 & \ddots & g_m \\
f_0 & \vdots & & \vdots & & & & \\
 & f_0 & \ddots & \vdots & & & \ddots & \\
 & & & f_0 & & & & g_0
\end{bmatrix}
\end{array}
\begin{bmatrix} a_{m-1}\\ a_{m-2}\\ \vdots \\ a_0 \\ b_{n-1}\\ b_{n-2}\\ \vdots\\ b_0\end{bmatrix}
=
\begin{bmatrix} h_{m+n-1}\\ h_{m+n-2}\\ \\ \\ \\ \\ \\ \\ \end{bmatrix}
$$

Let $s = \sum_{k=0}^{m-1} a_k x^k$, $t = \sum_{k=0}^{n-1} b_k x^k$, $f = \sum_{k=0}^{n} f_k x^k$, $g = \sum_{k=0}^{m} f_k x^k$.
Then

$$\boxed{s\,f + t\,g = h = \sum_{k=0}^{n+m-1} h_k\,x^k}$$

$$\Updownarrow$$

$$
\begin{array}{cc}
 & \overbrace{\hphantom{f_{n-1}\quad f_n\quad \ddots\quad f_n}}^{m}\quad \overbrace{\hphantom{g_{m-1}\quad g_m\quad \ddots\quad \ddots\quad g_m}}^{n} \\
\begin{array}{c} m\left\{\vphantom{\begin{array}{c}1\\1\\1\\1\end{array}}\right. \\ n\left\{\vphantom{\begin{array}{c}1\\1\\1\\1\\1\\1\end{array}}\right. \end{array} &
\begin{bmatrix}
f_n & 0 & & g_m & & & \\
f_{n-1} & f_n & \ddots & g_{m-1} & g_m & & \\
\vdots & \vdots & & & \vdots & & \\
\vdots & \vdots & f_n & g_1 & \vdots & & \\
\vdots & \vdots & \vdots & g_0 & g_1 & & \\
\vdots & \vdots & \vdots & & g_0 & \ddots & g_m \\
f_0 & \vdots & \vdots & & & \ddots & \\
 & f_0 & \vdots & & & & \\
 & & \ddots & & & & \\
 & & f_0 & & & & g_0
\end{bmatrix}
\end{array}
\begin{bmatrix} a_{m-1} \\ a_{m-2} \\ \vdots \\ a_0 \\ b_{n-1} \\ b_{n-2} \\ \vdots \\ b_0 \end{bmatrix}
=
\begin{bmatrix} h_{m+n-1} \\ h_{m+n-2} \\ \vdots \\ \vdots \\ \vdots \\ h_0 \end{bmatrix}
$$

Let $s = \sum_{k=0}^{m-1} a_k x^k$, $t = \sum_{k=0}^{n-1} b_k x^k$, $f = \sum_{k=0}^{n} f_k x^k$, $g = \sum_{k=0}^{m} f_k x^k$.
Then

$$\boxed{s\,f + t\,g = h = \sum_{k=0}^{n+m-1} h_k\, x^k}$$

$$\Updownarrow$$

$$\begin{array}{cc}
 & \begin{array}{cc} \overbrace{\hspace{8em}}^{m} & \overbrace{\hspace{10em}}^{n} \end{array} \\
\begin{array}{c} m\left\{\vphantom{\begin{array}{c}1\\1\\1\\1\end{array}}\right. \\ n\left\{\vphantom{\begin{array}{c}1\\1\\1\\1\\1\end{array}}\right. \end{array} &
\underbrace{\begin{bmatrix}
f_n & 0 & & & g_m & & & \\
f_{n-1} & f_n & \ddots & & g_{m-1} & g_m & & \\
\vdots & \vdots & & f_n & g_1 & \vdots & & \\
\vdots & \vdots & & \vdots & g_0 & g_1 & & \\
\vdots & \vdots & & \vdots & & g_0 & \ddots & g_m \\
f_0 & \vdots & & \vdots & & & \ddots & \\
 & f_0 & \ddots & \vdots & & & & \\
 & & & f_0 & & & & g_0
\end{bmatrix}}_{=:\ \mathrm{Syl(f,g)}}
\begin{bmatrix} a_{m-1} \\ a_{m-2} \\ \vdots \\ a_0 \\ b_{n-1} \\ b_{n-2} \\ \vdots \\ b_0 \end{bmatrix}
=
\begin{bmatrix} h_{m+n-1} \\ h_{m+n-2} \\ \vdots \\ \\ \\ \\ \vdots \\ h_0 \end{bmatrix}
\end{array}$$

Thm. Let $f, g \in \mathbb{F}[x]^*$ with $n = \deg(f)$, $m = \deg(g)$. Then:

1. $\gcd(f, g) = 1$ iff ϕ is an isomorphism.
2. If $\gcd(f, g) = 1$, then the output

   s_l and t_l

   of the EEA is the unique solution in $\mathbb{F}[x]_{<m} \times \mathbb{F}[x]_{<n}$ of $\phi(s_l, t_l) = 1$.

Thm. Let $f, g \in \mathbb{F}[x]^*$ with $n = \deg(f)$, $m = \deg(g)$. Then:

1. $\gcd(f, g) = 1$ iff ϕ is an isomorphism.
2. If $\gcd(f, g) = 1$, then the output

   s_l and t_l

   of the EEA is the unique solution in $\mathbb{F}[x]_{<m} \times \mathbb{F}[x]_{<n}$ of $\phi(s_l, t_l) = 1$.

$$\Updownarrow$$

Corollary $\mathbb{F}[x]$-res. Let $f, g \in \mathbb{F}[x]^*$ with $n = \deg(f)$, $m = \deg(g)$. Then:

1. $\gcd(f, g) = 1$ iff $\det(S) \neq 0$.
2. If $\gcd(f, g) = 1$ and the a_i, b_i are a solution of the system above, then

   $$s_l = \sum_{k=0}^{m-1} a_k x^k \qquad \text{and} \qquad t_l = \sum_{k=0}^{n-1} b_k x^k$$

   are the Bezout coefficients in $s_l\, f + t_l\, g = 1$ also produced by the EEA.

Thm. Let $f, g \in \mathbb{F}[x]^*$ with $n = \deg(f)$, $m = \deg(g)$. Then:

1. $\gcd(f, g) = 1$ iff ϕ is an isomorphism.
2. If $\gcd(f, g) = 1$, then the output

   s_l and t_l

   of the EEA is the unique solution in $\mathbb{F}[x]_{<m} \times \mathbb{F}[x]_{<n}$ of $\phi(s_l, t_l) = 1$.

$$\Updownarrow$$

Corollary $\mathbb{F}[x]$-res. Let $f, g \in \mathbb{F}[x]^*$ with $n = \deg(f)$, $m = \deg(g)$. Then:

1. $\gcd(f, g) = 1$ iff $\det(S) \neq 0$.
2. If $\gcd(f, g) = 1$ and the a_i, b_i are a solution of the system above, then

   $$s_l = \sum_{k=0}^{m-1} a_k x^k \qquad \text{and} \qquad t_l = \sum_{k=0}^{n-1} b_k x^k$$

   are the Bezout coefficients in $s_l\, f + t_l\, g = 1$ also produced by the EEA.

Corollary UFD-res. Let R be an UFD, $f, g \in R[x]$, not both zero. Then:

$$\gcd(f, g) \in R[x] \setminus R \quad \Leftrightarrow \quad \mathrm{res}(f, g) = 0 \text{ in } R.$$

1. Coefficients bounds in $\mathbb{F}[y]$

Theorem. Let $f, g \in \mathbb{F}[x,y]$ with $n = \deg_x(f)$ and $m = \deg_x(g)$ and $\deg_y(f), \deg_y(g) \le d$. Then

$$\deg_y \mathsf{res}_x(f,g) \le (n+m)d.$$

1. Coefficients bounds in $\mathbb{F}[y]$

Theorem. Let $f, g \in \mathbb{F}[x, y]$ with $n = \deg_x(f)$ and $m = \deg_x(g)$ and $\deg_y(f), \deg_y(g) \leq d$. Then

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

2. Coefficients bounds in $\mathbb{Z}$

For $f = \sum_{n=0}^{d} f_n\, x^n \in \mathbb{C}[x]$ define the 2-norm

$$\|f\|_2 = \Big(\sum_{n=0}^{d} |f_n|^2 \Big)^{1/2}, \quad |a| = (a \cdot \bar{a})^{1/2} \in \mathbb{R}$$

and the max-norm

$$\|f\|_\infty = \max\{|f_n| : 0 \leq n \leq d\}.$$

Note:

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

1. Coefficients bounds in $\mathbb{F}[y]$

Theorem. Let $f, g \in \mathbb{F}[x, y]$ with $n = \deg_x(f)$ and $m = \deg_x(g)$ and $\deg_y(f), \deg_y(g) \leq d$. Then

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

2. Coefficients bounds in $\mathbb{Z}$

For $f = \sum_{n=0}^{d} f_n\, x^n \in \mathbb{C}[x]$ define the 2-norm

$$\|f\|_2 = \Big(\sum_{n=0}^{d} |f_n|^2\Big)^{1/2}, \quad |a| = (a \cdot \bar{a})^{1/2} \in \mathbb{R}$$

and the max-norm

$$\|f\|_\infty = \max\{|f_n| : 0 \leq n \leq d\}.$$

Note:

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

Theorem. Let $f, g \in \mathbb{Z}[x]$ with $n = \deg(f)$ and $m = \deg(g)$. Then

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

Lemma. Let $f, g \in R[x]^*$ and I be an ideal in R with $I \neq R$. Suppose that[1] $\overline{\mathrm{lc}(f)} \in R/I$ is not a zero-divisor. Then:

1. $\overline{\mathsf{res}(f, g)} = \bar{0} \quad \Leftrightarrow \quad \mathsf{res}(\bar{f}, \bar{g}) = \bar{0}$.
2. If R/I is a UFD then

$$\overline{\mathsf{res}(f, g)} = \bar{0} \quad \Leftrightarrow \quad \gcd(\bar{f}, \bar{g}) \notin R/I.$$

Proof. (1) will be settled as a homework.

