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 $\max(U) = \{x \in U \mid \forall\, y \in U,\ y \leq x \text{ or } y \| x\}$

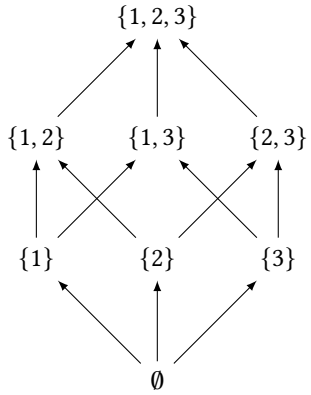


Figure 2.1: Hasse Diagram of $\left(2^{[3]}, \subseteq\right)$

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 $x \nparallel y$. Hence either $x < y$ or $y < x$. WLOG suppose $x < y$. Then y is not a minimal element since $y \notin x$. 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 $C^1_1, \ldots, C^1_{w(U_1)}$ and $C^1_1, \ldots, C^2_{w(U_2)}$ respectively where $C^1_i \cap C^2_i = \{x_i\}$ 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

Definition 2.6.2: Subposet

$P = (U, \leq_P)$ is a subposet of $Q = (V, \leq_Q)$ if there is an injective function $f : U \to V$ such that $\forall\, x_1, x_2 \in U$, $x_1 \leq_P x_2 \iff f(x_1) \leq_Q f(x_2)$. The function f is called an *embedding*.

We say $Q = (U, \leq_Q)$ is an *extension* of $P = (U, \leq_P)$ iff $\forall\, x_1, x_2 \in U, x_1 \leq_P x_2 \iff x_1 \leq_Q x_2$. Q is a *linear extension* of P if $\leq_Q$ is a total order.

Lemma 2.6.5

Let $P_1 = (U, \leq_1), P_2 = (U, \leq_2)$ be two posets on the same ground set U. Then we define $P = P_1 \cap P_2 := (U, \leq)$ with the relation $\leq := \leq_1 \cap \leq_2$, meaning

$$x \leq y \iff x \leq_1 y \text{ and } x \leq_2 y$$

Then P is a poset and P_1 and P_2 are extensions of P.

Proof: The $\leq$ relation is an partial order relation. Since all pairs that are related via $\leq$ are related via $\leq_1$ and $\leq_2$, $\leq_1, \leq_2$ are extensions of $\leq$. ∎

Definition 2.6.3: d−ary Dominance Poset

For $d \in \mathbb{N}$ the set $\mathbb{R}^d$ becomes a d−ary dominance poset via the *dominance order*, $\leq_{\text{dom}}$ where $x = (x_1, \ldots, x_d), y = (y_1, \ldots, y_d) \in \mathbb{R}^d$ we have

$$x \leq_{\text{dom}} y \iff \forall\, i \in [d],\ x_i \leq y_i$$

Then we have the following definition for d−dimensional posets $(U, \leq)$.

Definition 2.6.4: Dimension of Poset

The dimension of the poset $(U, \leq)$ is the smallest $d \in \mathbb{N}$ such that $(U, \leq)$ is a subposet of $(\mathbb{R}^d, \leq_{\text{dom}})$.

Theorem 2.6.6

Let $(U, \leq)$ be a poset and $d > 0$, $d \in \mathbb{N}$. We have that U is d−dimensional if and only if d is the smallest number such that U can be written as intersection of d−linear extensions of U.

Proof: " $\Leftarrow$ " : Let there are d-linear extensions of $(U, \leq)$, which are $(U, \leq_1), \ldots (U, \leq_d)$ such that

$$x \leq y \iff x \leq_i y\ \forall\, i \in [d]$$

We will construct an embedding $f : U \to \mathbb{R}^d$. For any $x \in U$ we take $f(u) = (r_1, \ldots, r_d)$ where $r_i = |\{y \in U : y \leq_i x\}|$. Now we will show f is indeed an embedding. Let $u, v \in U$. Then suppose $f(u) = (r_1^u, \ldots, r_d^u)$ and $f(v) = (r_1^v, \ldots, r_d^v)$. Now

$$\begin{aligned}
u \leq v &\iff u \leq_i v\ \forall\, i \in [d] \\
&\iff \Big(x \in \{y \in U : y \leq_i u\} \implies x \leq_i u \leq_i v \implies x \in \{y \in U : y \leq_i v\}\Big)\ \forall\, i \in [d] \\
&\iff r_i^u \leq r_i^v\ \forall\, i \in [d] \\
&\iff f(u) \leq_{\text{dom}} f(v)
\end{aligned}$$

Hence f is indeed a embedding.

" $\Rightarrow$ " : $(U, \leq)$ is d-dimensional. There exists an embedding $f : U \to \mathbb{R}$. Now $\forall\, x, y \in U$ we have

$$x \leq y \iff f(x) \leq_{\text{dom}} f(y)$$

Now we can assume no two points of U share a coordinate or else we can force this rule changing the values a little. Now we can think $f = (f_1, \ldots, f_n)$ where $f_i : U \to \mathbb{R}$ for all $i \in [d]$ such that $x \leq y \iff f_i(x) \leq f_i(y)$ for all $i \in [d]$. Then

we have the linear extensions of $(U, \leq)$, $(U, \leq_i)$ where $\forall\, x, y \in U, x \leq_i y \iff f_i(x) \leq f_i(y)$. ■

Lemma 2.6.7

The dimension of $(2^{[d]}, \subseteq)$ is d

Proof: The dimension is at most d because $\{0,1\}^d$ can be mapped to $\mathbb{R}^d$. Now we will show that lower than d embedding is not possible.

Suppose for the sake of contradiction that $(\{0,1\}^d, \leq)$ can be written as the intersection of $d-1$ linear extensions. Let $(\{0,1\}^d, \leq_i)$ for all $i \in [d-1]$ be the linear extensions of $(\{0,1\}^d, \leq)$. Now consider the pairs of sets $(\{i\}, \overline{\{i\}})$ for all $i \in [d]$. Now for all $i \in [d]$, we have $\{i\} \not\leq \overline{\{i\}}$. Hence $\exists\, j \in [d-1]$ such that $\{i\} \not\leq_j \overline{\{i\}} \implies \overline{\{i\}} <_j \{i\}$. Therefore $\exists\, i_1, i_2 \in [d]$ where $i_1 \neq i_2$ such that $\exists\, j \in [d-1]$ such that $\overline{\{i_1\}} <_j \{i_1\}$ and $\overline{\{i_2\}} <_j \{i_2\}$ by Pigeon Hole Principle. Since $i_1 \neq i_2$ we have $\{i_1\} \leq \overline{\{i_2\}} \implies \{i_1\} \leq_j \overline{\{i_2\}}$ and $\{i_2\} \leq \overline{\{i_1\}} \implies \{i_2\} \leq_j \overline{\{i_1\}}$. Therefore we have

$$\overline{\{i_1\}} <_j \{i_1\} \leq_j \overline{\{i_2\}} <_j \{i_2\} \leq_j \overline{\{i_1\}}$$

Hence contradiction ↯ ■

Theorem 2.6.8

For all $(U, \leq)$, $\dim U \leq w(U)$.

Proof: Firstly U can be decomposed into $w(U)$ many chains by Dilworth's Theorem. Let the chains are $C_1, \ldots, C_{w(U)}$. Let

$$C_i : \qquad x_{i,1} \leq x_{i,2} \leq \cdots \leq x_{i,k_i}$$

For all $x \in U$ define $N_i(x)$ to be the largest $j \in [k_i]$ such that $x_{i,j} \leq x$. With $j = 0$ if no such element exists. Now also define

$$S_{ij} = \{s \in U \setminus C_i : N_i(x) = j\}$$

For each $S_{i,j}$ take a topological sort.

