ADVANCED MATHEMATICAL STRUCTURES

END SEMESTER EXAM

Instructor: Girish Varma • Course Code: IMA410

Solve any 5 problems • 7 marks each

Counting

Show by a counting argument that the number of k-element subsets of $\{0,1,\dots,n-1\}$ that contain no two consecutive numbers modulo n, is exactly

$$\frac{n}{n-k}\binom{n-k}{k}.$$

Hint: We want to colour k non-consecutive points red. Consider two cases, 1 is coloured red, and otherwise. In the first case, consider n - k uncoloured points on a circle and place k red points in the spaces between them. Handle the second case similarly. (7 marks)

Cosets

Let H and K be subgroups of a group G.

- 1. Suppose A be coset of $H \cap K$ and B be coset of H. Show that either $A \cap B = \emptyset$ or $A \subseteq B$. (3.5 marks)
- 2. Suppose A is a coset of H and B is a coset of K. Prove that $A \cap B$ is either empty or else is a coset of the subgroup $H \cap K$. (3.5 marks)

3 Inclusion Exclusion

1. Consider a $2^n \times 2^n$ matrix \mathcal{I} with rows and columns indexed by subsets of [n] defined as follows:

$$\mathcal{I}_{A,B} = \begin{cases} 1 \text{ if } A \subseteq B \\ 0 \text{ otherwise} \end{cases}$$

The matrix \mathcal{I} is known as the set inclusion matrix. Find \mathcal{I}^{-1} explicitly, i.e. you should be able to write down $\mathcal{I}_{A,B}^{-1}$ for any $A,B\subseteq [n]$. (3.5 marks)

2. Using the first part or otherwise, show that the set disjointness matrix \mathcal{D} defined as:

$$\mathcal{D}_{A,B} = \begin{cases} 1 \text{ if } A \cap B = \emptyset \\ 0 \text{ otherwise} \end{cases}$$

is invertible. Find an explicit expression for \mathcal{D}^{-1} .

(3.5 marks)

4 Randomized Perfect Matching

Consider a bipartite graph G(V, V, E) with the left and right vertex set to be V = [n]. Let A be the matrix such that $A_{ij} = 1$ iff $(i, j) \in E$. Let

$$\operatorname{perm}(A) = \sum_{\sigma \in S_n} \left(\prod_{i \in [n]} A_{i\sigma(i)} \right) \quad \text{and} \quad \det(A) = \sum_{\sigma \in S_n} (-1)^{\operatorname{parity}(\sigma)} \left(\prod_{i \in [n]} A_{i\sigma(i)} \right)$$

- 1. Show that perm(A) is equal to the number of perfect matchings in G. (2 marks)
- 2. Let B be the matrix obtained from A by replacing A_{ij} with $x_{ij}A_{ij}$ where x_{ij} are some variables. Note that det(B), perm(B) are polynomials in these variables. Show that $det(B) \equiv 0$ (is the zero polynomial) if and only if there are no perfect matching. (2 marks)
- 3. Let B' be the random matrix obtained by substituting each x_{ij} with uniformly and independently chosen values from [2n]. Show that $\Pr[\det(B') = 0 | B \neq 0] \leq 1/2$. (1.5 marks)
- 4. Using the above give a randomized algorithm with one-sided error for checking whether a graph has perfect matching. (1.5 marks)

5 Turan's Theorem using Probabilistic Method

Turan's theorem (a weak version) states that:

Turan's Theorem: If G(V, E) is a graph with n vertices, m edges and d = 2m/n is the average degree, then there is an independent set in the graph of size at least n/2d.

We will prove this theorem using the probabilistic method. Let $S \subseteq V$ be a random subset of vertices chosen in such a way that we insert every vertex into S independently with probability p (we will choose a suitable value of p later).

Let X be the size of S. Find $\mathbb{E}X$.

(1 mark)

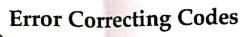
2, Let Y be the number of edges with both endpoints in S. Find EY.

(1 mark)

- 3. Show that there exists $S \subseteq V$ where the difference of the number of vertices in S and edges with both endpoints in S is at least $A(p) = np(1 \frac{1}{2}dp)$. (1.5 mark)
- 4. Show that there is an independent set in G with atleast A(p) vertices. (2 marks)
- 5. Choose value of p, so as to prove the Turan's Theorem. (1.5 marks)

6 Pairwise Independent Hash Family

Let p be a prime. For $a,b \in \mathbb{Z}_p$, define $h_{a,b} : \mathbb{Z}_p \to \mathbb{Z}_p$ by $h_{a,b}(x) = ax + b$. Then show that the collection of functions $H = \{h_{a,b} | a, b \in \mathbb{Z}_p\}$ is a pairwise independent hash family. (7 marks)



Let C be a binary code of block length n (odd number) and distance $d = \lceil n/2 \rceil$. Then the *Plotkin bound* says that $|C| \le 2n$.

You can prove this bound on your own to get all the 7 marks. Another option is to answer the following sequence of questions leading to the proof.

Let M be the maximum possible size of the code (|C|) such that minimum distance is $\lceil n/2 \rceil$. Assume C has size M (|C| = M).

- 1. Show that $\sum_{x,y \in C \times C: x \neq y} h(x,y) \ge M(M-1)d$ where h is the Hamming distance. (2 marks)
- 2. Consider the matrix $A \in \mathbb{F}_2^{M \times n}$ with the code words as the rows. Let s_i be the number of 1's in the *i*th column. Show that (3 marks)

$$\sum_{x,y\in C\times C: x\neq y} h(x,y) \leq \sum_{i=1}^{n} 2 \cdot s_i \cdot (M-s_i)$$

3. Show that $M \leq \frac{2d}{2d-n}$ and prove Plotkin's bound.

(2 marks)