[1] Note that $\deg(f) = \deg(\bar{f})$ and thus $\overline{\mathrm{lc}(f)} = \mathrm{lc}(\bar{f})$ does not hold in general.

Lemma. Let $f, g \in R[x]^*$ and I be an ideal in R with $I \neq R$. Suppose that[1] $\overline{\mathrm{lc}(f)} \in R/I$ is not a zero-divisor. Then:

1. $\overline{\mathsf{res}(f, g)} = \bar{0} \quad \Leftrightarrow \quad \mathsf{res}(\bar{f}, \bar{g}) = \bar{0}$.
2. If R/I is a UFD then

$$\overline{\mathsf{res}(f, g)} = \bar{0} \quad \Leftrightarrow \quad \gcd(\bar{f}, \bar{g}) \notin R/I.$$

Proof. (1) will be settled as a homework. (2) follows by

$$\overline{\mathsf{res}(f, g)} = \bar{0} \qquad \stackrel{(1)}{\Longleftrightarrow} \qquad \mathsf{res}(\bar{f}, \bar{g}) = \bar{0}$$

[1]Note that $\deg(f) = \deg(\bar{f})$ and thus $\overline{\mathrm{lc}(f)} = \mathrm{lc}(\bar{f})$ does not hold in general.

Lemma. Let $f, g \in R[x]^*$ and I be an ideal in R with $I \neq R$. Suppose that[1] $\overline{\mathrm{lc}(f)} \in R/I$ is not a zero-divisor. Then:

1. $\overline{\mathsf{res}(f,g)} = \bar{0} \quad \Leftrightarrow \quad \mathsf{res}(\bar{f},\bar{g}) = \bar{0}$.
2. If R/I is a UFD then

$$\overline{\mathsf{res}(f,g)} = \bar{0} \quad \Leftrightarrow \quad \gcd(\bar{f},\bar{g}) \notin R/I.$$

Proof. (1) will be settled as a homework. (2) follows by

$$\overline{\mathsf{res}(f,g)} = \bar{0} \quad \overset{(1)}{\Longleftrightarrow} \quad \mathsf{res}(\bar{f},\bar{g}) = \bar{0} \quad \overset{\text{Cor. UFD-res}}{\Longleftrightarrow} \quad \gcd(\bar{f},\bar{g}) \notin R/I.$$

[1] Note that $\deg(f) = \deg(\bar{f})$ and thus $\overline{\mathrm{lc}(f)} = \mathrm{lc}(\bar{f})$ does not hold in general.

GCD-Theorem. Let R be an ED, $f, g \in R[x]^*$ and $p \in R$ be prime with $p \nmid \gcd_R(\mathrm{lc}(f), \mathrm{lc}(g))$; let $\mathbb{F} = R/\langle p \rangle$ be its quotient field. Then:

(i) $\mathrm{lc}(\gcd_{R[x]}(f, g)) \mid \gcd_R(\mathrm{lc}(f), \mathrm{lc}(g))$.

GCD-Theorem. Let R be an ED, $f, g \in R[x]^*$ and $p \in R$ be prime with $p \nmid \gcd_R(\mathrm{lc}(f), \mathrm{lc}(g))$; let $\mathbb{F} = R/\langle p \rangle$ be its quotient field. Then:

(i) $\mathrm{lc}(\gcd_{R[x]}(f, g)) \mid \gcd_R(\mathrm{lc}(f), \mathrm{lc}(g))$.

(ii) $\deg(\gcd_{\mathbb{F}[x]}(\bar{f}, \bar{g})) \geq \deg(\gcd_{R[x]}(f, g))$.

GCD-Theorem. Let R be an ED, $f, g \in R[x]^*$ and $p \in R$ be prime with $p \nmid \gcd_R(\mathrm{lc}(f), \mathrm{lc}(g))$; let $\mathbb{F} = R/\langle p \rangle$ be its quotient field. Then:

(i) $\mathrm{lc}(\gcd_{R[x]}(f, g)) \mid \gcd_R(\mathrm{lc}(f), \mathrm{lc}(g))$.

(ii) $\deg(\gcd_{\mathbb{F}[x]}(\bar{f}, \bar{g})) \geq \deg(\gcd_{R[x]}(f, g))$.

(iii)
$$\deg(\gcd_{\mathbb{F}[x]}(\bar{f}, \bar{g})) = \deg(\gcd_{R[x]}(f, g))$$
$$\Updownarrow_1$$
$$\overline{\mathrm{lc}(\gcd_{R[x]}(f, g))} \cdot \gcd_{\mathbb{F}[x]}(\bar{f}, \bar{g}) = \overline{\gcd_{R[x]}(f, g)}$$
$$\Updownarrow_2$$
$$p \nmid_R \mathsf{res}\left(\frac{f}{\gcd_{R[x]}(f, g)}, \frac{g}{\gcd_{R[x]}(f, g)}\right)$$

Lecture 9: November 14, 2023

Algorithm modGCD for $\mathbb{F}[x,y]$ (big prime version)
Input: primitive $f, g \in \mathbb{F}[x,y] = R[x]$ with $R = \mathbb{F}[y]$ where $n = \deg_x(f) \geq \deg_x(g) \geq 1$ and $\deg_y(f), \deg_y(g) \leq d$ for some $d \in \mathbb{N}$.
Output: $h = \gcd(f,g) \in \mathbb{F}[x,y]$

1. Compute $b := \gcd_{\mathbb{F}[y]}(\mathrm{lc}_x(f), \mathrm{lc}_x(g)) \in \mathbb{F}[y]$ and set $\ell = d + 1 + \deg_y(b)$
2. repeat
3. choose a random monic irreducible $p \in \mathbb{F}[y]$ with $\deg_y(p) = \ell$
4. call the EEA for $\bar{f}, \bar{g} \in \mathbb{E}[x]$ over the field $\mathbb{E} = \mathbb{F}[y]/\langle p \rangle$ to get the monic $v \in R[x]$ with $\deg_y(v) < \ell$ such that $\bar{v} = \gcd(\bar{f}, \bar{g}) \in \mathbb{E}[x]$.
5. Compute $w, f^*, g^* \in R[x]$ with $\deg_y(w), \deg_y(f^*), \deg_y(g^*) < \ell$ where
$$\bar{w} = \overline{b\,v}, \quad \bar{f^*} = \frac{\bar{f}}{\bar{v}}, \quad \bar{g^*} = \frac{\bar{g}}{\bar{v}}$$
6. until $\deg_y(f^* w) = \deg_y(bf)$ and $\deg_y(g^* w) = \deg_y(bg)$
7. return $\mathrm{pp}_x(w)$

Theorem. Let $f, g \in R[x]$ be primitive where $R = \mathbb{F}[y]$. Let $h = \gcd_{R[x]}(f, g)$ and $r = \mathsf{res}_x(f/h, g/h) \in R$.
Let $w \in \mathbb{F}[x]$ as calculated in the algorithm above after one loop. Then:

1. $\deg(r) \leq 2nd$ where $n = \deg_x(f) \geq \deg_x(g) \geq 1$ and $d \geq \deg_y(f), \deg_y(g)$.
2. $p \nmid_R r$ if and only if the halting condition holds.
3. If $p \nmid_R r$ then $h = \mathsf{pp}_x(w)$.