Now we will create a linear extension of $(U, \leq)$, $L_i = (U, \leq_i)$ from C_i. Now for any $i \in [w(U)]$ for each $j \in [k_i] \cup \{0\}$ we take the ordering wrt $\leq_i$ inside $S_{i,j}$ to be a topological sort ordering of the elements. Now since for all $j \in [k_i] \cup \{0\}$, $N_i(x_{i,j}) = j - 1$ we have

$$\forall\, x \in S_{i,j},\ x_{i,j-1} \leq x \leq_i x_{i,j}$$

Therefore we have the following order of U with respect to $\leq_i$

$$S_{i,0} \quad x_{i,0} \quad S_{i,1} \quad x_{i,1} \quad \cdots \quad x_{i,k_i} \quad S_{i,k_i}$$

Therefore L_i is a linear extension of $(U, \leq)$.

Suppose $x, y \in U$ and $x \leq y$. Now if $x, y \in C_i$ for some $i \in [w(U)]$ then $x \leq_i y$. Then $x, y \in C_k$ for some $k \in [w(U)]$. then we already have $x \leq_i$. Otherwise let $x, y \in U$ and $x \leq y$. If for $i \in [w(U)] \setminus \{k\}$, $x, y \in S_{i,j}$ for some $j \in [k_i] \cup \{0\}$. Then since elements of $S_{i,j}$ are in topological sort order x is before y in $S_{i,j}$. Hence $x \leq_i y$. Otherwise for $i \in [w(U)] \setminus \{k\}$, $x \in S_{i,j}$ and $y \in S_{i,j'}$ for some $j, j' \in [k_i] \cup \{0\}$. In that case $N_i(x) < N_i(y)$ since $x_{i,N_i(x)} \leq x \leq y$. Hence $j < j'$. Therefore $x \leq_i y$. Hence for all $i \in [w(U)]$, $x \leq_i y$.

Suppose $x, y \in U$ and $\forall\, i \in [w(U)]$, $x \leq_i y$. If $x, y \in C_i$ for some $i \in [w(U)]$ then we already have $x \leq y$. Suppose $x \in C_i$ and $y \in C_j$ for some $i, j \in [w(U)]$ and $i \neq j$. We have $x \leq_i y$ and $x \leq_j y$. But since x, y are in different chains we have $x \| y$. In that case in C_i, $y \in S_{i,0}$ and hence $y <_i x$. But that is not possible. Hence contradiction ↯ We have x, y in the same chain and henceforth $x \leq y$.

Therefore L_i for all $i \in [w(U)]$ are linear extensions of $(U, \leq)$ such that $(U, \leq) = \bigcap_{i=1}^{w(U)} L_i$. Hence $\dim U \leq w(U)$. ■

Now we will show an use of this theorem to prove a very well know criterion for matching in a bipartite graph.

Theorem 2.6.9 Hall's Theorem
Let $G = (L, R, E)$ be a bipartite graph. G has a matching of size $|L|$ if and only if $\forall\, S \subseteq L$, $|S| \leq |N(S)|$.

Proof: We have $V = L \sqcup R$. be the set of vertices. Now define $u \to v \iff u \in L,\ v \in R$ and $(u, v) \in E$.

$$\begin{aligned}
G \text{ has a matching of size } |L| &\iff V \text{ can be partitioned into } |R| \text{ chains, } w(U) \leq |R| \\
&\iff w(U) = |R| \\
&\iff \text{Any subset of size } > |R| \text{ is not an antichain} \\
&\iff \Big(\forall\, A_L \subseteq L,\ A_R \subseteq R,\ |A_L| + |A_R| > |R| \implies \exists\, u \in A_L,\ v \in A_R,\ u \to v\Big) \\
&\iff \Big(\forall\, A_L \subseteq L,\ A_R \subseteq R,\ |A_L| + |A_R| > |R| \implies N(A_L) \cap A_R \neq \emptyset\Big) \\
&\iff \forall\, A_L \subseteq L,\ A_R \subseteq R\ |A_R| \leq |R| - |A_L| \text{ or } N(A_L) \cap A_R \neq \emptyset \\
&\iff \forall\, A_L \subseteq L,\ |\overline{N(A_L)}| \leq |R| - |A_L| \\
&\iff \forall\, A_L \subseteq L,\ |A_L| \leq |N(A_L)|
\end{aligned}$$

Hence we have the theorem ■

2.6.2 Boolean Lattice

For all $n > 0$ the Boolean Lattice $\mathcal{B}_n$ of order n is the poset $(\{0,1\}^n, \subseteq)$. We will prove a property of the Boolean Lattice and we will define general lattice later.

Theorem 2.6.10 Sperner's Theorem
For all $n \in \mathbb{Z}_+$

$$w(\mathcal{B}_n) = \binom{n}{\lceil \frac{n}{2} \rceil}$$

Proof: First of all take all the subsets of $\{0,1\}^n$ of size $\lceil \frac{n}{2} \rceil$ and this number is $\binom{n}{\lceil \frac{n}{2} \rceil}$. These sets form an anti-chain. Therefore we have $w(\mathcal{B}_n) \geq \binom{n}{\lceil \frac{n}{2} \rceil}$.

Let $A_1, \ldots, A_k \subseteq [n]$ form an antichain. We will show that $k \leq \binom{n}{\lceil \frac{n}{2} \rceil}$. Let $Sym(n)$ is the set of all permutations on $[n]$. Now for all $i \in [k]$ define

$$S_i = \{\pi \in Sym(n) \colon \{\pi(A_i)\} = A_i\}$$

Then we have $|S_i| = |A_i|!(n - |A_i|)!$. Now notice that $A_i \cap A_j = \emptyset$ for $i \neq j$. Therefore we have

$$n! \geq \sum_{i=1}^{k} |S_i| = \sum_{i=1}^{k} (n - |A_i|)!|A_i|! \geq \sum_{i=1}^{k} \left\lfloor \frac{n}{2} \right\rfloor! \left(n - \left\lfloor \frac{n}{2} \right\rfloor\right)! = k \left\lfloor \frac{n}{2} \right\rfloor! \left(n - \left\lfloor \frac{n}{2} \right\rfloor\right)! \implies \binom{n}{\lfloor \frac{n}{2} \rfloor} \geq k$$

Therefore we have the lemma. ■

Theorem 2.6.11 Erdős-Ko-Rado Theorem
Let $0 < k \leq \frac{n}{2}$. Let $\mathcal{A}$ be a family of subsets of $[n]$ of size k that are pairwise intersecting. Then $|\mathcal{A}| \leq \binom{n-1}{k-1}$.

Proof: Let $\mathcal{A} = \{A_1, \ldots, A_m\}$ be the family. For all $i \in [m]$ define

$$S_i = \{\pi \in Sym(n) \colon \exists\, j \in [n],\ \pi(j + [|A_i|]) = A_i\}$$

where $j + [|A_i|] \coloneqq \{l + j : l \in A_i\}$. We have $|S_i| = n(n-k)!k!$. Now each π is in at most k many different A_i. Then we have

$$kn! \geq m \times n(n-k)!k! \implies (n-1)! \geq m(n-k)!(k-1)! \implies \binom{n-1}{k-1} \geq m$$

Hence we have the lemma. ■

2.6.3 Symmetric Chain Decomposition

Below we will define some properties of chains in a poset $(U, \leq)$.

