CS201 Assignment

Soham Sammadar 200990
Akhil Agrawal 200076
Aditya Tanwar 200057

November 2021

Question 1. Define n-variate polynomials P_d and Q_d as:

$$P_d(x_1, x_2, \dots, x_n) = \sum_{\substack{J \subseteq [1,n] \\ |J|=d}} \prod_{r \in J} x_r$$

$$Q_d(x_1, x_2, \dots, x_n) = \sum_{\substack{0 \le i_1, i_2, \dots, i_n \le d \\ i_1+i_2+\cdots+i_n=d}} \prod_{r=1}^{n} x_r^{i_r}$$

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

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

Solution 1. For any arbitrary term $x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$, define its degree to be the sum of the exponents, i.e $\sum_{i=1}^{n} a_i$. We make the following three observations.

- All terms of $P_d(x_1, x_2, \dots, x_n)$ have degree d, i.e it is homogeneous with degree d. This is because exactly d variables out of $(x_1, x_2, \dots, x_n)$ are multiplied, each with exponent 1. Moreover we observe that each term in P_d has the same degree, d.

- All terms of $Q_d(x_1, x_2, \dots, x_n)$ have degree d and Q_d is homogeneous with degree d. This is clearly evident from the definition of Q_d.

- If $d > n$ we claim that upper limit of the summation can be reduced to n.
  For $m > n$, $P_m = 0$ trivially, since, we cannot make a set $J \subseteq [1, n]$ with more than n elements. As we cannot find any such J, each term in the summation is 0 for $m > n$. This allows us to split the sum $\sum_{m=0}^{d} (-1)^m P_m \, Q_{d-m}$ into two parts if $d > n$,

  $$\sum_{m=0}^{n} (-1)^m P_m \, Q_{d-m} + \sum_{m=n+1}^{d} (-1)^m P_m \, Q_{d-m}$$

  And since $P_m = 0$ for $m > n$, we obtain

  $$\sum_{m=n+1}^{d} (-1)^m P_m \, Q_{d-m} = 0$$

Therefore the expression reduces to:

$$\sum_{m=0}^{n}(-1)^m P_m\, Q_{d-m}$$

Where upper limit of the summation is n.

In the expression

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

Since every term of $P_m(x_1, x_2, \ldots, x_n)$ has degree m and every term of $Q_{d-m}(x_1, x_2, \ldots, x_n)$ has degree $d - m$, E is homogeneous in degree d.

Consider a general term with r variables (where $1 \leq r \leq n$) say $(x_{k_1}, x_{k_2}, x_{k_3} \ldots, x_{k_r})$ where $1 \leq k_j \leq n \; \forall \, j \in \{1,\ 2,\ \ldots,\ r\}$, in E, and let the exponents of these variables be $(i_1,\ i_2,\ i_3,\ \ldots,\ i_r)$ respectively.

$\therefore$ This term in E would be:

$$x_{k_1}^{i_1} \cdot x_{k_2}^{i_2} \cdot x_{k_3}^{i_3} \cdots x_{k_r}^{i_r}$$

with $\sum_{j=1}^{r} i_j \; = \; d$ and $i_j \geq 1 \; \forall \, j \in \{1,\ 2,\ 3,\ \ldots,\ r\}$

This term is obtained by product of P_m and Q_{d-m}. So if we fix a term coming from P_m, the term coming from Q_{d-m} will be fixed automatically.

We notice that the term under our consideration will appear exactly $\binom{r}{m}$ times for each m because, we can choose m variables, $(x_{l_1}, x_{l_2}, \ldots, x_{l_m})$ out of $(x_{k_1}, x_{k_2}, x_{k_3} \ldots, x_{k_r})$ to come from P_m. Also, since we have ensured that $i_j \geq 1$, we are assured the existence of the complementary term in Q_{d-m}.

$$\therefore \text{Sum of coefficients of this term} = \sum_{m=0}^{d}(-1)^m \cdot \binom{r}{m}$$

We chose r variables each with exponent ≥ 1. Since the total sum of exponents has to be d, we obtain $r \leq d$. Moreover, define $\binom{r}{m} = 0$ for $m > r$ because it is not possible to choose m variables out of a smaller set of r variables available.

$$\begin{aligned}
\text{Sum of coefficients} &= \sum_{m=0}^{r}(-1)^m \cdot \binom{r}{m} + \sum_{m=r+1}^{d}(-1)^m \cdot \binom{r}{m} \\
&= \sum_{m=0}^{r}(-1)^m \cdot \binom{r}{m} + \sum_{m=r+1}^{d}(-1)^m \cdot 0 \\
&= \sum_{m=0}^{r}(-1)^m \cdot \binom{r}{m} \\
&= 0
\end{aligned}$$

Hence we obtained the coefficient of any general term in the expression to be 0.

$$\Rightarrow E = 0$$

$\square\square\square$

Question 2. 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

$$\mid q\alpha - p \mid \leq \frac{1}{N}$$

<u>**Solution 2.**</u> We are given $\alpha \in \mathbb{R}$ and $N \in \mathbb{N}$.
Let $\{X\}$ denote the fractional part of X.

