Math 184

Lecture Notes Section 2.4 *

Instructor: Swee Hong Chan

NOTE: The notes is a summary for materials discussed in the class and is not supposed to substitute the textbook. In particular, the proofs here might omit some details for brevity, and are not supposed to be how you write proofs in the exam. Please refer back to the textbook when studying for exams; materials that appear in the textbook but do not appear in the lecture notes might still be tested. Please send me an email if you find typos.

1 Inclusion-exclusion principle

Lemma 1. *Let A and B be finite sets. Then we have*

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Proof. See the picture of Venn diagram drawn in the lecture. □

Example 2. The number of positive integers less than or equal to 300 that are divisible by at least one of 2 and 3 is 200. △

Proof. Let A and B be the set

$$A := \{n \in \{1, \ldots, 300\} \mid n \text{ is divisible by } 2\};$$
$$B := \{n \in \{1, \ldots, 300\} \mid n \text{ is divisible by } 3\}.$$

Note that the question is asking for $|A \cup B|$. Also note that $|A| = 150$ and $|B| = 100$ by direct counting. Now note that $A \cap B$ is given by

$$A \cap B := \{n \in \{1, \ldots, 300\} \mid n \text{ is divisible by } 6\}.$$

Note that $|A \cap B| = 50$ by direct counting. We now have

$$|A \cup B| = |A| + |B| - |A \cap B| = 150 + 100 - 50 = 200,$$

which answers the question. □

*Version date: Thursday 30$^{\text{th}}$ January, 2020, 17:46

Lemma 3. *Let A, B, C be finite sets. Then*

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|.$$

Proof. See the picture of Venn diagram drawn in the lecture. □

Example 4. Count the number of positive integers less than or equal to 300 that are divisible by at least one of 2, 3, and 5. △

Proof. Let A, B, and C be the set

$$\begin{aligned} A :=& \{n \in \{1, \ldots, 300\} \mid n \text{ is divisible by } 2\}; \\ B :=& \{n \in \{1, \ldots, 300\} \mid n \text{ is divisible by } 3\}; \\ C :=& \{n \in \{1, \ldots, 300\} \mid n \text{ is divisible by } 5\}. \end{aligned}$$

Note that the question is asking for $|A \cup B \cup C|$. Now note that $A \cap B$ is given by

$$\begin{aligned} A \cap B :=& \{n \in \{1, \ldots, 300\} \mid n \text{ is divisible by } 6\}; \\ A \cap C :=& \{n \in \{1, \ldots, 300\} \mid n \text{ is divisible by } 10\}; \\ B \cap C :=& \{n \in \{1, \ldots, 300\} \mid n \text{ is divisible by } 15\}; \\ A \cap B \cap C :=& \{n \in \{1, \ldots, 300\} \mid n \text{ is divisible by } 30\}. \end{aligned}$$

By direct counting,

$$\begin{aligned} &|A| = 150; \qquad |B| = 100; \qquad |C| = 60; \\ &|A \cap B| = 50; \qquad |A \cap C| = 30; \qquad |B \cap C| = 20; \\ &|A \cap B \cap C| = 10. \end{aligned}$$

We then have

$$\begin{aligned} |A \cup B \cup C| =& |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C| \\ =& 150 + 100 + 60 - 50 - 30 - 20 + 10 \\ =& 220, \end{aligned}$$

which answers the question. □

Theorem 5 (Inclusion-exclusion principle)**.** *Let $A_1, A_2, \ldots, A_n$ be finite sets. Then*

$$|A_1 \cup \ldots \cup A_n| = \sum_{j=1}^{n} (-1)^{j-1} \sum_{i_1, i_2, \ldots, i_j} |A_{i_1} \cap A_{i_2} \cap \ldots \cap A_{i_j}|,$$

where $\{i_1, \ldots, i_j\}$ ranges over all j-element subsets of $[n]$.

