CS 201: ASSIGNMENT

Harshit Bansal(200428), Jaya Gupta (200471), Pratyush Gupta(200717)

December 1, 2021

1. **Answer to question 1:**
   To prove: $\sum_{m=0}^{d} P_m(x_1, x_2, ...x_n)Q_{d-m}(x_1, x_2, ...x_n) = 0$ - **(i)**

   - Consider any general term of the above sigma of the form $T = x_{i_1}^{p_1}\ x_{i_2}^{p_2} ... x_{i_k}^{p_k}$ where $\Sigma p_i = d$. Such a term has **k** distinct variables$(x_1, x_2...., x_k)$.
   - The maximum number of distinct variables any term of the above sigma(eq. i) can contain is **d**.
   - Each term will be the product of two terms, one from P and the other from Q.
   - If a term has k distinct variables , then the maximum n for which P_n can contribute is k because P_{k+1} will contribute $k + 1$ distinct terms.
   - Let the term contributed by the polynomial P have n distinct variables$(0 <= n <= k)$. These variables will be drawn from the variables included in the term T, so the number of choices is $\binom{k}{n}$.
   - The rest of the term will be uniquely produced by the polynomial Q.
   - So the coefficient for this(when P chooses n distinct terms out of k from T) is $(-1)^n\binom{k}{n}$. $(0 <= n <= k)$.
   - Coefficient of T in the above sigma (eq. (i))is $\sum_{n=0}^{n=k}(-1)^n\binom{k}{n}$. This summation is 0 for all k. Hence the coefficient of every possible term will be 0.

2. **Answer to question 2:**
   $\alpha \in$ R and N is a natural number
   To prove : $|q\alpha - p| \leq \frac{1}{N}$ for some p , q $\in Z$
   Let's divide the interval $[0, 1]$ in N segments of length $1/N$ i.e. $[0, \frac{1}{N}], [\frac{1}{N}, \frac{2}{N}]$, ..., $[\frac{N-1}{N}, 1]$

   Let's consider N numbers
   $n_1 = \alpha - [\alpha]$
   $n_2 = 2\alpha - [2\alpha]$
   $n_2 = 3\alpha - [3\alpha]$
   .
   .
   .
   $n_{N+1} = (N + 1)\alpha - [(N + 1)\alpha]$
   where $n_1, n_2, n_3, ..., n_{N+1} \in [0, 1]$

Now, there are $N+1$ numbers in the interval $[0,1]$ and the interval $[0,1]$ is divided in N segments. According to pigeon-hole principle, there exists a segment which contains atleast two numbers.

So $\exists\ n_l, n_k \in \{n_1, n_2, ..., n_{N+1}\}$ $\quad l, k \in Z$ and $l > k$ such that
$|n_l - n_k| \leq \frac{1}{N}$

$\Rightarrow |\text{l}\alpha - [l\alpha] - k\alpha + [k\alpha]| \leq \frac{1}{N}$

$\Rightarrow |(\text{l-k})\alpha - ([l\alpha] - [k\alpha])| \leq \frac{1}{N}$

Take $q = l - k$ and $p = [l\alpha] - [k\alpha]$
$|q\alpha - p| \leq \frac{1}{N}$

3. **Answer to question 3:**
Case 1:No Swap
Define $g(m_i) = m_i \forall i$
$g(a_k) = a_k \ \ \& \ \ g(b_k) = b_k$ (given)
It can be clearly seen that if $(a_k, m_i) \in E$ then $(g(a_k), g(m_i)) = (a_k, m_i) \in E$.
Similarly for b_k

Case 2: One Swap

- Take any (a_i, b_i) and swap it (All cases can be proved in the same way)
- Swap $(a_1, b_1) \Rightarrow g(a_1) = b_1 \ \ \& \ \ g(b_1) = a_1$
- Now lets find all possible combinations of $g(m_i)$ which are preferred by each (a_i, b_i)

Swap Cases			
	(a_1, b_1)	(a_2, b_2)	(a_3, b_3)
$g(m_1)$	$m_3\ m_4$	$m_1\ m_3$	$m_1\ m_4$
$g(m_2)$	$m_3\ m_4$	$m_2\ m_4$	$m_2\ m_3$
$g(m_3)$	$m_1\ m_2$	$m_1\ m_3$	$m_2\ m_3$
$g(m_4)$	$m_1\ m_2$	$m_2\ m_4$	$m_1\ m_4$

Each entry in the table tells the possible value of $(g(m_i)$ **for every pair** (a_k, b_k).

- From the above table it can be shown that there are no values of $g(m_i)$ that satisfies all the pairs (a_k, b_k) .

Case 3 : Two swaps

- Take any two pairs of (a_i, b_i) and swap them (All other cases can be proved in the same way)
- Swap $(a_1, b_1) \Rightarrow g(a_1) = b_1 \ \ \& \ \ g(b_1) = a_1$
- Swap $(a_2, b_2) \Rightarrow g(a_2) = b_2 \ \ \& \ \ g(b_2) = a_2$
- Now lets find all possible combinations of $g(m_i)$ which are preferred by each (a_i, b_i)

Swap Cases			
	(a_1, b_1)	(a_2, b_2)	(a_3, b_3)
$g(m_1)$	$m_3\ m_4$	$m_2\ m_4$	$m_1\ m_4$
$g(m_2)$	$m_3\ m_4$	$m_1\ m_3$	$m_2\ m_3$
$g(m_3)$	$m_1\ m_2$	$m_2\ m_4$	$m_2\ m_3$
$g(m_4)$	$m_1\ m_2$	$m_1\ m_3$	$m_1\ m_4$

Each entry in the table tells the possible value of $(g(m_i)$ for every pair (a_k, b_k).

