CS-3334: Advanced Combinatorics **Fall 2022**

Lecture 2: September 20

Lecturer: Kuan Yang *Scribe: Weihao Zhu*

2.1 Schur's Theorem and Extensions

2.1.1 Schur's Theorem

Let's first recall **Schur's theorem**, which we have introduced last time.

Theorem 2.1 (Issai Schur, 1916) *Given any $c > 0$, there exists $S(c)$ such that no matter how we color $[S(c)]$ with c colors, there exists monochromatic x, y, z that $x + y = z$.*

Today, we will introduce another theorem proved by Issai Schur at the same time.

We all know that the famous Fermat's Last Theorem (proved by Andrew Wiles in 1994) states that $x^n + y^n = z^n$ has no nontrivial solutions as long as $n \geq 3$. However, this is not true in $\mathbb{F}_p$ for any sufficiently large prime p.

Theorem 2.2 (Issai Schur, 1916) *Let $n \geq 1$. There exists $S(n)$ such that for any prime $p > S(n)$,*

$$x^n + y^n \equiv z^n \pmod p$$

has an integer solution in $[p-1]$.

Proof: Let's first prove that there always exists a primitive root q for prime p, namely, $q^{p-1} \equiv 1 \pmod p$ and $q^r \not\equiv 1 \pmod p$ for all $1 \leq r \leq p-2$. Consider the order of each number in the group $([p-1], \times)$. Let $\psi(d)$ be the number of elements of order d, that is, the number of $x \in [p-1]$ such that $x^d \equiv 1 \pmod p$ and $x^{d'} \not\equiv 1 \pmod p$ for any $d' < d$. What we want to prove is $\psi(p-1) > 0$.

Define $\phi(d)$ be the number of integers $1 \leq d' \leq d$ such that d and d' are co-prime, i.e., $\gcd(d, d') = 1$. For any positive integer N, we have

$$\begin{aligned}
\sum_{d|N} \phi(d) &= \sum_{d|N} \phi(\frac{N}{d}) \\
&= \sum_{d|N} \sum_{t=1}^{N/d} [\gcd(t, N/d) = 1] \\
&= \sum_{d|N} \sum_{t=1}^{N} [\gcd(t, N) = d] \\
&= N.
\end{aligned}$$

In particular, $\sum_{d|p-1} \phi(d) = p-1$. According to the definition of $\psi(d)$, we also have $\sum_{d|p-1} \psi(d) = p-1$. Based on **Lagrange's Theorem**, $x^d \equiv 1 \pmod p$ has d roots: $1, m, \ldots, m^{d-1}$. If m^i has order d for some $0 \le i < d$, then i and d have to be co-prime, which implies that $\psi(d) \le \phi(d)$.

As $\sum_{d|p-1} \phi(d) = \sum_{d|p-1} \psi(d)$, we have $\phi(d) = \psi(d)$ for any $d \mid p-1$. In particular, $\psi(p-1) = \phi(p-1) > 0$. That is, there always exists a primitive root q for prime p.

Now we can rewrite $[p-1]$ as $[p-1] = \{q, q^2, \ldots, q^{p-1}\}$. In other words, each integer in $[p-1]$ can be represented as $q^{n \cdot s + r}$, where $s \ge 0, n > r \ge 0$. We color the integer with the r-th color. Based on Theorem 2.1, when p is sufficiently large, there exists s_1, s_2, s_3, r such that

$$q^{n \cdot s_1 + r} + q^{n \cdot s_2 + r} = q^{n \cdot s_3 + r},$$

which implies (since $\gcd(q, p) = 1$)

$$(q^{s_1})^n + (q^{s_2})^n \equiv (q^{s_3})^n \pmod p.$$

■

2.1.2 Several Related Theorems

Here is a generalized version of Theorem 2.1, which is often attributed to Folkman.

