CS201

Mathematics For Computer Science

Indian Institute of Technology, Kanpur

Group Number: 5

Devanshu Singla (190274), Sarthak Rout (190772), Yatharth Goswami (191178)

Assignment 3

Date of Submission: November 23, 2020

Question 1

1. Find the generating function for the following recurrence relation.

$$f(n+1) = \begin{cases} 1 & \text{if } n+1=0 \\ \sum_{i=0}^{n} f(i)f(n-i) & \text{if } n \geq 0 \end{cases}$$

2. Using the generating function and generalised binomial theorem for $\sqrt{1+y}$, find a closed form for $f(n)$.

Solution

1 Part I

Let $G(x) = \sum\limits_{i=0}^{\infty} f(i)x^i$. According to the question statement, $f(0) = 1$.

Consider also, $G(x) = \sum\limits_{j=0}^{\infty} f(j)x^j$. Then,

$$(G(x))^2 = \sum_{i=0}^{\infty} f(i)x^i \cdot \sum_{j=0}^{\infty} f(j)x^j = \sum_{i=0}^{\infty} \sum_{j=0}^{\infty} f(i)f(j)x^{i+j}$$

Let $i + j = n$.

$$(G(x))^2 = \sum_{n=0}^{\infty} (\sum_{i=0}^{n} f(i)f(n-i))x^n = \sum_{n=0}^{\infty} f(n+1)x^n \ (\ Eqn\ 1.1)$$

We also have,

$$G(x) = f(0) + xf(1) + x^2 f(2) \cdots \implies \frac{G(x) - f(0)}{x} = f(1) + xf(2) + x^2 f(3) \cdots = \sum_{n=0}^{\infty} f(n+1) x^n$$

So, from Eqn 1.1,

$$(G(x))^2 = \frac{G(x) - f(0)}{x} = \frac{G(x) - 1}{x}$$
$$\implies x(G(x))^2 - G(x) + 1 = 0$$
$$\implies G(x) = \frac{1 \pm \sqrt{1-4x}}{2x}$$

The denominator vanishes at $x = 0$. We also have $G(0) = f(0) = 1$. This implies, we must choose $-$ sign, so that the expression is of the form $\frac{0}{0}$ and not $\frac{\infty}{0}$, which allows us to manipulate expressions to remove singularities. Therefore,

$$G(x) = \frac{1 - \sqrt{1-4x}}{2x} = \frac{2}{1 + \sqrt{1+4x}}$$

2 Part II

We have generalised binomial theorem where n is any complex number :

$$(x+y)^n = \sum_{n=0}^{\infty} \binom{n}{k} x^k y^{n-k}$$

Using generalised binomial theorem for real exponent $\frac{1}{2}$ and $x = 1$, we have

$$\sqrt{1+y} = \sum_{n=0}^{\infty} \binom{\frac{1}{2}}{n} y^n$$
$$\implies \sqrt{1-4x} = \sum_{n=0}^{\infty} \binom{\frac{1}{2}}{n} (-4)^n x^n = 1 + \sum_{n=1}^{\infty} \binom{\frac{1}{2}}{n} (-4)^n x^n$$
$$1 - \sqrt{1-4x} = -\sum_{n=1}^{\infty} \binom{\frac{1}{2}}{n} (-4)^n x^n = -\sum_{n=0}^{\infty} \binom{\frac{1}{2}}{n+1} (-4)^{n+1} x^{n+1}$$
$$\implies \frac{1 - \sqrt{1-4x}}{2x} = \frac{-1}{2} \cdot \sum_{n=0}^{\infty} \binom{\frac{1}{2}}{n+1} (-4)^{n+1} x^n$$

Simplifying the expression for $\binom{\frac{1}{2}}{n+1}$ further,

$$\binom{\frac{1}{2}}{n+1} = \frac{1}{(n+1)!} \cdot \frac{1}{2}\frac{-1}{2}\frac{-3}{2}\dots\frac{-(2n-1)}{2}$$

$$= \frac{(-1)^n}{2^{n+1}}\frac{1.3\dots(2n-1)}{(n+1)!}$$

$$= \frac{(-1)^n}{2^{n+1}}\frac{1.3\dots(2n-1)}{(n+1)!} \cdot \frac{2.4.6\dots(2n)}{2^n n!}$$

$$= \frac{(-1)^n}{2^{n+1}}\frac{1.2.3.4\dots(2n-1).(2n)}{2^n(n+1)!n!}$$

$$= \frac{(-1)^n}{2^{n+1}}\frac{(2n)!}{2^n n!(n+1)!} = \frac{(-1)^n}{2^{n+1}}\frac{(2n)!}{2^n n!n!(n+1)}$$

$$= \frac{(-1)^n}{2.4^n(n+1)}\binom{2n}{n}$$

This implies that,

$$\frac{1-\sqrt{1-4x}}{2x} = \frac{-1}{2} \cdot \sum_{n=0}^{\infty}\binom{\frac{1}{2}}{n+1}(-4)^{n+1}x^n = \frac{-1}{2}\sum_{n=0}^{\infty}(-4)^{n+1} \cdot \frac{(-1)^n}{2.4^n(n+1)}\binom{2n}{n}x^n$$

$$= \sum_{n=0}^{\infty}(-1)^{2n+2} \cdot \frac{4}{2.2} \cdot \frac{1}{n+1} \cdot \binom{2n}{n}x^n = \sum_{n=0}^{\infty}\frac{1}{n+1} \cdot \binom{2n}{n}x^n$$

