CSS.102.1 Mathematical Foundations of Computer Science

Instructor: Raghuvansh Saxena

TIFR 2024, Aug-Dec

Scribe: Soham Chatterjee

sohamchatterjee999@gmail.com
Website: sohamch08.github.io

Contents

Chapter 1

Linear Algebra

Chapter 2

Combinatorics

2.1 Twelve Problems: n Balls in m Bins

Theorem 2.1.1

	≤ 1 balls/bin ($m \geq n$)	≥ 1 balls/bin ($m \leq n$)	Unrestricted
Identical Balls, Identical Bins	1	$P(n,m)$	$\sum_{i=1}^{m} P(n,i)$
Identical Balls, Distinguishable Bins	$\binom{m}{n}$	$\binom{m-1}{n-1}$	$\binom{n+m-1}{m-1}$
Distinguishable Balls, Identical Bins	1	$S_2(n,m)$	$\sum_{i=1}^{m} S_2(ni)$
Distinguishable Balls, Distinguishable Bins	$\binom{m}{n} n!$	$S_2(n,m)m!$	m^n

***Proof*:**

■

2.2 Stirling Numbers

2.2.1 Stirling Number of Second Kind

Definition 2.2.1: Stirling Number of The Second Kind

It is the number of ways to partition the set $[n]$ into m nonempty parts.

Clearly if we take the n balls to be the set $[n]$ the balls become distinguishable and each partition is bin and the order order of the partition doesn't matter the bins are identical. So the it becomes the number of ways n distinguishable balls divided into m identical bins.

Now we will see some recursion relations of the Stirling number of the first kind.

Lemma 2.2.1

$S_2(n,m) = S_2(n-1,m-1) + mS_2(n-1,m)$

Combinatorial Proof: We have the balls $[n]$. Then there are two cases. The bin containing ball '1' can has only 1 ball or it can have ≥ 2 balls.

For the first case the bin containing ball '1' has only one balls. So the rest of the $n-1$ balls are divided into the rest of the $m-1$ bins. The number of ways this is done is $S_2(n-1, m-1)$.

For the second case the bin containing ball '1' has at least 2 balls. In that case apart from the ball '1' all the other balls are filled into m identical bins where each bin has at least 1 ball. So we can think this scenario in other way that is first we fill bins with all the balls except '1' and then we choose where to put the ball '1'. So the number of ways the balls, $\{2, 3, \ldots, n\}$ i.e. $n-1$ distinguishable balls can be divided into m bins is $S_2(n-1, m)$. Now there are m choices for the ball '1' to be partnered up. Hence for this case there are $mS_2(n-1, m)$ many ways.

Therefore the total number of ways the n distinguishable balls can be divided into m bins so that each bin has at least 1 ball is $S_(n-1, m-1) + mS_2(n-1, m)$. Therefore we get $S_2(n, m) = S_2(n-1, m-1) + mS_2(n-1, m)$. ■

Theorem 2.2.2

$$S_2(n+1, m+1) = \sum_{i=m}^{n} \binom{n}{i} S_2(i, m)$$

Combinatorial Proof: On the *LHS* we are counting the number of ways to partition $[n+1]$ into $m+1$ parts.

For the *RHS* let's focus on the element $n+1$. So we drop the element from $[n+1]$ in the $(m+1)^{th}$ part. The $(m+1)^{th}$ block can have k elements from $[n]$ which are partnered by $n+1$ where $0 \leq k \leq n-m$. We have $k \leq n-m$ since all the other m parts have at least 1 element that leaves us $n-m$ elements to choose. So there are $\binom{n}{k}$ ways to choose the k elements. The remaining $n-k$ elements are divided into m parts which can be done in $S_2(n-k, m)$ many choices. So in total we have $\sum +k = 0^{n-m} S_2(n-k, m)$ ways to divide $[n+1]$ into $m+1$ parts. Therefore we have

$$S_2(n+1, m+1) = \sum_{i=0}^{n-m} \binom{n}{i} S_2(n-i, m) = \sum_{i=0}^{n-m} \binom{n}{n-i} S_2(n-i, m) = \sum_{i=m}^{n} \binom{n}{i} S_2(i, m)$$

■

Algebraic Proof: We will prove by Induction.

