CS355: Applied Zero Knowledge Proofs	**Spring 2025**

Assignment #3

Due: 11:59pm on Thu, May 29, 2025, on Gradescope (each answer on a separate page)

Problem 1. (*PCS batch opening*) Recall that a polynomial commit scheme (PCS) lets one to commit to a univariate polynomial $f \in \mathbb{F}^{(\leq d)}[X]$ by computing a commitment string com_f. Later the committer can prove that for a given $x, y \in \mathbb{F}$, the committed polynomial satisfies:

$$f(x) = y \quad \text{and} \quad f \in \mathbb{F}^{(\leq d)}[X].$$

In other words, the PCS provides a proof system for the instance-witness relation

$$\mathcal{R} := \Big\{ \big((com_f, x, y), f\big) \;:\; f(x) = y,\; f \in \mathbb{F}^{(\leq d)}[X],\; com_f = \text{Commit}(f) \Big\}$$

Suppose that the committer wants to open the committed polynomial f at k distinct points $x_1, \ldots, x_k \in \mathbb{F}$, where $k < d$. That is, it wants a proof system for the relation

$$\mathcal{R}_k := \Big\{ \Big(\big(com_f, \{x_i, y_i\}_{i=1}^k\big), f\Big) \;:\; \{f(x_i) = y_i\}_{i=1}^k,\; f \in \mathbb{F}^{(\leq d)}[X],\; com_f = \text{Commit}(f) \Big\}$$

Clearly it can run the PCS opening proof k times, once for each x_i. Our goal is to design a proof system for $\mathcal{R}_k$ that only runs the PCS opening proof *twice*. This is called a batch opening proof.

a. Let $v(X) := \prod_{i=1}^k (X - x_i)$ and let $u(X)$ be a degree $k-1$ polynomial that satisfies $u(x_i) = y_i$ for $i = 1, \ldots, k$. Prove that $f(x_i) = y_i$ for $i = 1, \ldots, k$ if and only if v divides $f - u$.

b. Suppose that $f(x_i) = y_i$ for $i = 1, \ldots, k$. Then $q(X) := (f - u)/v$ is a polynomial in $\mathbb{F}^{(\leq d-k)}[X]$. The prover will send a commitment com_q for $q(X)$ to the verifier. Now use the fact that $q \cdot v = f - u$ to design a proof system for $\mathcal{R}_k$, where the prover only sends one opening proof for f and one opening proof for q. Describe your proof system for $\mathcal{R}_k$ as an interactive proof between the prover and the verifier. Note that the verifier can compute u and v on its own.

c. Show that your proof system from part (b) has soundness error at most d/p, where $p := |\mathbb{F}|$. That is, the verifier will be fooled into accepting an incorrect statement with probability at most d/p.

Problem 2. (*a univariate PCS from a multilinear PCS*) In class we constructed a univariate PCS for polynomials in $\mathbb{F}^{(\leq d)}[X]$ and a multilinear PCS for polynomials in $\mathbb{F}^{(\leq 1)}[X_1, \ldots, X_k]$. Suppose you are given a multilinear PCS for polynomials in $\mathbb{F}^{(\leq 1)}[X_1, \ldots, X_k]$. Show how to use it to directly construct a univariate PCS for polynomials in $\mathbb{F}^{(\leq d)}[X]$, for $d = 2^k - 1$.

a. First, explain how to commit to a polynomial $f \in \mathbb{F}^{(\leq d)}[X]$.
Hint: to commit to $f \in \mathbb{F}^{(\leq d)}[X]$ first show how to map it to a multilinear polynomial g in $\mathbb{F}^{(\leq 1)}[X_1, \ldots, X_k]$ and then commit to g using the PCS at your disposal.

b. Next, explain how to open the committed polynomial at $x \in \mathbb{F}$.

Problem 3. (*Low degree test*) You are given a univariate PCS for polynomials in $\mathbb{F}^{(\leq d)}[X]$. For $k < d$, your goal is to design a proof system for the relation

$$\mathcal{R}_k := \left\{ (com_f, f) \ : \ f \in \mathbb{F}^{(\leq k)}[X], \ com_f = \text{Commit}(f) \right\}$$

That is, the verifier should only accept a commitment to a polynomial whose degree is at most k. **Hint:** First prove that for all $f \in \mathbb{F}^{(\leq d)}[X]$ we have that $\deg(f) \leq k$ if and only if $f(1/X) \cdot X^k$ is in $\mathbb{F}^{(\leq d)}[X]$. Use this fact to build your proof system. One can alternatively use the fact that $f \in \mathbb{F}^{(\leq d)}[X]$ satisfies $\deg(f) \leq k$ if and only if $f \cdot X^{d-k} \in \mathbb{F}^{(\leq d)}[X]$, but we prefer that you use the first fact to design your proof system.

Problem 4. (*Univariate table lookup*) You are given a univariate PCS for polynomials in $\mathbb{F}^{(\leq d)}[X]$. For a set $H \subseteq \mathbb{F}$ define $f(H) := \{f(x) \mid x \in H\}$. Let $H := \{1, \omega, \omega^2, \ldots, \omega^{d-1}\} \subseteq \mathbb{F}$. Your goal is to design a proof system for the relation

$$\mathcal{R}_H := \left\{ \big((com_f, com_g), (f, g)\big) \ : \ f(H) \subseteq g(H), \ com_f = \text{Commit}(f), \ com_g = \text{Commit}(g) \right\}$$

To simplify the problem, you may assume that f takes every value in $f(H)$ at most twice, that is for all pair-wise distinct $x, y, z \in H$ we cannot have $f(x) = f(y) = f(z)$.

Hint: For $h \in \mathbb{F}^{(\leq d)}[X]$ define the polynomial $\hat{h}(X) := \prod_{a \in H}(X - h(a))$. Observe that $f(H) \subseteq g(H)$ if and only if $\hat{f}$ divides $(\hat{g})^2$. Now try to build your proof system using a product check.

Discussion: This proof system is quite important — it can be used to ensure that all the entries in a computation trace are in a prescribed table. One can give an efficient proof system for this problem even without the simplifying assumption above. If you are curious to see how, take a look at this paper.