Theorem 2.3 *For any $c, r > 0$, there exists $N = N(c, r)$ such that no matter how we color $[N]$ with c colors, $\exists\ x_1, x_2, \ldots, x_r \in [N]$ and $\sum_{i=1}^{r} < N$ such that all $2^r - 1$ partial sums are of the same color.*

Schur's theorem states that when N is large enough, any c-coloring of $[N]$ will lead to one color with a solution $x + y - z = 0$. Does there exists monochromatic x, y, z such that $x + y - 2z = 0$? In this case $\{x, z, y\}$ forms an arithmetic progression of length 3. Here we present some other theorems on arithmetic progressions.

Theorem 2.4 (van der Waerden, 1927) *For any c, l, there is $W = W(c, l)$ such that any c-coloring of $[W]$ contains a monochromatic arithmetic progression of length l.*

Theorem 2.5 (Endre Szemerédi, 1975) *For any integer k, any subset S with positive upper density, i.e.,*

$$\limsup_{n \to \infty} \frac{|S \cup [n]|}{n} > 0,$$

contains infinitely many arithmetic progressions of length k.

Theorem 2.6 (Green-Tao, 2004) *Prime numbers contains arbitrarily long arithmetic progressions.*

What if we change $x + y = z$ into other linear equations? Rado proved the following theorem in 1933.

Theorem 2.7 (Richard Rado, 1933) *Consider a linear equation $E : \sum a_i x_i = 0$, where a_i are all integers. Then the following are equivalent:*

(a) For any $c > 0$, there exists $N = N(c)$ such that any c-coloring of $[N]$ contains a solution to E where $x_i \in [N]$ are of the same color.

(b) There is a non-trivial 0-1 solution to E.

2.2 Closest Pair in Two-Dimensional Space

In this section, we introduce an algorithmic application of the pigeonhole principle, the divide-and-conquer algorithm to find the closest pair among n vertices in a two-dimensional space.

Firstly, we sort all vertices according to their horizontal coordinates. Assume that the $\lceil \frac{n}{2} \rceil$-th vertex is P. Denote S_1, S_2 as the set of vertices on the left, right side of P, respectively. Then, we recursively find the distance of the closest pair in S_1 and S_2. Suppose that two distances we find are h_1 and h_2. Define $h := \min\{h_1, h_2\}$. Now, we only need to consider if there exists one vertex in S_1 and another in S_2 such that their distance is less than h.

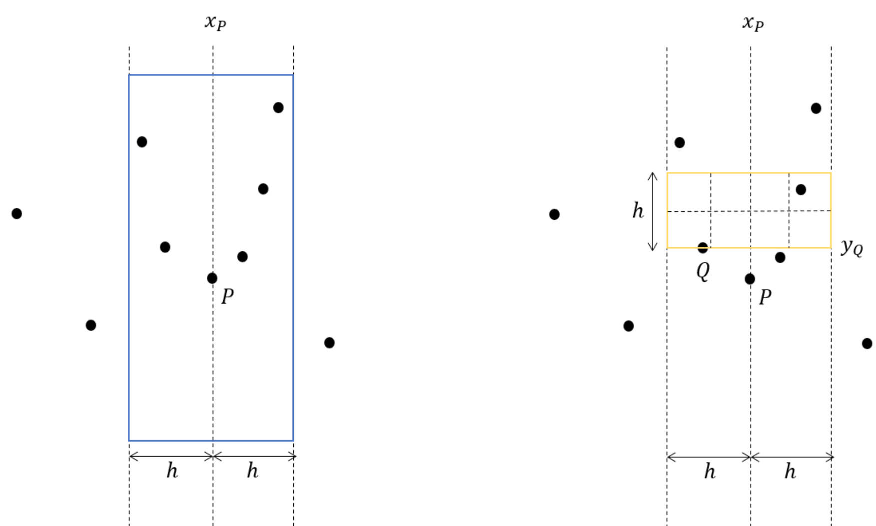

Figure 2.1: An instance of the problem with 9 vertices.