For $f = \sum_{n=0}^{d} f_n\, x^n \in \mathbb{C}[x]$ define the q-norm ($q \in \mathbb{N}^*$)

$$\|f\|_q = \Big(\sum_{n=0}^{d} |f_n|^q\Big)^{1/q}, \quad |a| = (a \cdot \bar{a})^{1/2} \in \mathbb{R}$$

and the max-norm

$$\|f\|_\infty = \max\{|f_n| : 0 \le n \le d\}.$$

For $f = \sum_{n=0}^{d} f_n \, x^n \in \mathbb{C}[x]$ define the q-norm $(q \in \mathbb{N}^*)$

$$\|f\|_q = \Big(\sum_{n=0}^{d} |f_n|^q \Big)^{1/q}, \quad |a| = (a \cdot \bar{a})^{1/2} \in \mathbb{R}$$

and the max-norm

$$\|f\|_\infty = \max\{|f_n| : 0 \le n \le d\}.$$

Note (Ex. 18):

$$\|f\|_\infty \le \|f\|_2 \le (n+1)^{1/2} \, \|f\|_\infty$$
$$\|f\|_2 \le \|f\|_1 \le (n+1) \, \|f\|_\infty$$

For $f = \sum_{n=0}^{d} f_n\, x^n \in \mathbb{C}[x]$ define the q-norm ($q \in \mathbb{N}^*$)

$$\|f\|_q = \Big(\sum_{n=0}^{d} |f_n|^q \Big)^{1/q}, \quad |a| = (a \cdot \bar{a})^{1/2} \in \mathbb{R}$$

and the max-norm

$$\|f\|_\infty = \max\{|f_n| : 0 \le n \le d\}.$$

Note (Ex. 18):

$$\|f\|_\infty \le \|f\|_2 \le (n+1)^{1/2}\, \|f\|_\infty$$
$$\|f\|_2 \le \|f\|_1 \le (n+1)\, \|f\|_\infty$$

Theorem Mignotte. Let $f, g, h \in \mathbb{Z}[x]$ with $\deg(f) = n$, $\deg(g) = m$ and $\deg(h) = k$. Suppose that $g\, h \mid f$. Then

$\|g\|_\infty\, \|h\|_\infty \le \|g\|_2\, \|h\|_2$

For $f = \sum_{n=0}^{d} f_n \, x^n \in \mathbb{C}[x]$ define the q-norm ($q \in \mathbb{N}^*$)

$$\|f\|_q = \Big(\sum_{n=0}^{d} |f_n|^q \Big)^{1/q}, \quad |a| = (a \cdot \bar{a})^{1/2} \in \mathbb{R}$$

and the max-norm

$$\|f\|_\infty = \max\{|f_n| : 0 \le n \le d\}.$$

Note (Ex. 18):

$$\begin{aligned} \|f\|_\infty &\le \|f\|_2 \le (n+1)^{1/2} \, \|f\|_\infty \\ \|f\|_2 &\le \|f\|_1 \le (n+1) \, \|f\|_\infty \end{aligned}$$

Theorem Mignotte. Let $f, g, h \in \mathbb{Z}[x]$ with $\deg(f) = n$, $\deg(g) = m$ and $\deg(h) = k$. Suppose that $g\,h \mid f$. Then

$$\|g\|_\infty \, \|h\|_\infty \le \|g\|_2 \, \|h\|_2 \le \|g\|_1 \, \|h\|_1$$

For $f = \sum_{n=0}^{d} f_n\, x^n \in \mathbb{C}[x]$ define the q-norm ($q \in \mathbb{N}^*$)

$$\|f\|_q = \Big(\sum_{n=0}^{d} |f_n|^q\Big)^{1/q}, \quad |a| = (a \cdot \bar{a})^{1/2} \in \mathbb{R}$$

and the max-norm

$$\|f\|_\infty = \max\{|f_n| : 0 \le n \le d\}.$$

Note (Ex. 18):

$$\|f\|_\infty \le \|f\|_2 \le (n+1)^{1/2}\, \|f\|_\infty$$
$$\|f\|_2 \le \|f\|_1 \le (n+1)\, \|f\|_\infty$$

Theorem Mignotte. Let $f, g, h \in \mathbb{Z}[x]$ with $\deg(f) = n$, $\deg(g) = m$ and $\deg(h) = k$. Suppose that $g\,h \mid f$. Then

$$\|g\|_\infty\, \|h\|_\infty \le \|g\|_2\, \|h\|_2 \le \|g\|_1\, \|h\|_1 \overset{\text{Ex.}}{\le} 2^{m+k}\, \|f\|_2$$

For $f = \sum_{n=0}^{d} f_n\, x^n \in \mathbb{C}[x]$ define the q-norm ($q \in \mathbb{N}^*$)

$$\|f\|_q = \Big(\sum_{n=0}^{d} |f_n|^q \Big)^{1/q}, \quad |a| = (a \cdot \bar{a})^{1/2} \in \mathbb{R}$$

and the max-norm

$$\|f\|_\infty = \max\{|f_n| : 0 \le n \le d\}.$$

Note (Ex. 18):

$$\begin{aligned} \|f\|_\infty &\le \|f\|_2 \le (n+1)^{1/2}\, \|f\|_\infty \\ \|f\|_2 &\le \|f\|_1 \le (n+1)\, \|f\|_\infty \end{aligned}$$

Theorem Mignotte. Let $f, g, h \in \mathbb{Z}[x]$ with $\deg(f) = n$, $\deg(g) = m$ and $\deg(h) = k$. Suppose that $g\,h \mid f$. Then

$$\|g\|_\infty\, \|h\|_\infty \le \|g\|_2\, \|h\|_2 \le \|g\|_1\, \|h\|_1 \overset{\text{Ex.}}{\le} 2^{m+k}\, \|f\|_2 \le (n+1)^{1/2} 2^{m+k}\, \|f\|_\infty$$

For $f = \sum_{n=0}^{d} f_n\, x^n \in \mathbb{C}[x]$ define the q-norm ($q \in \mathbb{N}^*$)

$$\|f\|_q = \Big(\sum_{n=0}^{d} |f_n|^q \Big)^{1/q}, \quad |a| = (a \cdot \bar{a})^{1/2} \in \mathbb{R}$$

and the max-norm

$$\|f\|_\infty = \max\{|f_n| : 0 \le n \le d\}.$$

Note (Ex. 18):

$$\|f\|_\infty \le \|f\|_2 \le (n+1)^{1/2}\, \|f\|_\infty$$
$$\|f\|_2 \le \|f\|_1 \le (n+1)\, \|f\|_\infty$$

Theorem Mignotte. Let $f, g, h \in \mathbb{Z}[x]$ with $\deg(f) = n$, $\deg(g) = m$ and $\deg(h) = k$. Suppose that $g\, h \mid f$. Then

$$\|g\|_\infty\, \|h\|_\infty \le \|g\|_2\, \|h\|_2 \le \|g\|_1\, \|h\|_1 \overset{\text{Ex.}}{\le} 2^{m+k}\, \|f\|_2 \le (n+1)^{1/2} 2^{m+k}\, \|f\|_\infty$$

Special case ($g = 1$):

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

Corollary. Let $f, g \in \mathbb{Z}[x]$ with $n = \deg(f) \geq \deg(g) \geq 1$ and $\|f\|_\infty, \|g\|_\infty \leq A$. Then

$$\|\gcd(f,g)\|_\infty \leq (n+1)^{1/2} 2^n A.$$

Lemma. Let $f, g \in \mathbb{Z}[x]$ with $\|f\|_\infty, \|g\|_\infty < \frac{p}{2}$. Then

$$\bar{f} = \bar{g} \quad \Leftrightarrow \quad f = g.$$

Recall: **Algorithm modGCD** for $\mathbb{F}[x,y]$ (big prime version)
Input: primitive $f, g \in \mathbb{F}[x,y] = R[x]$ with $R = \mathbb{F}[y]$ where $n = \deg_x(f) \geq \deg_x(g) \geq 1$ and $\deg_y(f), \deg_y(g) \leq d$ for some $d \in \mathbb{N}$.
Output: $h = \gcd(f,g) \in \mathbb{F}[x,y]$

1. Compute $b := \gcd_{\mathbb{F}[y]}(\mathrm{lc}_x(f), \mathrm{lc}_x(g)) \in \mathbb{F}[y]$ and set $\ell = d + 1 + \deg_y(b)$
2. repeat
3. choose a random monic irreducible $p \in \mathbb{F}[y]$ with $\deg_y(p) = \ell$
4. call the EEA for $\bar{f}, \bar{g} \in \mathbb{E}[x]$ over the field $\mathbb{E} = \mathbb{F}[y]/\langle p \rangle$ to get the monic $v \in R[x]$ with $\deg_y(v) < \ell$ such that $\bar{v} = \gcd(\bar{f}, \bar{g}) \in \mathbb{E}[x]$.
5. Compute $w, f^*, g^* \in R[x]$ with $\deg_y(w), \deg_y(f^*), \deg_y(g^*) < \ell$ where
$$\bar{w} = \overline{b\,v}, \quad \bar{f^*} = \frac{\bar{f}}{\bar{v}}, \quad \bar{g^*} = \frac{\bar{g}}{\bar{v}}$$
6. until $\deg_y(f^* w) = \deg_y(bf)$ and $\deg_y(g^* w) = \deg_y(bg)$
7. return $\mathrm{pp}_x(w)$

Algorithm modGCD for $\mathbb{Z}[x]$ (big prime version)
Input: primitive $f, g \in \mathbb{Z}[x]$ with $n = \deg(f) \geq \deg(g) \geq 1$ and $\|f\|_\infty, \|g\|_\infty \leq A$ for some $A \in \mathbb{N}$.
Output: $h = \gcd(f, g) \in \mathbb{Z}[x]$

1. Compute $b := \gcd_{\mathbb{Z}}(\mathrm{lc}(f), \mathrm{lc}(g))$ and set $B = (n+1)^{1/2} 2^n A\, b$
2. repeat
3. choose a random prime p with $2B < p$
4. call the EEA for $\bar{f}, \bar{g} \in \mathbb{Z}_p[x]$ over the finite field $\mathbb{Z}_p$ to get the monic $v \in R[x]$ with $\|v\|_\infty < p/2$ such that $\bar{v} = \gcd(\bar{f}, \bar{g}) \in \mathbb{Z}_p[x]$.
5. Compute $w, f^*, g^* \in \mathbb{Z}[x]$ with $\|w\|_\infty, \|f^*\|_\infty, \|g^*\|_\infty < p/2$ where

$$\bar{w} = \overline{b\, v}, \quad \bar{f^*} = \frac{\bar{f}}{\bar{v}}, \quad \bar{g^*} = \frac{\bar{g}}{\bar{v}}$$

6. until $\|f^*\|_1 \|w\|_1 \leq B$ and $\|g^*\|_1 \|w\|_1 \leq B$
7. return $\mathrm{pp}(w)$

Recall: **Theorem.** Let $f, g \in R[x]$ be primitive where $R = \mathbb{F}[y]$. Let $h = \gcd_{R[x]}(f, g)$ and $r = \mathsf{res}_x(f/h, g/h) \in R$.
Let $w \in \mathbb{F}[x]$ as calculated in the algorithm above after one loop. Then:

1. $\deg(r) \leq 2nd$ where $n = \deg_x(f) \geq \deg_x(g) \geq 1$ and $d \geq \deg_y(f), \deg_y(g)$.
2. $p \nmid_R r$ if and only if the halting condition holds.
3. If $p \nmid_R r$ then $h = \mathsf{pp}_x(w)$.

