2 Polynomials over Finite Fields

In this section bitblock cryptography is “reduced” to algebra with polynomials.

Let K be a field. Given a polynomial $\varphi \in K[T_1, \ldots, T_n]$ in n indeterminates $T_1, \ldots, T_n$, we define a function $F_\varphi \colon K^n \longrightarrow K$ by evaluating the polynomial φ at n-tuples $(x_1, \ldots, x_n) \in K^n$,

$$F_\varphi(x_1, \ldots, x_n) := \varphi(x_1, \ldots, x_n).$$

Note that we carefully distinguish between polynomials and polynomial functions. Polynomials are elements of the polynomial ring $K[T_1, \ldots, T_n]$ where the elements T_i—the “indeterminates”—are a set of algebraically independent elements. That means that the infinitely many monomials $T_1^{e_1} \cdots T_n^{e_n}$ are linearly independent over K.

In general (for infinite fields) there are many more (“non-polynomial”) functions on K^n. But not so for finite fields—in other words, over a finite field all functions are polynoms:

Theorem 1 *Let K be a finite field with q elements, and $n \in \mathbb{N}$. Then every function $F \colon K^n \longrightarrow K$ is given by a polynomial $\varphi \in K[T_1, \ldots, T_n]$ of partial degree $\leq q-1$ in each T_i.*

The proof of Theorem 1 is in Appendix B, a more elementary proof for the case $K = \mathbb{F}_2$ is in Appendix C.

Corollary 1 *Let $m, n \in \mathbb{N}$. Then every map $F : K^n \longrightarrow K^m$ is given by an m-tuple $(\varphi_1, \ldots, \varphi_m)$ of polynomials $\varphi_i \in K[T_1, \ldots, T_n]$ of partial degree $\leq q-1$ in each T_i.*

Corollary 2 *Every map $F \colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^m$ is given by an m-tuple $(\varphi_1, \ldots, \varphi_m)$ of polynomials $\varphi_i \in \mathbb{F}_2[T_1, \ldots, T_n]$ all of whose partial degrees are ≤ 1.*

From this the **algebraic normal form (ANF)** of a Boolean function $F \colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ derives: For a subset $I = \{i_1, \ldots, i_r\} \subseteq \{1, \ldots, n\}$ let x^I be the monomial

$$x^I = x_{i_1} \cdots x_{i_r}.$$

Then F has a unique representation as

$$F(x_1, \ldots, x_n) = \prod_I a_I x^I \quad \text{for all } x = (x_1, \ldots, x_n) \in K^n \text{ where } a_I = 0 \text{ or } 1.$$

In particular the 2^n monomial functions $x \mapsto x^I$ constitute a basis of the vector space $\mathrm{Map}(\mathbb{F}_2^n, \mathbb{F}_2)$ over $\mathbb{F}_2$, and the number of these functions is 2^{2^n}.