$$
\begin{aligned}
&S_2(n+1,m+1) = S_2(n,m) + (m+1)S_2(n,m+1)\\
&= \sum_{i=m-1}^{n-1}\binom{n-1}{i}S_2(i,m-1) + (m+1)\sum_{j=m}^{n-1}\binom{n-1}{j}S_2(j,m)\\
&= \sum_{i=m-1}^{n-1}\binom{n-1}{i}S_2(i,m-1) + m\sum_{j=m}^{n-1}\binom{n-1}{j}S_2(j,m) + \sum_{j=m}^{n-1}\binom{n-1}{j}S_2(j,m)\\
&= \sum_{i=m}^{n}\binom{n-1}{i-1}S_2(i-1,m-1) + m\sum_{j=m}^{n-1}\binom{n-1}{j}S_2(j,m) + \sum_{j=m}^{n-1}\binom{n-1}{j}S_2(j,m)\\
&= \sum_{i=m}^{n}\binom{n-1}{i-1}S_2(i-1,m-1) + m\sum_{j=m}^{n-1}\binom{n-1}{j}S_2(j,m) + \sum_{j=m}^{n-1}\left[\binom{n}{j} - \binom{n-1}{j-1}\right]S_2(j,m)\\
&= \sum_{i=m}^{n}\binom{n-1}{i-1}S_2(i-1,m-1) + m\sum_{j=m}^{n-1}\binom{n-1}{j}S_2(j,m) + \sum_{j=m}^{n-1}\binom{n}{j}S_2(j,m) - \sum_{j=m}^{n-1}\binom{n-1}{j-1}S_2(j,m)\\
&= \sum_{i=m}^{n}\binom{n-1}{i-1}S_2(i-1,m-1) + m\sum_{j=m}^{n-1}\binom{n-1}{j}S_2(j,m) + \sum_{j=m}^{n-1}\binom{n}{j}S_2(j,m) - \sum_{j=m}^{n-1}\binom{n-1}{j-1}\left[S_2(j-1,m-1) + mS_2(j-1,m)\right]\\
&= S_2(n-1,m-1) + \cancel{\sum_{i=m}^{n-1}\binom{n-1}{i-1}S_2(i-1,m-1)} + m\sum_{j=m}^{n-1}\binom{n-1}{j}S_2(j,m) + \sum_{j=m}^{n-1}\binom{n}{j}S_2(j,m) - \cancel{\sum_{j=m}^{n-1}\binom{n-1}{j-1}S_2(j-1,m-1)}\\
&\qquad\qquad - m\sum_{j=m}^{n-1}\binom{n-1}{j-1}S_2(j-1,m)\\
&= S_2(n-1,m-1) + m\sum_{j=m}^{n-1}\binom{n-1}{j}S_2(j,m) + \sum_{j=m}^{n-1}\binom{n}{j}S_2(j,m) - m\sum_{j=m+1}^{n-1}\binom{n-1}{j-1}S_2(j-1,m)\\
&= S_2(n-1,m-1) + m\sum_{j=m}^{n-1}\binom{n-1}{j}S_2(j,m) + \sum_{j=m}^{n-1}\binom{n}{j}S_2(j,m) - m\sum_{j=m}^{n-2}\binom{n-1}{j}S_2(j,m)\\
&= S_2(n-1,m-1) + mS_2(n-1,m)\sum_{j=m}^{n-1}\binom{n}{j}S_2(j,m)\\
&= S_2(n,m) + \sum_{j=m}^{n-1}\binom{n}{j}S_2(j,m) = \sum_{j=m}^{n}\binom{n}{j}S_2(j,m)
\end{aligned}
$$

■

2.2.2 Stirling Number of First Kind

Definition 2.2.2: Stirling Number of The First Kind

It is the number of permutations of $[n]$ with exactly m cycles. The *signed version* of Stirling number of the first kind is $(-1)^{n-m}S_1(n,m)$.

Now we will see some recursion relations of the Stirling number of the first kind.

Lemma 2.2.3

$S_1(n,m) = S_1(n-1,m-1) + (n-1)S_1(n-1,m)$

Combinatorial Proof: The *LHS* is the number of permutations of $[n]$ into m cycles by Definition.

In the *RHS* we can break the permutations into two different kinds: permutations where $1 \mapsto 1$ and permutations where $1 \not\mapsto 1$. For the permutations $1 \mapsto 1$ this alone forms a cycle. So the rest of the $n-1$ elements have to be permuted into $m-1$ cycles. Hence the number of such permutations is $S_1(n-1, m-1)$.

For permutations where $1 \not\mapsto 1$ take any permutation σ. We will consider the permutation σ' on the elements $\{2, \ldots, n\}$ where if $\sigma(k) = 1$ then $\sigma'(k) = \sigma \circ \sigma(k)$ and otherwise for all $k \in \{2, \ldots n\}$, $\sigma'(k) = \sigma(k)$. So σ' is now a permutation of $\{2, \ldots, n\}$. For all such permutations where $1 \not\mapsto 1$ we get a new unique permutation σ'. So the number of cycles in σ is same as σ'. Hence it is enough to for now count the number of permutations of $\{2, \ldots, n\}$ into m cycles is $S_1(n-1, m)$. Now for any such permutation π we can create new $n-1$ many permutations where $\forall\ i \in \{2, \ldots, n\}$ where $\pi_i(i) = 1$, $\pi_i(1) = \pi(i)$. In this way for each permutation we get $n-1$ new permutations. Hence the number of permutations where $1 \not\mapsto 1$ is $(n-1)S_2(n-1, m)$.

Hence total number of permutations of $[n]$ into m cycles is $S_1(n-1, m-1) + (n-1)S_1(n-1, m)$. Therefore we get the lemma. ■

Lemma 2.2.4

$$S_1(n, m)\binom{m}{k} = \sum_{j=k}^{n+k-m} \binom{n}{j} S_1(j, k) S_1(n-j, m-k)$$

Combinatorial Proof: In *LHS*, $S_1(n, m)$ is the number of permutations on $[n]$ with exactly m cycles. Hence $S_1(n, m)\binom{m}{k}$ is the number of ways to choose k cycles among the m cycles from permutations on $[n]$ with exactly m cycles. This is same as first constructing the chosen k cycles with some elements of $[n]$ and then with the rest of elements construct the rest $m-k$ cycles.

In *RHS* first we select j elements for the k cycles from n in $\binom{n}{j}$ ways. Then for the chosen j elements we create k cycles in $S_1(j, k)$ ways. So the number of ways we can create k cycles by j elements from $[n]$ is $\binom{n}{j}S_1(j, k)$ ways. Now for the rest of the elements we create the rest $m-k$ cycles which we can do in $S_1(n-j, m-k)$. Therefore the number of ways to construct k cycles and with the rest of the elements construct the remaining $m-k$ cycles with elements from $[n]$ is $\sum_{j=k}^{n+k-m} \binom{n}{j} S_1(j, k) S_1(n-j, m-k)$. Therefore we have

$$S_1(n, m)\binom{m}{k} = \sum_{j=k}^{n+k-m} \binom{n}{j} S_1(j, k) S_1(n-j, m-k)$$

■

Theorem 2.2.5

$$S_1(n+1, m+1) = \sum_{j=m}^{n} \binom{j}{m} S_1(n, j).$$

Combinatorial Proof: Consider the permutations on $[n]$ which has at least m cycles. So take a permutation σ which has j cycles where $m \leq j \leq n$. So for any cycle consider the smallest element in that cycle to be the leading element. So let the permutation is

$$\sigma = (a_1 \ldots a_{\ell_1})(a_{\ell_1+1} \ldots a_{\ell_2}) \ldots (a_{\ell_{j-1}+1} \ldots a_j)$$