Theorem. Let $f, g \in \mathbb{Z}[x]$ be primitive. Let $h = \gcd_{\mathbb{Z}[x]}(f, g)$ and $r = \mathsf{res}(f/h, g/h) \in \mathbb{Z}$; note that $\mathrm{lc}(h) > 0$.
Let $w \in \mathbb{Z}[x]$ as calculated in the algorithm above after one loop. Then:

[2] There is the improved version $|r| \leq (n+1)^n A^{2n}$.

Recall: **Theorem.** Let $f, g \in R[x]$ be primitive where $R = \mathbb{F}[y]$. Let $h = \gcd_{R[x]}(f, g)$ and $r = \mathsf{res}_x(f/h, g/h) \in R$.
Let $w \in \mathbb{F}[x]$ as calculated in the algorithm above after one loop. Then:

1. $\deg(r) \leq 2nd$ where $n = \deg_x(f) \geq \deg_x(g) \geq 1$ and $d \geq \deg_y(f), \deg_y(g)$.
2. $p \nmid_R r$ if and only if the halting condition holds.
3. If $p \nmid_R r$ then $h = \mathsf{pp}_x(w)$.

Theorem. Let $f, g \in \mathbb{Z}[x]$ be primitive. Let $h = \gcd_{\mathbb{Z}[x]}(f, g)$ and $r = \mathsf{res}(f/h, g/h) \in \mathbb{Z}$; note that $\mathrm{lc}(h) > 0$.
Let $w \in \mathbb{Z}[x]$ as calculated in the algorithm above after one loop. Then:

1. $|r| \leq (n+1)^n A^{2n} 4^n$ where[2] $n = \deg(f) \geq \deg(g) \geq 1$ and $A \geq \|f\|_\infty, \|g\|_\infty$.

[2] There is the improved version $|r| \leq (n+1)^n A^{2n}$.

Recall: **Theorem.** Let $f, g \in R[x]$ be primitive where $R = \mathbb{F}[y]$. Let $h = \gcd_{R[x]}(f, g)$ and $r = \mathrm{res}_x(f/h, g/h) \in R$.
Let $w \in \mathbb{F}[x]$ as calculated in the algorithm above after one loop. Then:

1. $\deg(r) \leq 2nd$ where $n = \deg_x(f) \geq \deg_x(g) \geq 1$ and $d \geq \deg_y(f), \deg_y(g)$.
2. $p \nmid_R r$ if and only if the halting condition holds.
3. If $p \nmid_R r$ then $h = \mathrm{pp}_x(w)$.

Theorem. Let $f, g \in \mathbb{Z}[x]$ be primitive. Let $h = \gcd_{\mathbb{Z}[x]}(f, g)$ and $r = \mathrm{res}(f/h, g/h) \in \mathbb{Z}$; note that $\mathrm{lc}(h) > 0$.
Let $w \in \mathbb{Z}[x]$ as calculated in the algorithm above after one loop. Then:

1. $|r| \leq (n+1)^n A^{2n} 4^n$ where[2] $n = \deg(f) \geq \deg(g) \geq 1$ and $A \geq \|f\|_\infty, \|g\|_\infty$.
2. $p \nmid_{\mathbb{Z}} r$ if and only if the halting condition holds.

[2]There is the improved version $|r| \leq (n+1)^n A^{2n}$.

Recall: **Theorem.** Let $f, g \in R[x]$ be primitive where $R = \mathbb{F}[y]$. Let $h = \gcd_{R[x]}(f, g)$ and $r = \mathsf{res}_x(f/h, g/h) \in R$.
Let $w \in \mathbb{F}[x]$ as calculated in the algorithm above after one loop. Then:

1. $\deg(r) \leq 2nd$ where $n = \deg_x(f) \geq \deg_x(g) \geq 1$ and $d \geq \deg_y(f), \deg_y(g)$.
2. $p \nmid_R r$ if and only if the halting condition holds.
3. If $p \nmid_R r$ then $h = \mathsf{pp}_x(w)$.

Theorem. Let $f, g \in \mathbb{Z}[x]$ be primitive. Let $h = \gcd_{\mathbb{Z}[x]}(f, g)$ and $r = \mathsf{res}(f/h, g/h) \in \mathbb{Z}$; note that $\mathrm{lc}(h) > 0$.
Let $w \in \mathbb{Z}[x]$ as calculated in the algorithm above after one loop. Then:

1. $|r| \leq (n+1)^n A^{2n} 4^n$ where[2] $n = \deg(f) \geq \deg(g) \geq 1$ and $A \geq \|f\|_\infty, \|g\|_\infty$.
2. $p \nmid_{\mathbb{Z}} r$ if and only if the halting condition holds.
3. If $p \nmid_{\mathbb{Z}} r$ then $h = \mathsf{pp}(w)$.

---

[2] There is the improved version $|r| \leq (n+1)^n A^{2n}$.

Algorithm modGCD for $\mathbb{F}[x,y]$ (small prime version)
Input: primitive $f, g \in \mathbb{F}[x,y] = R[x]$ with $R = \mathbb{F}[y]$ where $n = \deg_x(f) \geq \deg_x(g) \geq 1$ and $\deg_y(f), \deg_y(g) \leq d$ for some $d \in \mathbb{N}$.
Output: $h = \gcd(f,g) \in \mathbb{F}[x,y]$

1. Compute $b := \gcd_{\mathbb{F}[y]}(\mathrm{lc}_x(f), \mathrm{lc}_x(g)) \in \mathbb{F}[y]$ and set $\ell = d + 1 + \deg_y(b)$
2. repeat
3. choose a set $S \subseteq \mathbb{F}$ of ℓ evaluation points u with $b(u) \neq 0$.
4. for each $u \in S$ call the EEA to get $v_u = \gcd_{\mathbb{F}[x]}(f(x,u), g(x,u))$

7. Compute by interpolation each coefficient in $\mathbb{F}[y]$ of the polynomials $w, f^*, g^* \in R[x]$ with $\deg_y(w), \deg_y(f^*), \deg_y(g^*) < \ell$ such that for each $u \in S$ we have
$$w(x,u) = b(u)v_u, \quad f^*(x,u) = \frac{f(x,u)}{v_u}, \quad g^*(x,u) = \frac{g(x,u)}{v_u}.$$
8. until $\deg_y(f^* w) = \deg_y(bf)$ and $\deg_y(g^* w) = \deg_y(bg)$
9. return $\mathrm{pp}_x(w)$

Algorithm modGCD for $\mathbb{F}[x, y]$ (small prime version)
Input: primitive $f, g \in \mathbb{F}[x, y] = R[x]$ with $R = \mathbb{F}[y]$ where $n = \deg_x(f) \geq \deg_x(g) \geq 1$ and $\deg_y(f), \deg_y(g) \leq d$ for some $d \in \mathbb{N}$.
Output: $h = \gcd(f, g) \in \mathbb{F}[x, y]$

1. Compute $b := \gcd_{\mathbb{F}[y]}(\mathrm{lc}_x(f), \mathrm{lc}_x(g)) \in \mathbb{F}[y]$ and set $\ell = d + 1 + \deg_y(b)$
2. repeat
3. choose a set $S \subseteq \mathbb{F}$ of 2ℓ evaluation points u with $b(u) \neq 0$.
4. for each $u \in S$ call the EEA to get $v_u = \gcd_{\mathbb{F}[x]}(f(x, u), g(x, u))$

7. Compute by interpolation each coefficient in $\mathbb{F}[y]$ of the polynomials $w, f^*, g^* \in R[x]$ with $\deg_y(w), \deg_y(f^*), \deg_y(g^*) < \ell$ such that for each $u \in S$ we have
$$w(x, u) = b(u)v_u, \quad f^*(x, u) = \frac{f(x,u)}{v_u}, \quad g^*(x, u) = \frac{g(x,u)}{v_u}.$$
8. until $\deg_y(f^* w) = \deg_y(bf)$ and $\deg_y(g^* w) = \deg_y(bg)$
9. return $\mathrm{pp}_x(w)$

Algorithm modGCD for $\mathbb{F}[x,y]$ (small prime version)
Input: primitive $f, g \in \mathbb{F}[x,y] = R[x]$ with $R = \mathbb{F}[y]$ where $n = \deg_x(f) \geq \deg_x(g) \geq 1$ and $\deg_y(f), \deg_y(g) \leq d$ for some $d \in \mathbb{N}$.
Output: $h = \gcd(f,g) \in \mathbb{F}[x,y]$

