Math 480A2, Homework 13
Due December 1, 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. (5 points) Let F be a finite field, and let M be an $n \times n$ matrix with entries in F. Recall that an *eigenvector* of M is a nonzero vector $\mathbf{v}$ such that $M\mathbf{v} = \alpha\mathbf{v}$ for some $\alpha \in F$. Give an R1CS instance which, in conjunction with the polynomial IOP for R1CS-Sat we learned about in lecture, allows a prover to convince a verifier that they know an eigenvector of M. (*Hint.* A vector $\mathbf{v}$ is nonzero if and only if there exists a vector $\mathbf{w}$ whose dot product with $\mathbf{v}$ is equal to 1.)

Problem 2. (5 points) Review the steps of the polynomial IOP for R1CS-Satisfiability we discussed in class, and make a list of all of the polynomial commitments sent from the prover to the verifier in the protocol, the degree bounds for the committed polynomials, and the number of times each commitment is opened. For this list, you may interpret the bivariate polynomials $\hat{M}$ as polynomial commitments of "degree" less than n^2. Do the number of commitments and the number of openings depend on the size of the input R1CS instance?