Now among these j cycles we choose m cycles in $\binom{j}{m}$ ways. Let the first m cycles are chosen. Then we create the last $(m+1)^{th}$ cycle using the $n+1$ in the following way

$$\begin{pmatrix} n+1 & a_{\ell_m}+1 & \ldots & a_{\ell_{m+1}} & a_{\ell_{m+1}}+1 & \ldots & a_j \end{pmatrix}$$

Hence for each chosen set of m cycles we can join the rest of the cycles and $n+1$ to get the $(m+1)^{th}$ cycle. So now the number of permutations on $[n]$ with j cycles is $S_1(n, j)$. Then we can choose the m cycles among j cycles in $\binom{j}{m}$ ways. So

the number of permutations on $[n+1]$ with $m+1$ cycles is $\sum_{j=m}^{n} \binom{j}{m} S_1(n,j)$. Therefore we have

$$S_1(n+1,m+1) = \sum_{j=m}^{n} \binom{j}{m} S_1(n,j)$$

■

Algebraic Proof: First we will prove an identity of $S_1(n+1,m+1)$ then we will dive into the prove of this expression. We will show that $S_1(n+1,m+1) = \sum_{k=m}^{n} \frac{n!}{k!} S_1(k,m)$. We can use induction on $n+m+2$

$$\begin{aligned} S_1(n+1,m+1) &= S_1(n,m) + nS_1(n,m+1) \\ &= S_1(n,m) + n\sum_{k=m}^{n-1} \frac{(n-1)!}{k!} S_1(k,m) \\ &= \frac{n!}{n!} S_1(n,m) + \sum_{k=m}^{n-1} \frac{n!}{k!} S_1(k,m) \\ &= \sum_{k=m}^{n} \frac{n!}{k!} S_1(k,m) \end{aligned}$$

Now we will prove this inductively.

$$\begin{aligned} \sum_{j-m}^{n} \binom{j}{m} S_1(n,j) &= \sum_{j=m}^{n} \sum_{k=m}^{n+m-j} \binom{n}{k} S_1(k,m) S_1(n-k, j-m) && \text{[Using Lemma 2.2.4]} \\ &= \sum_{k=m}^{n} \binom{n}{k} S_1(k,m) \sum_{j=m}^{n+m-k} S_1(n-k, j-m) \\ &= \sum_{k=m}^{n} \binom{n}{k} S_1(k,m) \sum_{j=0}^{n-k} S_1(n-k, j) \\ &= \sum_{k=m}^{n} \binom{n}{k} S_1(k,m)(n-k)! && \left[\text{Since } \sum_{j=0}^{n-k} S_1(n-k,j) \text{ is number of permutations on } [n-k]\right] \\ &\sum_{k=m}^{n} \frac{n!}{k!} S_1(k,m) \\ &= S_1(n+1,m+1) \end{aligned}$$

■

Now we will show you a property of the signed Stirling number of the first kind.

Theorem 2.2.6

$$S_1(n,m) = \sum_{i=m}^{n} (-1)^{i-m} \binom{i}{m} S_1(n+1, i+1)$$

Proof:

$$\begin{aligned}
\sum_{i=m}^{n}(-1)^{i-m}\binom{i}{m}S_1(n+1,i+1) &= (-1)^{i-m}\binom{i}{m}\sum_{j=i}^{n}\binom{j}{i}S_1(n,j)\\
&= \sum_{j=m}^{n}S_1(n,j)\sum_{i=m}^{j}(-1)^{i-m}\binom{i}{m}\binom{j}{i}\\
&= \sum_{j=m}^{n}S_1(n,j)\sum_{i=m}^{j}(-1)^{i-m}\binom{j}{m}\binom{j-m}{i-m}\\
&= \sum_{j=m}^{n}\binom{j}{m}S_1(n,j)\sum_{i=0}^{j-m}(-1)^{i}\binom{j-m}{i}\\
&= \sum_{j=m+1}^{n}\binom{j}{m}S_1(n,j)\underbrace{\sum_{i=0}^{j-m}(-1)^{i}\binom{j-m}{i}}_{=0}+\binom{m}{m}S_1(n,m)(-1)^{0}\binom{0}{0}\\
&= S_1(n,m)
\end{aligned}$$

■

2.2.3 Connecting the Two Stirling Numbers

Theorem 2.2.7

Let S_1 and S_2 be $k\times k$ matrix where for any $n,m\in[k]$ with $n\geq m$ we have $(S_1)_{n,m}=(-1)^{n-m}S_1(n,m)$ and $(S_2)_{n,m}=S_2(n,m)$ and 0 otherwise then $S_1S_2=I$i.e.

$$\sum_{i=m}^{n}(-1)^{n-i}S_1(n,i)S_2(i,m)=\mathbb{1}(n=m)$$

Proof: We will induct on $n+m$. Then we have

$$\begin{aligned}
\sum_{i=m}^{n}(-1)^{n-i}S_1(n,i)S_2(i,m) &= \sum_{i=0}^{\infty}(-1)^{n-i}(S_1(n-1,i-1)+(n-1)S_1(n-1,i))S_2(i,m)\\
&= \sum_{i=0}^{\infty}(-1)^{n-i}S_1(n-1,i-1)S_2(i,m)+(n-1)\sum_{i=0}^{\infty}(-1)^{n-i}S_1(n-1,i)S_2(i,m)\\
&= \sum_{i=0}^{\infty}(-1)^{n-i}S_1(n-1,i-1)[S_2(i-1,m-1)+mS_2(i-1,m)]-(n-1)\mathbb{1}(n-1=m)\\
&= \sum_{i=0}^{\infty}(-1)^{n-i}S_1(n-1,i-1)S_2(i-1,m-1)+m\sum_{i=0}^{\infty}(-1)^{n-i}S_1(n-1,i-1)S_2(i-1,m)\\
&\qquad -(n-1)\mathbb{1}(n-1=m)\\
&= \mathbb{1}(n=m)+m\mathbb{1}(n-1=m)-(n-1)\mathbb{1}(n-1=m)\\
&= \mathbb{1}(n=m)+(m-n+1)\mathbb{1}(n-1=m)=\mathbb{1}(n=m)
\end{aligned}$$

