Math 480A2, Homework 12
Due November 17, 2022

Homework is graded out of a total of 10 points. Collaboration is permitted, but you must list all coauthors on a problem's solution at the top of the page, and your writing must be your own.

Problem 1. (3 points) Suppose that (U, V) is an (extractable) KZG commitment for a polynomial q with coefficients in $\mathbb{Z}/p\mathbb{Z}$. Given access to the "toxic waste" parameter τ of the key generation protocol, how could you produce opening information which causes a verifier to accept the claim "$q(z) = v$" for an incorrect value of v? You may assume that $z \neq \tau$.

Problem 2. (3 points) Let F be a finite field. Give an arithmetic circuit $\mathcal{C}$ over F representing the equation $f(x_1, x_2) = x_1^3 + x_1 x_2 - x_2^2 = y_1$ for inputs x_1 and x_2 and output y_1. If the input x_2 is changed to an auxiliary input w_1, what is the circuit satisfiability problem for $\mathcal{C}$ on input x_1 and output y_1?

Problem 3. (4 points) Let F be a field, and let $a, b, c \in F$. Construct an R1CS instance over F which is satisfiable if and only if $b \neq 0$ and $ab^{-1} = c$. In your solution, you may use the numbers a, b, and c as entries of your matrices, but not any more complicated arithmetic expressions in terms of these numbers. (*Note.* You may accomplish this either by translating an appropriate circuit satisfiability problem into an equivalent R1CS instance, or by constructing an R1CS instance "from scratch" without reference to any arithmetic circuit.)