CS201

Mathematics For Computer Science

Indian Institute of Technology, Kanpur

Group Number: 35

Parag Gupta (180500), Satvik Jain (180678), Samarth Varma (180655)

End-Sem

Exam

Date of Submission: 22/12/2020

Question 1

Define two classes of n-variate polynomials as:

$$\begin{aligned} P_d(x_1, x_2, \ldots, x_n) &= \sum_{\substack{0 \le i_1, i_2, \ldots, i_n \le 1 \\ i_1 + i_2 + \cdots + i_n = d}} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n} \\ Q_d(x_1, x_2, \ldots, x_n) &= \sum_{\substack{0 \le i_1, i_2, \ldots, i_n \le d \\ i_1 + i_2 + \cdots + i_n = d}} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n} \end{aligned}$$

for all $d \ge 0$. Prove that:

$$\sum_{0 \le d \le r} (-1)^d P_d \cdot Q_{r-d} = 0$$

for all $r \ge 1$.

Solution

Let us define a function

$$F(y) = \prod_{i=1}^{N} (1 - x_i y) \tag{1.1}$$

$$\implies \frac{1}{F(y)} = \frac{1}{\prod_{i=1}^{N} (1 - x_i y)} \tag{1.2}$$

We will now prove that the co-efficients of y^d is related to $P_d(x_1, x_2, \ldots, x_n)$ and $Q_d(x_1, x_2, \ldots, x_n)$.

For equation (1.1), $F(y) = \prod_{i=1}^{N} (1 - x_i y) = (1 - x_1 y)(1 - x_2 y)(1 - x_3 y)...(1 - x_n y)$.

Here, the coefficients of y^d are given by collecting x_i's d times at once and summing over all the possible combinations.

Therefore, the coefficient is given by:

$$F(y) = \sum_{d=0}^{n} k_d y^d$$

Define $J = \{1, 2, 3..., n\}$. Now,

$$\begin{aligned} k_d &= \sum_{\substack{0 \le i_1, i_2, \ldots, i_n \le 1 \\ i_1 + i_2 + \cdots + i_n = d}} \prod_{r \in J} -(x_r)^{i_r} \\ &= (-1)^d \sum_{\substack{0 \le i_1, i_2, \ldots, i_n \le 1 \\ i_1 + i_2 + \cdots + i_n = d}} \prod_{r \in J} x_r^{i_r} \\ &= (-1)^d P_d(x_1, x_2, \ldots, x_n) \end{aligned} \tag{1.3}$$

Now, For equation (1.2), $\frac{1}{F(y)}$ can be written as

$$\frac{1}{F(y)} = \frac{1}{(1 - x_1 y)(1 - x_2 y) \ldots (1 - x_n y)}$$

From each basket $(1 - x_d y)^{-1}$, take out y^{d_k}, whose coefficient is given by $\binom{-1}{d_k}(-x_k)^{d_k}$ The collection of y^{d_k}'s such that $\sum_{k=1}^{n} d_k = d$ gives the coefficient of y^d. Here $0 \le d_1, d_2, \ldots, d_n \le d$. Therefore the coefficient of y^d becomes

$$\begin{aligned} &\sum_{\substack{0 \le d_1, d_2, \ldots, d_n \le d \\ d_1 + d_2 + \cdots + d_n = d}} \prod_{r=1}^{n} \binom{-1}{d_r} (-x_r)^{d_r} \\ &= \sum_{\substack{0 \le d_1, d_2, \ldots, d_n \le d \\ d_1 + d_2 + \cdots + d_n = d}} \prod_{r=1}^{n} x_r^{d_r} \\ &= \sum_{d \ge 0} Q_d(x_1, x_2, \ldots x_n) \end{aligned} \tag{1.4}$$

Therefore from equation (1.3) and (1.4), we get that

$$F(y) = \sum_{d=0}^{n} (-1)^d P_d(x_1, x_2, x_3 \ldots, x_n) y^d$$

$$\frac{1}{F(y)} = \sum_{d=0}^{n} Q_d(x_1, x_2, x_3 \ldots, x_n) y^d$$

Multiplying both $F(y)$ and $\frac{1}{F(y)}$, we get

$$\begin{aligned} 1 &= \left(\sum_{r \geq 0} (-1)^r P_r(x_1, x_2, x_3, \ldots, x_n) y^r \right) \left(\sum_{r \geq 0} Q_r(x_1, x_2, x_3, \ldots, x_n) y^r \right) \\ &= \sum_{r \geq 0} \left(\sum_{d=0}^{r} (-1)^d P_d(x_1, x_2, x_3, \ldots, x_n) Q_{r-d}(x_1, x_2, x_3, \ldots, x_n) \right) y^r \end{aligned} \tag{1.5}$$

