Gröbner bases & cryptographic applications

Prof. dr. ir. Frederik Vercauteren

COSIC, KU Leuven

Computer Algebra for Cryptography (B-KUL-H0E74A)

2022-2023

Polynomial systems

Resultant

Ideals and varieties

Gröbner bases

Cryptographic applications

Polynomial systems of equations

- Let F be a field, and let $R = F[x_1, \ldots, x_n]$ be the ring of polynomials with coefficients in F in n variables.
- What is the solution set described by a system of m polynomial equations:

$$\begin{cases} f_1(x_1, \ldots, x_n) = 0 \\ \vdots \\ f_m(x_1, \ldots, x_n) = 0 \end{cases}$$

- Any solutions? Finite/infinite? Where do they live (in F or some extension)?
- **Def:** The set of solutions

$$V_F(f_1, \ldots, f_m) = \{(a_1, \ldots, a_n) \in F^n \mid f_i(a_1, \ldots, a_n) = 0, \forall i\}$$

is called the **affine variety** (over F) defined by $f_1, \ldots, f_m$.

Example I: linear polynomials

- If $f_1, \ldots, f_m$ are linear:

$$\begin{cases} f_1(x_1, \ldots, x_n) & = & a_{1,1}x_1 + \ldots + a_{1,n}x_n - b_1 & = & 0 \\ & \vdots & & & \\ f_m(x_1, \ldots, x_n) & = & a_{m,1}x_m + \ldots + a_{m,n}x_n - b_m & = & 0 \end{cases}$$

- Solutions iff

$$\operatorname{rank}\begin{pmatrix} a_{1,1} & \ldots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{m,1} & \ldots & a_{m,n} \end{pmatrix} = \operatorname{rank}\begin{pmatrix} a_{1,1} & \ldots & a_{1,n} & b_1 \\ \vdots & \ddots & \vdots & \vdots \\ a_{m,1} & \ldots & a_{m,n} & b_m \end{pmatrix}.$$

- Infinitely many solutions iff this rank $< n$.
- If solutions exist, they do exist over F.
- Efficient determination via **Gaussian elimination**.

Example II: univariate polynomials

- Case $m = 1$:

$$f(x) = x^d + a_{d-1}x^{d-1} + \ldots + a_0 = 0, \qquad a_i \in F$$

- At most d solutions.
- Solutions may exist over extension of F only!
  - Example: $f(x) = x^2 + 1$ over $F = \mathbb{R}$ vs. $F = \mathbb{C}$
- Finding solutions via dedicated **root finding algorithms**
- Case $m > 1$ reduces to case $m = 1$:

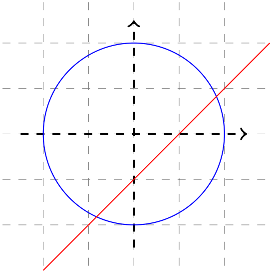
$$\begin{cases} f_1(x) = 0 \\ f_2(x) = 0 \end{cases} \quad \Leftrightarrow \quad \gcd(f_1(x), f_2(x)) = 0$$

  Proof: by XGCD there exist $\alpha(x), \beta(x) \in F[x]$ such that

$$\gcd(f_1(x), f_2(x)) = \alpha(x)f_1(x) + \beta(x)f_2(x).$$

Another example

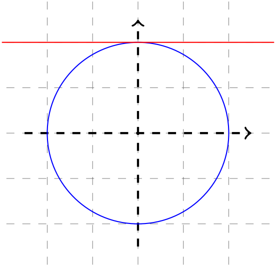
- Let $f_1(x, y) = x^2 + y^2 - 4$ and $f_2 = x - y - 1$, then we can plot the solution set to each:



- Eliminate $y = x - 1 \Rightarrow 2x^2 - 2x - 3 = 0 \Rightarrow x = (1 \pm \sqrt{7})/2$
- No solutions over $\mathbb{Q}$, two solutions over $\mathbb{R}$, so $V_{\mathbb{Q}}(f_1, f_2) = \emptyset$, $V_{\mathbb{R}}(f_1, f_2) = \{(\frac{1+\sqrt{7}}{2}, \frac{-1+\sqrt{7}}{2}), (\frac{1-\sqrt{7}}{2}, \frac{-1-\sqrt{7}}{2})\}$
- Approach: eliminate variables to reduce to univariate case

Another example

- Let $f_1(x, y) = x^2 + y^2 - 4$ and $f_2 = y - 2$, then we can plot the solution set to each:



- System reduces to $y = 2$ and $x^2 = 0$, so $V_{\mathbb{Q}}(f_1, f_2) = \{(0, 2)\}$
- Remark: equations contain more information, namely multiplicity, than corresponding variety ("fat points")
- MAGMA :

```
> QQ := Rationals();
> R<x,y> := PolynomialRing(QQ, 2);
> Variety(Ideal([x^2 + y^2 - 4,y - 2]));
[ <0,2>]
```

Polynomial systems

Resultant

Ideals and varieties

Gröbner bases

Cryptographic applications

Bivariate polynomials: elimination approach

- Given $f(x,y), g(x,y) \in F[x,y]$, find the solutions to

$$f(x,y) = 0 \quad \text{and} \quad g(x,y) = 0 \tag{1}$$

- Can try to "eliminate y" by finding a combination

$$a(x,y)f(x,y) + b(x,y)g(x,y) = h(x)$$

- Any common solution (x_0, y_0) to (1) will satisfy $h(x_0) = 0$ (converse does not necessarily apply, but can test solutions)

Bivariate polynomials: GCD approach

- Consider $f(x,y), g(x,y)$ as univariate polynomials in y with coefficients in the field $F(x)$

$$f(x,y) = \sum_{i=0}^{d_{f,y}} f_i(x) y^i \qquad g(x,y) = \sum_{i=0}^{d_{g,y}} g_i(x) y^i$$