Consider a set

$$\mathbb{A} = \{\{\alpha\}, \{2\alpha\}, \{3\alpha\}, ..., \{N\alpha\}\}$$

and a set of intervals

$$\mathbb{S} = \{ \left[\frac{1}{N}, \frac{2}{N}\right), \left[\frac{2}{N}, \frac{3}{N}\right) ..., \left[\frac{N-1}{N}, 1\right) \}$$

Lemma 2.1: For any $X \in \mathbb{R}$, $\{X\}$ either lies in interval $\left[0, \frac{1}{N}\right)$ or in an interval Y with $Y \in S$.
Proof: Fractional part of any number is a non-negative real number less than one. Hence $\{X\}$ either belongs to interval $\left[0, \frac{1}{N}\right)$ or to the interval $\left[\frac{1}{N}, 1\right)$.
If $\{X\} \in \left[0, \frac{1}{N}\right)$, then the lemma holds trivially.
Otherwise $\{X\} \in \left[\frac{1}{N}, 1\right)$. Now observe that $\bigcup_{Y \in \mathbb{S}} Y = \left[\frac{1}{N}, 1\right)$.
$\therefore \exists\ Y \in \mathbb{S}$ such that $\{X\} \in Y$ as $\{X\} \in \bigcup_{Y \in \mathbb{S}} Y$.
Hence proved.

We show the desired result in 2 cases:

<u>Case 1</u>: $\exists\ X \in \mathbb{A}$ such that $X \in \left[0, \frac{1}{N}\right)$
For such an X, let the corresponding element in $\mathbb{A}$ be $\{q\alpha\}$. Choosing $p = [q\alpha]$ (where $[X]$ denotes greatest integer less than equal to X), we have

$$\begin{aligned} &\mid q\alpha - p \mid \\ =&\mid q\alpha - [q\alpha] \mid \\ =&\mid \{q\alpha\} \mid \\ \leq& \frac{1}{N} \end{aligned}$$

<u>Case 2</u>: When no element of $\mathbb{A}$ lies in interval $\left[0, \frac{1}{N}\right)$.
By *Lemma 2.1*, every element of $\mathbb{A}$ will belong to some element in set $\mathbb{S}$.

According to the pigeon hole principle, if n + 1 objects are kept in n boxes then at least one box has more than one object.

Let elements of $\mathbb{A}$ be objects (N in number) and elements of $\mathbb{S}$ be boxes ($N-1$ in number). Therefore by the pigeon hole principle, at least 2 elements of $\mathbb{A}$ will belong to same element in $\mathbb{S}$. Let those two elements of $\mathbb{A}$ be $\{q_1\alpha\}, \{q_2\alpha\}$ (assume $q_1 > q_2$ without loss of generality) and the common interval they lie in be
$[\frac{r}{N}, \frac{r+1}{N})$ (where $1 \leq r \leq N-1$). Hence we have,

$$\frac{r}{N} \leq \{q_1\alpha\} < \frac{r+1}{N}$$

$$\frac{r}{N} \leq \{q_2\alpha\} < \frac{r+1}{N}$$

$$\implies \frac{-1}{N} < \{q_1\alpha\} - \{q_2\alpha\} < \frac{1}{N}$$

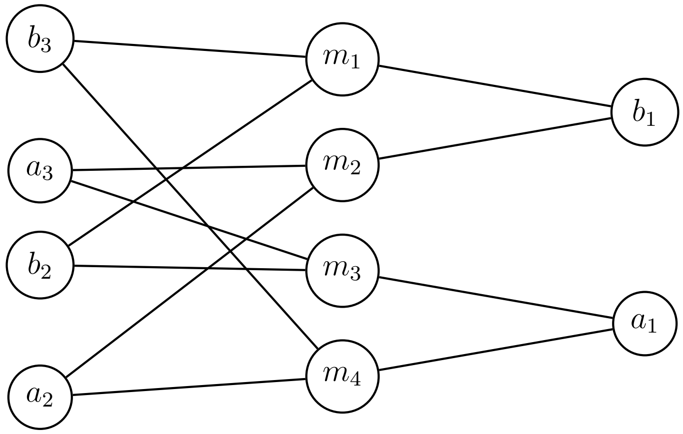
Let $q = q_1 - q_2$ and $p = [q_1\alpha] - [q_2\alpha]$ (where $[X]$ denotes greatest integer less than or equal to X), we have