- It can be seen from the above table that g can be extended to automorphism with the following definition.

$$\begin{gathered} g(m_1) = m_4 \\ g(m_2) = m_3 \\ g(m_3) = m_2 \\ g(m_4) = m_1 \\ g(a_1) = b_1 \quad \& \quad g(b_1) = a_1 \\ g(a_2) = b_2 \quad \& \quad g(b_2) = a_2 \\ g(a_3) = a_3 \quad \& \quad g(b_3) = b_3 \end{gathered}$$

Case 4 : Three swaps

- Swap $(a_1, b_1) \Rightarrow g(a_1) = b_1 \quad \& \quad g(b_1) = a_1$
- Swap $(a_2, b_2) \Rightarrow g(a_2) = b_2 \quad \& \quad g(b_2) = a_2$
- Swap $(a_3, b_3) \Rightarrow g(a_3) = b_3 \quad \& \quad g(b_3) = a_3$
- Now lets find all possible combinations of $g(m_i)$ which are preferred by each (a_i, b_i)

Swap Cases			
	(a_1, b_1)	(a_2, b_2)	(a_3, b_3)
$g(m_1)$	m_3 m_4	m_2 m_4	m_2 m_3
$g(m_2)$	m_3 m_4	m_1 m_3	m_1 m_4
$g(m_3)$	m_1 m_2	m_2 m_4	m_1 m_4
$g(m_4)$	m_1 m_2	m_1 m_3	m_2 m_3

Each entry in the table tells the possible value of $(g(m_i)$ for every pair (a_k, b_k).

- From the above table it can be shown that there are no values of $g(m_i)$ that satisfies all the pairs (a_k, b_k) .

Hence it is proved that g can be extended to automorphism if and only if the number of swaps are even.

4. **Answer to question 4:**

Given: $\phi : F_p \rightarrow F_p$ $\qquad \phi(x) = x^p$ $\qquad p \in$Prime Number

$(F_p = \{0, 1, 2......, p-1\}, \bigoplus, \bigotimes)$ with arithmetic modulo p

- Elements of F_p are equivalence classes, so ϕ can be more explicity written as

$$\phi(x) = (x^p)\%p$$

For ϕ to be homomorphism:

$$\begin{gathered} \phi(x_1 \bigoplus x_2) = \phi(x_1) \bigoplus \phi(x_2) \\ \phi(x_1 \bigotimes x_2) = \phi(x_1) \bigotimes \phi(x_2) \\ \text{where } x_1, x_2 \in F_p \end{gathered}$$

Some properties of modulo used: (% = modulo symbol)

(a) $([(p_1+p_2)\%p]^p)\%p = (p_1+p_2)^p\ \%p$

(b) $([(p_1*p_2)\%p]^p)\%p = (p_1*p_2)^p\ \%p$

(c) According to Fermat's Little theorem in modulo arithmetic

$$a^p\%p = a\%p$$

Proving ϕ is a homomorphism :

- **Property 1**

$$\phi(x_1 \bigoplus x_2) = \phi(x_1) \bigoplus \phi(x_2), \qquad x_1, x_2 \in F_p$$
$$(x_1 \bigoplus x_2)^p\%p = (x_1)^p\%p \bigoplus (x_2)^p\%p$$

According to Big Fermat's Little theorem

$$(x_1)^p\ \%p = x_1\%p$$

$$(\ x_1 \bigoplus x_2)^p\ \%p = ((\mathrm{x}_1 + \mathrm{x}_2)\%p)^p\ \%p = (x_1+x_2)^p\ \%p = (x_1+x_2)\%p$$

(Using property (a) and (c))

$$(x_1+x_2)\%p = x_1\%p \bigoplus x_2\%p$$

Since x_1, $x_2 \in F_p$

$$x_1\%p = x_1$$

$$(x_1+x_2)\%p = x_1 \bigoplus x_2$$

$$(x_1+x_2)\%p = (x_1+x_2)\%p$$

- **Property 2**

$$\phi(x_1 \bigotimes x_2) = \phi(x_1) \bigotimes \phi(x_2), \qquad x_1, x_2 \in F_p$$
$$(x_1 \bigotimes x_2)^p\%p = (x_1)^p\%p \bigotimes (x_2)^p\%p$$

$$((x_1 * x_2)\%p)^p\%p = (x_1)^p\%p \bigotimes (x_2)^p\%p$$

Using property (b) and (c)

$$(x_1 * x_2)^p\%p = (x_1)\%p \bigotimes (x_2)\%p$$

$$(x_1 * x_2)\%p = (x_1)\%p \bigotimes (x_2)\%p$$

Since x_1, $x_2 \in F_p$

$$x_1\%p = x_1$$

$$(x_1 * x_2)\%p = x_1 \bigotimes x_2$$

$$(x_1 * x_2)\%p = (x_1 * x_2)\%p$$

Hence proved that ϕ is a endomorphism