Proof. Read the textbook Section 2.4 for a proof, or try to derive it yourself as an exercise to test your understanding. □

Remark 6. Perhaps a more intuitive way to understand the inclusion-exclusion principle is to write it in the following form:

$$\begin{aligned}
&|A_1 \cup A_2 \ldots \cup A_n| \\
=&+|A_1| + |A_2| + \ldots |A_n| \\
&-|A_1 \cap A_2| - |A_1 \cap A_3| - \ldots - |A_{n-1} \cap A_n| \\
&+|A_1 \cap A_2 \cap A_3| + |A_1 \cap A_2 \cap A_4| + \ldots + |A_{n-2} \cap A_{n-1} \cap A_n| \\
&\ldots \\
&+(-1)^{n-1}|A_1 \cap A_2 \cap \ldots \cap A_n|.
\end{aligned}$$

△

2 Applications: formula for Stirling number

Recall that a set partition of $[n]$ into k parts is a set $\{B_1, B_2, \ldots, B_k\}$ of subsets of $[n]$ such that

$$\begin{aligned}
&B_i \neq \varnothing \text{ for all } i; \quad B_i \cap B_j = \varnothing \text{ for distinct } i, j; \\
&B_1 \cup B_2 \cup \ldots \cup B_k = [n].
\end{aligned}$$

Also recall that the Stirling number of second kind is

$$\left\{ {n \atop k} \right\} := \text{number of set partitions of } [n] \text{ into } k \text{ parts.}$$

Theorem 7. *For any positive integer n and any nonnegative integer $k \leq n$,*

$$\left\{ {n \atop k} \right\} = \frac{1}{k!} \sum_{j=0}^{k} (-1)^j \binom{k}{j} (k-j)^n.$$

We now build toward the proof of Theorem 7, which uses the following theorem.

Theorem 8. *Let n be a positive integer and k be a nonnegative integer such that $k \leq n$. Then the number of surjections from $[n]$ to $[k]$ is equal to*

$$\sum_{j=0}^{k} (-1)^j \binom{k}{j} (k-j)^n.$$

Proof. We will prove this theorem using the inclusion-exclusion principle. For any $i \in [k]$, we write

$$A_i := \{f : [n] \to [k] \ \mid \ f(x) \neq i \text{ for all } x \in [n]\}.$$

That is to say, A_i contains all the functions from $[n]$ to $[k]$ for which i is not contained in the image of the function.

Now note that, for any distinct $i_1, i_2, \ldots i_j \in [k]$, we have

$$A_{i_1} \cap A_{i_2} \cap \ldots \cap A_{i_j} = \{f : [n] \to [k] \ \mid \ f(x) \in \{i_1, i_2, \ldots, i_k\} \text{ for all } x \in [n]\}.$$

That is to say, $A_{i_1} \cap A_{i_2} \cap \ldots \cap A_{i_j}$ consists of functions for which $i_1, \ldots, i_j$ are all not contained in the image of the function.

We now count the number of functions contained in $A_{i_1} \cap A_{i_2} \cap \ldots \cap A_{i_j}$. Note that for each element $x \in [n]$, the value $f(x)$ is contained in $k - \{i_1, \ldots, i_j\}$, which has $k - j$ elements. By the product principle, we then have

$$|A_{i_1} \cap A_{i_2} \cap \ldots \cap A_{i_j}| = (k-j)^n.$$

By the inclusion exclusion principle, we then have

$$\begin{aligned}
|A_1 \cup \ldots \cup A_n| &= \sum_{j=1}^{n} (-1)^{j-1} \sum_{i_1, i_2, \ldots, i_j} |A_{i_1} \cap A_{i_2} \cap \ldots \cap A_{i_j}|, \\
&= \sum_{j=1}^{n} (-1)^{j-1} \sum_{i_1, i_2, \ldots, i_j} (k-j)^n \\
&= \sum_{j=1}^{n} (-1)^{j-1} \binom{k}{j} (k-j)^n \qquad \text{(why?)}.
\end{aligned}$$