Therefore from the above equation, the coefficient of y^r should be zero for every $r \geq 1$. Hence, for any $r > 0$

$$\sum_{d=0}^{r} (-1)^d P_d(x_1, x_2, \ldots, x_n) Q_{r-d}(x_1, x_2, \ldots, x_n) = 0.$$

Hence Proved

Question 2

The algorithm in Lecture 18 for finding a perfect matching is wrong. Find a counter example, i.e., a bipartite graph on which the algorithm fails. Fix the algorithm by suitably modifying the definition of subgraph H.

Solution

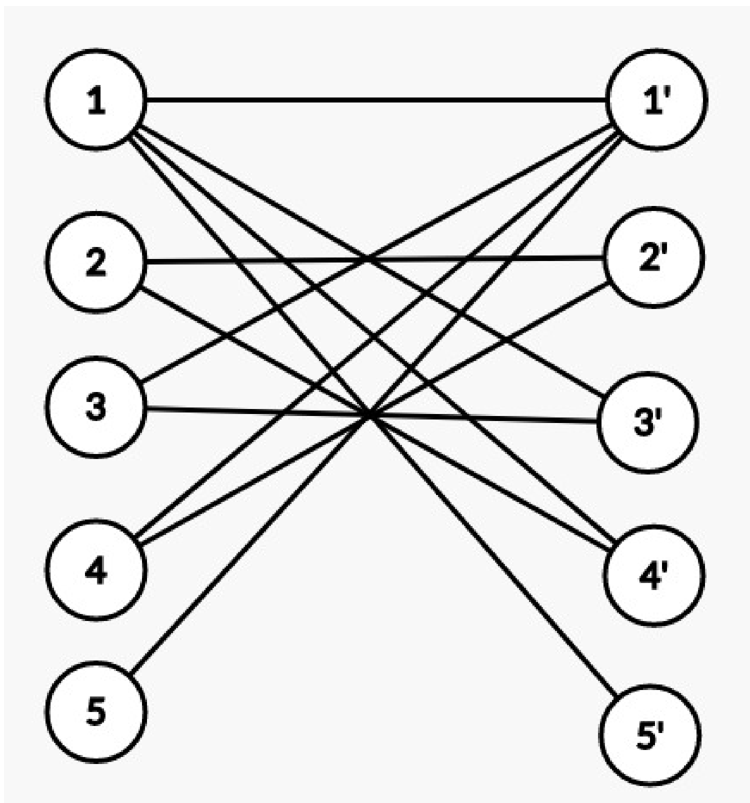

Figure 1: Graph G

Let $G = (V, E)$ be a bipartite graph such that $V = V_1 \cap V_2, V_1 \cap V_2 = \phi, E \subseteq V_1 \times V_2$
Let $V_1 = \{1, 2, 3, 4, 5\}$ and $V_2 = \{1', 2', 3', 4', 5'\}$
The graph G with it's edge set is given in figure 1. For convienience, We have represented the graph in the adjacency list-

- $a \to \{b, c\}$

This represents that there is an undirected edge connecting vertices a to b and a to c.

- $1 \rightarrow \{1', 3', 4', 5'\}$
- $2 \rightarrow \{2', 4'\}$
- $3 \rightarrow \{1', 3'\}$
- $4 \rightarrow \{1', 2'\}$
- $5 \rightarrow \{1'\}$

The graph formed by the above vertices and their respective edges is precisely given in figure 1 and it is a counter example to the algorithm given in lecture 18.
The explanation is as follows-

- After 3 iterations, we have $U = \{1, 2, 3\}$ and $\pi(U) = \{1', 2', 3'\}$ such that $\pi(1) = 1', \pi(2) = 2'$ and $\pi(3) = 3'$. This is easy to see because in all the first 3 iterations, there exists a $v \in V_2 \backslash \pi(U)$ and we simply set $\pi(u) = v$.
- In our next iteration, we take $u = 5$ and construct the graph H. Graph H is given in figure 2.
- Now we take $u' = 2$ and $v' = 4'$.
- Taking $u' = 2$ immediately leads to a problem as the path in T from u to u' is $5 - 1 - 4 - 2$. Here, π does not operate on 4 as it is not in U.
- Hence the path $v_0 = u, w_1, v_1, w_2, v_2, ..., w_k, v_k = u'$ in graph G, with $v_i = \pi^{-1}(w_i)$ for $1 \leq i \leq k$ can never be constructed.