$$\begin{aligned}
&|q\alpha - p| \\
&= |(q_1\alpha - q_2\alpha) - ([q_1\alpha] - [q_2\alpha])| \\
&= |(q_1\alpha - [q_1\alpha]) - (q_2\alpha - [q_2\alpha])| \\
&= |\{q_1\alpha\} - \{q_2\alpha\}| \\
&\leq \frac{1}{N}
\end{aligned}$$

Hence proved.

$\square\square\square$

Question 3. 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.

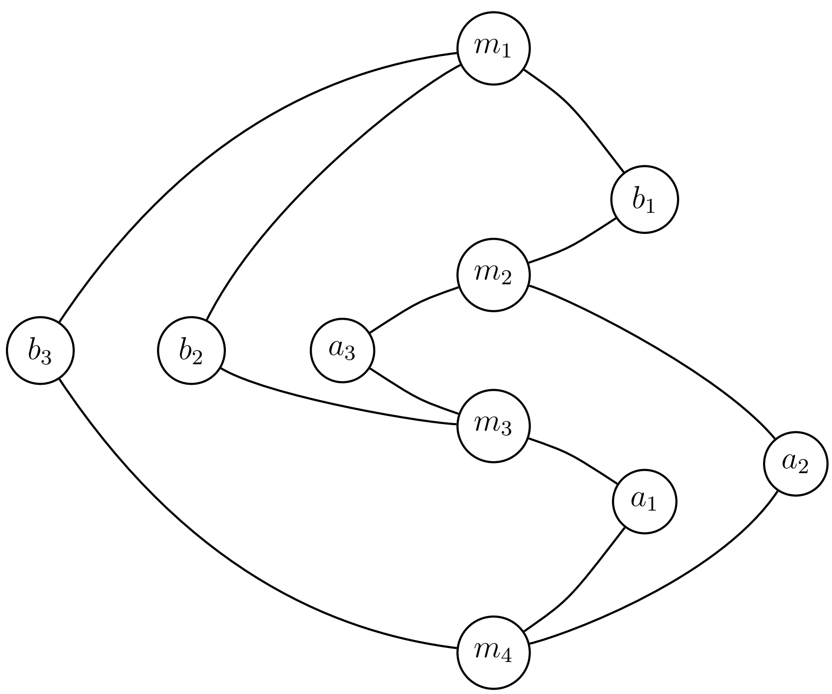


Let $A = \{a_1, a_2, a_3\},\ B = \{b_1, b_2, b_3\},\ M = \{m_1, m_2, m_3, m_4\}$. Then, the vertex set of the above graph is $V = A \cup B \cup M$. Consider a bijective mapping $g : A \cup B \to A \cup B$ such that $g(a_i) \in \{a_i, b_i\}$ and $g(b_i) \in \{a_i, b_i\}$ for all $i \in \{1, 2, 3\}$, i.e., 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.

<u>Solution 3.</u>

We first re-draw the graph in the following manner which increases clarity and allows us to make some valuable observations-



Before we list the observations, we introduce some new notations for more concise statements-

- $V_u :=$ The set of vertices having an edge directly with vertex $u \in V$
- $f(V_u) := \{f(v) \mid v \in V_u\}$ where $f\colon V \mapsto V$
- $f(E) := \{(f(u),\ f(v)) \mid u, v \in V_u\}$ where $f\colon V \mapsto V$
- $(u, V_u) := \{(u, v) \mid v \in V_u\}$
- $(u, V_u) \xrightarrow{f} (v, W) :=\ f(u) = v$ and $f(V_u) = W$