Now note that it follows from the definition that

$$A_1 \cup \ldots \cup A_n = \{ f : [n] \to [k] \ \mid \ f \text{ is not surjective } \}.$$

Combining all the conclusions we derive from above, we conclude that

$$\begin{aligned}
\#\text{ surjective } f : [n] \to [k] \ &= (\# f : [n] \to [k]) \ - \ |A_1 \cup \ldots \cup A_n| \\
&= k^n - \sum_{j=1}^{n} (-1)^{j-1} \binom{k}{j} (k-j)^n \\
&= \sum_{j=0}^{k} (-1)^{j} \binom{k}{j} (k-j)^n,
\end{aligned}$$

and our proof is complete. □

Proof of Theorem 7. We will show that the number of ordered subsets $(B_1, B_2, \ldots, B_k)$ for which $\{B_1, B_2, \ldots, B_k\}$ is a set partition of $[n]$ is equal to

$$\sum_{j=0}^{k} (-1)^{j} \binom{k}{j} (k-j)^n.$$

Indeed, once we show the equation above, the conclusion of the theorem will immediately follow from the division principle.

Now note that, these two sets are in bijection with each other:

- the set of ordered subsets $(B_1, B_2, \ldots, B_k)$ for which $\{B_1, B_2, \ldots, B_k\}$ is a set partition of $[n]$; and
- the set of surjections from $[n]$ to $[k]$.

Indeed, given any ordered set $(B_1, B_2, \ldots, B_k)$, we associate this set to the surjection $f : [n] \to [k]$ given by

$$f(x) = i \quad \text{for } i \text{ such that } \quad x \in B_i.$$

Checking that this correspondence is indeed a bijection is left as an exercise.

It then follows from Theorem 8 that the number of ordered subsets $(B_1, B_2, \ldots, B_k)$ for which $\{B_1, B_2, \ldots, B_k\}$ is a set partition of $[n]$ is equal to

$$\sum_{j=0}^{k} (-1)^j \binom{k}{j} (k-j)^n.$$

This completes our proof. □

3 Euler's totient function

Definition 9 (Euler's totient function)**.** For any positive integer n, The *Euler's totient function* $\phi(n)$ is

$$\phi(n) := |\{x \in \{1, \ldots, n\} \mid \gcd(x, n) = 1\}|.$$

That is to say, $\phi(n)$ is the number of positive integers less than n that is coprime to n. △

This function has important applications in abstract algebra (e.g., counting invertible elements in the group $\mathbb{Z}/n\mathbb{Z}$, number theory (e.g., solving Diophantine equations), and combinatorics (e.g., counting necklaces).

Theorem 10. *Let n be any positive integer, and let $p_1, p_2, \ldots p_t$ be the prime divisors of n. Then*

$$\phi(n) = n \prod_{i=1}^{t} \left(1 - \frac{1}{p_i}\right) = n \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \ldots \left(1 - \frac{1}{p_t}\right).$$

Remark 11. The theorem above can be rewritten into the following possibly more friendly form. Let the following be the prime factorization of n:

$$n = p_1^{d_1} p_2^{d_2} \ldots p_t^{d_t}.$$

Then, we have

$$\phi(n) = p_1^{d_1 - 1}(p_1 - 1)\, p_2^{d_2 - 1}(p_2 - 1) \ldots p_t^{d_t - 1}(p_t - 1).$$

In particular, it is immediate from the formula above that $\phi(n)$ is an integer. △

We now build toward the proof of Theorem 10.

