My notes on cryptography

Omid Bodaghi

March 3, 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 [**rareskills_finitefields**].

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 $x \in \mathbb{F}^\ell$.

Definition 1.3. In a polynomial function $f(X)$, an element x is called a *root* (or *zero*) of f if $f(x) = 0$.

1.1 SZDL Lemma

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. □

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, $f(X) = g(X)$.

Part II

Zero Knowledge Proofs

Chapter 2

Plonk Proof System

This section provides an overview of the PLONK proof system for arithmetic circuits. In this chapter, we assume the existence of a polynomial commitment scheme (e.g., the KZG commitment scheme) and show how to use such a commitment to construct the PLONK proof system.

Throughout this chapter, we denote the commitment of polynomial function f as com_f.

2.1 Vanishing Polynomial

Let $\mathbb{F}_p$ be a field of large prime order p, and let $\Omega \subseteq \mathbb{F}_p$ be a subset with $|\Omega| = k$. In the following sections, we define efficient polynomial IOPs (Interactive Oracle Proofs) for various tasks over Ω.

Remark 2.1. Using a specific subset Ω rather than the entire field $\mathbb{F}_p$ allows us to work with a manageable set of evaluation points. If the entire field were used, the corresponding vanishing polynomial would have degree p, which is impractical for computation.

Definition 2.1 (Vanishing Polynomial)**.** The *vanishing polynomial* of Ω, denoted by $Z_\Omega(X)$, is the unique polynomial that evaluates to zero at every point in Ω. Thus, we have

$$Z_\Omega(X) = \prod_{a \in \Omega} (X - a),$$

which implies that the degree of $Z_\Omega(X)$ is $|\Omega|$.

For the specific case where w is a primitive kth root of unity (i.e., $w^k = 1$) and

$$\Omega = \{1, w, w^2, \ldots, w^{k-1}\} \subset \mathbb{F}_p,$$

the vanishing polynomial simplifies to

$$Z_\Omega(X) = X^k - 1.$$

Remark 2.2. In the case where $\Omega = \{1, w, w^2, \ldots, w^{k-1}\}$, the vanishing polynomial can be evaluated efficiently using exponentiation by squaring, which requires approximately $\log_2 k$ multiplications; when counting both squaring and multiplication steps, the total comes to roughly $2 \log k$ operations. In contrast, for a general subset Ω, directly computing

$$Z_\Omega(X) = \prod_{a \in \Omega} (X - a)$$

would require $k - 1$ multiplications, making it much less efficient for large k.

This significant speedup is why, in the subsequent sections, we restrict ourselves to the case

$$\Omega = \{1, w, w^2, \ldots, w^{k-1}\}.$$

2.2 Zero Test

Assume a prover P wants to prove to a verifier V that

$$f(a) = 0 \quad \text{for all } a \in \Omega,$$

and the verifier already holds a commitment com_f to the polynomial f. Let $\Omega \subset \mathbb{F}_p$ be a subset of size $|\Omega| = k$, and assume $\deg(f) \leq d$.

The naive approaches for the verifier are:

