Anish Banerjee, Shankh Gupta
Problem Set - 1
COL759: Cryptography
August 2023

Problem 1
An IPL tournament is played between n cricket teams, where each team plays exactly one match with every other team. How many matches are played? (This is easy.) Assume that no match ends in a tie. We say that a subset S of teams is *consistent* if it is possible to order teams in S as $T_1, \ldots, T_{|S|}$ (think of this as the strongest to weakest ordering) such that for every i, j with $1 \leq i < j \leq |S|$, T_i beats T_j. Prove that irrespective of the outcomes of the matches, there always exists a consistent subset S with $|S| \geq \log_2 n$.

Solution: The number of matches played is given by $\binom{n}{2} = \frac{n(n-1)}{2}$. For the second claim, we proceed using the Strong Induction. Consider the claim:

$$p(k) : \text{In a tournament of } k \text{ teams, always exists a consistent subset } S \text{ such that } |S| \geq \log_2(n+1)$$

Base Case: For $n = 2$, there are only two teams T_1 and T_2. Say T_1 wins against T_2. Then $\{T_1, T_2\}$ form a consistent subset with T_1T_2 being the required ordering. $|S| = 2 \geq \log_2 3$. So $P(2)$ is true. For $n = 3$, consider the outcome of any one match. Say T_1 wins against T_2. Consider the set $S = \{T_1, T_2\}$, which is consistent under the ordering T_1T_2. Also, $|S| = 2 \geq \log_2(n+1) = \log_2 4$.

Induction Hypothesis: Let $P(k)$ be true $\forall\ k < n$, $k \geq 2$.

Induction Step: Consider a tournament of n teams. We will construct a consistent subset for this tournament. Note that there will be $\frac{n(n-1)}{2}$ wins distributed amongst n teams, and so by Pigeon-Hole principle, exists a team T such that T wins at least $\lceil \frac{n(n-1)}{2n} \rceil = \lceil \frac{n-1}{2} \rceil$ matches.

Suppose the set of teams T wins against is X. Since $\lceil \frac{n-1}{2} \rceil < |X| < n$, by the induction hypothesis, there exists a consistent subset S of the teams in X such that,

$$|S| \geq \log_2(|X| + 1)$$

Thus, $\exists$ ordering $T_1T_2...T_{|S|}$ such that T_i beats $T_j\ \forall\ i < j$. Note that T wins against $T_k\ \forall\ T_k \in S$ and so the set $S' = \{T\} \cup X$ is also consistent, with the required ordering $TT_1T_2...T_{|S|}$. Now we have, $|S'| = |S| + 1 \geq \log_2(|X| + 1) + 1$. Since $\lceil \frac{n-1}{2} \rceil < |X|$ we have,

$$|S'| \geq \log_2\left(\left\lceil \frac{n-1}{2} \right\rceil + 1\right) + 1 \geq \log_2\left(\frac{n-1}{2} + 1\right) + 1 \geq \log_2(n+1)$$

Thus, we have $S' = T \cup S$ is the required consistent subset. ■

Problem 2 : Secure/Insecure PRGs PRFs

Solution:

Problem 3
Prove "Claim 2" from the proof of Schröder-Bernstein Theorem discussed in Lecture 5. Here is the statement of the claim. Let A and B be infinite sets, f be an injection from A to B, and g be an injection from B to A. Let $B' = \{b \in B \mid \exists b^* \in B \setminus \text{Im}(f)\ \exists k \in \mathbb{N} \cup \{0\} :\ b = (f \circ g)^k(b^*)\}$, and $A' = \{g(b) \mid b \in B'\}$. Then for every $b \in B$, the following statements are equivalent.

1. $b \in B'$.

2. If $f^{-1}(b)$ exists, then it is in A'.

3. $g(b) \in A'$.

Solution: **(1 $\implies$ 2)** Consider any $b \in B'$. By definition, suppose $a = f^{-1}(b)$, or $f(a) = b$. Now by the definition of B', we have that $b = (f \circ g)^k(b^*)$ for some $k \in \mathbb{N} \cup \{0\}$ and $b^* \in B \setminus \text{Im}(f)$. Thus we may write,

$$f(a) = (f \circ g)^k(b^*)$$

By definition of B', $b \neq b^*$ since $b \in Im(f)$ and so $k \geq 1$. Also, by injectivity of f we must have,

$$a = g\left((f \circ g)^{k-1}(b^*)\right) = g(\bar{b}),\ \bar{b} \in B'$$

Hence, $a \in A'$.