- For any $u \in U$ $\text{rank}(x) = \max\{|C| : \max(C) = x\}$
- $(U, \leq)$ is *ranked* if all maximal chains ending in an element $u \in U$ have the same size.
- A chain C is *unrefinable* if $\nexists\, u \in U - C$ with $\min(C) < u < \max(C)$ such that $C \cup \{u\}$ is a chain. If U is ranked then a chain C is unrefinable if and only if it does not skip any rank
- A chain C is *symmetric* if it is unrefinable and $\text{rank}(\min(C)) + \text{rank}(\max(C)) = h(U) + 1$

Definition 2.6.5: Symmetric Chain Decomposition

A symmetric chain decomposition of a poset $(U, \leq)$ is a partition of the elements of U into symmetric chains.

For any $n \in \mathbb{Z}_+$ in the boolean lattice $\mathcal{B}_n$ for any subset $A \subseteq [n]$ we have $\text{rank}(A) = |A| + 1$ and $h(\mathcal{B}_n) = n + 1$. Hence in case of boolean lattice for any unrefinable chain $C : A_1 \subseteq A_2 \subseteq \cdots \subseteq A_k$ it is symmetric when

$$\text{rank}(\min(C)) + \text{rank}(\max(C)) = h(U) + 1 \iff (|A_1| + 1) + (|A_k| + 1) = (n+1) + 1 \iff |A_1| + |A_k| = n$$

The symmetric chain decomposition of the boolean lattice $\mathcal{B}_n$ if a partition of subsets of $[n]$ into chains such that for any chain in the partition $A_1 \subseteq A_2 \subseteq \cdots \subseteq A_k$ we have

- $|A_1| + |A_k| = n$
- $\forall\, j \in [k]$, $|A_j| = |A_{j-1}| + 1$.

Now for any $n \in \mathbb{Z}_+$ the boolean lattice

$$\mathcal{B}_n = \underbrace{\{\{0,1\} \times \{0,1\} \times \cdots \times \{0,1\}\}}_{n \text{ times}} = \{1 \cdot 1, 1 \cdot 2, 1 \cdot 3, \ldots, 1 \cdot k\}$$

We define the general poset $B(m_1, m_2, \ldots, m_k)$ for any $k \in \mathbb{Z}_+$ to be the set

$$B(m_1, m_2, \ldots, m_k) = \text{Submultisets of } M = \{m_1 \cdot 1, m_2 \cdot 2, \ldots, m_k \cdot k\}$$

ordered by inclusion where $m_i \in \mathbb{Z}_+$ for all $i \in [k]$. Therefore $\mathcal{B}_n = B(1, 1, \cdots, 1)$. $B(m_1, \ldots, m_k)$ is ranked and in $B(m_1, \ldots, m_k)$ for any sets $A = \{r_1 \cdot 1, \ldots, r_k \cdot k\}$, $\text{rank}(A) = r_1 + r_2 + \cdots + r_k - 1$ and $h(u) = m_1 + m_2 + \cdots + m_k + 1$. Call the sum $m_1 + m_2 + \cdots + m_k$ to n

Theorem 2.6.12

$B(m_1, \ldots, m_k)$ has a symmetric chain decomposition for all $k \in \mathbb{Z}_+$ and $m_i \in \mathbb{Z}_+$ $\forall\, i \in [k]$.

Proof: We will prove this using induction on k. If $k = 1$ then $B(m_1) = \{0, \ldots, m_1\}$ which is a symmetric chain of length $m_1 + 1$. So the trivial partition i.e. $\{\{i\} : i \in B(m_1)\}$ is a symmetric chain decomposition of $B(m_1)$. Hence the base case follows.

Let this is true for $B(m_1, \ldots, m_{k-1})$. We have

$$B(m_1, \ldots, m_k) = B(m_1, \ldots, m_{k-1}) \cup \{m_k \cdot k\}$$

By inductive hypothesis $\exists$ a symmetric chain decomposition $\mathcal{A} = (C_1, \ldots, C_l)$ of $B(m_1, \ldots, m_{k-1})$ where

$$C_i : \qquad A_{i,1} \subseteq A_{i,2} \subseteq \cdots \subseteq A_{i,k_i}$$

where $\forall\ i \in [l]$ and $\forall\ j \in [k_i]$

$$\operatorname{rank}(A_{i,1}) + \operatorname{rank}(A_{i,k_i}) = n + 1 - m_k, \qquad \operatorname{rank}(A_{i,j}) = \operatorname{rank}(A_{i,j-1}) + 1 = \operatorname{rank}(A_{i,k_i}) - (k_i - j)$$

Now since C_i's are unrefinable we have for all $j \in [k_i]$, $\operatorname{rank}(A_{i,j}) = \operatorname{rank}(A_{i,1}) + (j-1)$. Since $B(m_1, \ldots, m_{k-1}) = \bigsqcup_{i=1}^{l} C_i$ we have $B(m_1, \ldots, m_k) = \bigsqcup_{i=1}^{l} Cur_i$ i.e. $\{Cur_i : i \in [l]\}$ is a partition of $B(m_1, \ldots, m_k)$ where

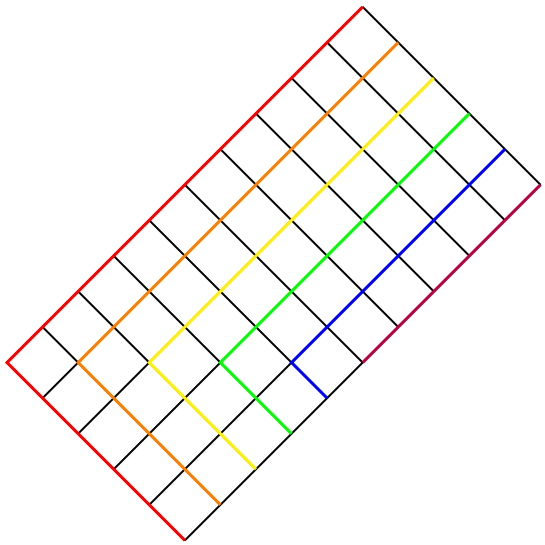
$$Cur_i = C_i \times \{0, \ldots, m_k\}$$

Now we will focus on each of the Cur_i's. Now informally each of the Cur_i looks like a grid of size $m_k \times k_i$.

Now denote $z_i = \min\{m_k + 1, k_i\}$. We will now create z_i many chains which follows the same properties followed by $\{C_i : i \in [l]\}$. Now for all $j \in [z_i]$ define the chain $C_{i,j}$

$$C_{i,j} : A_{i,1} \cup \{(j-1)\cdot k\} \subseteq A_{i,2} \cup \{(j-1)\cdot k\} \subseteq \cdots \subseteq A_{i,k_i-j+1} \cup \{(j-1)\cdot k\} \subseteq A_{i,k_i-j+1} \times \{j \cdot k\} \subseteq \cdots \subseteq A_{i,k_i-j+1} \cup \{m_k \cdot k\}$$

The construction of the new chains basically looks like the following picture.



Now for all $i \in [l]$ and $j \in [z_i]$ then we have

$$\begin{aligned} \operatorname{rank}(A_{i,1} \cup \{(j-1)\cdot k\}) + (\operatorname{rank}\left(A_{i,k_i-j+1} \cup \{m_k \cdot k\}\right) &= \operatorname{rank}(A_{i,1}) + (j-1) + \operatorname{rank}(A_{i,k_i-j+1}) + m_k \\ &= \operatorname{rank}(A_{i,1}) + \operatorname{rank}(A_{i,k_i}) - (j-1) + m - k + (j-1) \\ &= n + 1 - m_k + m_k = n + 1 \end{aligned}$$

Hence the new collection of chains $\mathcal{A}' = \{C_{i,j} : i \in [l],\ j \in [z_i]\}$ forms a symmetric chain decomposition of $B(m_1, \ldots, m_k)$. Hence by mathematical induction we have the theorem. ∎

2.6.4 General Lattices

Definition 2.6.6: Lattice

A poset $U(,\leq)$ is a lattice $\forall\, x, y \in U$, then least upper bound of x, y, $x \vee y$ i.e.

$$x \vee y \geq x, y \text{ and } \forall\, z \in U:\ z \geq x, y \implies z \geq x \vee y$$

also called *join* of x, y exists and the greatest lower bound of x, y, $x \wedge y$ i.e.

$$x \wedge y \leq x, y \text{ and } \forall\, z \in U:\ z \leq x, y \implies z \leq x \wedge y$$

also called *meet* of x, y exists.