We have the correct algorithm as follows-

- Let $G = (V_1, V_2, E)$ be a bipartite graph with $|V_1| = |V_2| = n$.
- We represent the perfect matching as a bijection $\pi : V_1 \rightarrow V_2$.
- We solve the algorithm iteratively and suppose that π has been defined for a subset U of V_1.
- Take any vertex $u \in V_1 \backslash U$.

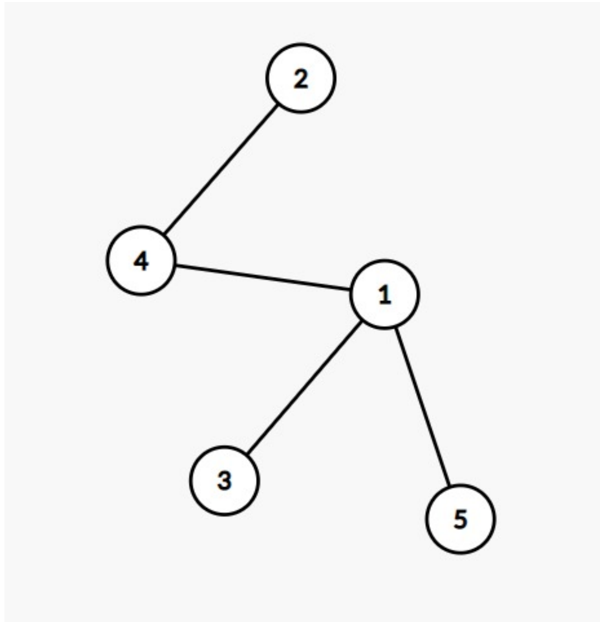

Figure 2: Graph H

- If there exists some $v \in V_2 \backslash \pi(U)$ such that $(u, v) \in E$, then let $\pi(u) = v$ and add u to the set U extending π. We are done and proceed for the next iteration.
- If $N(\{u\}) \subseteq \pi(U)$ we proceed as follows-
  - We now construct a graph $H = (V_1, E_H)$ such that there exists a **DIRECTED** edge from u_1 to $\pi^{-1}(u_2)$ iff $(u_1, u_2) \in E$ where $u_1 \in V_1$ and $u_2 \in \pi(U)$
  - Compute a spanning forest of H, and consider a tree T of this forest rooted at u.
  - We have $|N(T) \cap \pi(U)| \leq |T| - 1$ in G. This is easy to see because $v \in N(T) \cap \pi(U), \pi^{-1}(v) \in T$. Moreover, $u \in T$ but it is not possible to get u using π^{-1} as $u \notin U$. Since π is a one to one bijection, we can atmost map each v to $|T| - 1$ distinct elements and hence the bound.
  - It follows that if $N(T) \subseteq \pi(U)$ then $|N(T)| \leq |T| - 1$ and there is no perfect matching.
  - Now consider otherwise and consider a vertex $u' \in T$ such that $N(\{u'\}) \not\subseteq \pi(U)$ and u' is **reachable** from u in the directed graph H. Moreover, let $v' \in N(\{u'\}) \backslash \pi(U)$
  - Let $v_0 = u, v_1, v_2, ..., v_k = u$ be the path in T from u to u'

- This path corresponds to the path $v_0 = u, w_1, v_1, w_2, v_2, ..., w_k, v_k = u'$ in graph G, with $v_i = \pi^{-1}(w_i)$ for $1 \leq i \leq k$.
- Now, we simply redefine π as

$$\pi(u) = w_1, \pi(v_1) = w_2, \dots \pi(v_{k-1}) = w_k, \pi(u') = v'$$

.

- This extends π to one more vertex increasing the size of U.

• Repeating this iteratively until $U = V_1$ eventually makes π a perfect matching.

Question 3

Let G be connected graph on $n \geq 4$ vertices with $2n - 2$ edges. Prove that G has two cycles of equal length.