- Compute univariate GCD using Euclid to obtain

$$d(x,y) = \alpha(x,y) f(x,y) + \beta(x,y) g(x,y)$$

- Multiply by common denominator $\gamma(x)$ (only depends on x)

$$d(x,y)\gamma(x) = a(x,y) f(x,y) + b(x,y) g(x,y)$$

If $deg_y(d(x,y)) > 0$, then ∞ many solutions over alg. closure.
If $deg_y(d(x,y)) = 0$, then found an expression

$$a(x,y) f(x,y) + b(x,y) g(x,y) = h(x)$$

Bivariate polynomials: resultant

- **Resultant**: easy and robust method for computing $h(x)$ without using GCD with denominators
- Given $f, g \in R[y]$ with $f = \sum_{i=0}^{n} f_i y^i$ and $g = \sum_{i=0}^{m} g_i y^i$
- Here R is any **ring**, so not necessarily a field
- Sylvester matrix of f and g is $(m+n) \times (m+n)$ matrix

$$\mathrm{Syl}(f,g) = \begin{array}{cl} \left(\begin{array}{cccccccc} f_0 & f_1 & \cdots & f_n & 0 & \cdots & & 0 \\ 0 & f_0 & f_1 & \cdots & f_n & 0 & \cdots & 0 \\ \vdots & & & & & & & \vdots \\ 0 & \cdots & & f_0 & \cdots & & f_{n-1} & f_n \\ g_0 & g_1 & \cdots & g_m & 0 & \cdots & & 0 \\ 0 & g_0 & g_1 & \cdots & g_m & 0 & \cdots & 0 \\ \vdots & & & & & & & \vdots \\ 0 & \cdots & & g_0 & \cdots & & g_{m-1} & g_m \end{array}\right) & \begin{array}{l} \left.\vphantom{\begin{array}{c}0\\0\\\vdots\\0\end{array}}\right\} m \text{ rows} \\ \left.\vphantom{\begin{array}{c}0\\0\\\vdots\\0\end{array}}\right\} n \text{ rows} \end{array} \end{array}$$

- $\boxed{\textbf{Resultant}\text{: } \mathrm{Res}(f,g) = \det(\mathrm{Syl}(f,g))}$

Resultant

- **Theorem**: given $f, g \in R[y]$, there exist polynomials $A, B \in R[y]$ such that

$$Af + Bg = \mathrm{Res}(f, g)$$

  and the coefficients of A, B are integer polynomial expressions in the coefficients of f and g
- **Exercise:** Prove this.
  - First show that $\mathrm{Syl}(f, g)^T$ is a matrix of the linear map

$$R[y]_{\deg < m} \times R[y]_{\deg < n} \to R[y]_{\deg < m+n} : (A, B) \mapsto Af + Bg$$

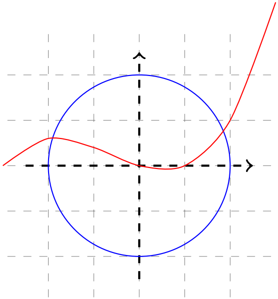
  - Use formula $M \cdot \mathrm{adj}(M) = (\det M)I$ applied to $M = \mathrm{Syl}(f, g)^T$

Resultant: applications

- $R = \mathbb{Z}$:
  - Given $f, g \in \mathbb{Z}[y]$, can find $A, B \in \mathbb{Z}[y]$ such that
    $$A(y)f(y) + B(y)g(y) = \text{Res}(f, g) \in \mathbb{Z}$$
  - If $\text{Res}(f, g) \neq 0$, then no common solutions (not even over $\mathbb{C}$)
  - If $p \nmid \text{Res}(f, g)$: same conclusion for reductions $\overline{f}, \overline{g} \in \mathbb{F}_p[y]$
- $R = F[x]$:
  - Given $f, g \in F[x][y] = F[x, y]$, so: bivariate polynomials with coefficients in F
  - Can find $A(x, y), B(x, y) \in F[x, y]$ such that
    $$A(x, y)f(x, y) + B(x, y)g(x, y) = \text{Res}(f, g) \in F[x]$$
  - If $\text{Res}(f, g) \neq 0$: have eliminated the variable y

Resultant: example

- Let $f(x, y) = y^2 + (x^2 - 4)$ and $g = -10y + x(x-1)(x+3)$



Resultant: example

- Sylvester matrix:

$$Syl(f,g,y) = \begin{pmatrix} x^2-4 & 0 & 1 \\ x(x-1)(x+3) & -10 & 0 \\ 0 & x(x-1)(x+3) & -10 \end{pmatrix}$$

- $\mathrm{Res}(f,g,y) = x^6 + 4x^5 - 2x^4 - 12x^3 + 109x^2 - 400$
- All common solutions have x-coordinate a zero of $\mathrm{Res}(f,g,y)$
- Over $\mathbb{R}$:

$$x_0 \in \{-1.90599741272488, 1.849299981919\}$$

- MAGMA :

```
QQ := Rationals();
R<x,y> := PolynomialRing(QQ, 2);
f := y^2 + x^2 - 4;
g := -10*y + x*(x-1)*(x+3);
Resultant(f, g, y);
```

Polynomial systems

Resultant

Ideals and varieties

Gröbner bases

Cryptographic applications

Ideals

- **Def:** An **ideal** is a subset $I \subset F[x_1, \ldots, x_n]$ such that
  - If $f, g \in I$, then $f + g \in I$
  - If $f \in I$ and $h \in F[x_1, \ldots, x_n]$, then $hf \in I$
- **Def:** The ideal generated by polynomials $f_1, \ldots, f_m$ is given by

$$I = \langle f_1, \ldots, f_m \rangle = \left\{ \sum_{i=0}^{m} h_i f_i \mid h_i \in F[x_1, \ldots, x_n] \right\}$$

- The polynomials $f_1, \ldots, f_m$ are called a **basis** for I
- Clearly $V_F(f_1, \ldots, f_m) = V_F(I)$, so solution set only depends on I and not on the chosen basis
- **Goal:** find more useful basis for the ideal that allows us to determine solutions explicitly

Ideals vs. varieties

- An ideal $I \subset F[x_1, \ldots, x_n]$ determines a variety $V_F(I)$ as the zero set of **all** polynomials in I
- Given a subset $V \subset F^n$, can look at all polynomials in $F[x_1, \ldots, x_n]$ that vanish on V

$$I(V) = \{f \in F[x_1, \ldots, x_n] \mid \\ \forall(\alpha_1, \ldots, \alpha_n) \in V : f(\alpha_1, \ldots, \alpha_n) = 0\}$$