Theorem 2.6.13 Tarski's Fixed Point Theorem

Let (U, leq) be a finite lattice and $f : U \to U$ be a monotone function (i.e. $x \leq \implies f(x) \leq f(y)$) then define

$$z_{max} = \bigvee_{x \leq f(x)} x, \qquad z_{\min} = \bigwedge_{f(x) \leq x} x$$

Then $z_{\max}$ is the largest fixed point and z_{min} is the smallest fixed point.

Proof: Define the sets

$$S_{\max} = \{x \in U : x \leq f(x)\} \qquad S_{\min} = \{x \in U : f() \leq x\}$$

Now observe that $S_{\max} \neq \emptyset$ since $\min(U) \in S_{\max}$. And similarly $S_{min} \neq \emptyset$ as $\max(U) \in S_{\min}$.

Now $\forall\, x \in S_{\max}$ we have

$$x \leq z_{\max} \implies f(x) \leq f(z_{\max}) \implies x \leq f(z_{\max})$$

Now it follows that

$$z_{\max} \leq f(z_{\max}) \implies f(z_{\max}) \leq f\left(f(z_{\max})\right) \implies f(z_{\max}) \in S_{\max} \implies f(z_{\max}) \leq z_{max} \implies z_{\max} = f(z_{\max})$$

Therefore $z_{\max}$ is a fixed point. Now $z_{\max}$ is also largest fixed point since all the fixed points are in $S_{\max}$.

Similarly we get that $z_{\min}$ is the fixed point and it is the smallest fixed point since all fixed points are in $S_{\min}$. Hence we have the theorem. ∎

Remark: Tarski's Fixed Point Theorem is not true for infinite lattices. For example take $U = \mathbb{Z}$ and take $f : \mathbb{Z} \to \mathbb{Z}$ where $f(n) = n^2 + 1$. Then f has no fixed point.

2.7 Probabilistic Method

The probabilistic method is a powerful tool for tackling many problems in discrete mathematics. Roughly speaking, the method works as follows: trying to prove that a structure with certain desired properties exists, one defines an appro- priate prob- ability space of structures and then shows that the desired properties hold in these structures with positive probability.

2.7.1 Ramsey Numbers

Definition 2.7.1: Ramsey Number

For $k > 0$, the $\mathscr{R}(k)$ is the smallest integer such that any graph with $\mathscr{R}(k)$ vertices has either a clique of size k or an independent set of size k.

Lemma 2.7.1

For all $k > 4$, $\mathscr{R}(k) > 2^{\frac{k}{2}}$ i.e $\exists$ a graph with $2^{\frac{k}{2}}$ vertices that does not have a k size clique or k size independent set.

Proof: Let $n = 2^{\frac{k}{2}}$ and consider a random graph (i.e. each edge appears with $\frac{1}{2}$ probability) with n vertices. Let G be such a graph. We will show that

$$\mathop{\mathbb{P}}_{G}[\exists\, S \subseteq [n] \colon |S| = k,\ S \text{ is not a clique or independent set}] < 1$$

Now using the union bound it is enough to show that

$$\sum_{S\subseteq[n],\ |S|=k} \mathop{\mathbb{P}}_{G}[S \text{ is aa clique or independent set}] < 1$$

Now we have

$$\sum_{S\subseteq[n],\ |S|=k} \mathop{\mathbb{P}}_{G}[S \text{ is aa clique or independent set}] = \sum_{S\subseteq[n],\ |S|=k} 2 \times \left(\frac{1}{2}\right)^{\binom{k}{2}} = \binom{n}{k}\frac{2}{2^{\binom{k}{2}}}$$

Hence it suffices to show that

$$\binom{n}{k}\frac{2}{2^{\binom{k}{2}}} < 1 \iff 2\binom{n}{k}2^{-\frac{k^2-k}{2}} < 1 \iff \frac{\cancel{n^k}}{k!}\frac{2^{\frac{k}{2}}+1}{\cancel{2^{\frac{k^2}{2}}}} < 1 \iff \frac{2^{\frac{k}{2}+1}}{2^{\frac{k^2}{2}}} < 1$$

The last inequality is true when $k > 4$.

Hence when $k > 4$ we have $\mathop{\mathbb{P}}_{G}[\exists\, S \subseteq [n] \colon |S| = k,\ S \text{ is a clique or independent set}] < 1$. Hence

$$\mathop{\mathbb{P}}_{G}[\forall\, S \subseteq [n] \colon |S| = k,\ S \text{ is not a clique or independent set}] > 0$$

Therefore there exists a graph G with $2^{\frac{k}{2}}$ many vertices which does not have a k size clique or k size independent set. ■

2.7.2 Turan's Theorem

Theorem 2.7.2 Turan's Theorem

Let $k > 0$ and G be a graph with n vertices without a clique of size $k+1$. The number of edges in $G < \left(1 - \frac{1}{k}\right)\frac{n^2}{2}$.

Proof: We will show that if $|E| < \binom{n}{2} - \left(1 - \frac{1}{k}\right)\frac{n^2}{2}$ then there is an independent set of size $k+1$. Then by flipping the graph i.e. taking the edge set which is the complement of the edge set of $G' = (V, E)$ we get a clique of size $k+1$.

Consider an uniformly random permutation of vertices $[n]$ and let S be the set of vertices that occur before all their neighbors. Hence S forms an independent set. Therefore we have

$$\mathbb{E}[|S|] = \sum_{i\in[n]} \mathbb{P}[i \in S] = \sum_{i\in[n]} \frac{1}{d_i + 1}$$

Here the last step is true because the vertex i has d_i many neighbors and if we arrange all the neighbors and the vertex i one after another what is the probability the vertex i comes at first among them.

Now by Jensen Inequality we have

$$\mathbb{E}[|S|] = \sum_{i\in[n]} \frac{1}{d_i+1} \geq \frac{n}{\frac{1}{n}\left(\sum\limits_{i\in[n]} d_i\right) + 1} = \frac{n}{\frac{2}{n}|E| + 1} = \frac{n^2}{2|E| + n}$$

Since $|E| < \binom{n}{2} - \left(1 - \frac{1}{k}\right)\frac{n^2}{2} = \frac{n(n-1)}{2} - \left(1 - \frac{1}{k}\right)\frac{n^2}{2} = \frac{1}{2}\left(\frac{n^2}{k} - n\right)$. Therefore we have

$$\mathbb{E}[|S|] \geq \frac{n^2}{2|E| + n} > \frac{n^2}{\frac{n^2}{k} - n + n} = k$$

Hence $\mathbb{E}[|S|] > k$ and since $|S|$ is always a positive integer we have $\mathbb{E}[|S|] \geq k+1$. Since the average cannot exceed the maximum we have the largest independent set has size at least $k+1$. Therefore if we take the complement graph there is a $k+1$ size clique. Hence

Hence if we have $|E| \geq \binom{n}{2} - \left(1 - \frac{1}{k}\right)\frac{n^2}{2}$ there is no independent set of size $k+1$. And therefore the complement graph also has no clique of size $k+1$. ■