Therefore, the closed form for $f(n)$ is,

$$f(n) = \frac{1}{n+1} \cdot \binom{2n}{n}$$

Question 2

Define n-varaiate polynomials P_d and Q_d as:

$$\begin{aligned} P_d(x_1, x_2, \ldots, x_n) &= \sum_{\substack{J \subseteq [1,n] \\ |J|=d}} \prod_{r \in J} x_r \\ Q_d(x_1, x_2, \ldots, x_n) &= \sum_{\substack{0 \le i_1, i_2, \ldots, i_n \le d \\ i_1 + i_2 + \cdots + i_n = d}} \prod_{r=1}^{n} x_r^{i_r}, \end{aligned}$$

and $P_0(x_1, x_2, \ldots, x_n) = 1 = Q_0(x_1, x_2, \ldots, x_n)$. Show that for any $d > 0$:

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

Solution

Consider the polynomial $F(y) = \prod_{i=1}^{n}(1 - x_i y)$.
It can be clearly seen that coefficient of y^k is the sum of all such terms obtained by multiplying the second term of each i-th factor $(1 - x_i y)$ which is $-x_i y$, which is linear in y, from any k mono-polynomials being multiplied and first term i.e. 1 from rest of the mono-polynomials.
Note: Here, a mono-polynomial is a factor in the expression for $F(y)$. Ex: $(1 - x_2 y)$

$$\begin{aligned} \therefore \text{ coefficient of } y^k \text{ in } F(y) &= \sum_{\substack{J \subseteq [1,n] \\ |J|=k}} \prod_{r \in J} (-x_r) \\ &= (-1)^k \sum_{\substack{J \subseteq [1,n] \\ |J|=k}} \prod_{r \in J} (x_r) \\ &= (-1)^k P_k(x_1, x_2, \ldots, x_n) \end{aligned}$$

Functional equation for $\frac{1}{F(y)}$:

$$\frac{1}{F(y)} = \prod_{i=1}^{n} \frac{1}{1 - x_i y}$$

$$
\begin{aligned}
&= \prod_{i=1}^{n}\sum_{j\geq 0}(x_i^j y^j) \\
&= \sum_{d\geq 0}\Big(\sum_{\substack{0\leq i_1,i_2,\ldots,i_n\leq d \\ i_1+i_2+\cdots+i_n=d}}\prod_{r=1}^{n} x_r^{i_r}\Big)y^d \\
&= \sum_{d\geq 0} Q_d(x_1,x_2,\ldots,x_n)y^d
\end{aligned}
$$

Multiplying both of these functional equations,

$$
\begin{aligned}
F(y)\Big(\frac{1}{F(y)}\Big) &= \Big(\sum_{d\geq 0}(-1)^d P_d(x_1,x_2,\ldots,x_n)y^d\Big)\Big(\sum_{d\geq 0} Q_d(x_1,x_2,\ldots,x_n)y^d\Big) \\
1 &= \sum_{d\geq 0}\Big(\sum_{m=0}^{d}(-1)^m P_m(x_1,x_2,\ldots,x_n)Q_{d-m}(x_1,x_2,\ldots,x_n)\Big)y^d
\end{aligned}
$$

Equating powers of y on both sides,

$$
\implies \quad \sum_{m=0}^{d}(-1)^m P_m(x_1,x_2,\ldots,x_n)Q_{d-m}(x_1,x_2,\ldots,x_n) = 0, \text{ for } d > 0
$$

Question 3

1. Let $\alpha \in \mathbb{R}$ and N be a natural number. Using pigeon-hole principle, show that there exists integers p and q such that $1 \leq q \leq N$ and
$$|q\alpha - p| \leq \frac{1}{N}$$
2. Let $\alpha_1, \alpha_2, \ldots, \alpha_n \in R$ and N be a natural number. Using pigeon-hole principle, show that there exists integers $p_1, p_2, \ldots, p_n, q$ such that $1 \leq q \leq N^n$ and for all $i \in \{1, \ldots, n\}$
$$|\alpha_i - \frac{p_i}{q}| \leq \frac{1}{q^{1+1/n}}$$

Solution

3.1

Let us split the interval $\Big[0{,}1\Big)$ into N equal sized intervals:

$$\Big[0, \frac{1}{N}\Big), \Big[\frac{1}{N}, \frac{2}{N}\Big) \ldots \Big[\frac{N-1}{N}, 1\Big)$$

Consider, $N+1$ numbers, $0, \alpha, 2\alpha \ldots N\alpha$. There fractional part lies in the interval $\Big[0{,}1\Big)$. There are $N+1$ real numbers (not necessarily all distinct) and N intervals, hence, by **Pigeonhole Principle** two of the numbers must have their fractional part in the same interval.