1. Compute $b := \gcd_{\mathbb{F}[y]}(\mathrm{lc}_x(f), \mathrm{lc}_x(g)) \in \mathbb{F}[y]$ and set $\ell = d + 1 + \deg_y(b)$
2. repeat
3. choose a set $S \subseteq \mathbb{F}$ of 2ℓ evaluation points u with $b(u) \neq 0$.
4. for each $u \in S$ call the EEA to get $v_u = \gcd_{\mathbb{F}[x]}(f(x,u), g(x,u))$
5. $\lambda = \min\{\deg(v_u) \mid u \in S\}$ and refine $S := \{u \in S \mid \deg(v_u) = \lambda\}$
6. if $|S| \geq \ell$ then remove $|S| - \ell$ points from S else goto 3.
7. Compute by interpolation each coefficient in $\mathbb{F}[y]$ of the polynomials $w, f^*, g^* \in R[x]$ with $\deg_y(w), \deg_y(f^*), \deg_y(g^*) < \ell$ such that for each $u \in S$ we have
$$w(x,u) = b(u)v_u, \quad f^*(x,u) = \frac{f(x,u)}{v_u}, \quad g^*(x,u) = \frac{g(x,u)}{v_u}.$$
8. until $\deg_y(f^*w) = \deg_y(bf)$ and $\deg_y(g^*w) = \deg_y(bg)$
9. return $\mathrm{pp}_x(w)$

Recall: **Theorem.** Let $f, g \in R[x]$ be primitive where $R = \mathbb{F}[y]$. Let $h = \gcd_{R[x]}(f, g)$ and $r = \mathsf{res}_x(f/h, g/h) \in R$.
Let $w \in \mathbb{F}[x]$ as calculated in the algorithm above after one loop. Then:

1. $\deg(r) \leq 2nd$ where $n = \deg_x(f) \geq \deg_x(g) \geq 1$ and $d \geq \deg_y(f), \deg_y(g)$.
2. $p \nmid_R r$ if and only if the halting condition holds.
3. If $p \nmid_R r$ then $h = \mathsf{pp}_x(w)$.

Theorem. Let $f, g \in R[x]$ be primitive where $R = \mathbb{F}[y]$. Let $h = \gcd_{R[x]}(f, g)$ and $r = \mathsf{res}_x(f/h, g/h) \in R$.
Let $w \in \mathbb{F}[x]$ as calculated in the algorithm above after one loop using the ℓ given points from S. Then:

Recall: **Theorem.** Let $f, g \in R[x]$ be primitive where $R = \mathbb{F}[y]$. Let $h = \gcd_{R[x]}(f, g)$ and $r = \mathsf{res}_x(f/h, g/h) \in R$.
Let $w \in \mathbb{F}[x]$ as calculated in the algorithm above after one loop. Then:

1. $\deg(r) \leq 2nd$ where $n = \deg_x(f) \geq \deg_x(g) \geq 1$ and $d \geq \deg_y(f), \deg_y(g)$.
2. $p \nmid_R r$ if and only if the halting condition holds.
3. If $p \nmid_R r$ then $h = \mathsf{pp}_x(w)$.

Theorem. Let $f, g \in R[x]$ be primitive where $R = \mathbb{F}[y]$. Let $h = \gcd_{R[x]}(f, g)$ and $r = \mathsf{res}_x(f/h, g/h) \in R$.
Let $w \in \mathbb{F}[x]$ as calculated in the algorithm above after one loop using the ℓ given points from S. Then:

1. $\deg(r) \leq 2nd$ where $n = \deg_x(f) \geq \deg_x(g) \geq 1$ and $d \geq \deg_y(f), \deg_y(g)$.

Recall: **Theorem.** Let $f, g \in R[x]$ be primitive where $R = \mathbb{F}[y]$. Let $h = \gcd_{R[x]}(f, g)$ and $r = \mathrm{res}_x(f/h, g/h) \in R$.
Let $w \in \mathbb{F}[x]$ as calculated in the algorithm above after one loop. Then:

1. $\deg(r) \leq 2nd$ where $n = \deg_x(f) \geq \deg_x(g) \geq 1$ and $d \geq \deg_y(f), \deg_y(g)$.
2. $p \nmid_R r$ if and only if the halting condition holds.
3. If $p \nmid_R r$ then $h = \mathrm{pp}_x(w)$.

Theorem. Let $f, g \in R[x]$ be primitive where $R = \mathbb{F}[y]$. Let $h = \gcd_{R[x]}(f, g)$ and $r = \mathrm{res}_x(f/h, g/h) \in R$.
Let $w \in \mathbb{F}[x]$ as calculated in the algorithm above after one loop using the ℓ given points from S. Then:

1. $\deg(r) \leq 2nd$ where $n = \deg_x(f) \geq \deg_x(g) \geq 1$ and $d \geq \deg_y(f), \deg_y(g)$.
2. $r(s) \neq 0$ for all $s \in S$ if and only if the halting condition holds.

Recall: **Theorem.** Let $f, g \in R[x]$ be primitive where $R = \mathbb{F}[y]$. Let $h = \gcd_{R[x]}(f, g)$ and $r = \text{res}_x(f/h, g/h) \in R$.
Let $w \in \mathbb{F}[x]$ as calculated in the algorithm above after one loop. Then:

1. $\deg(r) \leq 2nd$ where $n = \deg_x(f) \geq \deg_x(g) \geq 1$ and $d \geq \deg_y(f), \deg_y(g)$.
2. $p \nmid_R r$ if and only if the halting condition holds.
3. If $p \nmid_R r$ then $h = \text{pp}_x(w)$.

Theorem. Let $f, g \in R[x]$ be primitive where $R = \mathbb{F}[y]$. Let $h = \gcd_{R[x]}(f, g)$ and $r = \text{res}_x(f/h, g/h) \in R$.
Let $w \in \mathbb{F}[x]$ as calculated in the algorithm above after one loop using the ℓ given points from S. Then:

1. $\deg(r) \leq 2nd$ where $n = \deg_x(f) \geq \deg_x(g) \geq 1$ and $d \geq \deg_y(f), \deg_y(g)$.
2. $r(s) \neq 0$ for all $s \in S$ if and only if the halting condition holds.
3. If $r(s) \neq 0$ for all $s \in S$ then $h = \text{pp}_x(w)$.

Algorithm modGCD for $\mathbb{Z}[x]$ (small prime version)
Input: primitive $f, g \in \mathbb{Z}[x]$ with $n = \deg(f) \geq \deg(g) \geq 1$
and $\|f\|_\infty, \|g\|_\infty \leq A$ for some $A \in \mathbb{N}$.
Output: $h = \gcd(f, g) \in \mathbb{Z}[x]$

1. Compute $b := \gcd_{\mathbb{Z}}(\mathrm{lc}(f), \mathrm{lc}(g))$ and set $B = (n+1)^{1/2} 2^n A\, b$.
   Take $\ell = \log_2(2B + 1)$
2. repeat
3. choose a set S of 2ℓ primes p with $p \nmid b$.
4. for each $p \in S$ call the EEA to get the monic $v_p \in \mathbb{Z}[x]$ where the coefficients are from $\{0, \ldots, p-1\}$ with $\bar{v}_p = \gcd_{\mathbb{Z}_p[x]}(\bar{f}, \bar{g})$
5. $\lambda = \min\{\deg(v_p) \mid p \in S\}$ and refine $S := \{p \in S \mid \deg(v_p) = \lambda\}$
6. if $|S| \geq \ell$ then remove $|S| - \ell$ points from S else goto 3.
7. Compute by CRA the coefficients of the polynomials $w, f^*, g^* \in \mathbb{Z}[x]$ with $\|w\|_\infty, \|f^*\|_\infty, \|g^*\|_\infty < (\prod_{p \in S} p)/2$ s.t. for each $p \in S$ we have
$$\bar{w} = \overline{b\, v_p}, \quad \bar{f^*} = \frac{\bar{f}}{\bar{v_p}}, \quad \bar{g^*} = \frac{\bar{g}}{\bar{v_p}} \quad \text{(reduction mod } p\text{)}$$
8. until $\|f^*\|_1 \|w\|_1 \leq B$ and $\|g^*\|_1 \|w\|_1 \leq B$
9. return pp(w)

Recall: **Theorem.** Let $f, g \in \mathbb{Z}[x]$ be primitive. Let $h = \gcd_{\mathbb{Z}[x]}(f, g)$ and $r = \mathrm{res}(f/h, g/h) \in \mathbb{Z}$; note that $\mathrm{lc}(h) > 0$.
Let $w \in \mathbb{Z}[x]$ as calculated in the algorithm above after one loop. Then:

1. $|r| \leq (n+1)^n A^{2n}$ where $n = \deg(f) \geq \deg(g) \geq 1$ and $A \geq \|f\|_\infty, \|g\|_\infty$.
2. $p \nmid_{\mathbb{Z}} r$ if and only if the halting condition holds.
3. If $p \nmid_{\mathbb{Z}} r$ then $h = \mathrm{pp}(w)$.