2.7.3 Magnitude of Boolean Quadratic Forms

Lemma 2.7.3 Magnitude of Boolean Quadratic Forms

Let $n > 0$ and $a_{i,j} \in \{1, -1\}$ for all $i, j \in [n]$. Then

$$\max_{x_1,\ldots,x_n \in \{1,-1\}} \max_{y_1,\ldots,y_n \in \{1,-1\}} \sum_{i,j \in [n]} a_{i,j} x_i y_j \geq \Omega\left(n^{1.5}\right)$$

Proof: Let B denote the *LHS* of given expression i.e.

$$B \coloneqq \max_{x_1,\ldots,x_n \in \{1,-1\}} \max_{y_1,\ldots,y_n \in \{1,-1\}} \sum_{i,j \in [n]} a_{i,j} x_i y_j$$

Now

$$\begin{aligned}
B &= \max_{x_1,\ldots,x_n \in \{1,-1\}} \max_{y_1,\ldots,y_n \in \{1,-1\}} \sum_{i,j \in [n]} a_{i,j} x_i y_j \\
&= \max_{x_1,\ldots,x_n \in \{1,-1\}} \max_{y_1,\ldots,y_n \in \{1,-1\}} \sum_{j=1}^{n} y_j \sum_{i=1}^{n} a_{i,j} x_i \\
&= \max_{x_1,\ldots,x_n \in \{1,-1\}} \sum_{j=1}^{n} \max_{y_1,\ldots,y_n \in \{1,-1\}} y_j \sum_{i=1}^{n} a_{i,j} x_i \\
&= \max_{x_1,\ldots,x_n \in \{1,-1\}} \sum_{j=1}^{n} \left| \sum_{i=1}^{n} a_{i,j} x_i \right|
\end{aligned}$$

Now it is enough to show that

$$\mathop{\mathbb{E}}_{X_1,\ldots,X_n} \left[\sum_{j=1}^{n} \left| \sum_{i=1}^{n} a_{i,j} X_i \right| \right] = \sum_{j=1}^{n} \mathop{\mathbb{E}}_{X_1,\ldots,X_n} \left[\left| \sum_{i=1}^{n} a_{i,j} X_i \right| \right] \geq \Omega(n^{1.5}) \implies \mathop{\mathbb{E}}_{X_1,\ldots,X_n} \left[\left| \sum_{i=1}^{n} a_{i,j} X_i \right| \right] \geq \Omega(n^{0.5})$$

Now in the expression $\mathop{\mathbb{E}}_{X_1,\ldots,X_n} \left[\left| \sum_{i=1}^{n} a_{i,j} X_i \right| \right]$ the $a_{i,j}$ doesn't matter as they take the values of 1 or -1 and X_i also takes the values 1 or -1 we can think $Y_i = a_{i,j} X_i$ where Y_i takes values 1 or -1. Then we have

$$\mathop{\mathbb{E}}_{X_1,\ldots,X_n} \left[\left| \sum_{i=1}^{n} a_{i,j} X_i \right| \right] = \mathop{\mathbb{E}}_{Y_1,\ldots,Y_n} \left[\left| \sum_{i=1}^{n} Y_i \right| \right] = \frac{1}{2^n} \sum_{k=0}^{n} \binom{n}{k} |2k - n|$$

Now we have

$$\sum_{k=0}^{n}\binom{n}{k}|n-2k| = 2\sum_{k=0}^{\lfloor n/2\rfloor}\binom{n}{k}(n-2k) = 2\left(n\sum_{k=0}^{\lfloor n/2\rfloor}\binom{n}{k} - 2\sum_{k=0}^{\lfloor n/2\rfloor}k\binom{n}{k}\right)$$

$$= 2n\left(\sum_{k=0}^{\lfloor n/2\rfloor}\binom{n}{k} - 2\sum_{k=0}^{\lfloor n/2\rfloor}\binom{n-1}{k-1}\right) = 2n\left(\sum_{k=0}^{\lfloor n/2\rfloor}\left(\binom{n}{k} - \binom{n-1}{k-1}\right) - \sum_{k=0}^{\lfloor n/2\rfloor}\binom{n-1}{k-1}\right)$$

$$= 2n\left(\sum_{k=0}^{\lfloor n/2\rfloor}\binom{n-1}{k} - \sum_{k=0}^{\lfloor n/2\rfloor}\binom{n-1}{k-1}\right) = 2n\left(\sum_{k=0}^{\lfloor n/2\rfloor}\binom{n-1}{k} - \sum_{k=0}^{\lfloor n/2\rfloor-1}\binom{n-1}{k}\right) = 2n\binom{n-1}{\lfloor n/2\rfloor} = \Omega(n^{0.5})$$

Hence we have $\mathop{\mathbb{E}}_{X_1,\ldots,X_n}\left[\left|\sum_{i=1}^{n} a_{i,j}X_i\right|\right] = \Omega(n^{0.5})$. Therefore $B \geq \Omega(n^{1.5})$. ■

2.7.4 Lovász-Local Lemma

Now we will prove a very strong result called the Lovász-Local Lemma. But before that first we need the define Dependency Graph of finite set of events.

Definition 2.7.2: Dependency (di)graph

Let $E_1, \ldots, E_n$ be events. For each i there is some subset $N(i) \subseteq [n]$ such that A_i is independent from $\{A_j : j \notin N(i) \cup \{i\}\}$. Here event A is independent from $\{B_1, \ldots, B_k\}$ means A is independent of every event of the form $\bigwedge_{i=1}^{k} C_i$ where C_i is either B_i or $\overline{B}_i$.

We can represent the above relations by the Dependency Graph which is a directed whose vertices is $[n]$ and the set of neighbors of $i \in [n]$ is the set $N(i)$.

Theorem 2.7.4 Lovász-Local Lemma

Let $E_1, \ldots, E_n$ be events and $G = ([n], E)$ be the dependency graph of these events. Suppose $x_1, \ldots, x_n$ satisfy

$$\forall i \in [n] \quad \mathbb{P}[E_i] \leq x_i \prod_{j:(i,j)\in E}(1-x_j)$$

Then

$$\mathbb{P}\left[\bigwedge_{i=1}^{n}\overline{E}_i\right] \geq \prod_{i=1}^{n}(1-x_i)$$

Proof: We will first prove the following claim:

Claim 2.7.1

$\forall\, i \in [n]$ and $\forall\, S \subseteq [n]$, $i \notin S$ we have

$$\mathbb{P}\left[E_i \mid \bigwedge_{j\in S}\overline{E}_j\right] \leq \frac{\mathbb{P}[E_i]}{\prod_{j\in S,\ (i,j)\in E}(1-x_j)}$$

Proof: We will prove this using induction on $|S|$. For base case let $S = \emptyset$. Then $S \cap \{j : (i,j) \in E\} = \emptyset$. Then $\prod_{j\in S,\ (i,j)\in E}(1-x_j) = 1$. And since S in empty $\mathbb{P}\left[E_i \mid \bigwedge_{j\in S}\overline{E}_j\right] = \mathbb{P}[E_i]$. Therefore the base case follows.

Suppose $|S| = k$. If $S \cap \{j\colon (i,j) \in E\} = \emptyset$, E_i is independent of E_j for all $j \in S$. Therefore $\mathbb{P}\left[E_i \mid \bigwedge_{j\in S} \overline{E}_j\right] = \mathbb{P}[E_i]$. Also since $S \cap \{j\colon (i,j) \in E\} = \emptyset$ we have $\prod_{j\in S,\ (i,j)\in E} (1-x_j) = 1$. Therefore the claim follows.