Hence, for some non-negative integers a and b s.t. $0 \leq a, b \leq N$ and $a > b$ without a loss of generality, the difference of fractional parts must be less than $\frac{1}{N}$;

$$\implies |\ \{a\alpha\} - \{b\alpha\}\ | < \frac{1}{N}$$
$$\implies |\ (a-b)\alpha - (\lfloor a\alpha \rfloor - \lfloor b\alpha \rfloor)\ | < \frac{1}{N}$$

Then, let $q = (a-b)$ and $p = (\lfloor a\alpha \rfloor - \lfloor b\alpha \rfloor)$.
As $0 \leq b < a \leq N$, $0 < a - b \leq N \implies 1 \leq a - b \leq N$.
Hence, $1 \leq q \leq N$ and we have two integers, p and q satisfying the given requirement.

3.2

As

$$\frac{1}{q^{\frac{1}{n}}} \geq \frac{1}{N}$$

$$\iff \frac{1}{qN} \leq \frac{1}{q^{1+\frac{1}{n}}}$$

Therefore, we must show that

$$\mid \alpha_i - \frac{p_i}{q} \mid < \frac{1}{qN} \leq \frac{1}{q^{1+\frac{1}{n}}}$$

which will imply

$$\mid \alpha_i - \frac{p_i}{q} \mid < \frac{1}{q^{1+\frac{1}{n}}}$$

This implies we must show that,

$$\mid q\alpha_i - p_i \mid < \frac{1}{N}$$

for all such p_i and q. Let $\mathcal{A}$ be the set of N intervals defined (also in the previous part) by partitioning $[0, 1)$ into N equal parts. That is,

$$A = \{[0, \frac{1}{N}), [\frac{1}{N}, \frac{2}{N}) \dots [\frac{N-1}{N}, 1)\}$$

For a integer t, consider $\{I : \{t\alpha_i\} \in I\}$ a set of n intervals where $I \in A$. Let it be referred as a **$\mathbf{n}$-tuple** of intervals.
Then, we have N^n possibilities of the n-tuple.
Consider, $N^n + 1$ integers, from 0 to N^n. For each of them, we define such an n-tuple (which are not necessarily distinct).

By **Pigeonhole Principle**, as we have N^n+1 integers and only N^n choices for intervals, two integers, say x and y must have the same n-tuple where $0 \leq x, y, \leq N^n$. Without a loss of generality, we may assume $x > y$.
As both of the n-tuple belong to the same interval, for each i, $\{x\alpha_i\}$ and $\{y\alpha_i\}$ differ by no more than $\frac{1}{N}$.

$$\implies \mid \{x\alpha_i\} - \{y\alpha_i\} \mid < \frac{1}{N} \; \forall \, 1 \leq i \leq n$$

$$\implies |\ (x-y)\alpha_i - (\lfloor x\alpha_i \rfloor - \lfloor y\alpha_i \rfloor)\ | < \ \frac{1}{N}$$

Let $q = x - y$. As $x > y$, $q > 0$ and as $0 < y < x < N^n$, we have, $-N^n \leq q \leq N^n$. Hence, $0 \leq q \leq N^n$. Also, let $p_i = (\lfloor x\alpha_i \rfloor - \lfloor y\alpha_i \rfloor)$.

Therefore, we obtain p_i and q where $1 \leq i \leq n$ where

$$|\ q\alpha_i - p_i\ | < \ \frac{1}{N}$$

as required.

Question 4

Give a proof for Ramsey's theorem for general case.

Solution

The general case of Ramsey's theorem states that for any $c, n_1, n_2, \ldots, n_c, k \geq 1$, there exists a number $N(n_1, n_2, \ldots, n_c, k) > 0$ such that for any set X with $|X| \geq N(n_1, n_2, ..., n_c, k)$, and any mapping $f : X^k \mapsto \{1, 2, ..., c\}$, there exists a $i, 1 \leq i \leq c$ and a subset Y $\subseteq X$, |Y| = n$_i$, with $f(Y^k) = i$.

Theorem 4.1. [Strong Form of Pigeon Hole Principle] Let $q_1, q_2, \ldots, q_n$ be positive integers. If

$$q_1 + q_2 + \cdots + q_n - n + 1$$

objects are put into n boxes, then either the $1st$ box contains atleast q_1 objects, or the $2nd$ box contains at least q_2 objects, …, the nth box contains at least q_n objects.

Proof. Suppose, it is not true and the ith box contains at most $q_i - 1$ objects, $i = 1, 2, \ldots, n$. Then the total number of objects contained in the n boxes can be atmost

$$(q_1 - 1) + (q_2 - 1) + \cdots + (q_n - 1) \; = \; q_1 + q_2 + \cdots + q_n - n,$$

which is one less than the number of objects distributed. This results in a contradiction. $\square$

Proof. Let us introduce a new symbol $R_k(n_1, n_2, \ldots, n_c)$ as the smallest value of such a number $N(n_1, n_2, \ldots, n_c, k)$ as referred in the definition. We will try to prove the ramsey's theorem using an induction on k. For $k = 1$, we can choose $R_1(n_1, \ldots, n_c) = n_1 + n_2 + \cdots + n_c - c + 1$, and this when used with **Theorem 4.1** will imply that there will exist a set Y with cardinality atleast n_i for some i and for which all elements will be mapped to i. Hence, the claim is true for $k = 1$. In the induction step, suppose that the claim is already true for numbers upto $k - 1$.