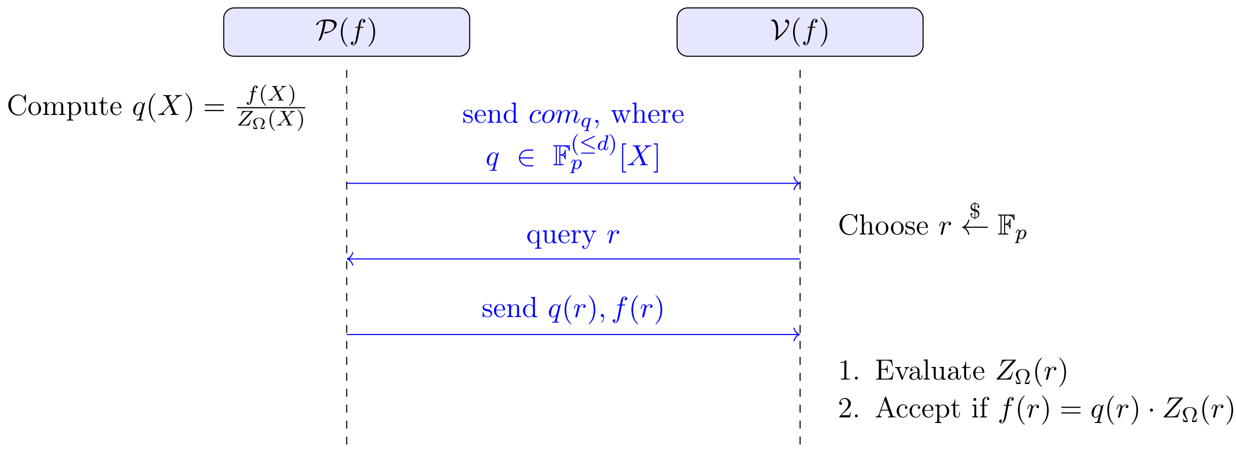
1. The verifier directly evaluates f on every point in Ω and checks if each evaluation is zero. This requires $\mathcal{O}(k)$ polynomial evaluations, which is inefficient for large k.

2. The verifier queries the prover to prove correctness of $f(a) = 0$ for each $a \in \Omega$. This yields $\mathcal{O}(k)$ individual proofs, also inefficient.

By using an Interactive Oracle Proof (IOP) and a vanishing polynomial, we can reduce the complexity significantly. The key observation is:

$$\text{If } f(a) = 0 \text{ for all } a \in \Omega, \quad \text{then} \quad f(X) = q(X) \cdot Z_\Omega(X),$$

where $Z_\Omega(X)$ is the vanishing polynomial over Ω.



Protocol Overview

1. **Compute and Commit to q:** The prover computes the polynomial $q(X)$ such that $f(X) = q(X)\, Z_\Omega(X)$. Since $\deg(f) \leq d$, we have $\deg(q) \leq d$. The prover sends a *commitment* to q (denoted com_q) to the verifier.

2. **Random Challenge:** The verifier samples a random challenge $r \in \mathbb{F}_p$ (public-coin protocol). The verifier sends r to the prover.

3. **Opening the Commitments:** The prover returns:

$$f(r), \quad q(r),$$

along with proofs (in the polynomial commitment scheme) that these openings are consistent with the committed polynomials f and q. This ensures the prover cannot lie about the polynomial values.

4. **Check the Factorization:** The verifier locally computes $Z_\Omega(r)$. Then it checks the relation
$$f(r) \stackrel{?}{=} q(r) \cdot Z_\Omega(r).$$
If this holds, the verifier accepts; otherwise, it rejects.

Informal Security Argument. If $f(X)$ truly vanishes on Ω, then there is a valid $q(X)$ of degree at most d, and the relation $f(r) = q(r)\, Z_\Omega(r)$ holds for all r. The verifier accepts.

Conversely, define
$$h(X) \;=\; f(X) \;-\; q(X)\, Z_\Omega(X).$$
If $f(X)$ does *not* vanish on Ω, then no polynomial $q(X)$ of degree at most d can satisfy $f(X) = q(X)\, Z_\Omega(X)$. Consequently, $h(X)$ is a nonzero polynomial. A nonzero polynomial of degree $\deg(h)$ over $\mathbb{F}_p$ can have at most $\deg(h)$ roots. Hence, when the verifier selects a random $r \in \mathbb{F}_p$, the probability that $h(r) = 0$ is at most $\deg(h)/|\mathbb{F}_p|$. Therefore, except with negligible probability, the verifier's check
$$f(r) \stackrel{?}{=} q(r)\, Z_\Omega(r)$$
will fail, and the verifier will reject. □

2.3 Product Check

2.4 Premutation Check

2.5 Prescribed Permutation Check