Solution

G is a connected graph. We arbitrarily root the tree at some node(say r) and consider a spanning tree of the graph. The longest path in the tree(diameter) must be of at most $n - 1$ length when the graph is a bamboo. Also, the spanning tree must contain exactly $n-1$ edges. So, we need to add exactly $(2n-2)-(n-1) = n-1$ more edges to the graph. Let the maximum distance between two nodes be d such that $2 \leq d \leq n - 1$. Hence there are at most $n - 2$ distinct distances possible between any two nodes. This boils down to choosing $n - 1$ objects from at most $n - 2$ distinct options. By pigeon-hole principle, one distance k must be repeated. Hence two pairs of nodes at a distance k apart must be connected by an edge. This means that the graph has two cycles of length $k + 1$.

Question 4

A completed Sudoku puzzle is a 9×9 grid filled in with numbers 1 to 9 according to the rules of Sudoku. We say two such puzzles are the same if one can be obtained from other by any of the following operations and their compositions:

- Rotation by 90, 180, and 270 degrees
- Flips along vertical, horizontal, and diagonal axes
- Rotation by 180 degree of each of the 3×3 subgrid simultaneously

Describe the subgroup made up of above three operations. Assuming total number of completed puzzles to be N, calculate the number of distinct completed puzzles.

Solution

- Let S be the set of all completed Sudoku Puzzles. It is given that $|S| = N$.
- Define $R : S \to S$,$F_V : S \to S$, $F_H : S \to S$, $F_{d1} : S \to S$, $F_{d2} : S \to S$ and $R_s : S \to S$ where for $t \in S$:
  - $R(t)$ rotates t by 90 degrees.
  - $F_V(t)$ and $F_H(t)$ flips t along vertical and horizontal axes respectively.
  - $F_{d1}(t)$ flips t along the diagonal going from top-left to bottom-right.
  - $F_{d2}(t)$ flips t along the diagonal going from top-right to bottom-left.
  - $R_s(t)$ rotates each subgrid by 180 degrees simultaneously.
- All R ,F_V, F_H, F_{d1}, F_{d2} and R_s are bijective functions.
- Set of bijections from S to itself is a group under composition. Denote the group by S_9.
- Operation of any composition of R ,F_V, F_H, F_{d1}, F_{d2} and R_s will give essentially the same Sudoku.
- We observe the following identities:
  1. $F_v \circ R = F_{d1}$

2. $R \circ R = F_{d2}$
3. $R \circ R \circ F_V = F_H$.
4. $F_V \circ R_s = R_s \circ F_V$
5. $R_s \circ R = R \circ R_s$
6. $R^4 = e$, $F_V^2 = e$ and $R_s^2 = e$.
7. $R \circ F_V \circ R \circ F_V = e \implies R \circ F_V = F_V^{-1} \circ R^{-1} = F_V \circ R^3$.

- 6. is obvious.
- 1., 2., 3. and 7. can be proved as follows:
  - Let $a_{i,j}$ represent the element in $i-th$ row and $j-th$ column.
  - $a_{i,j} \xrightarrow{R} a_{j,10-i} \xrightarrow{F_V} a_{j,i}$, which gives $F_v \circ R = F_{d1}$.
  - $a_{i,j} \xrightarrow{R} a_{j,10-i} \xrightarrow{R} a_{10-i,10-j}$, which gives $R \circ R = F_{d2}$.
  - $a_{i,j} \xrightarrow{F_V} a_{i,10-j} \xrightarrow{R} a_{10-j,10-i} \xrightarrow{R} a_{10-i,j}$, which gives $R \circ R \circ F_V = F_H$.
  - $a_{i,j} \xrightarrow{F_V} a_{i,10-j} \xrightarrow{R} a_{10-j,10-i} \xrightarrow{F_V} a_{10-j,i} \xrightarrow{R} a_{i,j}$ which gives $R \circ F_V \circ R \circ F_V = e$
- 4. and 5. follows from the following argument:
  - Rotation of subgrid by 180 degrees can be seen as flip along it's(subgrid) vertical axis followed by flip along the horizontal axis or vice-versa.
  - F_V flips the individual subgrid along subgrid's vertical axis and swaps the first subgrid with 3rd, 4th with 6th and 7th with 9th.
  - So in both, $F_V \circ R_s$ and $R_s \circ F_V$ a subgrid goes throgh two vertical flips and one horizontal flip, which ultimately lead to just a horizontal flip of subgrid. Hence, $F_V \circ R_s = R_s \circ F_V$.
  - When R rotates the sudoku by 90 degrees, each subgrid rotates by 90 degrees along the subgrid's center..
  - $R_s \circ R$ and $R \circ R_s$ both gives 1 verticle flip, 1 horizontal flip and rotation by 90 degrees to the each subgrid and moves the subgrid to position such that its center is at 90 degrees clockwise to its old position.
  - The order in which all this happened doesn't really matter. So,$R_s \circ R = R \circ R_s$.

