Introduction to Combinatorics Lecture 12

Principle of Counting

- We consider the sets A which are countable, i.e., A is either a finite set or A has the same cardinality as the set of positive integers $\mathbb{N}$.
- For convenience, we use $|A|$ to denote the cardinality of A.

Facts

1. If there exists a function f from A into B, then $|A| \leq |B|$, $|A| \geq |B|$ provided f is onto.
2. (Fundamental idea of counting) If $f : A \to B$ is a bijection, then $|A| = |B|$.
3. The number of k-subsets (distinct) of an n-set is equal to $n \cdot (n-1) \cdot \cdots \cdot (n-k+1)/k! = \frac{n!}{(n-k)!k!}$, denoted by $\binom{n}{k}$ (n-chooses-k).
4. There are $n!$ permutations on n elements. (It is known as the order of a symmetric group of order n.)
5. If we select k elements from an n-set and the order is en-counted, then there are $n!/k!$ ways to get the job done.

Definition 12.1 (Principle of Inclusion and Exclusion, PIE)**.**
Let $A_1, A_2, ..., A_n$ be n countable sets. Then

$$|\bigcup_{i=1}^{n} A_i| = \sum_{i=1}^{n} |A_i| - \sum_{1 \leq i < j \leq n} |A_i \cap A_j| + \cdots + (-1)^{n-1} |\bigcap_{i=1}^{n} A_i|.$$

e.g. For A, B and C, $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$.

Definition 12.2 (Euler totient function on relative primes)**.**

$$n \in \mathbb{N},\ \phi(n) = |\{k | 1 \leq k \leq n, gcd(n, k) = 1\}|.$$

e.g. $\phi(1) = 1,\ \phi(2) = 1,\ \phi(3) = 2,\ \phi(4) = 2,\ \phi(5) = 4,\ \phi(6) = 2.$

Proposition 12.1. *By PIE, if* $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$*, then*

$$\begin{aligned}\phi(n) &= n - \sum_{i=1}^{r} \frac{n}{p_i} + \sum_{1 \le i < j \le r} \frac{n}{p_i p_j} - \cdots + (-1)^r \frac{n}{p_1 p_2 \cdots p_r} \\ &= n - \left[\sum_{i=1}^{r} \frac{n}{p_i} - \sum_{1 \le i < j \le r} \frac{n}{p_i p_j} + \cdots + (-1)^{r-1} \frac{n}{p_1 p_2 \cdots p_r} \right]\end{aligned}$$

Proof. Let A_i be the set of integers in $[1, n]$ which are multiple of p_i. Then $\phi(n) = n - |\bigcup_{i=1}^{r} A_i| = |\overline{A_1} \cap \overline{A_2} \cap \overline{A_3} \cap \cdots \cap \overline{A_r}|$. □

Proposition 12.2. *Another famous example of PIE is the derangement. Let* $\mathbb{D}_n$ *denote the set of permutations* σ *of* $[1, n]$ *such that* $\sigma(i) \neq i$ *for each* $i \in [1, n]$*. Then,*

$$|\mathbb{D}_n| = D_n = n!(1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \cdots + (-1)^n \frac{1}{n!}).$$

Proposition 12.3.

$$\sum_{d|n} \phi(d) = n.$$

Proof. Consider the partition on $[1, n]$ into subsets $A_d = \{m | m \in [1, n] \text{ and } gcd(m, n) = d\}$. Since $gcd(m, n) = d$, $gcd(\frac{m}{d}, \frac{n}{d}) = 1$. Hence, there are $\phi(\frac{m}{d})$ such $\frac{m}{d}$'s. This implies that $|A_d| = \phi(\frac{n}{d})$. Thus,

$$n = \sum_{d|n} |A_d| = \sum_{d|n} \phi(\frac{n}{d}) = \sum_{d|n} \phi(d).$$

□

Note that $\forall \bar{m} \in \mathbb{Z}_n$, $\langle \bar{m} \rangle$ generates a subgroup of $\mathbb{Z}$ of order $n/gcd(m, n)$ and there are $\phi(n/gcd(m, n))$ m's. This implies the conclusion as above.

