CS 70 Discrete Mathematics and Probability Theory
Fall 2025 Sabin, Hug

DIS 7A

Preparing For The Midterm

The midterm is tomorrow! The goal of today is to allow you to practise the style of questions that will be asked on the midterm. The questions on this worksheet are most similar to the long-answer questions on the midterm. On tomorrow's midterm, there will also be multiple choice and true/false questions.

Please refer to our post on Ed for all the midterm logistics.

And remember, it's important to come to the exam well rested. Make sure to get some sleep and relax before the midterm. Alongside this discussion, we're also offering support in office hours if you have any questions or concepts you'd like to clarify.

Best of luck! You've got this.

1 Induction

Note 3

Prove that $\forall n \in \mathbb{N}$, we have $1^3 + 2^3 + \cdots + n^3 = (1 + 2 + \cdots + n)^2$.

Hint: You may use the fact that $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$. *You should not need to expand* $(n+1)^3$.

2 Polynomials

Note 8

(a) Working under GF(5), the degree 2 polynomial that passes through the points $(0,1)$, $(1,2)$, and $(2,0)$ can be written in the form ax^2+bx+c for some coefficients a, b, and c. What are the coefficients of this polynomial? (Hint: this might be easier with linear equations rather than Lagrange.)

(b) Suppose we have a degree 1 polynomial $P(x)$ in GF(5). The points $(0,1)$, $(1,3)$, $(2,1)$, and $(3,2)$ are received from a communication channel that has at most 1 corruption.

(i) What is $P(x)$?

(ii) What is the error polynomial, $E(x)$?

3 Graph Proof

Note 5

Let $G = (V, E)$ be a disconnected graph with no self-loops. Prove that its complement $\overline{G} = (V, \overline{E})$ is connected. (Recall that the complement of a graph is defined such that for $u, v \in V$: $(u, v) \in E$ if and only if $(u, v) \notin \overline{E}$.)

4 Secret Sharing

Note 8

The planning committee for The International Conference on Hackathon Organization has designed the following secret sharing scheme:

- 70 points of a 49-degree shared polynomial have each been assigned to the 70 delegations, one point per delegation.
- Each delegation contains 10 delegates.
- They each receive a point of a degree 5 delegation-specific polynomial.
- Delegates can come together to recover their delegation's point on the shared polynomial using the delegation-specific polynomial.

A *rogue delegate* is an all-powerful delegate: they know all of the polynomials and have control over which delegation that they are placed in. The rogue delegates purposely manipulate their point on their delegation-specific polynomial to mess up the conference.

The planning committee will use the Berlekamp-Welch algorithm on the delegation-specific polynomials and on the shared polynomial to attempt to recover the (stable) correct secret. What is the largest number of rogue delegates that can attend the conference such that the committee is guaranteed to recover the correct secret? Justify your answer.

5 How Many Solutions?

Note 6

Consider the equation $ax \equiv b \pmod{p}$ for prime p. In the below three parts, all values a,b,x are defined as values in the range $\{0,1,\dots p-1\}$. In addition, include justification for your answers to all the subparts of this problem.

(a) For how many pairs (a,b) does the equation have a unique solution?

(b) For how many pairs (a,b) does the equation have no solution?

(c) For how many pairs (a,b) does the equation have p solutions?

Now, consider the equation $ax \equiv b \pmod{pq}$ for distinct primes p,q. In the below three parts, all values a,b,x are defined as values in in the range $\{0,1,\dots pq-1\}$.

(d) If $\gcd(a,pq) = p$, show that there exists a solution if and only if $b = 0 \pmod{p}$. (Hint: Try to relate modular equations to their corresponding algebraic equations, and vice versa.)

(e) If $\gcd(a,pq) = p$ and there is a solution x, show that there are exactly p solutions. (Hint: consider how you can generate another solution $x + \_\_\_$)

(f) For how many pairs (a,b) are there exactly p solutions?