And here are the observations with short explanations listed wherever possible-

1. $V_{b_i} = \{m_1, m_{i+1}\} \Rightarrow m_1 \in V_{b_i}$ $\qquad \forall\ i \in \{1, 2, 3\}$
2. $V_{a_i} = M \setminus V_{b_i} \Rightarrow m_1 \notin V_{a_i}$ and $V_{b_i} = M \backslash V_{a_i}$ $\qquad \forall\ i \in \{1, 2, 3\}$
3. $V_{a_i} \cap V_{b_i} = \varnothing$ and $V_{a_i} \cup V_{b_i} = M$ $\qquad \forall\ i \in \{1, 2, 3\}$
4. $|V_u| = 2$ & $|M \backslash V_u| = 2$ and $V_u \subset M$ $\qquad \forall\ u \in A \cup B$
5. $V_{b_i} \cap V_{b_j} = \{m_1\}$ and $V_{b_i} \backslash V_{b_j} = \{m_{i+1}\}$ $\qquad \forall\ i \neq j$ & $i,\ j \in \{1, 2, 3\}$
   $\because m_1$ is the only node common to all V_{b_i} as observed in 1.
6. $V_{b_i} \cap V_{a_j} = \{m_{i+1}\}$ and $V_{b_i} \backslash V_{a_j} = \{m_1\}$ $\qquad \forall\ i \neq j$ & $i,\ j \in \{1, 2, 3\}$
   $$\because V_{b_i} \backslash V_{b_j} = (M \cap V_{b_i}) \cap (M \backslash V_{b_j}) = (M \cap V_{b_i}) \cap (V_{a_j})$$
   $$= (M \cap V_{a_j}) \cap (V_{b_i} \cap V_{a_j}) = V_{b_i} \cap V_{a_j}$$
7. $|V_u \cap V_v| = 1$ for $u,\ v \in A \cup B$ if and only if, $\{u, v\} \neq \{a_i, b_i\}$ for some $i \in \{1, 2, 3\}$

$\star$ If f extends g and is an *automorphism*, with $f(u) = u$ for some $u \in A \cup B$, then $f(V_u) = V_u$. Similarly, if $f(u) \neq u$ for some $u \in A \cup B$, then $f(V_u) = M \backslash V_u$.
As $(u, V_u) \xrightarrow{f} (f(u), f(V_u))$ and f is an *automorphism*, we should have $V_{f(u)} = f(V_u)$ which can be simplified using 2^{nd} observation if $f(u) \neq u$.

$\diamond$ If $(u, V_u) \xrightarrow{f} (f(u), f(V_u))$ and $V_{f(u)} = f(V_u) \forall u \in V$, then f is an *automorphism*.
Follows straight from the definition of *automorphism* and notations used.

<u>*Case* 1</u>: When *0 swaps* are performed by g.
This implies $g(u) = u\ \forall\ u \in A \cup B$. Extend g to the function f such that

$$f(u) = \begin{cases} g(u) & \text{if } u \in A \cup B \\ u & \text{otherwise} \end{cases}$$

Therefore the function f is trivially an *automorphism* as $(u, V_u) \xrightarrow{f} (u, V_u)$.

<u>*Case* 2</u>: When *1 swap* is performed by g.
Let the pair *swapped* by g be $\{a_i, b_i\}$, and remaining pairs be $\{a_j, b_j\}$ and $\{a_k, b_k\}$. Let there be a function f which is an *automorphism*. Then, f should map as follows:

$$f(V_{a_i}) = V_{b_i} \qquad (= M \backslash V_{a_i})$$

$$\begin{aligned} f(V_{b_i}) &= V_{a_i} && (= M \backslash V_{b_i}) \\ f(V_{a_x}) &= V_{a_x} && (\text{where } x \in \{j, k\}) \\ f(V_{b_x}) &= V_{b_x} && (\text{where } x \in \{j, k\}) \end{aligned}$$

By *Obs. 5*, $m_1 \in V_{b_i} \cap V_{b_j}$, and by using definition of f defined above, $f(m_1) \in V_{a_i}$ and $f(m_1) \in V_{b_j}$.

$$\begin{aligned} &\Rightarrow f(m_1) \in V_{a_i} \cap V_{b_j} \\ &\Rightarrow f(m_1) \in (M \backslash V_{b_i}) \cap V_{b_j} \end{aligned}$$

Similarly, $m_1 \in V_{b_i} \cap V_{b_j}$, and by a similar argument,

$$\Rightarrow f(m_1) \in (M \backslash V_{b_i}) \cap V_{b_k}$$

Using above two equations, we obtain,

$$\Rightarrow f(m_1) \in (M \backslash V_{b_i}) \cap V_{b_j} \cap V_{b_k}$$

Again, from *Obs. 5*, we have $V_{b_j} \cap V_{b_k} = \{m_1\}$, and from *Obs. 1*, we have $V_{b_i} = \{m_1, m_{i+1}\}$. Therefore, we obtain,

$$\begin{aligned} &\Rightarrow f(m_1) \in (M \backslash \{m_1, m_{i+1}\}) \cap \{m_1\} \\ &\Rightarrow f(m_1) \in \phi \end{aligned}$$

Which is a contradiction, as f has to map vertex m_1 to some other vertex. Hence no extension of g can be made such that f is an *automorphism*.