Assume that the horizontal coordinate of P is x_P. Obviously, we only need to consider all vertices of which horizontal coordinates range in $[x_P - h, x_P + h]$, which is the blue part in Figure 2.1. For any vertex Q in this part, suppose its vertical coordinate is y_Q. We enumerate all vertices of which vertical coordinates range in $[y_Q, y_Q + h]$, which is the yellow part in Figure 2.1, and check their distances from Q.

We can see that for any vertex Q, its corresponding yellow part can be divided into two squares of size $h \times h$. Furthermore, either square of size $h \times h$ can be divided into four smaller squares of size $(h/2) \times (h/2)$. According to the definition of h, there exists at most one vertex in each smaller square. (Otherwise, their distance will be smaller than h.) That is, there exists at most 8 vertices in the whole yellow part (using the pigeonhole principle). Thus, the running time of the algorithm satisfies $T(n) = 2T(n/2) + O(n)$, which implies that $T(n) = O(n \log n)$.

2.3 Double Counting

Double counting is an essential skill in combinatorics. We start from two simple examples.

Problem 2.1 *Given two positive integers n and k. Prove that the number of ways to partition n into at* *most k positive integers equals to the number of ways to partition n into several positive integers no larger than k.*

Proof: Consider any partition $n = \sum_{i=1}^{m} a_i$, where $1 \leq a_1 \leq a_2 \ldots \leq a_m \leq k$. For $1 \leq j \leq k$, define b_j as the number of indices $1 \leq i \leq m$ such that $a_i \leq j$. It's easy to show that $0 \leq b_j$ for $1 \leq j \leq k$, and

$$\sum_{i=1}^{m} a_i = n = \sum_{j=1}^{k} b_j,$$

which completes the proof. ■

Lemma 2.8 (Euler, 1736) *For any graph $G = (V, E)$, the sum of degrees of all vertices is an even number.*

Note that Lemma 2.8 implies that the number of vertices with odd degrees is even.

2.3.1 Sperner's Lemma

Now, we start to introduce **Sperner's Lemma**.

Lemma 2.9 (Emanuel Sperner, 1928) *Subdivide ΔABC into a triangulation (small triangles meet edge-by-edge) and color the vertices by A, B, C. Each vertex that lies along any edge of ΔABC can be only colored with the two colors of the endpoints of the edge, where the interior vertices can be colored arbitrarily. Then, there exists a small "tri-colored" triangles.*

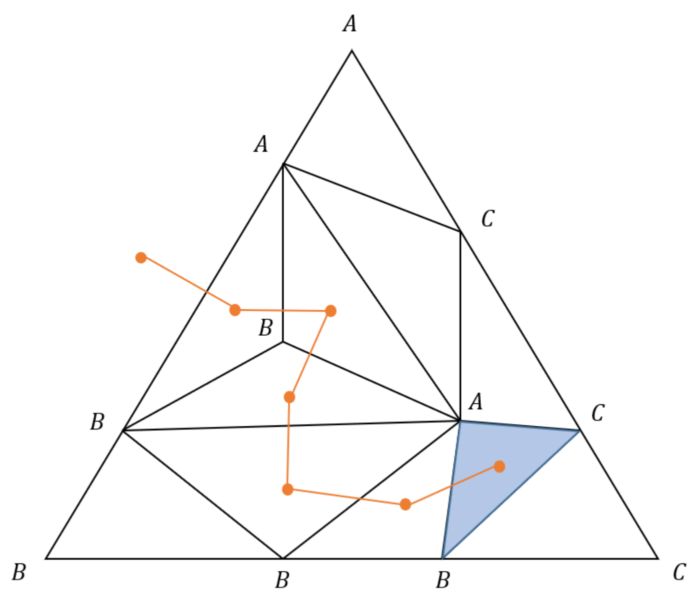

Figure 2.2: The picture shows a triangulation of ΔABC. The blue triangle is a small "tri-colored" triangle. The orange vertices and edges show the dual graph.