Theorem. Let $f, g \in \mathbb{Z}[x]$ be primitive. Let $h = \gcd_{\mathbb{Z}[x]}(f, g)$ and $r = \mathrm{res}(f/h, g/h) \in \mathbb{Z}$; note that $\mathrm{lc}(h) > 0$.
Let $w \in \mathbb{Z}[x]$ as calculated in the algorithm above after one loop using the ℓ primes given in S. Then:

Recall: **Theorem.** Let $f, g \in \mathbb{Z}[x]$ be primitive. Let $h = \gcd_{\mathbb{Z}[x]}(f, g)$ and $r = \text{res}(f/h, g/h) \in \mathbb{Z}$; note that $\mathrm{lc}(h) > 0$.
Let $w \in \mathbb{Z}[x]$ as calculated in the algorithm above after one loop. Then:

1. $|r| \leq (n+1)^n A^{2n}$ where $n = \deg(f) \geq \deg(g) \geq 1$ and $A \geq \|f\|_\infty, \|g\|_\infty$.
2. $p \nmid_{\mathbb{Z}} r$ if and only if the halting condition holds.
3. If $p \nmid_{\mathbb{Z}} r$ then $h = \text{pp}(w)$.

Theorem. Let $f, g \in \mathbb{Z}[x]$ be primitive. Let $h = \gcd_{\mathbb{Z}[x]}(f, g)$ and $r = \text{res}(f/h, g/h) \in \mathbb{Z}$; note that $\mathrm{lc}(h) > 0$.
Let $w \in \mathbb{Z}[x]$ as calculated in the algorithm above after one loop using the ℓ primes given in S. Then:

1. $|r| \leq (n+1)^n A^{2n}$ where $n = \deg(f) \geq \deg(g) \geq 1$ and $A \geq \|f\|_\infty, \|g\|_\infty$.

Recall: **Theorem.** Let $f, g \in \mathbb{Z}[x]$ be primitive. Let $h = \gcd_{\mathbb{Z}[x]}(f, g)$ and $r = \text{res}(f/h, g/h) \in \mathbb{Z}$; note that $\mathrm{lc}(h) > 0$.
Let $w \in \mathbb{Z}[x]$ as calculated in the algorithm above after one loop. Then:

1. $|r| \leq (n+1)^n A^{2n}$ where $n = \deg(f) \geq \deg(g) \geq 1$ and $A \geq \|f\|_\infty, \|g\|_\infty$.
2. $p \nmid_{\mathbb{Z}} r$ if and only if the halting condition holds.
3. If $p \nmid_{\mathbb{Z}} r$ then $h = \text{pp}(w)$.

Theorem. Let $f, g \in \mathbb{Z}[x]$ be primitive. Let $h = \gcd_{\mathbb{Z}[x]}(f, g)$ and $r = \text{res}(f/h, g/h) \in \mathbb{Z}$; note that $\mathrm{lc}(h) > 0$.
Let $w \in \mathbb{Z}[x]$ as calculated in the algorithm above after one loop using the ℓ primes given in S. Then:

1. $|r| \leq (n+1)^n A^{2n}$ where $n = \deg(f) \geq \deg(g) \geq 1$ and $A \geq \|f\|_\infty, \|g\|_\infty$.
2. $p \nmid_{\mathbb{Z}} r$ for all $p \in S$ if and only if the halting condition holds.

Recall: **Theorem.** Let $f, g \in \mathbb{Z}[x]$ be primitive. Let $h = \gcd_{\mathbb{Z}[x]}(f, g)$ and $r = \mathrm{res}(f/h, g/h) \in \mathbb{Z}$; note that $\mathrm{lc}(h) > 0$.
Let $w \in \mathbb{Z}[x]$ as calculated in the algorithm above after one loop. Then:

1. $|r| \leq (n+1)^n A^{2n}$ where $n = \deg(f) \geq \deg(g) \geq 1$ and $A \geq \|f\|_\infty, \|g\|_\infty$.
2. $p \nmid_{\mathbb{Z}} r$ if and only if the halting condition holds.
3. If $p \nmid_{\mathbb{Z}} r$ then $h = \mathrm{pp}(w)$.

Theorem. Let $f, g \in \mathbb{Z}[x]$ be primitive. Let $h = \gcd_{\mathbb{Z}[x]}(f, g)$ and $r = \mathrm{res}(f/h, g/h) \in \mathbb{Z}$; note that $\mathrm{lc}(h) > 0$.
Let $w \in \mathbb{Z}[x]$ as calculated in the algorithm above after one loop using the ℓ primes given in S. Then:

1. $|r| \leq (n+1)^n A^{2n}$ where $n = \deg(f) \geq \deg(g) \geq 1$ and $A \geq \|f\|_\infty, \|g\|_\infty$.
2. $p \nmid_{\mathbb{Z}} r$ for all $p \in S$ if and only if the halting condition holds.
3. If $p \nmid_{\mathbb{Z}} r$ for all $p \in S$ then $h = \mathrm{pp}(w)$.

Lecture 8: December 7, 2023

Definition. A monomial order on $\mathbb{F}[\mathbf{x}]$ is a relation $<$ on $\mathbb{N}^n$ such that

1. $<$ is a total order;
2. For all $\alpha, \beta, \gamma \in \mathbb{N}^n$:

$$\alpha < \beta \qquad \Rightarrow \qquad \alpha + \gamma < \beta + \gamma$$

3. $<$ is well-ordered, i.e.,

$$\forall S \subseteq \mathbb{N}^n \; \exists m \in S \; \forall s \in S : \; m \leq s$$

$$\Updownarrow$$

$$\forall s \in \mathbb{N}^n : \; s \geq \mathbf{0}.$$

Definition. A monomial order on $\mathbb{F}[\mathbf{x}]$ is a relation $<$ on $\mathbb{N}^n$ such that

1. $<$ is a total order;
2. For all $\alpha, \beta, \gamma \in \mathbb{N}^n$:

$$\alpha < \beta \qquad \Rightarrow \qquad \alpha + \gamma < \beta + \gamma$$

3. $<$ is well-ordered, i.e.,

$$\forall S \subseteq \mathbb{N}^n \; \exists m \in S \; \forall s \in S : \; m \leq s$$

$$\Updownarrow$$

$$\forall s \in \mathbb{N}^n : \; s \geq \mathbf{0}.$$

Lemma Deg. Let $<$ be a monomial order on $\mathbb{F}[\mathbf{x}]$ and $f, g \in \mathbb{F}[\mathbf{x}]^*$. Then:

1. $\deg(f\,g) = \deg(f) + \deg(g)$;
2. If $f + g \neq 0$ then

$$\deg(f + g) \leq \max(\deg(f), \deg(g));$$

   equality holds if $\deg(f) \neq \deg(g)$.

Algorithm PolynomialReduce

Input: $f, g_1, \ldots, g_s \in \mathbb{F}[x_1, \ldots, x_n] =: R$ with a monomial order $<$.

Output: $r, q_1, \ldots, q_s \in R$ with $f = r + q_1\, g_1 + \cdots + q_s\, g_s$

1. $r = 0$, $p = f$, $q_i = 0$ for $1 \leq i \leq s$
2. while $p \neq 0$ do
3. if $\mathsf{lt}(g_i) \mid \mathsf{lt}(p)$ for some $1 \leq i \leq s$ then
4. choose such an i and set $q_i = q_i + \frac{\mathsf{lt}(p_i)}{\mathsf{lt}(g_i)}$

   $$p = p - \frac{\mathsf{lt}(p_i)}{\mathsf{lt}(f_i)} g_i$$
5. else
6. $r = r + \mathsf{lt}(p)$, $p = p - \mathsf{lt}(p)$
7. fi
8. od
9. return $q_1, \ldots, q_s$, r

Remark: If $s = n = 1$ then $q_1 = \mathrm{quot}\,(f, g_1)$ and $r = \mathrm{rem}\,(f, g_1)$

Algorithm PolynomialReduce

Input: $f, g_1, \ldots, g_s \in \mathbb{F}[x_1, \ldots, x_n] =: R$ with a monomial order $<$.

Output: $r, q_1, \ldots, q_s \in R$ with $f = r + q_1\, g_1 + \cdots + q_s\, g_s$ where no monomial in r is divisible by $\mathrm{lt}(g_i)$ for all $1 \le i \le s$.

