CS5760: Topics in Cryptanalysis **24 July 2025**

Lecture 8: Introduction to Gröbner Bases

Instructor: Maria Francis *Scribe: Gautam Singh*

Gröbner bases are a powerful tool for solving nonlinear polynomial systems. They generalize the concept of a basis in linear algebra to polynomial ideals. In cryptography, it was mainly used to compute signatures, namely the F5 signature scheme.

8.1 Introduction

Definition 8.1 (Monomial)**.** A monomial in $k[x_1, x_2, \ldots, x_n]$ is an expression of the form $x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$ where a_i are non-negative integers.

The *degree* of a monomial $x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$ is defined as the sum of the exponents, i.e., $a_1 + a_2 + \cdots + a_n$. A shorthand notation for a monomial is x^a where $a = (a_1, a_2, \ldots, a_n)$. In particular, $x^\alpha = 1$ when $\alpha = (0, 0, \ldots, 0)$.

Definition 8.2 (Polynomial)**.** A polynomial f in $k[x_1, x_2, \ldots, x_n]$ with coefficients in k is a finite linear combination of monomials. Mathematically, a polynomial can be represented as $f = \sum_\alpha a_\alpha x^\alpha$ where $a_\alpha \in k$ and the sum is taken over a finite set of n-tuples $\alpha = (a_1, a_2, \ldots, a_n) \in \mathbb{N}^n$.

In particular, a_α is called the *coefficient* of the monomial x^α and the product $a_\alpha x^\alpha$ is called a *term*.

Polynomials are closed in the ring $k[x_1, x_2, \ldots, x_n]$ under addition and multiplication. However, in the usual sense, multiplicative inverses of polynomials do not exist.

Definition 8.3 (Affine Space)**.** Given a field k and $n \in \mathbb{N}$, the n-dimensional affine space over k is given by

$$k^n \triangleq \{(a_1, a_2, \ldots, a_n) \mid a_i \in k \ \forall \ i = 1, 2, \ldots, n\}. \tag{8.1}$$

Affine spaces connect algebra with geometry.

Proposition 8.1. *Let k be an infinite field and $f \in k[x_1, x_2, \ldots, x_n]$ be a polynomial. Then, f is a zero function iff f is the zero polynomial.*

Notice that this may not be the case in finite fields such as $\mathbb{F}_2$.

Corollary 8.2. *Let k be an infinite field and $f, g \in k[x_1, x_2, \ldots, x_n]$. Then, $f = g$ in $k[x_1, x_2, \ldots, x_n]$ iff f and g are the same function.*

Theorem 8.3 (The Fundamental Theorem of Algebra)**.** *Every non-constant $f \in \mathbb{C}[x]$ has a root in $\mathbb{C}$.*

Polynomials that have roots in their field of coefficients are called *algebraically closed*.

Definition 8.4 (Affine Varieties)**.** Let k be a field and $f_1, f_2, \ldots, f_s \in k[x_1, x_2, \ldots, x_n]$. Then, the affine variety defined by $f_1, f_2, \ldots, f_s$ is defined as

$$V(f_1, f_2, \ldots, f_s) \triangleq \{(a_1, a_2, \ldots, a_n) \in k^n \mid f_i(a_1, a_2, \ldots, a_n) = 0 \ \forall \ i = 1, 2, \ldots, s\} \tag{8.2}$$

In other words, the affine variety is the set of solutions to the polynomial system defined by $f_1, f_2, \ldots, f_s$. In particular, this reduces to Gaussian Elimination when considering linear polynomials.

Definition 8.5 (Ideal)**.** A subring $I \subseteq k[x_1, x_2, \ldots, x_n]$ is called an *ideal* if it satisfies the following properties.

1. (Absorption) If $f \in I$ and $h \in k[x_1, x_2, \ldots, x_n]$, then $hf \in I$.
2. (Closure) If $f, g \in I$, then $f + g \in I$.

Definition 8.6. Let $f_1, f_2, \ldots, f_s \in k[x_1, x_2, \ldots, x_n]$. Then, the ideal generated by $f_1, f_2, \ldots, f_s$ is given by

$$\langle f_1, f_2, \ldots, f_s \rangle \triangleq \left\{ \sum_{i=1}^{s} h_i f_i \mid h_i \in k[x_1, x_2, \ldots, x_n] \ \forall \ i = 1, 2, \ldots, s \right\}. \tag{8.3}$$

An ideal can have many generators. In particular, if $\langle f_1, f_2, \ldots, f_s \rangle = \langle g_1, g_2, \ldots, g_t \rangle$, then $V(f_1, f_2, \ldots, f_s) = V(g_1, g_2, \ldots, g_t)$.

We can also have the notion of an ideal given a variety space. That is, the ideal of a variety V is defined as

$$I(\mathcal{V}) \triangleq \{ f \in k[x_1, x_2, \ldots, x_n] \mid f(a_1, a_2, \ldots, a_n) = 0 \ \forall \ (a_1, a_2, \ldots, a_n) \in \mathcal{V} \}. \tag{8.4}$$

Note that for a given ideal J, we have $J \subseteq I(V(J))$.