Lemma 12. *Let p be a prime number. Then*

$$\phi(p) = p - 1.$$

Proof. Since p is a prime number, we have

$$\{x \in \{1, \ldots, p\} \mid \gcd(x, p) = 1\} = \{1, 2, \ldots, p - 1\}.$$

The lemma now follows. □

Lemma 13. *Let p be a prime number. Then*

$$\phi(p^2) = p(p-1).$$

Proof. Since p is a prime number, we have

$$\{x \in \{1, \ldots, p^2\} \mid \gcd(x, p^2) > 1\} = \{p, 2p, \ldots, (p-1)p, p^2\}.$$

Hence it follows that

$$\begin{aligned}\phi(p^2) =& \left|[p^2]\right| - \left|\{x \in \{1, \ldots, p^2\} \mid \gcd(x, p) > 1\}\right| \\ =& p^2 - p \\ =& p(p-1).\end{aligned}$$

This proves the lemma. □

Lemma 14. *Let p be a prime number and let $d \geq 1$. Then*

$$\phi(p^d) = p^{d-1}(p-1).$$

Proof. Since p is a prime number, we have

$$\{x \in \{1, \ldots, p^d\} \mid \gcd(x, p^d) > 1\} = \{p, 2p, 3p, \ldots, (p^{d-1}-1)p, p^d\}.$$

Hence it follows that

$$\begin{aligned}\phi(p^d) =& \left|[p^d]\right| - \left|\{x \in \{1, \ldots, p^d\} \mid \gcd(x, p) > 1\}\right| \\ =& p^d - p^{d-1} \\ =& p^{d-1}(p-1).\end{aligned}$$

This proves the lemma. □

We are now ready to prove the main theorem.

Proof of Theorem 10. We write, for $i \in \{1, \ldots, t\}$,

$$A_i := \{x \in [n] \mid x \text{ is divisible by } p_i\}.$$

It follows that

$$A_i = \{p_i, 2p_i, 3p_i, \ldots, n = \frac{n}{p_i}p_i\},$$

and it follows by direct counting that

$$|A_i| = \frac{n}{p_i}.$$

By the same principle, we have, for any distinct $i_1, \ldots, i_j \in \{1, \ldots, t\}$,

$$\begin{aligned} A_{i_1} \cap A_{i_2} \cap \ldots \cap A_{i_j} =& \left\{ k\, p_{i_1} p_{i_2} \ldots p_{i_j} \;\mid\; 1 \leq k \leq \frac{n}{p_{i_1} p_{i_2} \ldots p_{i_j}} \right\}; \\ |A_{i_1} \cap A_{i_2} \cap \ldots \cap A_{i_j}| =& \frac{n}{p_{i_1} p_{i_2} \ldots p_{i_j}}. \end{aligned}$$

It then follows from the inclusion-exclusion principle that

$$\begin{aligned} |A_1 \cup A_2 \cup \ldots \cup A_t| =& \sum_{j=1}^{t} (-1)^{j-1} \sum_{i_1, i_2, \ldots, i_j} |A_{i_1} \cap A_{i_2} \cap \ldots \cap A_{i_j}| \\ =& \sum_{j=1}^{t} (-1)^{j-1} \sum_{i_1, i_2, \ldots, i_j} \frac{n}{p_{i_1} p_{i_2} \ldots p_{i_j}}. \end{aligned}$$

On the other hand, note that

$$A_1 \cup A_2 \cup \ldots \cup A_t = \{x \in [n] \;\mid\; \gcd(x, n) > 1\}.$$

Hence, it follows from all the arguments outlined above that

$$\begin{aligned} \phi(n) =& |\{x \in \{1, \ldots, n\} \;\mid\; \gcd(x, n) = 1\}| \\ =& |[n]| - |\{x \in \{1, \ldots, n\} \;\mid\; \gcd(x, n) > 1\}| \\ =& n \;-\; \sum_{j=1}^{t} (-1)^{j-1} \sum_{i_1, i_2, \ldots, i_j} \frac{n}{p_{i_1} p_{i_2} \ldots p_{i_j}} \\ =& n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \ldots \left(1 - \frac{1}{p_t}\right) \qquad \text{(why?)}. \end{aligned}$$

This completes our proof. □

Exercise 15. Read Textbook Section 2.4, and familiarize yourself with other examples (e.g., derangements) not presented in the lecture. △