Now Suppose $S \cap \{j\colon (i,j) \in E\} \neq \emptyset$. Let $S_1 \coloneqq S \cap \{j\colon (i,j) \in E\}$ and $S_2 \coloneqq S \setminus S_1$. Then we have

$$\mathbb{P}\left[E_i \mid \bigwedge_{j\in S} \overline{E}_j\right] = \frac{\mathbb{P}\left[E_i \wedge \left(\bigwedge_{j\in S_1} \overline{E}_j\right) \mid \bigwedge_{j\in S_2} \overline{E}_j\right]}{\mathbb{P}\left[\bigwedge_{j\in S_1} \overline{E}_j \mid \bigwedge_{j\in S_2} \overline{E}_j\right]} \leq \frac{\mathbb{P}\left[E_i \mid \bigwedge_{j\in S_2} \overline{E}_j\right]}{\mathbb{P}\left[\bigwedge_{j\in S_1} \overline{E}_j \mid \bigwedge_{j\in S_2} \overline{E}_j\right]} \leq \frac{\mathbb{P}[E_i]}{\mathbb{P}\left[\bigwedge_{j\in S_1} \overline{E}_j \mid \bigwedge_{j\in S_2} \overline{E}_j\right]}$$

So we will now give a lower bound on $\mathbb{P}\left[\bigwedge_{j\in S_1} \overline{E}_j \mid \bigwedge_{j\in S_2} \overline{E}_j\right]$. Now we have

$$\begin{aligned}
\mathbb{P}\left[\bigwedge_{j\in S_1} \overline{E}_j \mid \bigwedge_{j\in S_2} \overline{E}_j\right] &= \prod_{k\in S_1} \mathbb{P}\left[E_k \;\middle|\; \left(\bigwedge_{j\in S_2} \overline{E}_j\right) \wedge \left(\bigwedge_{j<k,\ j\in S_1} \overline{E}_j\right)\right] \\
&\geq \prod_{k\in S_1} \left(1 - \frac{\mathbb{P}[E_k]}{\prod\limits_{\substack{j\in S_2 \\ (k,j)\in E}} (1-x_k) \prod\limits_{\substack{j\in S_1,\, j<k \\ (k,j)\in E}} (1-x_k)}\right) && \text{[Inductive Hypothesis]} \\
&\geq \prod_{k\in S_1} (1-x_k) && \left[\mathbb{P}[E_k] \leq x_k \prod_{j:(k,j)\in E} (1-x_j)\right]
\end{aligned}$$

Therefore we have

$$\mathbb{P}\left[E_i \mid \bigwedge_{j\in S} \overline{E}_j\right] \leq \frac{\mathbb{P}[E_i]}{\prod\limits_{k\in S_1} (1-x_k)} = \frac{\mathbb{P}[E_i]}{\prod\limits_{k\in S,(i,k)\in E} (1-x_k)}$$

Hence we have the claim ■

Now using the claim we have

$$\mathbb{P}\left[\bigwedge_{i=1}^{n} \overline{E}_i\right] = \prod_{i=1}^{n} \mathbb{P}\left[\overline{E}_i \mid \bigwedge_{j<i} \overline{E}_j\right]$$

■

Using Lovaász Local Lemma we have the following corollary:

Corollary 2.7.5

Suppose G has degree $\leq d$ and $x_1 = x_2 = \cdots = x_n = \frac{1}{d+1}$. If $\forall\ i \in [n]$

$$\mathbb{P}[E_i] \leq \frac{1}{e(d+1)} \implies \mathbb{P}\left[\bigwedge_{i=1}^{n} \overline{E}_i\right] > 0$$

Definition 2.7.3: Negative Dependency (di)graph

G is a negatve dependency (di)graph if for every event E_i and every subset $S \subseteq [n] \setminus N(i) \cup \{i\}$ we have

$$\mathbb{P}\left[E_i \cap \bigcup_{j\in S} E_j\right] \geq \mathbb{P}[E_i]\mathbb{P}\left[\bigcup_{j\in S} E_j\right]$$

Theorem 2.7.6 Lopsided Lovász Local Lemma

Suppose G is a negative dependency (di)graph for events $E_1, \dots, E_n$ and there exists $x_1, \dots, x_n$ which satisfy

$$\forall i \in [n] \quad \mathbb{P}[E_i] \leq x_i \prod_{j:(i,j)\in E} (1 - x_j)$$

Then

$$\mathbb{P}\left[\bigwedge_{i=1}^{n} \overline{E}_i\right] \geq \prod_{i=1}^{n} (1 - x_i)$$

2.8 Linear Algebraic Techniques in Combinatorics

2.8.1 Odd Town Even Town

Lemma 2.8.1 Odd Town

Let $\mathcal{F} \subseteq 2^{[n]}$ be such that $|A|$ is odd for every $A \in \mathcal{F}$ and $|A \cap B|$ is even for every distinct $A, B \in \mathcal{F}$. Then $|\mathcal{F}| \leq n$.

Proof: Define x_A for every $A \in \mathcal{F}$ to be the characteristic vector in $\{0,1\}^n$ where $x_A(i) = 1 \iff i \in A$. We will show that x_A's for all $A \in \mathcal{F}$ are linearly independent over $\mathbb{F}_2$. This suffices to show that $|\mathcal{F}| \leq n$ since

$$|\mathcal{F}| = |\{x_A : A| \in \mathcal{F}\}| \leq \dim_{\mathbb{F}_2} \{0,1\}^n = n$$

Suppose $\exists\ \alpha_A \in \mathbb{F}_2$ for all $A \in \mathcal{F}$ such that $\sum_{A\in\mathcal{F}} \alpha_A x_A = 0$. Hence we have

$$\sum_{A\in\mathcal{F}} \alpha_A x_A = 0 \implies \forall\ j \in [n],\ \sum_{A\in\mathcal{F}} \alpha_A x_A(j) = 0 \implies \forall\ A \in \mathcal{F},\ \sum_{j\in A} \sum_{B\in\mathcal{F}} \alpha_B x_B(j) = 0$$

Hence we have for any $A \in \mathcal{F}$

$$\sum_{j\in A} \sum_{B\in\mathcal{F}} \alpha_B x_B(j) = \sum_{B\in\mathcal{F}} \sum_{j\in A} \alpha_B x_B(j) = \sum_{B\in\mathcal{F}} \alpha_B \sum_{j\in A} x_B(j) = \sum_{B\in\mathcal{F}} \alpha_B \sum_{j\in A\cap B} x_B(j) = \alpha_A \sum_{j\in A} x_A(j) + \sum_{B\in\mathcal{F}, B\neq A} \alpha_B \sum_{j\in A\cap B} x_B(j) = 0$$

Now $|A|$ is odd and for all $B \in \mathcal{A}$ such that $B \neq A$, $|A \cap B|$ is even. Therefore $\sum_{j\in A} x_A(j) = |A| = 1$ and $\sum_{j\in A\cap B} x_B(j) = |A \cap B| = 0$. Therefore

$$\sum_{j\in A} \sum_{B\in\mathcal{F}} \alpha_B x_B(j) = \alpha_A \sum_{j\in A} x_A(j) + \sum_{B\in\mathcal{F}, B\neq A} \alpha_B \sum_{j\in A\cap B} x_B(j) = \alpha_A = 0$$

Therefore for all $A \in \mathcal{F}$ we have $\alpha_A = 0$. Hence $\{x_A : A \in \mathcal{F}\}$ are linearly independent. Hence we have $|\mathcal{F}| \leq n$. ■

Lemma 2.8.2 Even Town

Let $\mathcal{F} \subseteq 2^{[n]}$ be such that $|A|$ is even for every $A \in \mathcal{F}$ and $|A \cap B|$ is even for every distinct $A, B \in \mathcal{F}$. Then $|\mathcal{F}| \leq 2^{\frac{n}{2}}$

Proof: Define x_A for every $A \in \mathcal{F}$ to be the characteristic vector in $\{0,1\}^n$ where $x_A(i) = 1 \iff i \in A$. Define $U = \langle x_A : A \in \mathcal{F} \rangle \subseteq \mathbb{F}_2^n$. We will show that $\dim U \leq \frac{n}{2}$. Let U^0 be the annihilator of U. Now we have $\dim U + \dim U^0 = n$. Consider the following map $\varphi : U \to U^0$ where for any $u \in U$, $\varphi(u)(x) = \sum_{i=1}^{n} u_i x_i \bmod 2$.