■

2.3 Inclusion Exclusion Principle

Theorem 2.3.1 Inclusion-Exclusion Principle

Let $A_1, \ldots, A_n$ be finite sets. Then

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{J\subseteq[n], J\neq\emptyset} (-1)^{|J|+1} \left|\bigcap_{j\in J} A_j\right|$$

Proof: We will prove this using induction on n.

$$\begin{aligned}
\left|\bigcup_{i=1}^{n} A_i\right| &= \left|\bigcup_{i=1}^{n-1} A_i\right| + |A_n| - \left|\left(\bigcup_{i=1}^{n-1} A_i\right) \cap A_n\right| \\
&= \left|\bigcup_{i=1}^{n-1} A_i\right| + |A_n| - \left|\bigcup_{i=1}^{n-1} (A_i \cap A_n)\right| \\
&= \sum_{J\subseteq[n-1],\, J\neq\emptyset} (-1)^{|J|+1} \left|\bigcap_{j\in J} A_j\right| + |A_n| - \sum_{J\subseteq[n-1],\, J\neq\emptyset} (-1)^{|J|+1} \left|A_n \cap \left(\bigcap_{j\in J} A_j\right)\right| \\
&= \sum_{J\subseteq[n-1],\, J\neq\emptyset} (-1)^{|J|+1} \left|\bigcap_{j\in J} A_j\right| + |A_n| - \sum_{\substack{J\subseteq[n] \\ J\neq\{n\},\, n\in J}} (-1)^{|J|+1} \left|A_n \cap \left(\bigcap_{j\in J-\{n\}} A_j\right)\right| \\
&= \sum_{J\subseteq[n-1],\, J\neq\emptyset} (-1)^{|J|+1} \left|\bigcap_{j\in J} A_j\right| + \sum_{J=\{n\}} (-1)^{|J|+1} \left|\bigcap_{j\in J} A_j\right| + \sum_{\substack{J\subseteq[n] \\ J\neq\{n\},\, n\in J}} (-1)^{|J|+1} \left|\bigcap_{j\in J} A_j\right| \\
&= \sum_{\substack{J\subseteq[n] \\ J\neq\emptyset,\, n\notin J}} (-1)^{|J|+1} \left|\bigcap_{j\in J} A_j\right| + \sum_{J=\{n\}} (-1)^{|J|+1} \left|\bigcap_{j\in J} A_j\right| + \sum_{\substack{J\subseteq[n] \\ J\neq\{n\},\, n\in J}} (-1)^{|J|+1} \left|\bigcap_{j\in J} A_j\right| \\
&= \sum_{J\subseteq[n],\, J\neq\emptyset} (-1)^{|J|+1} \left|\bigcap_{j\in J} A_j\right|
\end{aligned}$$

Hence by mathematical induction we have the theorem. ∎

Corollary 2.1

If $\forall\, i \in [n], A_i = \{0\}$. Then

$$1 = \sum_{i=0}^{n} (-1)^{i+1} \binom{n}{i}$$

Proof: Using the Inclusion-Exclusion Principle we have

$$1 = \left|\bigcup_{i=1}^{n} A_i\right| = \sum_{J\subseteq[n], J\neq\emptyset} (-1)^{|J|+1} \left|\bigcap_{j\in J} A_j\right| = \sum_{J\subseteq[n], J\neq\emptyset} (-1)^{|J|+1} = \sum_{i=1}^{n} (-1)^{i+1} \binom{n}{i}$$

∎

Corollary 2.3.2

There are $\sum_{k=0}^{n} \binom{m}{k} (-1)^k (m-k)^n$ onto functions from $[n] \to [m]$

2.3.1 Strong Inclusion-Exclusion Principle

Theorem 2.3.3 Strong Inclusion-Exclusion

Let $f : 2^{[n]} \to \mathbb{R}$. Define $g : 2^{[n]} \to \mathbb{R}$ on a subset $T \subseteq [n]$ to be as follows

$$g(T) = \sum_{S \subseteq T} f(S) \quad T \subseteq [n]$$

Then

$$f(T) = \sum_{S \subseteq T} (-1)^{|T|-|S|} g(S)$$

2.3.2 Mobius Inversion

Now we derive a weak version of Mobius Inversion Theorem directly using Strong Inclusion Exclusion Principle. If f is a function from all product of primes to $\mathbb{R}$ and $g(n) = \sum_{d|n} f(d)$ then we have

$$f(n) = \sum_{d|n} (-1)^{\#\text{divisors of } (\frac{n}{d})} g(d) = \sum_{d|n} (-1)^{\#\text{divisors of } (d)} g\left(\frac{n}{d}\right)$$

We we define a new function $\mu : \mathbb{N} \to \{-1, 0, 1\}$ such that

$$\mu(n) = \begin{cases} 0 & \text{If } n \text{ is not a product of distinct primes} \\ (-1)^{\#\text{prime divisors of } n} & \text{If } n \text{ is a product of distinct primes} \end{cases}$$

So μ gets rid of the all the natural numbers n which is not a product of distinct primes. So now we have the Mobius Inversion Theorem

Theorem 2.3.4 Mobius Inversion

Let $f : \mathbb{N} \to \mathbb{R}$ and define $g : \mathbb{N} \to \mathbb{R}$ such that $g(n) = \sum_{d|n} f(d)$ then if the function $\mu : \mathbb{N} \to \{-1, 0, 1\}$ is defined as above then we have

$$f(n) = \sum_{d|n} \mu(d)\, g\left(\frac{n}{d}\right)$$

2.3.3 Euler Totient Function

Definition 2.3.1: Euler Totient Function

Euler Totient Function, $\phi : \mathbb{N} \to \mathbb{N}$, $\phi(n)$ is the number of integers $m \leq n$ such that $gcd(m, n) = 1$.