For proving claim for k, we will use strong induction on c for k. For $c = 1$, it is trivially true by selecting any $Y \subseteq X, |Y| = n_1$. Suppose that the claim is true for $k, \forall c \leq r$ for some r, where $r \geq 1$. For $r = 1$, or $c = 1$, it has been proved above.

For proving claim for r, we will now induct on $n_1 + n_2 \cdots + n_r$ for the rest of the proof. Also, notice the fact that an implicit condition present in the theorem is that $k \leq min\{n_1, n_2, \ldots, n_c\}$. So, for handling the base case, we take $n_i = k$ for some i. We observe that if $n_i = k$ then, $R_k(n_1, n_2, \ldots, n_c) = R_k(n_1, \ldots, n_{i-1}, n_{i+1}, \ldots, n_r)$ by using the fact that either we will choose the color i or not. If we choose color i, then only k vertices are enough to find a Y of size k such that any arbitrary mapping f maps these k vertices to the color i, otherwise if we are not going to use the color i, then the minimum number of vertices would be same as $R_k(n_1, \ldots, n_{i-1}, n_{i+1}, \ldots, n_r)$. Now, since the term on the right hand side is finite by induction hypothesis, so the cases with $n_i = k$ have been dealt with. Now, we will try to show that

$$R_k(n_1, n_2, \ldots, n_r) \leq R_{k-1}(R_k(n_1-1, \ldots, n_r), \ldots, R_k(n_1, \ldots, n_i-1, \ldots, n_r), \ldots, R_k(n_1, \ldots, n_r-1))+1$$

We know that the right hand side is finite by the induction hypothesis on sum of k_i and also the Ramsey theorem for values less than k. Let the value of right hand side of the above equation be S. Let us choose a set X of cardinality S and an arbitrary mapping $f : X^k \mapsto \{1, 2 \ldots, r\}$. Let $\{A\}$ be an element of X. Let us define another set $X' = X - \{A\}$. Therefore $|X'| = |X| - 1$. Let us choose a mapping $g : (X')^{k-1} \mapsto \{1, 2, \ldots, r\}$ such that g maps any $k-1$ sized subset x' of X' to the same number which f maps $x' \cup \{A\}$ to.

Since $|X'| = R_{k-1}(R_k(n_1-1, \ldots, n_r), \ldots, R_k(n_1, \ldots, n_i-1, \ldots, n_r), \ldots, R_k(n_1, \ldots, n_r-1))$, therefore by definition of Ramsey's theorem, we can say that $\exists i$ such that $\exists Y \subseteq X'$ and $|Y| = R_k(n_1, \ldots, n_i - 1, \ldots, n_r),\ g(Y^{k-1}) = i$.

Now, using definition of Ramsey's theorem on this newly defined set Y with $|Y| = R_k(n_1, \ldots, n_i - 1, \ldots, n_r)$, we can say that $\exists j$ such that either $j \neq i$ and $\exists Z \subseteq Y,\ |Z| = n_j,\ f(Z^k) = \{j\}$, in which case we are done or $j = i$ in which case $\exists Z \subseteq Y,\ |Z| = n_i - 1,\ f(Z^k) = \{i\}$. Now in this case, since $Z \subseteq Y$, $g(Y^{k-1}) = \{i\} \implies g(Z^{k-1}) = \{i\}$. By definition of g, this implies that $g(z) = f(z \cup \{A\}) = \{i\}\, \forall\, z \in Z^{k-1}$. If we define a set $Z' = Z \cup \{A\}$, then, we have $f(z) = \{i\}\, \forall\, z \in (Z')^k$ and $|Z'| = n_i$. Therefore, we can say that by choosing a set X with cardinality S, we can find for any arbitrary mapping f, a subset Y' with cardinality n_i and $f((Y')^k) = i$ for some $i <= r$ and since $R_k(n_1, \ldots, n_r)$ is smallest such cardinality of set X, therefore it would be less than or equal to S which proves the above inequality and hence the finiteness of $R_k(n_1, n_2, \ldots, n_r)$ and hence the theorem in general. $\square$

Question 5

Consider the set $S_n = \{f \mid f : [n] \to [n] \text{ and } f \text{ is a bijection}\}$ which contains all bijective mapping from $[n]$ to $[n]$ where $[n] = \{1, 2, 3, \ldots, n\}$. In other words, any $f \in S_n$ simply permutes the elements in $[n]$.

1. A mapping $f \in S_n$ is called a **transposition** if there exists (i, j) such that $0 \leq i \neq j \leq n$ and

$$f(k) = \begin{cases} j & \text{if } k = i \\ i & \text{if } k = j \\ k & \text{otherwise} \end{cases}$$

   Show that any $g \in S_n$ can be written as a finite product $f_1 \circ f_2 \circ \cdots \circ f_m$ where each f_i is a transposition in S_n.

2. The **parity** of a function f in S_n denoted by $N(f)$ is defined as the number of pairs (i, j) such that $1 \leq i < j \leq n$ and $f(i) > f(j)$. Show that

$$N(f) \equiv m \ (\ mod\ 2)$$

   where $f = g_1 \circ g_2 \circ \cdots \circ g_m$ and each g_i is a transposition in S_n.