Case 3: When *2 swaps* are performed by g. Let i be the pair which is not *swapped* by g, and let j, k be the pairs which are *swapped* by g. We extend g to a function f so that f *"swaps"* the two m_r in V_{b_i}, i.e.,

$$f(m_1) = m_{i+1} \text{ and } f(m_{i+1}) = m_1$$

f similarly *"swaps"* the two m_r in V_{a_i} in place. So, we have $f(V_{b_i}) = V_{b_i}$ and $f(V_{a_i}) = V_{a_i}$ and hence f preserves all edges from $\{a_i, b_i\}$

Now, we need to show that f preserves all the edges from $\{a_j, a_k, b_j, b_k\}$. It suffices to show that

$$(a_x, V_{a_x}) \xrightarrow{f} (b_x, V_{b_x}) \text{ and } (b_x, V_{b_x}) \xrightarrow{f} (a_x, V_{a_x}) \qquad \text{for } x \in \{j, k\}$$

Obviously, $f(a_x) = b_x$ and $f(b_x) = a_x$ as f extends g and g *swaps* the pairs j and k. To show f's behaviour on V_{b_x} and V_{a_x},

- Let $V_y = V_{b_x}$ or V_{a_x}. For $m \in V_y$, either $m \in V_{a_i}$ or $m \in V_{b_i}$, but not both simultaneously (from *Obs. 3*).

- If $m = m_p \in V_{a_i}$, then f must have *"swapped"* m_p with the other m_s in V_{a_i}. So, we have

$$\begin{aligned} & f(m_p) = m_s \in V_{a_i} \backslash m_p \\ & \Rightarrow m_s \notin V_y && \text{from } \textit{Obs. 7} \\ & \Rightarrow m_s \in M \backslash V_y && m_s \in M \text{ and } m_s \notin V_y \end{aligned}$$

- If $m_q \in V_{b_i}$, then f must have *"swapped"* m_q with the other m_t in V_{b_i}. So, we have

$$\begin{aligned} & f(m_q) = m_t \in V_{b_i} \backslash m_q \\ & \Rightarrow m_t \notin V_y && \text{from } \textit{Obs. 7} \\ & \Rightarrow m_t \in M \backslash V_y && m_t \in M \text{ and } m_t \notin V_y \end{aligned}$$

- Now, $|M \backslash V_y| = 2$, and $V_{a_i} \ni m_p \neq m_q \in V_{b_i}$, $V_{a_i} \ni m_s \neq m_t \in V_{b_i}$ (follow from *Obs. 4* and *Obs. 3* respectively). Hence, $\{m_s, m_t\} = M \backslash V_y$.

Thus, all edges from $\{a_j, a_k, b_j, b_k\}$ are also preserved, and all edges from $\{a_i, b_i\}$ were shown to have been preserved earlier. So, we get,

$$E \subseteq f(E)$$

And, as $f : A \cup B \mapsto A \cup B$, and $f : M \mapsto M$, no new edges are created by f. So,

$$|f(E)| \leq |E|$$

Combining these results, we get $E = f(E)$, or, in other words, each edge in E is preserved by the bijective mapping $f : V \mapsto V$.
Hence, f is an *automorphism*.

Case 4: When all pairs are swapped by g.
Let there be a function f which is an *automorphism*. Then f is defined as follows

$$\begin{aligned} f(V_{a_x}) &= V_{b_x} && (\text{where } x \in \{i, j, k\}) \\ f(V_{b_x}) &= V_{a_x} && (\text{where } x \in \{i, j, k\}) \end{aligned}$$

By *Obs. 1*, $m_1 \in V_{b_x} \; \forall \, x \in \{1, 2, 3\}$,

$$\begin{aligned} & \Rightarrow f(m_1) \in V_{a_i} \;\; \& \;\; f(m_1) \in V_{a_j} \;\; \& \;\; f(m_1) \in V_{a_k} \\ & \Rightarrow f(m_1) \in V_{a_i} \cap V_{a_j} \cap V_{a_k} \\ & \Rightarrow f(m_1) \in \phi \end{aligned}$$

Which is again a contradiction, as f has to map vertex m_1 to some other vertex. Hence no extension of g can be made such that f is an *automorphism*.