- Clearly we have $I \subset I(V_F(I))$, but in general not an equality:
  - V_F forgets about multiplicities: $I(V_F(\langle x^2 \rangle)) = \langle x \rangle$
  - V_F does not see extension fields: $I(V_{\mathbb{R}}(\langle x^2 + 1 \rangle)) = \langle 1 \rangle$
- **Def:** The **radical** of an ideal I is

$$\sqrt{I} = \{f \in F[x_1, \ldots, x_n] \mid \exists t \in \mathbb{N} : f^t \in I\}$$

- Hilbert's Nullstellensatz:
  If F is **algebraically closed** then $I(V_F(I)) = \sqrt{I}$

Example I revisited: linear polynomials

- Consider $I = \langle f_1, \ldots, f_m \rangle \subset F[x_1, \ldots, x_m]$ with each f_i linear
  - What does $V_F(I)$ look like? Is it empty? How many elements?
  - Is there a nicer basis that allows us to see this?
  - Is there an efficient method to see if $h \in F[x_1, \ldots, x_n]$ is in I?
- Method: use Gauss elimination to bring the matrix

$$\begin{pmatrix} a_{1,1} & \ldots & a_{1,n} & b_1 \\ \vdots & \ddots & \vdots & \vdots \\ a_{m,1} & \ldots & a_{m,n} & b_m \end{pmatrix}$$

  in row echelon form and back substitute if there are solutions (also easy to test ideal membership, ...)
- **Row echelon form = nicer basis** for the ideal $\langle f_1, \ldots, f_m \rangle$
- Note: Gauss elimination **cancels terms** in x_1, then x_2, ...

Example II revisited: univariate polynomials

- Consider $I = \langle f, g \rangle$ with $f, g \in F[x]$. Again:
  - What does $V_F(I)$ look like? Is it empty? How many elements?
  - Is there a nicer basis that allows us to see this?
  - Is there an efficient method to see if $h \in F[x]$ is included in I?
- Method: compute $\mathrm{GCD}(f, g)$ via Euclid's algorithm and apply root finding algorithm
- **Exercise:** show that $I = \langle \mathrm{GCD}(f, g) \rangle \leftarrow$ **nicer basis**
- Conclusions:
  - One generator is sufficient, i.e., all ideals in $F[x]$ are **principal**
  - Efficient method to compute this generator (simple GCD computations)
  - Simple check to see if $h \in I$, namely check if $GCD(f, g) \mid h$
- Note: Euclid's algorithm repeatedly **cancels top terms**
- **Exercise:** what is $\sqrt{I}$ for $I = \langle \prod (x - \alpha_i)^{e_i} \rangle$ with $\alpha_i \neq \alpha_j$?

Example II revisited: univariate polynomials

- An example:
  - Let
    $$f = x^3 - x^2 - x - 2 \quad \text{and} \quad g = x^3 - 2x^2 - x + 2$$
    and consider $I = \langle f, g \rangle$
  - Let $h = x^2 - 3x + 2$, is it easy to see whether $h \in I$?
- Note that $\deg(h) < \deg(f)$ and $\deg(h) < \deg(g)$, so cannot try to divide h by f or g, i.e. direct approach is not possible
- Recall that $\langle f, g \rangle = \{u(x)f(x) + v(x)g(x) \mid u, v \in F[x]\}$
- To find elements of **small degree** in I, we need to **cancel top terms of f and g** using u and v, leading to GCD algorithm
- $\mathrm{GCD}(f, g) = x - 2$ and indeed $h(2) = 0$ so $h \in I$

Example III: monomial ideals

- **Def:** A **monomial** is a polynomial of the form

$$x_1^{e_1} \cdots x_n^{e_n}$$

- We will write such monomial as $\mathbf{x}^{\mathbf{e}}$
- **Def:** A **monomial ideal** is an ideal that can be generated by monomials $I = \langle \{\mathbf{x}^{\boldsymbol{\alpha}} \mid \boldsymbol{\alpha} \in A\} \rangle$ with possibly infinite $A \subset \mathbb{N}^n$
- Ideal membership is easy:
  - A polynomial h belongs to a monomial ideal if and only if all monomials in h belong to I
  - A monomial $\mathbf{x}^{\mathbf{e}}$ belongs to I if at least one $\boldsymbol{\alpha} \in A$ with $\mathbf{e} \geq \boldsymbol{\alpha}$
- **Dickson's Lemma**: a monomial ideal is generated by a finite number of monomials

Monomial orders and multivariate division

- To be able to define a division algorithm for multivariate polynomials, we need to identify "leading terms".
- **Def:** A monomial ordering $\succ$ is a total ordering on $F[x_1, \ldots, x_n]$ that satisfies
  - Compatibility: if $\mathbf{x}^{\boldsymbol{\alpha}} \succ \mathbf{x}^{\boldsymbol{\beta}}$ then $\mathbf{x}^{\boldsymbol{\alpha}}\mathbf{x}^{\gamma} \succ \mathbf{x}^{\boldsymbol{\beta}}\mathbf{x}^{\gamma}$
  - Well-ordering: any non-empty set of monomials contains a smallest element
- Note: we can also simply look at exponent vectors $\boldsymbol{\alpha}, \boldsymbol{\beta}, \boldsymbol{\gamma}$
- The **total degree** of a monomial $\deg \mathbf{x}^{\boldsymbol{\alpha}}$ is $\sum_i^n \alpha_i$

Monomial orders and multivariate division

- **Lexicographic ordering**: $\alpha \succ_{lex} \beta$ if and only if the first non-zero coefficient **from the left** of $\alpha - \beta$ is **positive**
- **Graded lexicographic ordering**: $\alpha \succ_{grlex} \beta$ if and only if
  - $\deg(\alpha) > \deg(\beta)$ or
  - $\deg(\alpha) = \deg(\beta)$ and $\alpha \succ_{lex} \beta$
- **Graded reverse lexicographic ordering**: $\alpha \succ_{grevlex} \beta$ if and only if
  - $\deg(\alpha) > \deg(\beta)$ or
  - $\deg(\alpha) = \deg(\beta)$ and $\alpha \succ_{revlex} \beta$ with $\alpha \succ_{revlex} \beta$ if and only if the first non-zero coefficient **from the right** of $\alpha - \beta$ is **negative**
- **Exercise:** Why is $\succ_{revlex}$ **not** a monomial ordering?