Proof: Consider the dual graph, where vertices are only connected by crossing an $A - B$ edge. Notice that the outside vertex has odd degrees, which implies that there exists another vertex with odd degrees. For other vertices, only those correspond to "tri-colored" triangles can have odd degrees, which completes the proof. ∎

We will also introduce several applications of **Sperner's Lemma**.

Theorem 2.10 (Paul Monsky, 1970) *It is impossible to divide a square into odd triangles of equal area.*

Complexity: Sperner's lemma can be generalized to n-dimensional simplex. Although it asserts that there always exists a sub-simplex whose different vertices are colored with different colors, it is difficult to find such a sub-simplex. Note that the decision problem cannot be NP-hard since the answer is always "yes". Roughly speaking, the function (NP) problem whose answer is promised to exist belongs to the complexity TFNP (Total Function NP). In particular, finding n-colored sub-simplex for a given Sperner coloring is PPAD-complete, where PPAD (Polynomial Parity Argument in Directed graphs) was defined by Christos Papadimitriou, in which problems are guaranteed to have solutions because of parity argument in directed graphs. The class is formally defined by specifying one of its complete problems, known as *End-of-the-Line*: Given a directed graph (possibly exponentially large) consisting of disjoint directed paths and directed cycles, the input is a source of a directed path and the goal is to find another source or sink other than the input.

Envy-free cake-cutting. Sperner's lemma is another form of Brouwer's fixed point. As we know, Nash equilibrium in game theory is also a kind of fixed point theorem. (In fact, examples of PPAD-complete problems includes many problems related to the fixed point theorem, for example, Xi Chen and Xiaotie Deng proved that 2-player Nash equilibrium is PPAD-complete and won the best paper award in FOCS 2006.) So Sperner's lemma also has applications in game theory, such as the envy-free cake cutting problem in fair division. Suppose there are n players and a cake. Different players may have different evaluation functions of each part of the cake (for example, one may prefer chocolate while another prefers fruits). A cake-cutting protocol is to divide the cake into n piece and give each piece to a player. The protocol is called "envy-free" if each person receives a piece that he values at least as much as every other's piece.

We now construct an (approximate) envy-free protocol according to the Sperner's lemma. Suppose there is one $[0,1]$ cake, which is divided into $x_1, \ldots, x_n$, where $\sum_{i=1}^n x_i = 1$. $(x_1, \ldots, x_n)$ form a $(n-1)$-dimensional simplex. Triangulate the simplex and assign each vertex to a player such that each sub-simplex has n distinct labels. For each vertex, ask the associated player: which piece do you prefer, and color it according to the answer. Then, there exists a sub-simplex such that different players prefer different pieces.

2.3.2 Forbidden Subgraphs Problems

In forbidden subgraphs problems, we usually consider the maximum number of edges in a graph if there is no given subgraph. Recall **Turán's Theorem** as follows.

Theorem 2.11 (Pál Turán, 1941) *If graph $G = (V, E)$ does not contain K_{r+1}, then $|E| \leq (1 - \frac{1}{r})\frac{n^2}{2}$.*

Let $ex(n, H)$ be the maximum number of edges in G of order n that does not contain H. **Erdős-Stone-Simonovits Theorem** is a generalization of Theorem 2.11 as follows.

Theorem 2.12 (Erdős-Stone, 1946 & Erdős-Simonovits, 1966) *Given a graph H. Then, $ex(n, H) = (1 - \frac{1}{\chi(H)-1})\binom{n}{2} + o(n^2)$.*

According to this theorem, When $\chi(H) > 2$, we can know that $ex(n, H)$ is approximately $(1 - \frac{1}{\chi(H)-1})\binom{n}{2}$. However, how about bipartite H? Let's first discuss the case when $H = C_4$.