1. $r = 0$, $p = f$, $q_i = 0$ for $1 \le i \le s$
2. while $p \ne 0$ do
3. if $\mathrm{lt}(g_i) \mid \mathrm{lt}(p)$ for some $1 \le i \le s$ then
4. choose such an i and set $q_i = q_i + \frac{\mathrm{lt}(p_i)}{\mathrm{lt}(g_i)}$

   $$p = p - \frac{\mathrm{lt}(p_i)}{\mathrm{lt}(f_i)} g_i$$
5. else
6. $r = r + \mathrm{lt}(p)$, $p = p - \mathrm{lt}(p)$
7. fi
8. od
9. return $q_1, \ldots, q_s$, r

Remark: If $s = n = 1$ then $q_1 = \mathrm{quot}\,(f, g_1)$ and $r = \mathrm{rem}\,(f, g_1)$

Lemma Mon. Let $I \trianglelefteq \mathbb{F}[\mathbf{x}]$ that is generated by a set M of monomials, and let h be a monomial. Then:

$$h \in I \qquad \Leftrightarrow \qquad \exists m \in M : \, m \mid h.$$

Lecture 11: January 11, 2024

Definition. Let $I \trianglelefteq \mathbb{F}[\mathbf{x}]$, $G \subseteq I$ finite, $<$ monomial order.

$$\langle \mathsf{LT}(I) \rangle = \langle \mathsf{LT}(G) \rangle \qquad \Leftrightarrow: \quad G \text{ is a GB of I}$$

Proposition Red. Let $I \trianglelefteq \mathbb{F}[\mathbf{x}]$, $G \subseteq I$ finite, $<$ monomial order. Then:

$$\langle \mathsf{LT}(I) \rangle = \langle \mathsf{LT}(G) \rangle \qquad \text{(i.e., } G \text{ is a GB of I)}$$

$$\Updownarrow$$

$$\forall p \in I \ \exists g \in G : \ \mathsf{lt}(g) \mid \mathsf{lt}(p).$$

Proposition Red. Let $I \trianglelefteq \mathbb{F}[\mathbf{x}]$, $G \subseteq I$ finite, $<$ monomial order. Then:

$$\langle \mathsf{LT}(I) \rangle = \langle \mathsf{LT}(G) \rangle \qquad \text{(i.e., } G \text{ is a GB of I)}$$
$$\Updownarrow$$
$$\forall p \in I \ \exists g \in G : \ \mathsf{lt}(g) \mid \mathsf{lt}(p).$$

Lemma. Let G be a GB for $I \trianglelefteq \mathbb{F}[\mathbf{x}]$ w.r.t. $<$ and $f \in \mathbb{F}[\mathbf{x}]$.
Then there is a unique $r \in \mathbb{F}[\mathbf{x}]$:

1. $f - r \in I$;
2. no term of r is divisible by any monomial in $\mathsf{LT}(G)$.

Proposition Red. Let $I \trianglelefteq \mathbb{F}[\mathbf{x}]$, $G \subseteq I$ finite, $<$ monomial order. Then:

$$\langle \mathsf{LT}(I) \rangle = \langle \mathsf{LT}(G) \rangle \qquad \text{(i.e., } G \text{ is a GB of I)}$$
$$\Updownarrow$$
$$\forall p \in I \; \exists g \in G : \; \mathsf{lt}(g) \mid \mathsf{lt}(p).$$

Lemma. Let G be a GB for $I \trianglelefteq \mathbb{F}[\mathbf{x}]$ w.r.t. $<$ and $f \in \mathbb{F}[\mathbf{x}]$.
Then there is a unique $r \in \mathbb{F}[\mathbf{x}]$:

1. $f - r \in I$;
2. no term of r is divisible by any monomial in $\mathsf{LT}(G)$.

Notation: For $G \subseteq \mathbb{F}[\mathbf{x}]$ finite, $f \in \mathbb{F}[\mathbf{x}]$,

$$f \operatorname{rem} G = \mathsf{PolynomialReduce}(f, G) = r \in \mathbb{F}[\mathbf{x}].$$

Proposition Red. Let $I \trianglelefteq \mathbb{F}[\mathbf{x}]$, $G \subseteq I$ finite, $<$ monomial order. Then:

$$\langle \mathsf{LT}(I) \rangle = \langle \mathsf{LT}(G) \rangle \qquad \text{(i.e., } G \text{ is a GB of I)}$$
$$\Updownarrow$$
$$\forall p \in I\ \exists g \in G:\ \mathsf{lt}(g) \mid \mathsf{lt}(p).$$

Lemma. Let G be a GB for $I \trianglelefteq \mathbb{F}[\mathbf{x}]$ w.r.t. $<$ and $f \in \mathbb{F}[\mathbf{x}]$.
Then there is a unique $r \in \mathbb{F}[\mathbf{x}]$:

1. $f - r \in I$;
2. no term of r is divisible by any monomial in $\mathsf{LT}(G)$.

Notation: For $G \subseteq \mathbb{F}[\mathbf{x}]$ finite, $f \in \mathbb{F}[\mathbf{x}]$,

$$f \operatorname{rem} G = \mathsf{PolynomialReduce}(f, G) = r \in \mathbb{F}[\mathbf{x}].$$

Lemma Red. Let G be a GB for $I \trianglelefteq \mathbb{F}[\mathbf{x}]$ w.r.t. $<$. Then

$$\forall f \in \mathbb{F}[\mathbf{x}]: \quad f \in I \qquad \Longleftrightarrow \qquad f \operatorname{rem} G = 0. \qquad (*)$$

Proposition Red. Let $I \trianglelefteq \mathbb{F}[\mathbf{x}]$, $G \subseteq I$ finite, $<$ monomial order. Then:

$$\langle \mathsf{LT}(I) \rangle = \langle \mathsf{LT}(G) \rangle \qquad \text{(i.e., } G \text{ is a GB of I)}$$
$$\Updownarrow$$
$$\forall p \in I \; \exists g \in G : \; \mathsf{lt}(g) \mid \mathsf{lt}(p).$$

Lemma. Let G be a GB for $I \trianglelefteq \mathbb{F}[\mathbf{x}]$ w.r.t. $<$ and $f \in \mathbb{F}[\mathbf{x}]$.
Then there is a unique $r \in \mathbb{F}[\mathbf{x}]$:

1. $f - r \in I$;
2. no term of r is divisible by any monomial in $\mathsf{LT}(G)$.

Notation: For $G \subseteq \mathbb{F}[\mathbf{x}]$ finite, $f \in \mathbb{F}[\mathbf{x}]$,

$$f \operatorname{rem} G = \mathsf{PolynomialReduce}(f, G) = r \in \mathbb{F}[\mathbf{x}].$$

Lemma Red. Let G be a GB for $I \trianglelefteq \mathbb{F}[\mathbf{x}]$ w.r.t. $<$. Then

$$\forall f \in \mathbb{F}[\mathbf{x}] : \quad f \in I \qquad \Longleftrightarrow \qquad f \operatorname{rem} G = 0. \qquad (*)$$

Proposition Red0. Let $I \trianglelefteq \mathbb{F}[\mathbf{x}]$, $G \subseteq I$ finite, $<$ monomial order. Then
G is a GB of I $\;\Leftrightarrow\;$ property (*) holds.

Lemma LT. Define

$$g_1, \ldots, g_s \in \mathbb{F}[\mathbf{x}]$$

$$f = \sum_{i=1}^{s} c_i \, \mathbf{x}^{\alpha_i} g_i \in \mathbb{F}[\mathbf{x}] \qquad \begin{array}{l} \alpha_1, \ldots, \alpha_s \in \mathbb{N}^n \\ c_1, \ldots, c_s \in \mathbb{F}^* \end{array}$$

Lemma LT. Define

$$f = \sum_{i=1}^{s} c_i \, \mathbf{x}^{\alpha_i} g_i \in \mathbb{F}[\mathbf{x}] \qquad \begin{array}{l} g_1, \ldots, g_s \in \mathbb{F}[\mathbf{x}] \\ \alpha_1, \ldots, \alpha_s \in \mathbb{N}^n \\ c_1, \ldots, c_s \in \mathbb{F}^* \end{array}$$

with the following extra properties.

1. There is $\delta \in \mathbb{N}^n$ such that for all $1 \leq i \leq n$:

$$\alpha_i + \deg(g_i) = \delta \qquad i.e., \qquad \deg(x^{\alpha_i} g_i) = \delta$$

Lemma LT. Define

$$f = \sum_{i=1}^{s} c_i \, \mathbf{x}^{\alpha_i} g_i \in \mathbb{F}[\mathbf{x}] \qquad \begin{array}{l} g_1, \ldots, g_s \in \mathbb{F}[\mathbf{x}] \\ \alpha_1, \ldots, \alpha_s \in \mathbb{N}^n \\ c_1, \ldots, c_s \in \mathbb{F}^* \end{array}$$

with the following extra properties.

1. There is $\delta \in \mathbb{N}^n$ such that for all $1 \leq i \leq n$:
$$\alpha_i + \deg(g_i) = \delta \qquad i.e., \qquad \deg(x^{\alpha_i} g_i) = \delta$$
2. we have
$$\deg(f) < \delta.$$

Lemma LT. Define

$$f = \sum_{i=1}^{s} c_i \, \mathbf{x}^{\alpha_i} g_i \in \mathbb{F}[\mathbf{x}] \qquad \begin{array}{l} g_1, \ldots, g_s \in \mathbb{F}[\mathbf{x}] \\ \alpha_1, \ldots, \alpha_s \in \mathbb{N}^n \\ c_1, \ldots, c_s \in \mathbb{F}^* \end{array}$$

with the following extra properties.

1. There is $\delta \in \mathbb{N}^n$ such that for all $1 \leq i \leq n$:

$$\alpha_i + \deg(g_i) = \delta \qquad i.e., \qquad \deg(x^{\alpha_i} g_i) = \delta$$

2. we have

$$\deg(f) < \delta.$$

Then for $\gamma_{i,j} \in \mathbb{N}^n$ with $\mathbf{x}^{\gamma_{i,j}} = \mathrm{lcm}(\mathsf{lm}(g_i), \mathsf{lm}(g_j))$ with $1 \leq i < j \leq s$:

(a) $\delta - \gamma_{i,j} \in \mathbb{N}^n$, i.e., $\mathbf{x}^{\delta - \gamma_{i,j}} \in \mathbb{F}[\mathbf{x}]$

Lemma LT. Define

$$f = \sum_{i=1}^{s} c_i\, \mathbf{x}^{\alpha_i} g_i \in \mathbb{F}[\mathbf{x}] \qquad \begin{array}{l} g_1, \ldots, g_s \in \mathbb{F}[\mathbf{x}] \\ \alpha_1, \ldots, \alpha_s \in \mathbb{N}^n \\ c_1, \ldots, c_s \in \mathbb{F}^* \end{array}$$

with the following extra properties.