Example monomial orderings

- The polymomial $f = 4xyz^2 + 4x^3 - 5y^4 + 7xy^2z \in F[x, y, z]$ is
- $\succ_{lex}$: $f = 4x^3 + 7xy^2z + 4xyz^2 - 5y^4$
- $\succ_{grlex}$: $f = 7xy^2z + 4xyz^2 - 5y^4 + 4x^3$
- $\succ_{grevlex}$: $f = -5y^4 + 7xy^2z + 4xyz^2 + 4x^3$

Multivariate division

- Given polynomials $f_1, \ldots, f_m$ and a polynomial f, we want to write
$$f = q_1 f_1 + \ldots + q_m f_m + r$$
for some quotients q_i and remainder r
- Will try to mimic univariate case, given monomial ordering $\succ$
- **Def:** Let $g = \sum_{\boldsymbol{\alpha} \in \mathbb{N}^n} c_{\boldsymbol{\alpha}} \mathbf{x}^{\boldsymbol{\alpha}}$, the **multidegree** of g wrt $\succ$ is
$$\operatorname{mdeg}(g) = \max_{\succ} \{\boldsymbol{\alpha} \in \mathbb{N}^n \mid c_{\boldsymbol{\alpha}} \neq 0\}$$
- **Def:** The **leading coefficient** $\operatorname{lc}(g)$ is $c_{\operatorname{mdeg}(g)}$
- **Def:** The **leading monomial** $\operatorname{lm}(g)$ is $\mathbf{x}^{\operatorname{mdeg}(g)}$
- **Def:** The **leading term** $\operatorname{lt}(g)$ is $\operatorname{lc}(g) \operatorname{lm}(g)$

Multivariate division

- Like in univariate case, we will try to cancel the leading term of f by substracting some multiple of the f_i
- If the leading term of f cannot be cancelled, we move it to the remainder
- Result: $f = q_1 f_1 + \ldots + q_m f_m + r$ such that no monomial in r is divisible by any $\operatorname{lt}(f_i)$

$\forall i \in [1 \ldots m]$: $q_i \leftarrow 0$, $r \leftarrow 0$, $h = f$
while $h \neq 0$ **do**
  if $\operatorname{lt}(f_i)$ divides $\operatorname{lt}(h)$ for some $i \in [1, \ldots, m]$ **then**
    $q_i \leftarrow q_i + \operatorname{lt}(h)/\operatorname{lt}(f_i)$, $h \leftarrow h - \operatorname{lt}(h)/\operatorname{lt}(f_i) f_i$
  else
    $r \leftarrow r + \operatorname{lt}(h)$, $h \leftarrow h - \operatorname{lt}(h)$
  end if
end while
return $q_1, \ldots, q_m, r$

Multivariate division

- Like in univariate case, multivariate division is **not sufficient** to test if $h \in \langle f_1, \ldots, f_m \rangle$
- **Main problem**: in $I = \langle f_1, \ldots, f_m \rangle$ there are possibly polynomials with smaller leading term (for $\succ$) than all $\mathrm{lt}(f_i)$
- Division algorithm only considers $\mathrm{lt}(f_i)$
  - moves any intermediate $\mathrm{lt}(h)$ to the remainder if it is not divisible by any of the $\mathrm{lt}(f_i)$
- Ideally: want basis $\langle g_1, \ldots, g_t \rangle$ of I such that

  $$\langle \mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_t) \rangle = \langle \mathrm{lt}(I) \rangle$$

  with $\mathrm{lt}(I)$ the set of leading terms of all polynomials in I
- $=$ definition of **Gröbner basis**

Multivariate division: example

- For $\succ_{lex}$ we will divide $f = x^2y + xy^2 + y^2$ by $f_1 = xy - 1$ and $f_2 = y^2 - 1$.

$$\begin{aligned} f &= x(xy-1) + xy^2 + x + y^2 \\ &= x(xy-1) + y(xy-1) + x + y^2 + y \end{aligned}$$

- Leading term is now x which is not divisible so we move it to remainder and continue

$$\begin{aligned} f &= (x+y)(xy-1) + (x) + (y^2-1) + (y+1) \\ &= (x+y)(xy-1) + (y^2-1) + x + y + 1 \end{aligned}$$

- Final remainder is $x + y + 1$

Multivariate division: example

- Same example but now instead of choosing f_1 always first, we can choose f_2

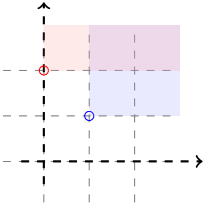
$$\begin{aligned} f &= x(xy-1) + x + x(y^2-1) + x + (y^2-1) + 1 \\ &= x(xy-1) + (x+1)(y^2-1) + 2x + 1 \end{aligned}$$

- Quotients, nor remainder are unique and depend on monomial order, but also on the order in which one chooses the f_i
- If smallest possible i is chosen, then obtain unique result, but again not good enough to test ideal membership
- Note: again the main problem is the existence of combinations of f_1 and f_2 with smaller leading term

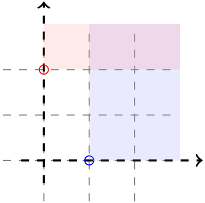
$$yf_1 - xf_2 = x - y$$

Multivariate division: example

- Looking at exponent vectors of the leading terms of $f_1 = xy - 1$ and $f_2 = y^2 - 1$ we get



- In particular: unclear if $F[x, y]$ mod I is finite-dimensional
- Gröbner basis for $\succ_{lex}$ is $f_1 = x - y$ and $f_2 = y^2 - 1$