Lemma 2.3.5

For any $n \in \mathbb{N}$,

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

Proof: Consider the list of numbers $S = \left\{\frac{1}{n}, \frac{2}{n}, \ldots, \frac{n}{n}\right\}$. If we express every number in S as simplified form i.e. $\frac{p}{q}$ form where $gcd(p, q) = 1$. Then the denominators are all the divisors of n.

Then for any $k \in [n]$ we have

$$\frac{k}{n} = \frac{\frac{k}{gcd(k,n)}}{\frac{n}{gcd(k,n)}}$$

Denote $d_k := \frac{n}{gcd(k,n)}$ then d_k is a factor of n. And since $gcd\left(\frac{k}{gcd(k,n)}, \frac{n}{gcd(k,n)}\right) = 1$ we have $\frac{k}{gcd(k,n)} \in \mathbb{Z}^*_{d_k}$. Let $k \in \mathbb{Z}^*_d$ then suppose l is such that $d \times l = n$ then the fraction $\frac{k}{d} = \frac{k \times l}{n} \in S$ and its simplified form is in fact $\frac{k}{d}$.

Hence for any $d \mid n$, the number of fractions with denominator d is $\varphi(d)$, since for all such fractions the numerators are the elements of $\mathbb{Z}^*_d$. Therefore we have $\sum_{d|n} \varphi(d) = n$.

■

Alternate Proof :

$$n = \sum_{i=1}^{n} 1 = \sum_{d|n} \sum_{\substack{i \le n, \\ gcd(i,n)=d}} 1 = \sum_{d|n} \sum_{\substack{d|i,\ i \le n, \\ gcd\left(\frac{i}{d}, \frac{n}{d}\right)=1}} 1 = \sum_{d|n} \sum_{\substack{j \le \frac{n}{d}, \\ gcd\left(\frac{n}{d}, j\right)=1}} 1 = \sum_{d|n} \phi\left(\frac{n}{d}\right) = \sum_{d|n} \phi(d)$$

■

Since $n = \sum_{d|n} \phi(d)$ this is already in the form $g(n) = \sum_{d|n} f(d)$. Hence take $g\mathbb{N} \to \mathbb{R}$ to be identity function and take f to be the Euler Totient function. Then by Mobius Inversion we have

$$\phi(n) = \sum_{d|n} \mu(d)\ g\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) \frac{n}{d} \implies \frac{\phi(n)}{n} = \sum_{d|n} \frac{\mu(d)}{d}$$

2.4 Generating Function

Question 2.4.1

What is the number of non-negative solutions of $x_1 + x_2 + x_3 + x_4 = 5$ for which $x_1 + x_2$ is even?

Solution: $x_1 + x_2$ is even. So it can be 0 or 2 or 4. In that case $x_3 + x_4$ can be 5 or 3 or 1 respectively. For any k, $x + y = k$ in $k + 1$ ways where x, y are non-negative. Then the total number of solutions is $1 \times 6 + 3 \times 4 + 5 \times 2 = 28$.

Another way of solving this is consider the power series

$$A(x) = 1 + 3x^2 + 5x^4 + \cdots = \sum_{i=0}^{\infty} a_i x^i \qquad B(x) = 1 + 2x + 3x^2 + \cdots = \sum_{i=0}^{\infty} b_i x^i$$

Where

$$a_i = \begin{cases} \#\text{solutions to } x_1 + x_2 = i & \text{when } i \text{ is even} \\ 0 & \text{when } i \text{ is odd} \end{cases}, \qquad b_i = \#\text{solutions to } x_1 + x_2 = i$$

Then for $A \cdot B = C = \sum_{i=0}^{\infty} c_i x^i$, $c_i = \#$solutions to $x_1 + x_2 + x_3 + x_4 = i$ where $x_1 + x_2$ is even. ■

Question 2.4.2

What is the number of subsets of $[n]$ of size k?

Solution: Suppose there are n variables $x_1, \ldots, x_n$. For each subset $S \subseteq [n]$ where $|S| = k$, we assign $x_i = 1$ if $i \in S$ and otherwise assign $x_i = 0$. Hence the number of subsets of $[n]$ of size k is same as the number of solutions of $\sum_{i=1}^{n} x_i = k$.

Consider the following generating function

$$(1 + x)^n = \sum_{i=0}^{n} \binom{n}{i} x^i = \sum_{i=0} a_i x^i$$

Here for each i, a_i = #solutions for $\sum_{i=1}^{n} x_i = k$. Therefore number of subsets of $[n]$ of size k is $\binom{n}{k}$. ■

Question 2.4.3

How many partitions of n are there?

Solution: We can find a nice generating function for number of partitions of n. We have

$$\sum_{n\geq 0} P(n)x^n = \prod_{r=1}^{\infty}\sum_{i=0}^{\infty} x^{i\cdot r}$$

For each $r \geq 1$ for any $i \geq 0$ think of $x^{i\cdot r}$ as the number of r's in a partition of n is i. So if P is a partition of n then suppose n_i be the number of i's in P. Hence we have $\sum_{i=1}^{n} i \cdot n_i = n$ Then the corresponding term x^n is generated by the $\prod_{i=1}^{n} x^{i\cdot n_i}$ where $x^{i\cdot n_i}$ comes form the $\sum_{j=0}^{\infty} x^{j\cdot n_i}$. Hence

$$\sum_{n\geq 0} P(n)x^n = \prod_{r=1}^{\infty}\sum_{i=0}^{\infty} x^{i\cdot r} = \prod_{r=1}^{\infty}\frac{1}{1-x^r}$$

■

2.4.1 Well Formed Parenthesis and Catalan Number

Definition 2.4.1: Well Formed Parenthesis

A sequence of parenthesis is well formed if #(= #) and any prefix has at least as many (as).