Solution

Consider the adjacent transpositions $e_i \in S_n, 1 \leq i < n$ be defined as:

$$e_i(x) = \begin{cases} i+1 & \text{if } x = i \\ i & \text{if } x = i+1 \\ x & \text{otherwise} \end{cases}$$

Lemma 5.1. If there exist a pair (i, j) s.t. $1 \leq i < j \leq n$ and $f(i) > f(j)$, then there exists a pair $(k, k+1)$ s.t. $1 \leq k < n$ and $f(k) > f(k+1)$.

Proof. Let us assume there does not exist any pair $(k, k+1)$ s.t. $i \leq k < j$ and $f(k) > f(k+1)$.

$\implies f(k) \leq f(k+1), \forall k \text{ s.t. } i \leq k < j$.

$\implies f(i) \leq f(i+1) \leq \cdots \leq f(j-1) \leq f(j)$
$\implies f(i) \leq f(j)$, which is clearly contradiction. $\square$

Lemma 5.2. If $N(f) = 0$ for some $f \in S_n$, then $f(x) = Id(x)$(identity function).

Proof. As $N(f) = 0$, it implies there does not exist any pair (i, j) such that $1 \leq i < j \leq n$ and $f(i) > f(j)$.
$\implies f(i) \leq f(j) \forall i, j$ s.t. $1 \leq i < j \leq n$.
$\implies f$ is increasing function.

Since f is both increasing and onto(bijective), it implies $f(x)$ needs to be identity function. $\square$

Inverse of lemma 5.2 is also true as can be easily seen $\forall i, j$ s.t. $1 \leq i < j \leq n \implies Id(i) < Id(j), \implies N(Id) = 0$.

Lemma 5.3. If $N(f) > 0$ for some $f \in S_n$, then there exist an adjacent transposition e_i for some i s.t. $N(e_i \circ f) = N(f) - 1$

Proof. $N(f) > 0 \implies$ there exist a pair (i, j) s.t. $1 \leq i < j \leq n$ and $f(i) > f(j)$
$\implies$ there exist a pair $(k, k+1)$ s.t. $1 \leq k < n$ and $f(k) > f(k+1)$. (from lemma 5.1).

Let us call the a pair (i, j) a bad pair w.r.t. $f \in S_n$ if $1 \leq i < j \leq n$ and $f(i) > f(j)$. Consider the adjacent transposition e_k. Consider the following disjoint cases of pairs (i, j) s.t. $1 \leq i < j \leq n$:

1. Case: $i, j \in [1, n] - \{k, k+1\}$

   $f(i) > f(j) \implies e_k(f(i)) > e_k(f(j))$ and $f(i) \leq f(j) \implies e_k(f(i)) \leq e_k(f(j))$

   Hence, the number of bad pairs are same w.r.t. f and $e_i \circ f$ in (i, j).

2. Case: $i \in \{k, k+1\}, n \geq j > k+1$

   $f(k) > f(j) \implies e_k(f(k+1)) > e_k(f(j))$ and $f(k) \leq f(j) \implies e_k(f(k+1)) \leq e_k(f(j))$

   So, the number of bad pairs in (k, j) w.r.t f are equal to number of bad pairs in $(k+1, j)$ w.r.t. $e_i \circ f$.

   Similarly, $f(k+1) > f(j) \implies e_k(f(k)) > e_k(f(j))$ and $f(k+1) \leq f(j) \implies e_k(f(k)) \leq e_k(f(j))$

   Hence, the number of bad pairs in $(k+1, j)$ w.r.t f are equal to number of bad pairs in (k, j) w.r.t. $e_i \circ f$.

Hence, the number of bad pairs are same w.r.t. f and $e_i \circ f$ in (i, j).

3. Case: $1 \leq i < k, j \in \{k, k+1\}$

   $f(i) > f(k) \implies e_k(f(i)) > e_k(f(k+1))$ and $f(i) \leq f(k) \implies e_k(f(i)) \leq e_k(f(k+1))$

   So, the number of bad pairs in (i, k) w.r.t f are equal to number of bad pairs in $(i, k+1)$ w.r.t. $e_i \circ f$.

   Similarly, $f(i) > f(k+1) \implies e_k(f(i)) > e_k(f(k))$ and $f(i) \leq f(k+1) \implies e_k(f(i)) \leq e_k(f(k))$

   Hence, the number of bad pairs in $(i, k+1)$ w.r.t f are equal to number of bad pairs in (i, k) w.r.t. $e_i \circ f$.

   Hence, the number of bad pairs are same w.r.t. f and $e_i \circ f$ in (i, j).

4. Case: $i = k, j = k+1$

   Since, $f(k) > f(k+1) \implies e_i(f(k)) <= e_i(f(k+1))$, $(i, j) = (k, k+1)$ is a bad pair w.r.t. f but not w.r.t. $e_i \circ f$.

Hence, except the last case the number of bad pairs w.r.t f and $e_i \circ f$ were same but in last case f had one more bad pair than $e_i \circ f$. Since, by definition of bad pairs, $N(f)$ = number of bad pairs in $f \implies N(e_k \circ f) = N(f) - 1$. □

Lemma 5.4. For a transposition f, transpositioning i and j where $i, j \in [1, n]$ and $i < j$, $N(f) = 2(i - j) - 1$.