- Conclusion: $F[x, y]$ mod I is 2-dimensional

Polynomial systems

Resultant

Ideals and varieties

Gröbner bases

Cryptographic applications

Gröbner basis

- **Def:** A **Gröbner basis** (wrt. $\succ$) for an ideal $I \subset F[x_1, \ldots, x_n]$ is a set of generators $\{g_1, \ldots, g_s\}$ such that $I = \langle g_1, \ldots, g_s \rangle$ and
$$\langle \mathrm{lt}(I) \rangle = \langle \mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_s) \rangle$$
- $\langle \mathrm{lt}(I) \rangle$ is the monomial ideal generated by all $\mathrm{lt}(f)$ with $f \in I$
- $\langle \mathrm{lt}(I) \rangle$ is sometimes called the **initial ideal**
- Dickson's lemma states that a finite number of monomials generates $\langle \mathrm{lt}(I) \rangle$ so Gröbner bases exist
- **Exercise:** any set of elements $\{g_1, \ldots, g_s\} \subset I$ such that $\langle \mathrm{lt}(I) \rangle = \langle \mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_s) \rangle$ is automatically a basis for I
- Conclusion: **Hilbert's basis theorem**: every ideal $I \subset F[x_1, \ldots, x_n]$ is finitely generated

Gröbner basis: ideal membership

- Given a **Gröbner basis** $\{g_1, \ldots, g_s\}$ for an ideal $I \subset F[x_1, \ldots, x_n]$, we now have the equivalence

$$f \in I \Leftrightarrow f \bmod \{g_1, \ldots, g_s\} = 0$$

- Write out multivariate division

$$f = q_1 g_1 + \ldots + q_s g_s + r$$

- $\Leftarrow$: If $r = 0$ then clearly $f \in I$.
- $\Rightarrow$: If $f \in I$, but $r \neq 0$, then $\mathrm{lt}(r) \in \langle \mathrm{lt}(I) \rangle$, so must be divisible by one of the $\mathrm{lt}(g_i)$, which is impossible due to division rules, so $r = 0$.

Gröbner basis: working modulo an ideal

- **Gröbner basis** $\{g_1, \ldots, g_s\}$ for an ideal $I \subset F[x_1, \ldots, x_n]$
- Given $f \in F[x_1, \ldots, x_n]$ we can write

$$f = q_1 g_1 + \ldots + q_s g_s + r$$

- r is **unique** and **does not depend on the chosen Gröbner basis**, but only on I (and the choice of monomial ordering $\succ$)
- **Exercise:** prove the above
- Note: the order of division also does not matter
- So we can write $r = f \bmod I$

S-polynomials

- Let $f, g \in I$, we are looking for combinations of multiples of f and g such that the leading terms of these multiples cancel
- Let $\mathrm{lm}(f) = \mathbf{x}^{\boldsymbol{\alpha}}$ and $\mathrm{lm}(g) = \mathbf{x}^{\boldsymbol{\beta}}$, and let

$$\gamma = (\max\{\alpha_1, \beta_1\}, \ldots, \max\{\alpha_n, \beta_n\})$$

- Note $\mathbf{x}^{\gamma} = \mathrm{lcm}(\mathrm{lm}(f), \mathrm{lm}(g))$
- **Def:** The S-**polynomial** (or principal syzygy) of f, g is defined as

$$S(f,g) = \frac{\mathbf{x}^{\gamma}}{\mathrm{lt}(f)} \cdot f - \frac{\mathbf{x}^{\gamma}}{\mathrm{lt}(g)} \cdot g$$

- Note: $\mathrm{lm}(S(f,g)) \prec \mathrm{lm}(\mathrm{lcm}(\mathrm{lm}(f), \mathrm{lm}(g)))$
- Clearly also $S(f,g) \in I$

Buchberger's algorithm

- Theorem (Buchberger): A set $\{g_1, \ldots, g_s\} \subset F[x_1, \ldots, x_n]$ is a Gröbner basis for the ideal $I = \langle g_1, \ldots, g_s \rangle$ if and only if

$$S(g_i, g_j) \bmod \{g_1, \ldots, g_s\} = 0 \qquad \forall i < j \in \{1, \ldots, s\}$$

- Buchberger's algorithm: if an S-polynomial fails the test, simply add the remainder of it to set of generators, until no more failures occur
- Approach has to finish, essentially since every ideal is finitely generated (apply it to union of initial ideals)

Buchberger's algorithm

Function Buchberger($\{f_1, \dots, f_m\}$, order $\succ$)

$G \leftarrow \{f_1, \dots, f_m\}$
repeat
  $S \leftarrow \emptyset$, label elements in G by $\{g_1, \dots, g_t\}$
  for $1 \leq i < j \leq t$ **do**
    $r \leftarrow S(g_i, g_j) \bmod \{g_1, \dots, g_t\}$
    if $r \neq 0$ **then**
      $S \leftarrow S \cup \{r\}$
    end if
  end for
  $G \leftarrow G \cup S$
until $S = \emptyset$
return G

Buchberger's algorithm

- Gröbner basis is not minimal, nor unique
  - Have to get rid of redundant polynomials g_i and also redundant terms in each g_i
  - Polynomial g_i is redundant if $\mathrm{lt}(g_i) \in \langle \mathrm{lt}(G \setminus \{g_i\}) \rangle$, since the leading term of g_i does not contribute anything new
  - Can replace G by $G \setminus \{g_i\}$
- **Def:** Gröbner basis is called **minimal** if $\forall g \in G : \mathrm{lc}(g) = 1$ and $\mathrm{lt}(g) \notin \langle \mathrm{lt}(G \setminus \{g\}) \rangle$
- **Def:** Element g is called **reduced** if no monomial in g belongs to $\langle \mathrm{lt}(G \setminus \{g\}) \rangle$
- **Def:** Gröbner basis is called **reduced** if it is minimal and all elements are reduced
- Theorem: each ideal I has a **unique reduced Gröbner basis** for a given order $\succ$