Now consider for any $i \geq 0$,

a_i = #Well formed parenthesis of length $2i$

b_i = #Well formed parenthesis such that the fist matches the last and length $2i$

Definition 2.4.2: Catalan Number

The n^{th} Catalan Number is the number of well formed parenthesis of length $2n$, i.e. a_i.

Observation 1. $b_n = a_{n-1}$.

Since for b_n the first matches with the last. So the internal $2(n-1)$ parenthesis forms a well formed parenthesis and that can be in a_{n-1} ways.

Observation 2. $a_n = \sum_{i=1}^{n} b_i a_{n-i} = \sum_{i=1}^{n} a_{i-1}a_{n-i}$.

Since there are $2n$ parenthesis the first (is matched with a) at any of the n)'s since inside them all the parenthesis are forms well formed parenthesis. Hence we consider each case where the first (matched with i^{th}) differently. If the first (is matched with i^{th}) then inside them there is $2(i-1)$ length well formed parenthesis and we can think of this case as b_i and the rest $2n-2i$ many parenthesis forms all possible well formed parenthesis which can be done in a_{n-i} ways. So the number of ways the first (is matched with i^{th}) is $b_i a_{n-i}$ ways.

Now define the power series $A(x) = \sum_{i\geq 0} a_i x^i$. Then we have

$$A^2(x) = \sum_{i\geq 0}\left(\sum_{j=0}^{i} a_j a_{i-j}\right)x^i$$

This is almost in the form $\sum_{i=1}^{n} a_{i-1}a_{n-i}$ for coefficient of x^i. So we do the following

$$xA^2(x) = x\sum_{i\geq 0}\left(\sum_{j=0}^{i} a_j a_{i-j}\right)x^i = \sum_{i\geq 0}\left(\sum_{j=0}^{i} a_j a_{i-j}\right)x^{i+1} = \sum_{i\geq 0}\left(\sum_{j=1}^{i+1} a_{j-1}a_{i+1-j}\right)x^{i+1} = \sum_{i\geq 0} a_{i+1}x^{i+1} = A(x) - 1$$

Hence we get a quadratic equation for $A(x)$ which is $A^2(x)x - A(x) + 1 = 0$. Therefore

$$A(x) = \frac{1 \pm \sqrt{1-4x}}{2x}$$

Now

$$\sqrt{1-4x} = 1 + \frac{1}{2}(-4x) + \frac{\frac{1}{2}\times\left(\frac{1}{2}-1\right)}{2!}(-4x)^2 + \frac{\frac{1}{2}\left(\frac{1}{2}-1\right)\left(\frac{1}{2}-2\right)}{3!}(-4x)^3 + \cdots = \sum_{i\geq 0}\binom{\frac{1}{2}}{i}(-4x)^i$$

Therefore

$$\frac{1+\sqrt{1-4x}}{2x} = \frac{1}{x} + \sum_{i\geq 1} 2\binom{\frac{1}{2}}{i}(-1)^i(4x)^{i-1}$$

Now as $x \longrightarrow 0$ we have $\frac{1+\sqrt{1-4x}}{2x}$ does not exists but we have

$$\frac{1-\sqrt{1-4x}}{2x} = \sum_{i\geq 1} 2\binom{\frac{1}{2}}{i}(-4x)^{i-1} = \sum_{i\geq 0} 2\binom{\frac{1}{2}}{i+1}(-4x)^i \quad \text{and} \quad \lim_{x\to 0}\sum_{i\geq 0} 2\binom{\frac{1}{2}}{i+1}(-4x)^i = 2\binom{\frac{1}{2}}{0+1}(-4)^0 = 2\frac{1}{2} = 1 = a_0$$

Therefore we have

$$A(x) = \frac{1-\sqrt{1-4x}}{2x} = \sum_{i\geq 0} 2\binom{\frac{1}{2}}{i+1}(-4x)^i$$

Now

$$a_i = 2\binom{\frac{1}{2}}{i+1} = 2\times(-4)^i\frac{\prod_{j=0}^{i}\left(\frac{1}{2}-j\right)}{(i+1)!} = \frac{2\times(-4)^i}{2^{i+1}}\frac{\prod_{j=0}^{i}(1-2j)}{(i+1)!} = 2^i\frac{\prod_{j=0}^{i}(2j-1)}{(i+1)!} = \frac{1}{i+1}\binom{2i}{i}$$

Hence the n^{th} Catalan Number is $\frac{1}{n+1}\binom{2n}{n}$.

2.4.2 Generating Function of Stirling Number of First Kind

Take the generating function for $S_1(m,m)$ to be $\sum_{m=0}^{n} S_1(n,m)x^m$. Then we have the following theorem

Theorem 2.4.1

$$\sum_{m=0}^{n} S_1(n,m)x^m = \prod_{m=0}^{n-1}(x+m)$$

***Proof*:** We will prove this by proving that the coefficients of *RHS* follows the recursion relation Lemma 2.2.3 and also the initial conditions are same as Stirling Number of the First Kind. For $n = 1$, we have

$$S_1(1,0) + S_1(1,1)x = 0 + x$$

Hence it is satisfied. For any n, $S(n,n) = 1$ and the coefficient of x^n in $\prod_{m=0}^{n-1}(x+m)$ is also 1. Therefore the initial conditions are satisfied. Now we will show that Lemma 2.2.3 is followed. We will use induction on n. The base case is

already followed.

$$\begin{aligned}
\prod_{m=1}^{n}(x+m-1) &= x\prod_{m=1}^{n-1}(x+j-1) + (n-1)\prod_{j=1}^{n-1}(x+j-1) \\
&= x\sum_{m=0}^{n-1} S_1(n-1,m)x^m + (n-1)\sum_{m=0}^{n-1} S_1(n-1,m)x^m && \text{[Induction Hypothesis]} \\
&= \sum_{m=1}^{n} S_1(n-1,m-1)x^m + (n-1)\sum_{m=0}^{n} S_1(n-1,m)x^m \\
&= \sum_{m=0}^{n} S_1(n-1,m-1)x^m + (n-1)\sum_{m=0}^{n} S_1(n-1,m)x^m \\
&= \sum_{m=0}^{n} \left(S_1(n-1,m-1) + (n-1)S_1(n-1,m)\right)x^m = \sum_{m=0}^{n} S_1(n,m)x^m
\end{aligned}$$

■

For signed Stirling number of the first kind we have the following generating function.

