CS5760: Topics in Cryptanalysis **26 June 2025**

Lecture 9: Introduction to Gröbner Bases

Instructor: Maria Francis *Scribe: Gautam Singh*

In multivariate polynomial rings, long division can yield different results depending on the monomial order chosen. Gröbner bases provide a systematic way to handle these variations by defining a canonical form for polynomials. In particular, the ordering of divisors does not matter in $k[x_1, \ldots, x_n]$.

9.1 Monomial Orders

We begin by defining a *monomial order* on the polynomial ring $k[x_1, \ldots, x_n]$.

Definition 9.1 (Monomial Order)**.** A monomial order is an order on the set of monomials in $k[x_1, \ldots, x_n]$ satisfying the following properties:

1. It is a *total ordering*.
2. If $\alpha > \beta$ are monomials, then $\alpha\gamma > \beta\gamma$ for any monomial γ.
3. It is *well ordering*, meaning every non-empty set of monomials has a least element.

An example of a monomial order is *lexicographic order* (lex), where we set an ordering on the variables such as $x_1 > x_2 > \ldots > x_n$ and compare monomials by considering the leftmost nonzero element in their pointwise difference. Accounting for the total degree of the monomials gives the *graded lexicographic order* (grlex) and *graded reverse lexicographic order* (grrevlex).

9.2 Monomial Ideals

Definition 9.2 (Monomial Ideal)**.** An ideal $I \subseteq k[x_1, \ldots, x_n]$ is called a *monomial ideal* if there is a finite subset $A \subset \mathbb{N}^n$ such that I consists of all polynomials that can be written as finite sums of monomials cx^α where $c \in k$ and $\alpha \in A$.

In other words, monomial ideals are those which have a generator solely consisting of monomials.

Lemma 9.1 (Dickson's Lemma)**.** *All monomial ideals in $k[x_1, \ldots, x_n]$ are finitely generated.*

Theorem 9.1 (Hilbert Basis Theorem)**.** *Any ideal in $R[x_1, \ldots, x_n]$ is finitely generated if and only if it is*

Definition 9.3. Let $I \in k[x_1, \ldots, x_n]$ be an ideal other than $\{0\}$. We define the following sets.

1. $\mathrm{LT}(I)$ is the set of leading terms of the polynomials in I.

Suppose that $I = \langle f_1, \ldots, f_s\rangle$ is an ideal. Then $\langle \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s)\rangle \subseteq \mathrm{LT}(I)$, with equality iff $\langle f_1, \ldots, f_s\rangle$ is a Gröbner basis of I.

Proposition 9.2 (Existence of Gröbner Bases)**.** *Let $I \subseteq k[x_1, \ldots, x_n]$ be an ideal. Then,*

1. *$\langle \mathrm{LT}(I) \rangle$ is a monomial ideal.*
2. *$\exists\, g_1, \ldots, g_t \in I$ such that $\langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle = \langle \mathrm{LT}(I) \rangle$.*

Definition 9.4 (Gröbner Basis)**.** Fix a monomial order. A finite subset $G = \{g_1, \ldots, g_t\}$ of an ideal I is said for be a Gröbner basis of I iff $\langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle = \langle \mathrm{LT}(I) \rangle$.

In particular, we also have $\langle g_1, \ldots, g_t \rangle = I$.

9.3 Properties of Gröbner Bases

1. Remainder on division of f by G is unique.

Definition 9.5 (S-Polynomial)**.** Let $f, g \in k[x_1, \ldots, x_n]$ be two polynomials with $\mathrm{lm}(f) = x^\alpha$ and $\mathrm{lm}(g) = x^\beta$ and γ be the least common multiple (LCM) of $\mathrm{lm}(f)$ and $\mathrm{lm}(g)$, i.e., $\gamma_i = \max(\alpha_i, \beta_i)$. The S-polynomial of f and g is defined as

$$S(f,g) \triangleq x^\gamma \left(\frac{f}{\mathrm{lt}(f)} - \frac{g}{\mathrm{lt}(g)} \right) \tag{9.1}$$

The S-polynomial is a way to combine two polynomials such that their leading terms are eliminated.

Theorem 9.3 (Buchberger's Criterion)**.** *Let I be a polynomial ideal. Then a basis $G = \{g_1, \ldots, g_t\}$ of I is a Gröbner basis of I iff for all $f, g \in I, f \neq g$, the S-polynomial $S(f,g)$ reduces to zero modulo G.*

This gives us *Buchberger's algorithm* for computing Gröbner bases.

9.4 Buchberger's Algorithm

Input: Finite set of polynomials $F = \{f_1, \ldots, f_s\}$.

Output: Gröbner basis G of the ideal generated by F.

1. Set $G \leftarrow F$.
2. For each pair of polynomials $f_i, f_j \in G$:
   (a) Compute the S-polynomial $S(f_i, f_j)$ using (9.1).
   (b) Reduce $S(f_i, f_j)$ modulo G.
   (c) If the result is non-zero, add it to G.
3. Repeat step 2 until no new polynomials are added to G.

To speed up this algorithm, especially the reduction step, we can use signatures of polynomials p to predict which polynomials in G will contribute to the reduction of p.