Examples I and II revisited one more time

- Example I: Linear polynomials
  - monomial order = variable order $x_1 \succ x_2 \succ \ldots \succ x_n$
  - S-polynomials: pivoting method in Gaussian elimination
  - Gröbner basis: any basis containing row echelon form
  - minimal Gröbner basis: row echelon form
  - reduced Gröbner basis: reduced row echelon form
- Main difference with Gauss: a priori equations are **added** instead of replaced
  - number of equations can **grow** very fast at every iteration
- Example II: Univariate polynomials
  - only one monomial order possible: $\ldots \succ x^3 \succ x^2 \succ x \succ 1$
  - Gröbner basis: any basis containing $\mathrm{GCD}(f,g)$
  - reduced Gröbner basis: $\{\mathrm{GCD}(f,g)\}$

Buchberger's algorithm: complexity

- Cannot be easy, e.g. can encode NP-complete problem such as knapsack problem with weights $w_i \in \mathbb{N}$ and target $s \in \mathbb{N}_0$

$$s = \sum_{i=1}^{n} x_i w_i \qquad x_i(1 - x_i) = 0$$

(see Lecture 5)
- General case: K. Kühnle and E.W. Mayr (1996) *Exponential space computation of Gröbner bases*
  - Computing Gröbner bases is EXPSPACE-complete problem and has doubly exponential time complexity
  - Exist ideals in polynomial rings of n variables such that Gröbner basis has at least $2^{2^{\alpha n}}$ polynomials each of degree at least $2^{2^{\beta n}}$ for some constants $\alpha, \beta \in \mathbb{R}_{>0}$

Buchberger's algorithm: complexity

- Practice: many problems give rise to 0-dimensional ideals, i.e. only finitely many solutions
- For system of m equations in n unknowns the complexity is

$$\mathcal{O}\left(\left(m\binom{n+d_{reg}-1}{d_{reg}}\right)^{\omega}\right)$$

  - ω complexity of matrix multiplication (practice $\omega \sim 3$)
  - d_{reg} the degree of regularity $=$ highest degree that appears in computation of Gröbner basis
  - $d_{reg} \leq \sum_{i=1}^{m}(d_i - 1) + 1$ with $d_i = \deg(f_i)$ (for grevlex)
  - n quadratic equations gives $d_{reg} \leq n + 1$, so complexity

$$\mathcal{O}\left(\left(n\binom{2n}{n}\right)^{\omega}\right)$$

Buchberger's algorithm: complexity

- For "semi-regular" systems = d_{reg} is **index** of first non-positive coefficient of

$$H(z) = \frac{\prod_{i=1}^{m}(1 - z^{d_i})}{(1 - z)^n}$$

for ideal $\langle f_1, \ldots, f_m \rangle$ with $\deg(f_i) = d_i$

- For quadratic equations and $n = 100$ have following table

m	d_{reg}
100	101
101	51
110	35
120	28
200	14
1000	4

- MAGMA :
```
R<z> := PowerSeriesRing(Integers(), 200);
H := &*[1-z^2 :i in [1..m]]/(1-z)^100;
```

Back to system solving: elimination

- Given ideal $I = \langle f_1, \ldots, f_m \rangle \subset F[x_1, \ldots, x_n]$
- Assume only finitely many solutions, so $V_F(I)$ is finite
- For each $i \in \{1, \ldots, n\}$ we have that the polynomial

$$g_i(x_i) = \prod_j (x_i - \tilde{x}_{i,j})$$

  with $\tilde{x}_{i,j}$ all x_i-coord of all elements in $V_F(I)$ is zero on $V_F(I)$
- Modulo "subtleties" (F not alg. closed, $I \neq \sqrt{I}$): $g_i(x_i) \in I$
- Motivates to look for univariate polynomials within ideal

Elimination ideals

- **Def:** Let $I = \langle f_1, \dots, f_m \rangle \subset F[x_1, \dots, x_n]$, then the ℓ-th elimination ideal is

$$I_\ell = I \cap F[x_{\ell+1}, \dots, x_n]$$

- Elements in I_ℓ do not depend on $x_1, \dots, x_\ell$
- In particular: I_{n-1} contains only polynomials in the variable x_n and is principal (since only 1 variable), so $I_{n-1} = \langle g(x_n) \rangle$
- All x_n coordinates of the points in $V_F(I)$ are zeros of $g(x_n)$
- **Elimination theorem**: If G is a Gröbner basis for I wrt. $\succ_{lex}$, then

$$G_\ell = G \cap F[x_{\ell+1}, \dots, x_n]$$

  is a Gröbner basis for the elimination ideal I_ℓ

Elimination ideals

- Elimination theorem implies that Gröbner basis for $\succ_{lex}$ automatically eliminates variables
- Example: $f_1 = x^2 + y^2 + z^2 - 4, f_2 = x^2 + 2y^2 - 5, f_3 = xz - 1$ has Gröbner basis wrt. $\succ_{lex}$

$$g_1 = x + 2z^3 - 3z, g_2 = y^2 - 1 - z^2, g_3 = 2z^4 - 3z^2 + 1$$

- Finding roots of g_3 and back substitution gives all solutions
- Not all partial solutions extend to full solutions
- Magma :

```
QQ := Rationals();
R<x,y,z> := PolynomialRing(QQ,3,"lex");
I := Ideal([x^2 + y^2 + z^2 - 4,
            x^2 + 2*y^2 - 5, x*z - 1]);
GroebnerBasis(I);
```

  (Note: Magma default is `"lex"`, so can be omitted)
- Compare with `EliminationIdeal(I, 2);`

The Shape Lemma

- Captures structure of systems of random equations, where all points have one coordinate that is all different
- **Shape Lemma**: Let $I \subset F[x_1, \dots, x_n]$ be a radical ideal such that $V_F(I)$ is finite. Assume that the x_n-coordinates of all points are different, then a Gröbner basis for I wrt. $\succ_{lex}$ has the following shape:

$$
\begin{aligned}
g_1 &= x_1 + h_1(x_n) \\
&\vdots \\
g_{n-1} &= x_{n-1} + h_{n-1}(x_n) \\
g_n &= x_n^m + h_n(x_n)
\end{aligned}
$$

- Roots of g_n give x_n-coordinates. Evaluation of g_i for $i < n$ gives values for $x_i = -h_i(x_n)$
- Gives m roots over algebraic closure