Theorem 2.4.2

$$\sum_{m=0}^{n}(-1)^{n-m}S_1(n,m)x^m = \prod_{m=0}^{n-1}(x-m)$$

2.4.3 Exponential Generating Function

Previously for any sequence $\{a_n\}_{n\geq 0}$ we constructed the generating function for this sequence by taking

$$A(x) = \sum_{n=0}^{\infty} a_n x^n$$

But in this case we will construct the exponential generating function like this

$$\hat{A}(x) = \sum_{n=0}^{\infty} a_n \frac{x^n}{n!}$$

Lemma 2.4.3

$$\sum_{n=0}^{\infty} S_2(n,m)\frac{x^n}{n!} = \frac{1}{n!}(e^x-1)^m$$

Proof: We will prove using induction on m.

$$\begin{aligned}
\frac{1}{m!}(e^x-1)^m &= \frac{e^x-1}{m}\times\frac{1}{(m-1)!}(e^x-1)^{m-1}\\
&= \frac{1}{m}\left(\frac{e^x}{(m-1)!}(e^x-1)^{m-1}-\frac{1}{(m-1)!}(e^x-1)^{m-1}\right)\\
&= \frac{1}{m}\left(\sum_{n=0}^{\infty}S_2(n+1,m)\frac{x^n}{n!}-\sum_{n=0}^{\infty}S_2(n,m-1)\frac{x^n}{n!}\right) \qquad \left[\frac{e^x(e^x-1)^{m-1}}{(m-1)!}=\frac{d}{dx}\frac{(e^x-1)^m}{m!}=\sum_{n=0}^{\infty}S_2(n+1,m)\frac{x^n}{n!}\right]\\
&= \frac{1}{m}\sum_{n=0}^{\infty}(S_2(n+1,m)-S_2(n,m-1))\frac{x^n}{n!}\\
&= \frac{1}{m}\sum_{n=0}^{\infty}mS_2(n,m)\frac{x^n}{n!}\\
&= \sum_{n=0}^{\infty}S_2(n,m)\frac{x^n}{n!}
\end{aligned}$$

Hence by mathematical induction we have the lemma. ■

Definition 2.4.3: Derangement

A derangement is a permutation π such that $\pi(i)\neq i$ for all i

Let d_n denote the number of derangements on $[n]$.

Lemma 2.4.4

$d_n=(n-1)(d_{n-1}+d_{n-2})$

Proof: content... ■

Now define the exponential generating function for derangements to be $D(x)=\sum\limits_{n=0}^{\infty}\frac{d_n}{n!}x^n$. Hence we have

$$D'(s)=\sum_{n=0}^{\infty}\frac{d_{n+1}}{n!}x^n=\sum_{n=0}^{\infty}\frac{d_n+d_{n-1}}{(n-1)!}x^n=x\left(\sum_{n>0}\frac{d_n}{(n-1)!}x^n+\sum_{n>0}\frac{d_{n-1}}{(n-1)!}x^{n-1}\right)=x(D'(x)+D(x))$$

Therefore we get the differential equation $D'(x)=x(D'(x+D(x))$. Hence we have

$$\frac{D'(x)}{D(x)}=\frac{x}{1-x}\implies \log D(x)=-x-\log(1-x)+C$$

where $C\in\mathbb{R}$. Now for $x=0$, $D(0)=0$. Hence $C=0$. Therefore

$$\log D(x)=-x-\log(1-x)\implies D(x)=\frac{e^{-x}}{1-x}=\left(\sum_{n=0}^{\infty}\frac{(-1)^n}{n!}x^n\right)\left(\sum_{n=0}^{\infty}x^n\right)=\sum_{n=0}^{\infty}\left(\sum_{k=0}^{n}\frac{(-1)^k}{k!}\right)x^n=\sum_{n=0}^{\infty}\frac{x^n}{n!}n!\left(\sum_{k=0}^{n}\frac{(-1)^k}{k!}\right)$$

Therefore we have $d_n=n!\left(\sum\limits_{k=0}^{n}\frac{(-1)^k}{k!}\right)$.

2.5 Partitions

2.6 Partially Ordered Sets (Poset)

Definition 2.6.1: Partially Ordered Sets (Posets)

Let U be a set. A relation $\leq$ on U is a partial order if we have

(i) **Reflexive:** $x \leq x$ for all $x \in U$

(ii) **Transitive:** $x \leq y, y \leq z \implies x \leq z, \forall\, x, y, z \in U$

(iii) **Anti-symmetric** $x \leq y, y \leq x \implies x = y$

Then the pair $(U, \leq)$ is called a partially ordered set

We will now define some terms which will be used a lot in this section:

1. *Total order* of a set U is partial order such that for all $x, y \in U$, either $x \leq y$ or $y \leq x$ (or both)
2. If $x \leq y$ and $x \neq y$ then $x < y$
3. $x \leq y \equiv y \geq x$
4. For any $x, y \in U$ if neither $x \leq y$ nor $y \leq x$ then x and y are *incomparable* and denoted by $x \| y$.
5. A *chain* is a totally ordered subset of U.
6. The *Height* of U, $h(U)$ is the length of the longest chain in U.
7. An *anti-chain* is a subset of incomparable elements
8. The *Width* of U, $w(U)$ is the size of the longest anti-chain in U.
9. The *minimal* elements of U is defined as $\min(U) = \{x \in U \mid \forall\, y \in U,\ x \leq y \text{ or } y \| x\}$
10. The *maximal* elements of U is defined as $\max(U) = \{x \in U \mid \forall\, y \in U,\ y \leq x \text{ or } y \| x\}$