Thus, any $g : A \cup B \mapsto A \cup B$ that performs an even number of swaps can be extended to an *automorphism*, while if it performs an odd number of swaps, it is impossible to extend it to an *automorphism*.

Hence, 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.

$\square\square\square$

Question 4. An *endomorphism* of a ring R is a ring homomorphism $\phi : R \mapsto R$. Prove that $\phi : F_p \mapsto F_p$, $\phi(x) = x^p$ is an endomorphism where p is a prime number.

<u>Solution 4.</u>

We denote addition by $\oplus$ and multiplication by $\odot$. These are also the operations we use on $F_p = \{0, 1, 2, \dots, p-1\}$.
Also, we take p to be a prime number throughout the rest of the discussion.

Lemma 4.1 p divides $\binom{p}{i}$ $\forall\ 1 \leq i \leq p-1,\ i \in \mathbb{N}$.

Proof. $\binom{p}{i}$ can be interpreted as number of ways of choosing k objects out of p given objects. Clearly then, $\binom{p}{i}$ is a positive integer. We use c to represent it.

$$\begin{aligned} c = \binom{p}{i} &= \frac{p!}{i!\,(p-i)!} \\ p! &= c \cdot i! \cdot (p-i)! \\ p \cdot (p-1)! &= c \cdot i! \cdot (p-i)! \end{aligned}$$

Now, $1 \leq p-1 \Rightarrow (p-1)! \in \mathbb{N} \therefore p$ divides the product $c \cdot i! \cdot (p-i)!$
We observe that p, being prime, cannot divide any product of positive numbers, in which the numbers are strictly lesser than p itself. And, as $1 \leq i,\ p-i \leq p-1$, every term in $i!$ and $(p-i)!$ is also lesser than p, hence p divides neither $i!$ nor $(p-i)!$.
So, the only possibility left is that p divides $c = \binom{p}{i}$. Hence, the *lemma* follows. $\square$

$\phi(x \oplus y) = \phi(x) \oplus \phi(y)$**:**

$$\begin{aligned} \phi(x \oplus y) &= (x+y)^p \\ &= \sum_{i=0}^{i=p} \binom{p}{i} \odot x^{p-i} \odot y^i && \text{Expansion using binomial theorem} \\ &= (x^p) \oplus \cancel{\left(\binom{p}{1} \odot x^{p-1} \odot y^1\right)} \oplus \cdots \oplus \cancel{\left(\binom{p}{p-1} \odot x^1 \odot y^{p-1}\right)} \oplus (y^p) \\ &= (x^p) \oplus (y^p) && \text{From Lemma 4.1} \\ &= \phi(x) \oplus \phi(y) \end{aligned}$$

$\phi(x \odot y) = \phi(x) \odot \phi(y)$**:**

$$\begin{aligned} \phi(x \odot y) &= (x \odot y)^p = (x)^p \odot (y)^p \\ &= \phi(x) \odot \phi(y) \end{aligned}$$

<u>*Note:*</u> The range of ϕ for the domain F_p is a subset of the given co-domain F_p, i.e., instances like $2^3 = 8 \notin F_3$ are not possible because the arithmetic $(\odot, \oplus)$ is modulo p.
In fact, the expression of $\phi(x) = x^p$ can even be simplified to $\phi(x) = x$.

Proof. The proof is by induction on x. It trivially holds for $x = 0$ and $x = 1$. We assume it to be valid for x, and then prove it for $x + 1$:

$$\begin{aligned}
\phi(x \oplus 1) &= (x \oplus 1)^p \\
&= \sum_{i=0}^{i=p} \binom{p}{i} \odot x^i && \text{Expansion using binomial theorem} \\
&= 1 \oplus \cancel{\binom{p}{1} \odot x^1} \oplus \cdots \oplus \cancel{\binom{p}{p-1} \odot x^{p-1}} \oplus x^p \\
&= 1 \oplus x && \text{Using } \textit{Lemma 4.1} \\
&= x \oplus 1
\end{aligned}$$

□

Since the domain and range of ϕ are equal, $\phi(x \oplus y) = \phi(x) \oplus \phi(y)$, and $\phi(x \odot y) = \phi(x) \odot \phi(y)$, so ϕ is an *endomorphism* from F_p to F_p, where p is a prime number.

□□□