The Shape Lemma: example

- Let $f_1 = xy + z$, $f_2 = y^2 + x + 1$, $f_3 = xz + yz + z^2$
- Normal lexicographic ordering $x \succ_{lex} y \succ_{lex} z$ gives Gröbner basis

$$x + y^2 + 1, \quad y^3 + y - z, \quad yz - z^3, \quad z^4 + z^3 - z$$

- Does not satisfy shape lemma (why not?)
- Changed lexicographic ordering $x \succ z \succ y$ gives Gröbner basis

$$x + y^2 + 1, \quad z - y^3 - y, \quad y^6 - y^5 + 3y^4 - 2y^3 + 2y^2 - y$$

Gröbner basis conversion

- Elimination theorem shows that $\succ_{lex}$ is useful to find solutions of systems of equations
- In practice: $\succ_{grevlex}$ much faster to compute Gröbner basis
- Change of monomial ordering going from $\succ_{grevlex}$ to $\succ_{lex}$
- Faugère, Gianni, Lazard and Mora (FGLM) for dimension 0 ideals
- Complexity: given Gröbner basis for $\succ_{grevlex}$, can compute Gröbner basis for $\succ_{lex}$ in time $\mathcal{O}(nD^3)$ with D the total number of solutions (over algebraic closure)

Polynomial systems

Resultant

Ideals and varieties

Gröbner bases

Cryptographic applications

Multivariate equations in cryptography: encryption

- Fact: finding solutions to systems of multivariate non-linear equations is NP-hard
- Basic idea for encryption:
  - Public key $= (f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n))$
  - Encrypt message $(m_1, \ldots, m_n)$ is evaluation

$$(c_1, \ldots, c_m) = (f_1(m_1, \ldots, m_n), \ldots, f_m(m_1, \ldots, m_n))$$

  - Decryption: given ciphertext $(c_1, \ldots, c_m)$ find solution to

$$\begin{cases} f_1(x_1, \ldots, x_n) = c_1 \\ \qquad\qquad \vdots \\ f_m(x_1, \ldots, x_n) = c_m \end{cases}$$

  - For decryption to work: solution should be unique (or easily recognizable from small set of solutions), so typically $m \geq n$

Multivariate equations in cryptography: signatures

- Basic idea for signatures:
  - Public key $= (f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n))$
  - To sign message M, compute its hash $H(M) = (h_1, \ldots, h_m)$
  - Signature is then a solution $(s_1, \ldots, s_n)$ to

$$\begin{cases} f_1(x_1, \ldots, x_n) = h_1 \\ \qquad\qquad \vdots \\ f_m(x_1, \ldots, x_n) = h_m \end{cases}$$

  - For signing to work: for each hash there should be at least one solution, so typically $m \leq n$
  - Verification: given M, public key and $(s_1, \ldots, s_n)$ simply verify above system of equations

Multivariate equations in cryptography: public key

- Public key $= (f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n))$
- Number of monomials of degree $\leq d$ is

$$\binom{n+d}{d}$$

- Size over $\mathbb{F}_q$ therefore is $m \cdot \binom{n+d}{d} \cdot \log q$
- Practice: $d = 2$

Multivariate equations in cryptography

- Main problem: solving random non-linear systems of equations is NP-hard, so basic idea is a no-go
- Solution (?): start from system of equations that is easy to solve, and then hide its structure

$$F = T \circ G \circ S$$

- G system of **easy to invert** quadratic multivariate polynomials (called central map)
- T and S are **invertible** affine maps

$$F : \mathbf{x} \overset{S}{\mapsto} \mathbf{y} = M_S\mathbf{x} + \mathbf{c}_S \overset{G}{\mapsto} \mathbf{z} = G(\mathbf{y}) \overset{T}{\mapsto} \mathbf{t} = M_T\mathbf{z} + \mathbf{c}_T$$

  - $\mathbf{x} = (x_1, \ldots, x_n)$, $\mathbf{t} = (t_1, \ldots, t_m)$
  - M_S is $n \times n$ matrix, $\mathbf{c}_S$ is $n \times 1$ vector
  - M_T is $m \times m$ matrix, $\mathbf{c}_T$ is $m \times 1$ vector

Oil-Vinegar polynomials

- Let $\mathbb{F}$ be a finite field and let $n = v + o$, define

$$f(x_1, \ldots, x_n) = \sum_{i=1}^{v} \sum_{j=i}^{v} \alpha_{i,j} x_i x_j + \sum_{i=1}^{v} \sum_{j=v+1}^{n} \beta_{i,j} x_i x_j + \sum_{i=1}^{n} \gamma_i x_i + \delta$$

- Vinegar variables: $x_1, \ldots, x_v$
- Oil variables: $x_{v+1}, \ldots, x_n$
- Coefficients $\alpha_{i,j}, \beta_{i,j}, \gamma_i, \delta \in \mathbb{F}$
- Note: there are no quadratic terms of type oil $\times$ oil
- Consequence: if we choose random values $x_1, \ldots, x_v$, then obtain a **linear** system of equations in oil variables
  - $\rightsquigarrow$ easy to solve

Oil-Vinegar signature scheme

- Flagship of multivariate crypto, invented by Patarin in 1998
- Central map consists of o oil-vinegar polynomials

$$g^{(k)}(x_1,\dots,x_n)=\sum_{i=1}^{v}\sum_{j=i}^{v}\alpha_{i,j}^{(k)}x_ix_j+\sum_{i=1}^{v}\sum_{j=v+1}^{n}\beta_{i,j}^{(k)}x_ix_j+\sum_{i=1}^{n}\gamma_i^{(k)}x_i+\delta^{(k)}$$

- Central map G is composed with invertible linear map $S:\mathbb{F}^n\to\mathbb{F}^n$ (affine change of variables)
- Public key is simply $F=G\circ S$ (no need for T)
- S mixes oil and vinegar variables

Oil-Vinegar signature scheme

- Signing message M: compute hash $H(M) = (h_1, \ldots, h_o) \in \mathbb{F}^o$
- Solve non-linear system of equations $F^{(k)}(x_1, \ldots, x_n) = h_k$
- Signer knows central map G, so he solves

$$\begin{cases} g^{(1)}(x_1, \ldots, x_n) = h_1 \\ \quad\quad \vdots \\ g^{(o)}(x_1, \ldots, x_n) = h_o \end{cases}$$

