My notes on cryptography

Omid Bodaghi

March 2, 2025

Contents

Part I

Prerequisites

Chapter 1

Polynomial Functions

Definition 1.1. A *polynomial function* f of degree d is a function of the form

$$f(x) = c_0 + c_1x + c_2x^2 + \cdots + c_dx^d,$$

where $c_d \neq 0$. Each term c_ix^i is called a monomial.

A polynomial function

$$f(X) \in \mathbb{F}^{(\leq d)}[X]$$

is said to be of degree at most d, where the coefficients are taken from the finite field $\mathbb{F}$.

In such a polynomial, all arithmetic operations—such as addition and multiplication—are performed in $\mathbb{F}$. For example, to compute the expression $c_0 + c_2x^2$, one first computes $x^2 = x \cdot x$ in $\mathbb{F}$, then multiplies by c_2, and finally adds c_0, with each operation carried out in $\mathbb{F}_p$.

Remark 1.1. Polynomials that have no roots in the real numbers may possess roots in a finite field, and conversely, polynomials that have real roots may have no roots in a finite field [Rar25].

Definition 1.2. A *multivariate polynomial function* $f(X_1, X_2, \ldots, X_n)$ is a polynomial function in more than one variable. A polynomial function in a single variable is called *univariate.*

In a multivariate polynomial function with ℓ variables, each term(monomial) has the form

$$c\, X_1^{d_1} X_2^{d_2} \cdots X_\ell^{d_\ell},$$

and its degree is given by $d_1 + d_2 + \cdots + d_\ell$. The *total degree* of the polynomial is the maximum degree among all its monomials. Multivariate polynomial functions over a filed $\mathbb{F}$ are commonly denoted either as $f(x_1, x_2, \ldots, x_\ell)$, with each $x_i \in \mathbb{F}$, or as $f(x)$ where $x \in \mathbb{F}^\ell$.

1.1 SZDL Lemma

Definition 1.3. In a polynomial function $f(X)$, an element x is called a *root* (or *zero*) of f if

$$f(x) = 0.$$

Theorem 1.1. *Let $f(X) \in \mathbb{F}^{(\leq d)}[X]$ be a polynomial of degree at most d over the finite field $\mathbb{F}$. Then $f(X)$ has at most d distinct roots.*

Proof. This an informal proof. Assume for the sake of contradiction that $f(X)$ has $d+1$ distinct roots, say $x_1, x_2, \ldots, x_{d+1}$. Then $f(X)$ is divisible by

$$(X - x_1)(X - x_2) \cdots (X - x_{d+1}),$$

which is a polynomial of degree $d + 1$. This contradicts the assumption that $f(X)$ is of degree at most d. Hence, $f(X)$ cannot have more than d distinct roots. $\square$

Lemma 1.2. *Schwartz-Zippel Lemma: Let $f(X_1, X_2, \ldots, X_\ell) \in \mathbb{F}[X_1, X_2, \ldots, X_\ell]$ be a nonzero multivariate polynomial with total degree d. If the variables $x_1, x_2, \ldots, x_\ell$ are chosen uniformly at random from $\mathbb{F}$, then*

$$\Pr\Big[f(x_1, x_2, \ldots, x_\ell) = 0\Big] \leq \frac{d}{|\mathbb{F}|},$$

where $|\mathbb{F}|$ denotes the size of the field.

The univariate case follows by setting $\ell = 1$.

1.1.1 Zero Polynomial

Consider a nonzero ℓ-variate polynomial function f of total degree d over $\mathbb{F}_p$. For a randomly chosen point $r \in \mathbb{F}_p^\ell$, we have

$$\Pr[f(r) = 0] \leq \frac{d}{|\mathbb{F}_p|}.$$

For example, if $\mathbb{F}_p$ is such that $|\mathbb{F}_p| \approx 2^{256}$ and the total degree is 2^{20}, then by Lemma 1.2,

$$\Pr[f(r) = 0] \leq \frac{2^{20}}{2^{256}} = \frac{1}{2^{236}},$$

which is an exceedingly small probability.

Consequently, if for a random r we find that $f(r) = 0$, we can conclude—with overwhelming probability— that f is the zero polynomial. Although there is a slight chance of error, it is negligible in practice.

1.1.2 Equality of Polynomial Functions

Consider two multivariate polynomial functions $f(X)$ and $g(X)$, each having total degree at most d. By the Schwartz-Zippel Lemma, if a randomly chosen point r satisfies $f(r) = g(r)$, then with high probability $f(X)$ and $g(X)$ are identical. To see this, define

$$h(X) = f(X) - g(X).$$

Then $h(X)$ has degree at most d, and if $f(r) = g(r)$, we have $h(r) = 0$. Since a nonzero polynomial of degree at most d vanishes with probability at most $d/|\mathbb{F}|$, it follows that with high probability h must be the zero polynomial. Hence, $f(X) = g(X)$.

References

[Rar25] RareSkills. *Finite Fields*. Accessed: 2025-03-01. 2025. URL: https://www.rareskills.io/post/finite-fields.

Part II

Zero Knowledge Proofs