Math 480A2, Homework 8
Due October 20, 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) Consider the following variant of Freivalds' algorithm for checking the product of two matrices. Let A, B, C be $n \times n$ matrices with entries in a finite field K. To check whether $AB = C$, let $x = (r_1, r_2, \ldots, r_n)$ be a vector with entries chosen uniformly at random from K, and check if $A(Bx) = Cx$. If this equality holds, conclude that $AB = C$, and otherwise, conclude that $AB \neq C$.

(Recall that in our original formulation of Freivalds' algorithm, we used a vector of the form $(1, r, r^2, \ldots, r^{n-1})$ for a single random value r in K. Now we instead choose all random entries.)

If $AB = C$, then it will always be the case that $A(Bx) = Cx$ because $A(Bx) = (AB)x$ for any matrices A and B. In the case that $AB \neq C$, use the Schwartz-Zippel lemma to prove that this algorithm will fail to successfully detect this fact with probability at most $1/|K|$.

Problem 2. (4 points) Give a possible transcript of the execution of the sum-check protocol in which a prover demonstrates to a verifier that, over $\mathbb{Z}/11\mathbb{Z}$,

$$\sum_{x,y,z \in \{0,1\}} 2x + y^2 z = 10$$

Problem 3. (3 points) Considering the sum from Problem 2 again, suppose a malicious prover $\mathcal{P}'$ knows ahead of time that the first random value chosen by $\mathcal{V}$ in the sum-check protocol will be $r_1 = 2$. What polynomial $g_1(y)$ can $\mathcal{P}'$ send to $\mathcal{V}$ as the first message of the first round so that $\mathcal{P}'$ can convince the verifier that the sum in Problem 2 is actually 3? How should $\mathcal{P}'$ proceed after this to cause $\mathcal{V}$ to accept the claim?