1. There is $\delta \in \mathbb{N}^n$ such that for all $1 \le i \le n$:

$$\alpha_i + \deg(g_i) = \delta \qquad i.e., \qquad \deg(x^{\alpha_i} g_i) = \delta$$

2. we have

$$\deg(f) < \delta.$$

Then for $\gamma_{i,j} \in \mathbb{N}^n$ with $\mathbf{x}^{\gamma_{i,j}} = \operatorname{lcm}(\mathsf{lm}(g_i), \mathsf{lm}(g_j))$ with $1 \le i < j \le s$:

(a) $\delta - \gamma_{i,j} \in \mathbb{N}^n$, i.e., $\mathbf{x}^{\delta - \gamma_{i,j}} \in \mathbb{F}[\mathbf{x}]$

(b) $\deg(\mathbf{x}^{\delta - \gamma_{i,j}} S(g_i, g_j)) < \delta$

Lemma LT. Define

$$f = \sum_{i=1}^{s} c_i \, \mathbf{x}^{\alpha_i} g_i \in \mathbb{F}[\mathbf{x}] \qquad \begin{array}{l} g_1, \ldots, g_s \in \mathbb{F}[\mathbf{x}] \\ \alpha_1, \ldots, \alpha_s \in \mathbb{N}^n \\ c_1, \ldots, c_s \in \mathbb{F}^* \end{array}$$

with the following extra properties.

1. There is $\delta \in \mathbb{N}^n$ such that for all $1 \leq i \leq n$:

$$\alpha_i + \deg(g_i) = \delta \qquad i.e., \qquad \deg(x^{\alpha_i} g_i) = \delta$$

2. we have

$$\deg(f) < \delta.$$

Then for $\gamma_{i,j} \in \mathbb{N}^n$ with $\mathbf{x}^{\gamma_{i,j}} = \operatorname{lcm}(\mathsf{lm}(g_i), \mathsf{lm}(g_j))$ with $1 \leq i < j \leq s$:

(a) $\delta - \gamma_{i,j} \in \mathbb{N}^n$, i.e., $\mathbf{x}^{\delta - \gamma_{i,j}} \in \mathbb{F}[\mathbf{x}]$

(b) $\deg(\mathbf{x}^{\delta - \gamma_{i,j}} S(g_i, g_j)) < \delta$

(c) There exist $c_{i,j} \in \mathbb{F}$ such that

$$f = \sum_{1 \leq i < j \leq s} c_{i,j} \mathbf{x}^{\delta - \gamma_{i,j}} S(g_i, g_j)$$

Lecture 11: January 18, 2024

Algorithm GetGroebnerBasis (Buchberger's algorithm)
Input: $f_1, \ldots, f_s \in \mathbb{F}[x_1, \ldots, x_n]$ with a monomial order $<$.
Output: A Gröbner basis G of $\langle f_1, \ldots, f_s \rangle$ w.r.t. $<$.

1. Set $G = \{f_1, \ldots, f_s\}$
2. repeat do
3. $S = \{\}$
       (*let $G = \{g_1, \ldots, g_\sigma\}$*)
4.   for all i, j with $1 \leq i < j < \sigma$ do
5. $r =$ PolynomialReduce$(S(g_i, g_j), G) = S(g_i, g_j)$ rem G
6.   if $r \neq 0$ then $S = S \cup \{r\}$ fi
7.   od
8.   if $S = \{\}$ then return G fi
9. $G = G \cup S$
10. od
11. return G

Definition. Let G be a GB of $I \trianglelefteq \mathbb{F}[\mathbf{x}]$ w.r.t. $<$. G is called reduced iff

1. $\mathrm{lc}(g) = 1$ for all $g \in G$.
2. for all $g \in G$ no monomial of g lies in $\langle \mathsf{LT}(G \setminus \{g\}) \rangle$.

Theorem ReducedGB.
There is an algorithm which computes for a given GB G of $I \trianglelefteq \mathbb{F}[\mathbf{x}]$ w.r.t. $<$ a reduced GB G' of I w.r.t. $<$.

Theorem UniqueGB.
Let G_1 and G_2 be two reduced GB of $I \trianglelefteq \mathbb{F}[\mathbf{x}]$ w.r.t. $<$. Then $G_1 = G_2$.

Lecture 12: January 25, 2024

Theorem-Summary. $I \trianglelefteq \mathbb{F}[\mathbf{x}]$, $G = \{g_1, \ldots, g_s\} \subseteq I$, $<$ monomial order. Then the following statements are equivalent.

1. $\langle \mathsf{LT}(I) \rangle = \langle \mathsf{LT}(G) \rangle$, i.e., G is a GB of I

Theorem-Summary. $I \trianglelefteq \mathbb{F}[\mathbf{x}]$, $G = \{g_1, \ldots, g_s\} \subseteq I$, $<$ monomial order. Then the following statements are equivalent.

1. $\langle \mathsf{LT}(I) \rangle = \langle \mathsf{LT}(G) \rangle$, i.e., G is a GB of I
2. $\forall p \in I \; \exists g \in G : \; \mathsf{lt}(g) \mid \mathsf{lt}(p)$.

Theorem-Summary. $I \trianglelefteq \mathbb{F}[\mathbf{x}]$, $G = \{g_1, \ldots, g_s\} \subseteq I$, $<$ monomial order. Then the following statements are equivalent.

1. $\langle \mathsf{LT}(I) \rangle = \langle \mathsf{LT}(G) \rangle$, i.e., G is a GB of I
2. $\forall p \in I \; \exists g \in G : \; \mathsf{lt}(g) \mid \mathsf{lt}(p)$.
3. $\forall f \in \mathbb{F}[\mathbf{x}]$:
$$f \in I \iff f \operatorname{rem} G = 0.$$

Theorem-Summary. $I \trianglelefteq \mathbb{F}[\mathbf{x}]$, $G = \{g_1, \ldots, g_s\} \subseteq I$, $<$ monomial order. Then the following statements are equivalent.

1. $\langle \mathsf{LT}(I) \rangle = \langle \mathsf{LT}(G) \rangle$, i.e., G is a GB of I
2. $\forall p \in I \; \exists g \in G : \; \mathsf{lt}(g) \mid \mathsf{lt}(p)$.
3. $\forall f \in \mathbb{F}[\mathbf{x}]$:
$$f \in I \iff f \operatorname{rem} G = 0.$$
4. `PolynomialReduce` implements a function,
i.e., for each input there is a unique output.
("don't care nondeterministic" $\to$ "don't know nondeterministic")

Theorem-Summary. $I \trianglelefteq \mathbb{F}[\mathbf{x}]$, $G = \{g_1, \ldots, g_s\} \subseteq I$, $<$ monomial order. Then the following statements are equivalent.

1. $\langle \mathsf{LT}(I) \rangle = \langle \mathsf{LT}(G) \rangle$, i.e., G is a GB of I
2. $\forall p \in I \; \exists g \in G : \; \mathsf{lt}(g) \mid \mathsf{lt}(p)$.
3. $\forall f \in \mathbb{F}[\mathbf{x}]$:
$$f \in I \iff f \operatorname{rem} G = 0.$$
4. `PolynomialReduce` implements a function,
   i.e., for each input there is a unique output.
   ("don't care nondeterministic" $\to$ "don't know nondeterministic")
5. $\forall 1 \leq i < j \leq s : \; S(g_i, g_j) \operatorname{rem} G = 0$

Theorem-Summary. $I \trianglelefteq \mathbb{F}[\mathbf{x}]$, $G = \{g_1, \ldots, g_s\} \subseteq I$, $<$ monomial order. Then the following statements are equivalent.

1. $\langle \mathsf{LT}(I) \rangle = \langle \mathsf{LT}(G) \rangle$, i.e., G is a GB of I
2. $\forall p \in I\ \exists g \in G :\ \mathsf{lt}(g) \mid \mathsf{lt}(p)$.
3. $\forall f \in \mathbb{F}[\mathbf{x}]$:
$$f \in I \iff f \operatorname{rem} G = 0.$$
4. `PolynomialReduce` implements a function,
i.e., for each input there is a unique output.
("don't care nondeterministic" $\rightarrow$ "don't know nondeterministic")
5. $\forall 1 \leq i < j \leq s :\ S(g_i, g_j) \operatorname{rem} G = 0$
6. $B = \{b + I \mid b \in \hat{B}\}$ forms a basis of the $\mathbb{F}$-vector space $\mathbb{F}[\mathbf{x}]/I$ with
$$\hat{B} = \{m \in [\mathbf{x}] \mid m \operatorname{rem} G = m\}.$$

Applications

1. Computation in the quotient ring $R = \mathbb{F}[\mathbf{x}]/I$
2. Ideal membership
3. Test ideal equality
4. Elimination property
5. Finding zeros
6. Radical ideal membership
7. Ideal operations (and the corresponding operations of varieties)
   (a) sum of ideals
   (b) product of ideals
   (c) intersection of ideals

$\vdots$