Proof. Consider following mutually exclusive cases of pairs (x, y) s.t. $x, y \in [1, n]$ and $x < y$:

1. Case: $x < i$

   for $y \notin \{i, j\}, x < y \implies f(x) < f(y)$, hence no bad pairs.

   for $y = j, x < i \implies f(x) < f(j) \implies f(x) < f(y)$, hence no bad pair

   Total bad pairs = 0.

2. Case: $x = i$

   for $i < y < j, y < j \implies f(y) < f(i) \implies f(y) < f(x)$, hence $j - i - 1$ bad pairs.

   for $y = j, i < j \implies f(j) < f(i) \implies f(y) < f(x)$, hence 1 bad pair.

   for $j < y < n, j < y \implies f(i) < f(y) \implies f(x) < f(y)$, hence no bad pairs.

   So, total bad pairs = $i - j$.

3. Case: $i < x < j$

   for $y \neq j, x < y \implies f(x) < f(y)$, hence no bad pairs.

   for $y = j, i < x \implies f(j) < f(x) \implies f(y) < f(x)$, hence $j - i - 1$ bad pair.

4. Case: $x \geq j$

   for $x = j, i < y \implies f(j) < f(y) \implies f(x) < f(y)$, hence no bad pair.

   for $x > j, x < y \implies f(x) < f(y)$, hence no bad pair.

Hence, total number of bad pairs, $N(f) = 2(j - i) - 1 \implies N(f) \equiv 1 (mod 2)$ □

Lemma 5.5. Let e_k be an adjacent transposition for some k and let $f \in S_n$. Then, $N(e_k \circ f) - N(f) \equiv 1$ (mod 2).

Proof. While proving lemma 5.3, it can be seen that in the cases 1-3, the argument holds for any general $f \in S_n$ and for e_k, for any k s.t. $1 \leq k < n$. Hence, the number of bad pairs are same for cases 1-3 w.r.t. f and $e_k \circ f$

For the case $i = k, j = k + 1$, if $f(i) < f(j) \implies (e_k \circ f)(j) < (e_k \circ f)(i) \implies N(f) = N(e_k \circ f) - 1$ or if $f(i) > f(j) \implies (e_k \circ f)(i) < (e_k \circ f)(j) \implies N(f) = N(e_k \circ f) + 1$.

$$\implies N(f) - N(e_k \circ f) \equiv 1 \text{ (mod 2)}$$

□

5.1

It can be seen that that the maximum number of bad pairs in any $g \in S_n$ are strictly less than the number of pair (i, j) s.t. $i < j$, hence parity of g is finite.

By lemma 5.3, $\exists$ adjacent transposition $h_1 = e_i$ for some i s.t. $N(e_i \circ f) = N(f) - 1$. Let $g_1 = e_1 \circ f$. Similarly, for $g_{k-1}, \exists h_k = e_i$ for some i s.t. $N(g_k) = N(g_{k-1}) - 1$, where $g_k = h_k \circ g_{k-1}$, for $1 < k \leq m$ where $N(g_m) = 0$. Since $N(g_k) = N(g_{k-1}) - 1$ and $N(g_1) = N(g) - 1 \implies N(g_i) = N(g) - i \implies N(g_m) = N(g) - m = 0$ (by inverse of lemma 5.3) $\implies m = N(g)$.

Since, $N(g_m) = 0 \implies g_m = Id$ (by lemma 5.2). It can also be easily seen that for any adjacent transposition e, $e(e(x)) = x, \forall x \implies e \circ e = Id$.

$$\text{As, } g_m = h_m \circ g_{m-1}$$

$$
\begin{aligned}
&= h_m \circ h_{m-1} \circ g_{m-2} \\
&= h_m \circ \cdots \circ h_1 \circ g \\
\implies h_1 \circ \cdots \circ h_m \circ Id &= h_1 \circ \cdots \circ h_m \circ h_m \circ \cdots \circ h_1 \circ g \qquad (\text{h}_m = Id) \\
\implies h_1 \circ \cdots \circ h_m &= g
\end{aligned}
$$

Hence, there exists transpositions $f_i = h_i$ for s.t. $g = f_1 \circ f_2 \circ \cdots \circ f_m$

5.2

As a corollary of part 5.1, it can be seen that any transposition, say g transpositioning i and j, can be represented as a product of $m = N(g)$ adjacent transpositions, say $e_1, e_2, \ldots, e_m$. By lemma 5.4, $m = N(g) = 2(i-j) - 1$. By lemma 5.5 for any $h \in S_n$,

$$N(e_k \circ e_{k+1} \circ \cdots \circ e_m \circ h) - N(e_{k+1} \circ \cdots \circ e_m \circ h) \equiv 1 \text{ (mod 2)}$$

Summing above equation for $k \in [1, m]$, we get

$$N(e_1 \circ \cdots \circ e_m \circ h) - N(h) \equiv = m \text{ (mod 2)}$$

$$\implies N(g \circ h) - N(h) \equiv 2(i-j) - 1 \text{ (mod 2)}$$

$$\implies N(g \circ h) - N(h) \equiv 1 \text{ (mod 2)}$$

$\implies$ For the functions f and $g_i, i \in [1, m]$ given in question,

$$N(g_i \circ g_{i-1} \circ \cdots \circ g_m \circ Id) - N(g_{i-1} \circ \cdots \circ g_m \circ Id) \equiv 1 \text{ (mod 2)}$$