Now φ is invective since

$$\varphi(u) = \varphi(u') \iff \forall\ i \in [n],\ \varphi(u)(e_i) = \varphi(u')(e_i) \iff u_i = u_i'\ \forall\ i \in [n] \iff u = u'$$

Fix any arbitrary $u \in U$. $\exists\, \alpha_A \in \mathbb{F}_2$ for all $A \in \mathcal{F}$ such that $\sum_{A\in\mathcal{F}} \alpha_A x_A = u$. Therefore for all $i \in [n]$, $u_i = \sum_{A\in\mathcal{F}} \alpha_A x_A(i)$. Hence for all $\beta_A \in \mathbb{F}_2$ for all $A \in \mathcal{F}$ we have

$$\varphi(u)\left(\sum_{A\in\mathcal{F}} \beta_A x_A\right) = \sum_{i=1}^{n} u_i \sum_{A\in\mathcal{F}} \beta_A x_A(i) = \sum_{i=1}^{n} \sum_{A\in\mathcal{F}} \alpha_A x_A(i) \sum_{B\in\mathcal{F}} \beta_B x_B(i) = \sum_{A\in\mathcal{F}} \sum_{B\in\mathcal{F}} \alpha_A \beta_B \underbrace{\sum_{i=1}^{n} x_A(i)x_B(i)}_{|A\cap B|} = 0$$

Therefore for all $v \in U$, $\varphi(u)(v) = 0$. Hence $\dim U \le \dim U^0 \implies \dim U \le \frac{n}{2} \implies |U| \le 2^{\frac{n}{2}} \implies |\mathcal{F}| \le 2^{\frac{n}{2}}$ ■

2.8.2 Fisher's Inequality

Theorem 2.8.3 Fisher's Inequality

Suppose that $\mathcal{F} \subseteq 2^{[n]}$ is a family of nonempty clubs such that for some fixed k, $|A \cap B| = k$ for every distinct $A, B \in \mathcal{F}$. Then $|\mathcal{F}| \le n$.

Proof: We will prove this using induction on k. For $k = 0$ we have all sets in $\mathcal{F}$ are disjoint. There there can be at most n many disjoint subsets of $[n]$. Therefore $|\mathcal{F}| \le n$. Hence the base case follows.

Now suppose this is true for $k-1$. Now let for all distinct $A, B \in \mathcal{F}$, $|A \cap B| = k$. Then for all $A \in \mathcal{F}$ we have $|A| > k > 0$. Define x_A for every $A \in \mathcal{F}$ to be the characteristic vector in $\{0,1\}^n$ where $x_A(i) = 1 \iff i \in A$ over $\mathbb{R}^n$. We will show $\{x_A : A \in \mathcal{F}\}$ are linearly independent over $\mathbb{R}^n$. This suffices because then we have

$$|\mathcal{F}| = |\{x_A : A| \in \mathcal{F}\}| \le \dim_{\mathbb{R}} \mathbb{R}^n = n$$

Suppose $\exists\, \alpha_A \in \mathbb{R}$ for all $A \in \mathcal{F}$ such that $\sum_{A\in\mathcal{F}} \alpha_A x_A = 0$. Hence we have

$$\sum_{A\in\mathcal{F}} \alpha_A x_A = 0 \implies \forall\, j \in [n],\ \sum_{A\in\mathcal{F}} \alpha_A x_A(j) = 0 \implies \forall\, A \in \mathcal{F},\ \sum_{j\in A} \sum_{B\in\mathcal{F}} \alpha_B x_B(j) = 0$$

So we have for any $A \in \mathcal{F}$

$$\sum_{j\in A} \sum_{B\in\mathcal{F}} \alpha_B x_B(j) = \sum_{B\in\mathcal{F}} \alpha_B \sum_{j\in A} x_B(j) = \sum_{B\in\mathcal{F}} \alpha_B \sum_{j\in A\cap B} x_B(j) = \alpha_A \sum_{j\in A} x_A(j) + \sum_{\substack{B\in\mathcal{F},\\ B\neq A}} \alpha_B \sum_{j\in A\cap B} x_B(j) = \alpha_A |A| + \sum_{\substack{B\in\mathcal{F},\\ B\neq A}} \alpha_B |A\cap B|$$

Therefore we get

$$\alpha_A|A| + k\sum_{\substack{B\in\mathcal{F},\\ B\neq A}} \alpha_B = 0 \iff \alpha_A(|A|-k) + k\sum_{B\in\mathcal{F}} \alpha_B = 0 \iff \alpha_A = -\frac{k\sum_{B\in\mathcal{F}} \alpha_B}{|A|-k} \iff \sum_{A\in\mathcal{F}} \alpha_A = -k\left(\sum_{B\in\mathcal{F}} \alpha_B\right) \sum_{A\in\mathcal{F}} \frac{1}{|A|-k}$$

The *LHS* and *RHS* have opposite signs. They can only be equal if both sides are zero. Hence $\sum_{A\in\mathcal{F}} \alpha_A = 0$. Then we have for any $A \in \mathcal{F}$, $\alpha_A = 0$. Therefore $\{x_A : A \in \mathcal{F}\}$ are linearly independent. Hence we have $|\mathcal{F}| \le n$. ■

2.8.3 RW Theorem

Definition 2.8.1: $\mathscr{L}$-Intersecting Family

Let $\mathscr{L}$ be a set of s positive integers. A family of nonempty subsets $\mathcal{F} \subseteq 2^{[n]}$ is called $\mathscr{L}$-intersecting family if $\forall\, i \neq j \in [n]$, $|S_i \cap S_j| \in \mathscr{L}$.

Then we have the following theorem:

Theorem 2.8.4 RW Theorem

Let $\mathscr{L}$ be a set of s positive integers and $\mathcal{F} \subseteq 2^{[n]}$ is a $\mathscr{L}$-intersecting family such that $|A| \notin \mathscr{L}$ for all $A \in \mathcal{F}$. Then $|\mathcal{F}| \leq \sum_{k=0}^{s} \binom{n}{k}$

Proof: For all $A \in \mathcal{F}$, define the $n-$variate polynomial

$$\tilde{p}_A(x_1, \ldots, x_n) = \prod_{l \in \mathscr{L}} \left(\sum_{i \in A} x_i - l \right)$$

Consider the multilinear version of these polynomials $\tilde{p}_A$ and call them p_A i.e. for all $i \in [n]$ replace all nonzero powers of x_i in $\tilde{p}_A$ by just x_i. Hence for all $a \in \{0,1\}^n$ we have $\tilde{p}_A(a) = p(a)$ for all $A \in \mathcal{F}$.