- The above identities tells any composition of R ,F_V, F_H, F_{d1}, F_{d2} and R_s can be written as composition of only R, F_V, and R_s.
- By 4., 5. and 7. we can push F_V to the front, and R to the end in any composition of F_V, R and R_s.
- Hence ,The subgroup is $G = \{F_v^j R_s^k R^i | 0 \leq j \leq 1, 0 \leq k \leq 1, 0 \leq i \leq 3\}$
- $|G| = 16$.
- Define a relation K on the set of S as:$t_1 K t_2$ for $t_1, t_2 \in S$ if there exists $\eta \in G$ such that $\eta(t_1) = t_2$.
- K is an equivalence relation. (Proved in Lecture 21)
- The number of distinct sudoku puzzles equals the number of equivalence classes of S under K.
- All 16 compositions of G result in different versions of the same sudoku puzzle, it devides set S into disjoint equivalence classes of 16 elements each.
  - Let $t_1 \in S$ such that it is in equivalence class P having greater than 16 elements, then by definition there exist $\eta_i \in G$ such that $\eta_i(t_1) = t_i$ for each i where, $1 \leq i \leq |P|$ which is not possible as there are only 16 elements in G.
  - Now Let $t_1 \in S$ such that it is in equivalence class P having less than 16 elements. But each operations of group G will give a different version of t_1, that is we will get 16 different versions of t_1. Hence P can't have less than 16 elements.
  - Hence all equivalence classes have 16 elements.
- Hence total number of distinct completely filled puzzles is $\frac{N}{16}$.

Question 5

Let $(G, \cdot)$ be a group. A proper subgroup of G is a subgroup which is a proper subset of G. H is a maximal subgroup of G if H is a proper subgroup of G and there is no other proper subgroup H' such that $H \subset H'$.

Give an example of a group that does not have a maximal subgroup. Under what conditions will G have a maximal subgroup?

Solution

The prüfer group defined as follows **does not** have a maximal subgroup:

The Prüfer p-group, where p is a prime number, is defined as the subgroup of the unit circle consisting of all $p\, n^{th}$ roots of unity:

$$\mathbb{Z}(p^{\infty}) = \{e^{2\pi i m/p^{n}} : m, n = 1, 2, 3 \ldots\}$$

Therefore, Prüfer group can also be written as a subgroup of $\mathbb{Q}/\mathbb{Z}$

The Prüfer p-group has no maximal element as it can be seen that any subgroup of $\mathbb{Z}(p^{\infty})$ is of the form $\mathbb{Z}/p^{n}\mathbb{Z}$, where n is a non negative integer. Hence, the subgroups form an infinite chain where

$$1 \subset \mathbb{Z}/p\mathbb{Z} \subset \mathbb{Z}/p^{2}\mathbb{Z} \ldots \mathbb{Z}(p^{\infty})$$

Therefore, Prüfer group has no maximal subgroup.

The above observations can be applied to find the condition when G has a maximal subgroup. We know that every finite group is a finite set, so every chain of proper subgroups of a finite group will have a maximal element. This implies that every finite group will have a maximal subgroup.

The formal proof can be given as:

Consider the set A = $\{S \leq G : S \neq G, H \leq G\}$.

The set A is a subset of $\mathcal{P}(G)$ and is therefore partially ordered by $\subseteq$. This set is also a finite set since the group in consideration G is also a finite group.

If A is empty, that means H is the maximal element.

If A is non-empty, let's **assume there is no maximal** subset H, that means there has to be an element $S_0 \in A$. Since S_0 is not a maximal subset, there has to be another element $S_1 \in A$ such that $S_1 \geq S_0, S_1 \neq S_0$. But then again, since S_1 is not the maximal subset, that means there has to be another $S_2 \in A \ldots$

This results in an infinite chain with increasing elements, $S_0 \leq S_1 \leq S_2 \ldots$.

This is a contradiction since A is a finite set, and hence $S_i's$ can't be infinite. Therefore, a maximal element H of G should exist. Note that this can be only achieved when A is a finite set, which is because G is a finite group.

Hence, maximal subgroup exist only for **finite** groups.

References