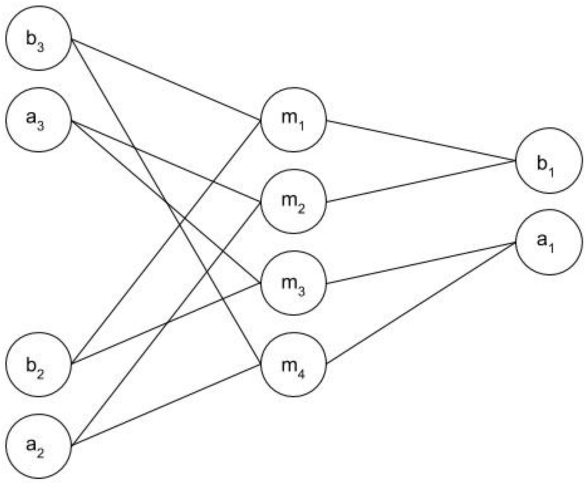
Summing above equation for $i \in [1, m]$, we get,

$$N(g_1 \circ g_2 \circ \cdots \circ g_m \circ Id) - N(Id) \equiv m \text{ (mod 2)}$$

$$\implies N(f) \equiv m \text{ (mod 2) (by inverse of lemma 5.2)}$$

Question 6

Let $G = (V, E)$ be a graph where V is the vertex set and E is the edge set. A bijective mapping $f : V \to V$ is an **automorphism** if it has the property that $(u, v) \in E \iff (f(u), f(v)) \in E$. Consider the following graph.



Let $A = \{a_1, a_2, a_3\}, B = \{b_1, b_2, b_3\}, M = \{m_1, m_2, m_3, m_4\}$. Then, the vertex set of the above graph is $V = A \cup B \cup M$. Consider a bijective mapping $g : A \cup B \to A \cup B$ such that $g(a_i) \in \{a_i, b_i\}$ and $g(b_i) \in \{a_i, b_i\}$ for all $i \in \{1, 2, 3\}$, i.e., g maps the ordered pair $[a_i, b_i]$ to either $[a_i, b_i]$ (no swap) or $[b_i, a_i]$ (swap).

Show that g can be extended to an automorphism f for the above graph if and only if the number of swaps performed by g is even.

Solution

We are asked to extend g to an automorphism f for the above graph. There are 4 cases in total for g i.e. either it performs 0, 1, 2 or 3 swaps. We will deal with each case individually. Also, note that given a particular bijection g on the set $A \cup B$, for extending it to another bijective function f on the set of vertices of the graph, we need to find a mapping for the set M to itself using f. So, we will use the fact that if such a mapping exists for which f turns out to be an automorphism then the case is possible otherwise not.

Case 1: No swaps

In this case, a simple identity mapping over the set M will work. We define the function f in the following way.

$$f(x) = x \,\forall\, x \;\in V$$

Therefore, we can say that $(u, v) \in E \iff (f(u), f(v)) \in E$.

For the rest of the cases, we will model the problem in a different way. Let us consider, an ordered set of tuples to represent the edge in the original graph between the set $A \cup B$ and M, where $\{(m_p, m_q), (m_r, m_s)\}$ and $p, q, r, s \in \{1, 2, 3, 4\}$ denote the nodes which are connected with the pair (a_i, b_i) for some $i \in \{1, 2, 3\}$ respectively. Let us call this set by a special name, say **E-set**. So, there will be three E-sets for the original graph.

$$\{(m_3, m_4), (m_1, m_2)\}\ for\ \{(a_1, b_1)\}$$
$$\{(m_2, m_4), (m_1, m_3)\}\ for\ \{(a_2, b_2)\}$$
$$\{(m_2, m_3), (m_1, m_4)\}\ for\ \{(a_3, b_3)\}$$

Case 2: One Swap

Without loss of generality, assume that pair of nodes (a_3, b_3) to get swapped by g. Now, notice the fact the node m_1 is connected to all the three b_i and therefore if we keep two of b_i unchanged then for the node $f(m_1)$ to remain connected to the unchanged b_i, we should have that

$$f(m_1) \;\in \{m_1, m_2\}$$

$$f(m_1) \in \;\{m_1, m_3\}$$

so from the above two relations we have that,

$$f(m_1) \;\in \{\{m_1, m_2\} \cap \{m_1, m_3\}\}$$

which implies that

$$f(m_1) = m_1$$

But we know that the pair (a_3, b_3) got swapped, therefore from it, we have the condition that the respective tuples of edges corresponding to a_3 and b_3 should also get reversed. And hence for m_1, we have the condition that

$$f(m_1) \in \{m_2, m_3\}$$

which is a contradiction to the fact that $f(m_1) = m_1$. Hence, there exists no mapping f that can be an automorphism for such a choice of g.

Case 3: Two Swaps
In this case, we can provide a simple mapping for which f becomes an automorphism. Say, for instance that the pair (a_i, b_i) was not swapped and let it's edge set be $\{(m_p, m_q), (m_r, m_s)\}$.