(2 $\implies$ 3) If $f^{-1}(b)$ exists and in A', then we have $a = f^{-1}(b) = g(\bar{b})$ for some $\bar{b} \in B'$. Write $\bar{b} = (f \circ g)^k(b^*)$ for some $k \in \mathbb{N} \cup \{0\}$ and $b^* \in B \setminus \text{Im}(f)$, and so we have,

$$b = f(a) = f \circ g\left((f \circ g)^k(b^*)\right) = (f \circ g)^{k+1}(b^*)$$

Hence, $b \in B'$ and $g(b) \in A'$.

(3 $\implies$ 1) Since $g(b) \in A'$, by definition of A' it follows that $b \in B'$ ■

Problem 4
Given a set A, the set of finite length strings over A is denoted by A^*. Prove that if A is a finite set, then A^* is necessarily countable. What can you say about the cardinality of A^* if A is countably infinite instead?

Solution: (a) Let s_P denoted a string over a set P, let s_i represent the i-th character of the string, and l_s denote the length of a string s. Define the set A_i as follows:

$$A_i = \{s_A \mid l_s = i\}$$

Note that,

$$A^* = \bigcup_{i=1}^{\infty} A_i$$

Given that A is a finite set, let us suppose it's cardinality is n. Then, cardinality of each A_i is, $|A_i| = n^i$. Thus, each A_i is finite.

We recall that if we have a countably infinite collection of sets, each of which is countable, then $\bigcup_{i=1}^{\infty} A_i$ is countable. Therefore, A^* is countable. ■

(b) By virtue of the countability of A we impose an ordering $a_1, a_2, ...$ on its elements. Define the set,

$$B_i = \{s_A \mid s_j \in \{a_1 a_2 ... a_i\}\ \forall\ j < l_s\}$$

B_i is the set of finite length strings over the finite set $\{a_1 a_2 ... a_i\}$. By part (a), B_i is countable. And we have,

$$A^* = \bigcup_{i=1}^{\infty} B_i$$

Once again, we have a countably infinite collection of sets, each of which is countable, and thus $\bigcup_{i=1}^{\infty} B_i$ is countable. Therefore, A^* is countable. ■

Problem 5
Prove by mathematical induction that every graph has at least two vertices having equal degree.

Solution: We proceed by induction on the number of vertices n of the graph. Consider the claim:

$$p(k) : \text{A graph with } k \text{ vertices at least two vertices with the same degree.}$$

Base Case: $n = 2$. If the two vertices of the graph are connected by an edge, then both have degree 1, else both have degree 0. So $P(2)$ is true.

Induction Hypothesis: Let $P(n-1)$ be true for some $n \geq 3,\ n \in \mathbb{N}$.

Induction Step: Consider a graph with n vertices. First consider the subgraph G' including any $n-1$ vertices, say $V = \{v_1, v_2, ...v_{n-1}\}$. By the induction hypothesis, $\exists$ vertices $v_i, v_j \in V$ of equal degree. Now when we consider the connection of the n-th vertex v_n there are three cases possible:

Case 1: v_n is connected to neither v_i nor v_j. Then their degrees remains unchanged and hence equal.

Case 2: v_n is connected to both v_i and v_j. Then their degrees are both increased by 1 and hence are still equal.

Case 3: If v_n is connected to v_i but not v_j (say). Let the degree of v_k be represented by d_k. Note that $d_k \in \{0, 1, 2, ...n-1\}\ \forall\ k \leq n$. However, if there exists $v : d_v = 0$ then cannot exist a vertex of degree $n-1$. Similarly if there exists $v : d_v = n-1$ then cannot exist a vertex of degree 0. So, $d_k \in \{0, 1, 2, ...n-2\}$ or $d_k \in \{1, 2, ...n-1\}$. So we have here $n-1$ pigeons (possible degrees) and n pigeonholes (vertices). Hence, by PHP, there must exist two vertices which have the same degree. ■