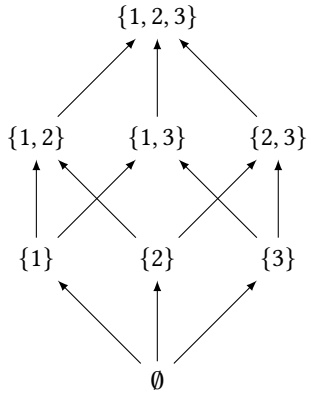

Figure 2.1: Hasse Diagram of $\left(2^{[3]}, \subseteq\right)$

Example 2.6.1

(a) $U = [n]$ and $\leq$ is the standard ordering.

(b) $U = 2^{[n]}$ and $\leq$ is inclusion.

Assumption. *We will assume U is always finite*

Lemma 2.6.1

$\min(U)$ and $\max(U)$ are anti-chains, non-empty (if U is non-empty) (possibly intersecting).

Proof: We will prove for $\min(U)$ and the same type of proof will also work for $\max(U)$. Since U is nonempty and finite $\exists\, x \in U$. Now if $x \notin \min(U)$ then $\exists\, y_1 \in U \setminus \{x\}$ such that $y_1 < x$. If $y_1 \notin U$ then $\exists\, y_2 \in U \setminus \{x, y_1\}$ such that $y_2 < y_1$. Continuing like this if $y_{|U|-2} \notin U$, $\exists\, y_{|U|-1} \in U \setminus \{x, y_i : i \in [|U| - 2]\}$. Then $y_{|U|-1}$ is the only element left in $U \setminus \{x, y_i : i \in [|U| - 2]\}$. Hence $y_{|U|-1}$ is the minimal element of U. So $y_{|U|-1} \in \min(U)$. Therefore $\min(U)$ is nonempty.

Suppose $\min(U)$ not a anti-chain then $\exists,\ x, y \in U$ and $x \neq y$ such that $x \not\| y$. Hence either $x < y$ or $y < x$. WLOG suppose $x < y$. Then y is not a minimal element since $y \not\leq x$. Hence contradiction. $\min(U)$ forms an anti-chain.

Let $U = [1]$ with standard ordering $\leq$. Then $\min(U) = \max(U) = [1]$. Hence $\min(U)$ and $\max(U)$ may intersect. ■

Observation. $\min(U)$ *and* $\max(U)$ *are singleton sets if it is a total order.*

Lemma 2.6.2

Any maximal chain has an element of $\min(U)$ and an element of $\max(U)$. These elements are same if length of the chain is 1

Theorem 2.6.3 Antichain Partitioning

Every poset $(U, \leq)$ can be partitioned into $h(U)$ many antichains (not less).

Proof: We will first show that U can not be partitioned into fewer than $h(U)$ many antichains. No antichain contains two elements from a chain, since elements of chains are pairwise com- parable and elements of antichains are pairwise incomparable. So each element of the longest chain in U are in distinct antichains. Since the longest chain in U has length $h(U)$, at least $h(U)$ many antichains are needed.

Now for all $x \in U$ define the *depth* of x, $d(x)$ in U to be the length of the longest chain that ends at x i.e.

$$d(x) = \max_{\text{chain } C,\ \max(C)=x} |C|$$

Hence by definition we have $d(x) \leq h(U)$ for all $x \in U$. Consider

$$A_i = \{x \in U : d(x) = i\} \quad \forall\, i \in [h(U)]$$

We will show $\forall\, i \in [h(U)]$, A_i is an antichain. The proof of A_i is antichain is similar to Lemma 2.6.1. ■

Theorem 2.6.4 Dilworth's Theorem

Every poset $(U, \leq)$ can be partitioned into $w(U)$ many chains (not less).

Proof: Clearly at lest $w(U)$ many chains are needed since any two elements of the longest antichain of U are incomparable and therefore they are in distinct chains and henceforth all the elements of the longest antichain are in distinct chains.

We will show there is such a partition we will induct on $|U|$. Consider the maximal antichain of U, $P = \{x_1, \ldots, x_{w(U)}\}$. Now we partition U into two posets of smaller size.

$$U_1 \coloneqq \{x \in U \mid \exists\, y \in P,\ y \leq x\} \qquad U_2 \coloneqq \{x \in U \mid \exists\, y \in P,\ x \leq y\}$$

with the same relations as for U. Now notice $U_1 \cap U_2 = P$. Therefore $w(U_1) = w(U_2) = w(U)$. Assuming $P \subsetneq U_1$ and $P \subsetneq U_2$ by inductive hypothesis we can partition U_1 and U_2 into chains $C_1^1, \ldots, C_{w(U_1)}^1$ and $C_1^1, \ldots, C_{w(U_2)}^2$ respectively where $C_i^1 \cap C_i^2 = \{x_i\}$ for all $i \in w(U)$. Hence we can take $C_i = C_1 \cup C_2$ and C_i is a chain for all $i \in w(U)$. So we get $w(U)$ many partitions of U.

Now we have $U_1 = U \iff U = \min(U)$ and $U_2 = U \iff U = \min(U)$. So we only have to consider the case where there is no largest antichain except for $\min(U)$, $\max(P)$ or both. In that case let C be any maximal chain. Then C has exactly one element of $\min(U)$ and exactly one element of $\max(U)$ by Lemma 2.6.2. So $w(U \setminus C) = w(U) - 1$ since only one element from each largest antichain is removed. Now by induction $U \setminus C$ can be partitioned into $w(U) - 1$ many chains. Hence U can be partitioned into $w(U)$ many chains. Hence we are done. ■

2.6.1 Subposets and Dimensions