Now define y_A for every $A \in \mathcal{F}$ to be the characteristic vector in $\{0,1\}^n$ where $y_A(i) = 1 \iff i \in A$ over $\mathbb{R}^n$. So $|\{p_A : A \in \mathcal{F}\}| = |\{y_A : A \in \mathcal{F}\}|$. Now for any $A, B \in \mathcal{F}$ we have

$$\tilde{p}_A(y_B) = p_A(y_B) = \begin{cases} \prod_{l \in \mathscr{L}} \left(\sum_{i \in A} y_A(i) - l \right) = \prod_{l \in \mathscr{L}} (|A| - l) \neq 0 & \text{When } A = B \\ \prod_{l \in \mathscr{L}} \left(\sum_{i \in A} y_B(i) - l \right) = \prod_{l \in \mathscr{L}} (|A \cap B| - l) = 0 & \text{When } A \neq B \end{cases}$$

Therefore we have $p_A(y_B) \neq 0 \iff A = B$. Hence the polynomials $\{p_A : A \in \mathcal{F}\}$ are linearly independent over $\mathbb{R}$.

Now for all $A \in \mathcal{F}$, $\deg p_A \leq |\mathscr{L}| = s$. The set of multilinear polynomials of degree $\leq s$ is a vector space of dimension $\sum_{k=0}^{s} \binom{n}{k}$. Hence

$$|\mathcal{F}| = |\{y_A : A \in \mathcal{F}\}| = |\{p_A : A \in \mathcal{F}\}| \leq \sum_{k=0}^{s} \binom{n}{k}$$

Hence we have the theorem. ∎

Lemma 2.8.5

Let $\mathscr{L}$ be a set of s positive integers and $\mathcal{F} \subseteq 2^{[n]}$ is a $\mathscr{L}$-intersecting family such that $\forall\, A \in \mathcal{F}$, $|A| = k$ and $\forall\, l \in \mathscr{L}, l < k$. Then $|\mathcal{F}| \leq \binom{n}{s}$.

Proof: For all $A \in \mathcal{F}$, define the $n-$variate polynomial

$$\tilde{p}_A(x_1, \ldots, x_n) = \prod_{l \in \mathscr{L}} \left(\sum_{i \in A} x_i - l \right)$$

Consider the multilinear version of these polynomials $\tilde{p}_A$ and call them p_A i.e. for all $i \in [n]$ replace all nonzero powers of x_i in $\tilde{p}_A$ by just x_i. Hence for all $a \in \{0,1\}^n$ we have $\tilde{p}_A(a) = p(a)$ for all $A \in \mathcal{F}$.

We will define another set of polynomials now. For all $T \subseteq [n]$ with $|T| < s$ define

$$\tilde{q}_(x_1, \ldots, x_n) = \left(\sum_{i=1}^{n} x_i - k \right) \prod_{t \in T} x_t$$

Like in case of $\tilde{p}_A$'s let q_T be the multilinear version of $\tilde{q}_T$. Hence for all $a \in \{0,1\}^n$, $\tilde{q}_T(a) = q_T(a)$ for all $T \subseteq [n], |T| < s$. We will show that $\{p_A : A \in \mathcal{F}\} \cup \{q_T : T \subseteq [n], |T| < s\}$ is linearly independent.

Now define y_T for every $T \subseteq [n]$ to be the characteristic vector in $\{0,1\}^n$ where $y_T(i) = 1 \iff i \in T$. Consider an arbitrary linear combination

$$\sum_{A \in \mathcal{F}} \alpha_A p_A + \sum_{\substack{T \subseteq [n], \\ |T| < s}} \beta_T q_T = 0 \implies \forall\, B \in \mathcal{F}, \sum_{A \in \mathcal{F}} \alpha_A p_A(y_B) + \sum_{\substack{T \subseteq [n], \\ |T| < s}} \beta_T q_T(y_B) = \alpha_B p_B(y_B) = 0 \implies \forall\, B \in \mathcal{F}, \alpha_B = 0$$

Hence we have now $\sum_{\substack{T\subseteq[n],\\|T|<s}} \beta_T q_T = 0$. Now let T^* be the smallest such that $\beta_{T^*} \neq 0$. Then we have

$$\sum_{\substack{T\subseteq[n],\\|T|<s}} \beta_T q_T = \sum_{\substack{T\subseteq[n],\\|T|<s,\ |T|\geq|T^*|}} \beta_T q_T(y_{T^*}) = \beta_{T^*} q_{T^*}(y_{T^*}) + \sum_{\substack{T\subseteq[n],|T|<s,\\T\neq T^*,|T|\geq|T^*|}} \beta_T q_T(y_{T^*}) = 0$$

Now if $T \neq T^*$ then $\exists\, i \in T \setminus T^*$. Therefore $y_{T^*}(i) = 0$. Hence $q_T(y_{T^*}) = 0$. Hence we have

$$\beta_{T^*} q_{T^*}(y_{T^*}) + \sum_{\substack{T\subseteq[n],|T|<s,\\T\neq T^*,|T|\geq|T^*|}} \beta_T q_T(y_{T^*}) = \beta_{T^*} q_{T^*}(y_{T^*}) \implies \beta_{T^*} q_{T^*}(y_{T^*}) = 0 \implies \beta_{T^*} = 0$$

But we assumed that $\beta_{T^*} \neq 0$. Hence contradiction. Therefore $\{p_A : A \in \mathcal{F}\} \cup \{q_T : T \subseteq [n], |T| < s\}$ is linearly independent. The set of multilinear polynomials of degree $\leq s$ is a vector space of dimension $\sum_{k=0}^{s} \binom{n}{k}$. Now $|\mathcal{F}| = |\{p_A : A \in \mathcal{F}\}| \leq \sum_{k=0}^{s} \binom{n}{k}$ and $\deg p_A \leq s$ for all $A \in \mathcal{F}$. Therefore we have

$$|\mathcal{F}| + |\{q_T : T \subseteq [n], |T| < s\}| = |\mathcal{F}| + \sum_{k=0}^{s-1} \binom{n}{k} \leq \sum_{k=0}^{s} \binom{n}{k} \implies |\mathcal{F}| \leq \binom{n}{s}$$

Hence we have the lemma. ■

2.9 Projective Planes

Definition 2.9.1: Projective Planes

Let $n > 0$ and $S_1, \ldots, S_m \subseteq [n]$ are a projective plane if

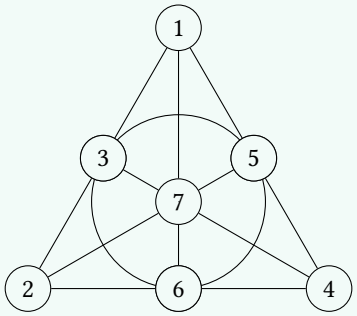
1. $|S_i| \geq 2$ for all $i \in [m]$
2. For all $i \neq j \in [n]$ $\exists!\ k \in [m]$ such that $i, j \in S_k$
3. For all $i \neq j \in [m]$, $S_i \cap S_j = \{j\}$ for some $j \in [n]$.
4. $\exists$ distinct $j_1, j_2, j_3, j_4 \in [n]$ such that for all $i \in [n]$, $|S_i \cap \{j_1, j_2, j_3, j_4\}| \leq 2$.

The elements in $[n]$ are called points and the subsets $S_i \subseteq [n]$ for all $i \in [m]$ are called lines.

Example 2.9.1 (Fano System)

For $n = 7$ consider the following sets

$S_1 = \{1, 3, 2\}$, $S_2 = \{2, 6, 4\}$, $S_3 = \{4, 5, 1\}$,
$S_4 = \{1, 7, 6\}$, $S_5 = \{2, 7, 5\}$, $S_6 = \{4, 7, 3\}$,
$S_7 = \{3, 5, 6\}$



This forms a projective plane as it follows all the conditions. This projective plane is represented like this:

Theorem 2.9.1

Let $S_1, \ldots, S_m \subseteq [n]$ be a projective plane. Then

1. $\exists\ s \geq 2$ such that each point is on $s+1$ lines and each line has $s+1$ points (s is the order of the projective plane)
2. $m = n = s^2 + s + 1$.

Chapter 3

Abstract Algebra

3.1 Group Theory