# MATH 7018: Probabilistic Combinatorics

Rui Gong

January 7, 2025

## Acknowledgements

These notes are based on the MATH 7018 lectures given by Professor *Xiaoyu He* in Spring 2025 at Georgia Institute of Technology.

# Contents

# 1 Introduction

We begin with three theorems.

**Theorem 1.1: Erdös, from Graph Theory**

*The Ramsey number $r(t,t)$ satisfies $r(t,t) \geq 2^{t/2}$.*

**Theorem 1.2: Erdös, from Additive Combinatorics**

*Every set $B$ of nonzero integers contains a sum-free subset $A \subseteq B$ of size $|A| \geq \frac{1}{3}|B|$.*

**Theorem 1.3: Spencer, from Extremal Set Theory**

*Any set family $\mathcal{F} \subseteq 2^{[n]}$ such that no $S, T \in \mathcal{F}$ satisfy $S \subsetneq T$ satisfies $|\mathcal{F}| \subseteq \binom{n}{\lfloor n/2 \rfloor}$.*

**Theorem 1.4: from Coding Theory**

*Any binary prefix code $C \subseteq \{0,1\}^*$ satisfies $\sum_{s \in C} \frac{1}{2^{|s|}} \leq 1$.*

**Definition 1.5**

*Ramsey number $r(t,t)$ is the smallest $n$ such that any graph $G$ on $n$ vertices has either a clique of size $t$ or an independent set of size $t$. Equivalently, any coloring of $E(K_n)$ in red, blue has either a monochromatic red or blue clique of size $t$. The equivalence can be seen by color all edges of $G$ as red and $E(K_n) \setminus E(G)$ as blue. For example, $r(3,3) = 6$, it is not 5 because $C_5$ and its complement do not have a triangle.*

*Proof of Theorem 1.1.* Let $G = G(n, 1/2)$ which is the Erdös-Renyi graph with $n$ vertices and each edge appears independently with probability $1/2$.

Look at $S \subseteq V(G)$ of size $t$. Then

$$\Pr[S \text{ is a clique}] = 2^{-\binom{t}{2}}$$
$$\Pr[S \text{ is an independent set}] = 2^{-\binom{t}{2}}.$$

Hence,

$$\begin{aligned}
&\Pr[G \text{ has a } t\text{-clique or } t\text{-independent set}] \\
\leq &\sum_{S \subseteq V(G)} \Pr[S \text{ is a } t\text{-clique or } t\text{-independent set}] \\
= &\binom{n}{t} \frac{2}{2^{\binom{t}{2}}} < \frac{n^t}{2^{\binom{t}{2}}} = 1 \text{ by picking } n = 2^{(t-1)/2}.
\end{aligned}$$

Notice the strict inequality is always true when $t \geq 2$. Thus, with positive probability, $G$ has no $t$-clique nor $t$-indpendent set. □

**Definition 1.6**

*$S \subseteq \mathbb{Z}$ is sum-free if $\nexists\, a, b, c \in S$ such that $a + b = c$.*
*Ex: $B = [n] = \{1, \ldots, n\}$. $A$ = odd numbers in $B$ is sum-free with $|A| \geq \lfloor \frac{1}{2}|B| \rfloor$; $A$ = largest $n/2$ numbers in $B$ is sum-free with $|A| \geq \lfloor \frac{1}{2}|B| \rfloor$.*

*Proof of Theorem 1.2.* Pick a big prime number $p > 2\max_{b\in B}|b|$, say $p = 3k+2$ (which exists by the prime number theorem). Define

$$A := \{b \in B | (xb \mod p) \in [k+1, 2k+1]\}$$

where $x$ is a uniformly random element of $[p-1]$.

$$\begin{aligned}\mathbb{E}[|A|] &= \sum_{b\in B} \Pr[xb \in [k+1, 2k+1]] \\ &= |B|\frac{k+1}{3k+1} > \frac{1}{3}|B|\end{aligned}$$

with positive probability $|A| > \frac{1}{3}|B|$. □

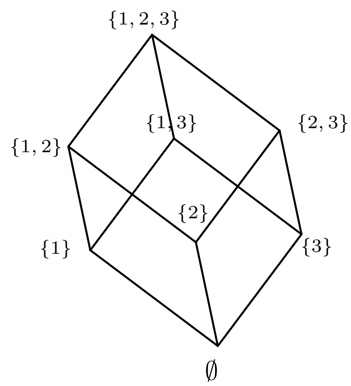


Figure 1: Subsets Diagram

*Example* 1.1. For $n = 3$, consider $2^{[n]}$. Look for biggest antichain in $2^{[n]}$, that is, choice of sets where no set lies above another. For example, $\{1\}, \{2\}, \{3\}$ and $\{1,2\}, \{1,3\}, \{2,3\}$ are biggest antichains.

*Proof of Theorem 1.3.* Let $\pi$ be a random element of $S_n$, which is a symmetric group. That is, $\pi = \pi_1\pi_2 \dots \pi_n$ is a random permutation of $[n]$. We consider all prefixes of $\pi$ and let $\mathcal{F}$ be an antichain in $2^{[n]}$. Define $X$ to be the number of elements in $\mathcal{F}$ which appear among prefix of $\pi$. Note that here we say appear among prefix, that is, if $\pi = 312$, then the $s$ appear among its prefix are $\emptyset, \{3\}, \{1,3\}, \{1,2,3\}$, where $\{1\}$ is not because any permutation of 1 does not make a prefix for 312.

First, notice that $X \leq 1$ by the fact that $\mathcal{F}$ is an antichain, so $\mathbb{E}[X] \leq 1$. Then

$$\begin{aligned}\mathbb{E}[X] &= \sum_{s\in\mathcal{F}} \Pr[s \text{ is a prefix of } \pi] \\ &= \sum_{s\in\mathcal{F}} \frac{1}{\binom{n}{|s|}} \geq \frac{\mathcal{F}}{\binom{n}{\lfloor n/2\rfloor}}.\end{aligned}$$

where the probability of $s$ being a prefix of $\pi$ is the probability of $\pi$ =(permutations of $s$)(permutations of $[n] \setminus s$. Thus, there are $s!\,(n-|s|)!$ of such $\pi$ and $n!$ possibly $\pi$ in total. The probability is as above. □

*Proof of Theorem 1.4.* $\{0,1\}^* := \cup_{n\geq 0}\{0,1\}^n$. A set $C \subseteq \{0,1\}^*$ is a prefix code if no $s, t \in C$ satisfy that $s$ is a prefix of $t$. For example, $C = \{00, 01, 10, 11\}, C = \{10, 110, 1110, 111110\}$ are prefix codes but $C = \{110, 1101\}$ is not. The theorem states that if we want $|C|$ to be large, then $|S|$ needs to be large in general.

Sample an infinite binary string $S$ uniformly at random. Let $X$ be the number of elements of $C$ that appear as a prefix of $S$ (not among like in the previous proof). Similarly, $X \leq 1$, or $C$ is not a prefix code. Hence, $\mathbb{E}[X] \leq 1$ and

$$\mathbb{E}[X] - = \sum_{s\in C} \frac{1}{2^{|s|}}$$

where $\frac{1}{2^{|s|}}$ is the probability of $s \in C$ being a prefix of the binary string $S$. □