- Choose random values for the vinegar variables $x_1, \ldots, x_v$
- Obtain linear system of equations in oil variables $x_{v+1}, \ldots, x_n$
- If linear system has no solutions, choose new vinegar variables
- Return signature $\mathbf{z} \in \mathbb{F}^n$ as $\mathbf{z} = S^{-1}\mathbf{x}$
- Signature verification: check that $F(\mathbf{z}) = H(M)$

Oil-Vinegar signature scheme: security

- Kipnis-Shamir (1999): beautiful polynomial time attack on balanced O-V scheme, i.e. where $v = o$
- In general: attack complexity is $\mathcal{O}(q^{v-o}o^4)$
- Currently: UOV, unbalanced Oil-Vinegar scheme with $v \approx \frac{3}{2}o$
- Direct attack using Gröbner bases appears to behave like for random systems
  - System under-determined, so filling in variables makes system look random
- Example: UOV($\mathbb{F}_{16}, o = 47, v = 71$) believed to meet NIST level I, public key size is 242kB, signature size 89B
- Rainbow: UOV variant submitted to NIST but broken in 2022 by Beullens in “a weekend on a laptop”
- Plain UOV will be submitted to renewed call in 2023
  - as well as variants such as MAYO (stirred up version of UOV)

Finite field extensions

- Recall finite field $\mathbb{F}_p$ (p prime) is simply modular arithmetic modulo p
- Extension field $\mathbb{F}_q$ with $q = p^n$ can be constructed as

$$\mathbb{F}_q = \mathbb{F}_p[w]/(f(w))$$

  with f a monic, irreducible polynomial over $\mathbb{F}_p$
- Element $a \in \mathbb{F}_q$ can be written as

$$a = \sum_{i=0}^{n-1} a_i w^i \quad a_i \in \mathbb{F}_p$$

- MAGMA :

```
> F2:=GF(2); R<w> := PolynomialRing(F2);
> F32<w> := ext< F2 | w^5 + w^2 + 1 >;
> Eltseq(w^8);
[1,0,1,1,0]
```

(read as: $w^8 = 1 + w^2 + w^3$)

Finite field extensions: multiplication & Frobenius

- Given two elements $a, b \in \mathbb{F}_q$, can compute product in $\mathbb{F}_q$

$$c = a \cdot b = \sum_{i=0}^{n-1} c_i w^i \quad c_i \in \mathbb{F}_p$$

- Easy to see: c_i are **quadratic** polynomial expressions in a_i, b_i
- p^k-Frobenius: given $a \in \mathbb{F}_q$ compute a^{p^k}

$$a^{p^k} = \sum_{i=0}^{n-1} a_i w^{ip^k} = \sum_{j=0}^{n-1} a'_j w^j$$

  where the a'_j are **linear** polynomials in the a_i
  - since w^{jp^k} can be written as fixed linear expression in w^i

Hidden Field Equations (HFE)

- Also Patarin (1996): take univariate polynomial in $\mathbb{F}_q[X]$

$$G(X) = \sum_{0 \le i \le j \le d} \alpha_{i,j} X^{p^i + p^j} + \sum_{0 \le i \le d} \beta_i X^{p^i} + \gamma$$

- Coefficients $\alpha_{i,j}, \beta_i, \gamma \in \mathbb{F}_q$ all have n coefficients in $\mathbb{F}_p$
- If we write $X = \sum_{i=0}^{n-1} x_i w^i$ with x_i unknowns (over $\mathbb{F}_p$), then
  - $G(X)$ is mapping $G : \mathbb{F}_p^n \to \mathbb{F}_p^n$
  - given by n quadratic multivariate polynomials in $\mathbb{F}_p[x_1, \ldots, x_n]$

$$G(X) = \sum_{i=0}^{n-1} g_i(x_1, \ldots, x_n) w^i$$

- Public key: n quadratic multivariate polynomials

$$F = T \circ G \circ S$$

with $T, S \in \mathbb{F}_p^{n \times n}$ invertible matrices

Hidden Field Equations (HFE): encryption / decryption

- Encryption: evaluate public key F in message $(m_1, \ldots, m_n)$
- Decryption:
  - given $(c_1, \ldots, c_n)$ compute $\mathbf{z} = T^{-1}\mathbf{c}$
  - Consider $\mathbf{z}$ as element $z \in \mathbb{F}_q$ as $z = \sum_{i=0}^{n-1} \mathbf{z}[i]w^i$
  - Find root x of **univariate** polynomial over $\mathbb{F}_q$ as $G(X) = z$
  - Compute message $(m_1, \ldots, m_n)$ as $S^{-1}\mathbf{x}$
- Decryption: need to compute root of univariate polynomial of degree $D \leq 2p^d$
- Cantor-Zassenhaus (Lecture 8): runtime $\mathcal{O}(D^3 + nD^2 \log p)$
  - d cannot be taken too large
  - Multiple roots are possible so need some form of redundancy in message
  - Also signature is possible, need counter to admit root for each message

Hidden Field Equations (HFE): direct attack

- Public key of HFE does **not** behave like random system of polynomials
- Upper bound for degree of regularity

$$d_{reg} \leq \frac{p-1}{2}(\lfloor \log_p(D-1) \rfloor + 1) + 2$$

- Much lower than for random systems, so HFE is not secure
- Variants of HFE: HFEv-, GUI, MHFEv
- Typical parameters: $p = 2$, $n \sim 128$, $D \sim 10$

Further reading

- Available on Toledo:
  - Chapter 11: Polynomial systems and Gröbner base computations of book “Algorithmic cryptanalysis” by Joux
  - Summer school slides on HFE and UOV/Rainbow by Petzoldt
- Short summary: “What is a Gröbner basis?” by Sturmfels `https://www.ams.org/notices/200510/what-is.pdf`
- Breaking Rainbow takes a weekend on a laptop, by Beullens `https://eprint.iacr.org/2022/214.pdf`