CMPT 981/409 Algebra and Computation
Homework 5
Due: Wednesday, November 25, 3:30pm

Instructions: You may work on and discuss homework problems with one another. Each student must individually write and submit their own solutions on Crowdmark. Be sure to list any collaborations in which you participated and any external sources you used. The use of generative AI in any form is prohibited.

1. (Testing properties of circuits using PIT.) Design and analyze randomized polynomial-time algorithms to solve the following problems. Your algorithms should succeed with probability at least 2/3.

   (a) Given a division-free arithmetic circuit C and an index i, decide if the polynomial computed by C depends on the variable x_i.

   (b) Given a division-free arithmetic *formula* C, compute the degree d of the polynomial computed by C.

2. (Efficient division elimination.) In class, we saw a proof of *divison elimination*: given an arithmetic circuit C of size s that computes a polynomial $f \in \mathbb{C}[x_1, \ldots, x_n]$, there is another circuit D of size $\text{poly}(n, s, d)$ that computes f without using any division gates.

   Design and analyze a randomized polynomial-time algorithm to solve the following problem: given an arithmetic circuit C with division gates, print a description of a division-free arithmetic circuit D that computes the same polynomial as C. Your algorithm should succeed with probability at least 2/3.

3. (Lower bounds for hitting sets.) Suppose that $\mathcal{H} \subseteq \mathbb{C}^n$ is a set such that for every nonzero n-variate degree-d polynomial $f(x_1, \ldots, x_n)$ of sparsity at most s, there is a point $a \in \mathcal{H}$ such that $f(a_1, \ldots, a_n) \neq 0$. Prove that $|\mathcal{H}| \geq s$.

4. (EXTRA CREDIT: Identity testing over small fields.) Let p be a prime number and let $\mathbb{F}_p$ be the finite field of size p, i.e., the integers with arithmetic done modulo p. Consider the following variant of the polynomial identity testing problem: given an n-variate arithmetic circuit C defined over $\mathbb{F}_p$, accept C if and only if it computes a nonzero *function* over $\mathbb{F}_p^n$. Prove that this version of the identity testing problem is NP-hard.

   You may use the fact that the following problem is NP-hard: given a boolean circuit C, decide whether there is an input on which C outputs TRUE.

   (Hint: Reduce from circuit satisfiability. Work over the integers modulo 2.)