Definition 12.3 (Möbius function)**.** If $m = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$, then

$$\mu(m) = \begin{cases} (-1)^r & \text{if } a_1 = a_2 = \cdots = a_r = 1 \text{ ; and} \\ 0 & \text{otherwise.} \end{cases}$$

Proposition 12.4. *For each $n > 1$,*

$$\sum_{d|n} \mu(d) = 0.$$

Proof. Let $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$. Hence, $\sum_{d|n} \mu(d) = \sum_{d} \mu(d)$ where d is a product of distinct primes. Thus

$$\sum_{d|n} \mu(d) = \sum_{i=0}^{r} \binom{r}{i} (-1)^i = \binom{r}{0} - \binom{r}{1} + \binom{r}{2} - \binom{r}{3} + \cdots + (-1)^r \binom{r}{r} = (1+(-1))^r = 0.$$

□

Proposition 12.5.

$$\frac{\phi(n)}{n} = \sum_{d|n} \frac{\mu(d)}{d}.$$

Proof. Let $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$. By **Proposition 12.1**,

$$\phi(n) = n - \sum_{i=1}^{r} \frac{n}{p_i} + \sum_{1 \le i < j \le r} \frac{n}{p_i p_j} - \cdots + (-1)^r \frac{n}{p_1 p_2 \cdots p_r}.$$

Hence,

$$\frac{\phi(n)}{n} = 1 - \sum_{i=1}^{r} \frac{1}{p_i} + \sum_{1 \le i < j \le r} \frac{1}{p_i p_j} - \cdots + (-1)^r \frac{1}{p_1 p_2 \cdots p_r}.$$

On the other hand, $\sum_{d|n} \frac{\mu(d)}{d} = \sum_{d} \frac{\mu(d)}{d}$ where d is a product of distinct primes in $\{p_1, p_2, ..., p_r\}$. This implies that

$$\sum_{d|n} \frac{\mu(d)}{d} = 1 - 1 - \sum_{i=1}^{r} \frac{1}{p_i} + \sum_{1 \le i < j \le r} \frac{1}{p_i p_j} - \cdots + (-1)^r \frac{1}{p_1 p_2 \cdots p_r}.$$

Thus, the proof follows. □

The following formula is known as "Möbius Inversion Formula".

Proposition 12.6 (Mödius Inversion Formula)**.** *If $f(n) = \sum_{d|n} g(d)$, then*

$g(n) = \sum_{d|n} \mu(d) f(\frac{n}{d})$.

Proof.

$$\begin{aligned}
\sum_{d|n}\mu(d)f(\frac{n}{d}) &= \sum_{d'|n} f(d')\mu(\frac{n}{d'}) \text{ where } d' = \frac{n}{d}\\
&= \sum_{d|n} f(d)\mu(\frac{n}{d})\\
&= \sum_{d|n}\mu(d)\cdot\sum_{d''|d} g(d'')\\
&= \sum_{d''|n} g(d'')\cdot\sum_{m|\frac{n}{d''}}\mu(m)\\
&= g(n) \text{ (when } d''=n) \ + \left\{\sum_{d''|n} g(d'')\cdot\sum_{m|\frac{n}{d''}}\mu(m) \text{ with } d''<n\right\}\\
&= g(n), \text{ since } \sum_{m|\frac{n}{d''}}\mu(m) = 0 \text{ provided } \frac{n}{d''} > 1.
\end{aligned}$$

□

Remark. We can use **Proposition 12.3** and **Proposition 12.6** to prove **Proposition 12.5**. Since $n = \sum_{d|n}\phi(d)$, $\phi(n) = \sum_{d|n}\mu(d)\frac{n}{d}$. Hence, we have $\frac{\phi(n)}{n} = \sum_{d|n}\frac{\mu(d)}{d}$.

Möbius Inversion Formula plays an important role in enumeration. We present a good example in what follows.

Review that in order to construct a finite field with p^n elements where p is a prime and $n \geq 1$, we need to find an irreducible polynomial $f(x)$ over $\mathbb{Z}_p$ and the finite field is obtained as $\mathbb{Z}_p[x]/\langle f(x)\rangle$. Therefore, the existence of such polynomials must be verified. In fact, we can enumerate the number of such polynomials which are monic, i.e., the coefficient of x^n is 1.

1. $x^{p^n} - x$ is a product of all monic irreducible polynomials over GF(p) (or $\mathbb{Z}_p$) whose degree $d|n$. (Extension field: from p^d elements to p^n elements, $d|n$ is obtained from dimension fact.)
2. Now, let N_d denote the number of monic irreducible polynomial of degree d over $\mathbb{Z}_p$ in the factorization $x^{p^n} - x$. Then, $p^n = \sum_{d|n} d\cdot N_d$ (over $\mathbb{Z}_p$).

3. Let $f(n) = p^n,\ g(d) = d \cdot N_d$. By Möbius Inversion Formula, $n \cdot N_n = \sum_{d|n} \mu(d) \cdot p^{n/d}$.

   Thus,

$$\begin{aligned} N_n &= \frac{1}{n} \sum_{d|n} \mu(d) \cdot p^{n/d} \\ &\geq \frac{1}{n}(p^n - p^{n/2}) > 0 \end{aligned}$$