Problem 2.2 *Calculate $ex(n, C_4)$.*

Answer: Consider the number of triples (u, v, w) such that $u \sim w$ and $v \sim w$. For each pair (u, v), there exists at most one w such that $u \sim w$ and $v \sim w$. For any vertex w, the number of its corresponding triples is at most $\binom{deg(w)}{2}$. Therefore, we have

$$\begin{aligned}
&\sum_u \binom{deg(u)}{2} \leq \binom{n}{2} \\
\Longrightarrow &\sum_u deg(u)^2 \leq n(n-1) + \sum_u deg(u) \\
\Longrightarrow &\frac{(2|E|)^2}{n} \leq n(n-1) + 2|E| && \text{(Cauchy-Schwartz inequality)} \\
\Longrightarrow &|E| \leq \frac{n}{4}(\sqrt{4n-3} + 1).
\end{aligned}$$

■

A more generalized theorem is as follows.

Theorem 2.13 (Bondy & Simonovits, 1974) *Let $t \geq 2$. There exists a constant $c > 0$ such that $ex(n, C_{2t}) \leq cn^{1+1/t}$.*

When $H = K_{t,t}$, we also have the following theorem.

Theorem 2.14 *Let $t \geq 2$. There exists a constant $c > 0$ such that $ex(n, K_{t,t}) \leq cn^{2-1/t}$.*

Proof: Suppose $m = |E|$. Consider the number of t-claws, that is, the number of $(u, \{v_1, \dots, v_t\}$ where $u \sim v_i$ for $1 \leq i \leq t$. For any t vertices $\{v_1, \dots, v_t\}$, there exists at most $(t-1)$ such u. For any vertex u, the number of its corresponding t-claws is $\binom{deg(u)}{t}$. Therefore, we have

$$\sum_u \binom{deg(u)}{t} \leq (t-1)\binom{n}{t}.$$

Notice that $f_t(x) = \binom{x}{t}$ is a convex function. By Jensen's inequality,

$$\sum_u \binom{deg(u)}{t} \geq n \cdot f_t(2m/n).$$

Notice that $\frac{1}{t!}(x-t)^t \leq f_t(x) \leq \frac{1}{t!}x^t$. Therefore, we have

$$\begin{aligned}
&\frac{n}{t!}(2m/n - t)^t \leq n \cdot f_t(2m/n) \leq (t-1)\binom{n}{t} \leq (t-1)\frac{n^t}{t!} \\
\Longrightarrow &2m/n - t \leq (t-1)^{1/t} n^{1-1/t} \\
\Longrightarrow &m \leq \frac{1}{2}(t-1)^{1/t} n^{2-1/t} + \frac{1}{2}tn,
\end{aligned}$$

which completes the proof. ■

2.4 Introduction to the Probabilistic Method

Paul Erdős is considered as the father of the probabilistic method. We start from a lower bound of Ramsey Number, which is proved by him.

Theorem 2.15 (Paul Erdős, 1947) *$R(k,k) > n$ holds if*

$$\binom{n}{k} \cdot 2^{1-\binom{k}{2}} < 1.$$

Proof: Color the edges of K_n independently and uniformly at random. Fix a set $S \in \binom{[n]}{k}$. Let $\mathcal{E}_S$ be the event that S induces a monochromatic K_k. It's easy to show that $\mathbf{Pr}[\mathcal{E}_S] = 2^{1-\binom{k}{2}}$. Thus, we have

$$\begin{aligned}
\mathbf{Pr}[\exists \text{ a monochromatic } K_k] &= \mathbf{Pr}[\cup \mathcal{E}_S] \\
&\leq \sum_S \mathbf{Pr}[\mathcal{E}_S] \\
&= \binom{n}{k} 2^{1-\binom{k}{2}} \\
&< 1.
\end{aligned}$$

It implies that the probability that no monochromatic K_k exists is not zero, which completes the proof. ∎