Claim : If f is such that, $f(m_p) = m_q$, $f(m_q) = m_p$ and $f(m_r) = m_s$, $f(m_s) = m_r$, then it is an automorphism.

Proof. We need to check that $(u, v) \in E \iff (f(u), f(v)) \in E$. In the case of the node, which does not get swapped, we know that f just swaps the two nodes it was connected to, so it still remains connected to both of them after f is applied. Now, in the case of a node that got swapped, say the pair (a_j, b_j), we know that the set of nodes with which a node is connected to for any two a_i and b_i are not the same and hence if m_p occurs in the set of connected nodes for a_j, then m_q occurs in the set of connected nodes of b_j. Exactly similar analysis will work for b_j and m_r as well. Therefore, if

$$(m_p, a_j) \in E$$

$$then,\ (m_q, b_j) \in E$$

$$or,\ (f(m_p), f(a_j)) \in E$$

Similar analysis can be done for proving the reverse direction. We need to prove that whenever $(f(u), f(v)) \in E$, $(u, v) \in E$. In the case of the node, which does not get swapped, we know that f just swaps the two nodes it was connected to, so if $(f(m_p), f(a_i)) \in E$, then $(m_r, a_i) \in E$ and using the forward direction proved above, we have $(f(m_r), a_i) \in E$ or $(m_p, a_i) \in E$. Now, in the case of a node that got swapped, say the pair (a_j, b_j).Therefore, if

$$(f(m_p), f(a_j)) \in E$$

$$then,\ (m_q, b_j)\ \in E$$

$$or,\ (f(m_q), f(b_j))\ \in E \text{ using the forward direction proved earlier}$$

$$therefore,\ (m_p, a_j)\ \in E$$

Exactly symmetrical analysis will work for $f(m_r)$ and b_j as well. Hence, the given function f is an automorphism of the original graph. $\square$

Case 4: Three Swaps

This case is easy to analyse. Notice, that using the three original E-sets present in the graph, if we try to find what would f map m_1 to, we can easily reach a contradiction. As, using the three E-sets we get the relations

$$f(m_1)\ \in \{m_3, m_4\}$$

$$f(m_1) \in\ \{m_2, m_4\}$$

$$f(m_1) \in\ \{m_2, m_3\}$$

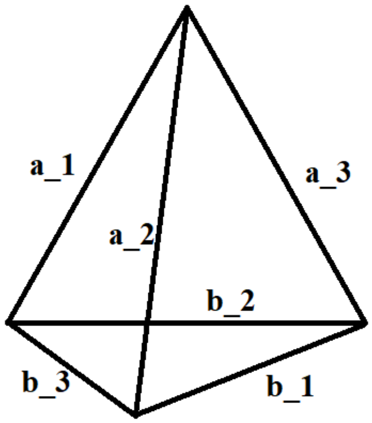
Therefore,

$$f(m_1)\ \in \{\{m_3, m_4\} \cap \{m_2, m_4\}\ \cap \{m_2, m_3\}\}$$

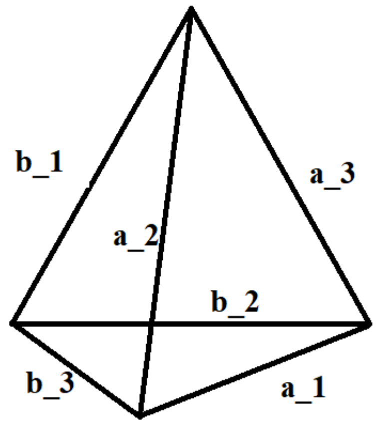
Hence, $f(m_1) \in \emptyset$ which is a contradiction since f is bijective in nature. Hence, there cannot exist any extension for such a g.

From the above cases, we can say that g can be extended to an automorphism f iff g performs even number of swaps. Hence, proved. $\square$

An Alternative Approach Consider these tetrahedrons (also **K4** graphs): In Fig.1,



Tet - 1



Tet - 2

- Each **face** represents m_i, and each **edge** represents a_i or b_i. Also, a_i and b_i are opposite to each other. **Automorphism**: $(u, v) \in E \iff (f(u), f(v)) \in E$
- For automorphism property, the faces should remain **same** after swapping because each set of common edges, (Ex: (a_1, a_2, b_3) with m_4) represent **common edges to** m_i, which should remain same $\forall$ a_i and b_i.
- Also, observe that all a_i originate from a **single vertex**. Let this property be called $P1$ .Also, all b_i **form a triangle**. Let this property be called $P2$.
- Note that, these properties P1 and P2 directly relate the relations of edge with each other and we can construct the whole tetrahedron given the properties for a_i and b_i and vice-versa with the "opposite edges property".
- Consider one swap between a_i and b_i, say $i = 1$ without a loss of generality. The resulting tetrahedron is Fig.2 . Here, a_i have $P2$ and b_i have $P1$. So, the properties $P1$ and $P2$ are **exchanged** between a_i and b_i .
- For automorphism, the faces should remain the same, hence, the properties for a_i and b_i should also remain same. But, a single swap also swaps or exchanges these properties between a_i and b_i.
- Hence, we need to do **even** number of swaps so that, these property remain the same for a_i and b_i. That is, at the end, we must have $P1$ for a_i and $P2$ for b_i.