7 The Pigeonhole Principle and Ramsey Theory

7.1 Ramsey number and pigeonhole

We start from an interesting problem.

Question 7.1. Suppose "being friends" is an undirected relation. Show that among 6 people either there exists 3 people such that each pair of them are friends, or there exists 3 people such that each pair of them are not friends.

Using graph theoretical terms, the problem can be written as: prove that for any yellow-or-blue 2-coloring of edges of K_6, there exists a yellow K_3 or a blue K_3.

Proof. Consider a vertex u in K_6, there are 5 edges connecting u, which implies that there exists at least 3 monochromatic edges connecting u. Without loss of generality, assume that there are 3 yellow edges connecting u and a, b, c, respectively. Now, consider the three edges between a, b, c. If all of them are blue, then they form a blue K_3. Otherwise, assume that the edge between a and b is yellow, then u, a, b form a yellow K_3, which completes the proof. □

It is easy to find a 2-coloring of edges of K_5 such that the conclusion does not hold.

Question 7.2. Prove that for any 2-coloring of edges of K_{10}, there exists a yellow K_3 or a blue K_4.

Proof. Consider a vertex u in K_{10}. Among the 9 edges connecting u, there exists 4 yellow ones or 6 blue ones.

If there are 4 yellow edges connecting u and a, b, c, d, respectively. Consider the edges between a, b, c, d. If all of them are blue, then they form a blue K_4. Otherwise, assume that the edge between a and b is yellow, then u, a, b form a yellow K_3.

If there are 6 blue edges connecting u and other 6 distinct vertices. Consider the induced subgraph of these 6 vertices. By the result in Question 7.1, there exists a yellow K_3 or a blue K_3. If a yellow K_3 exists, then the proof is completed. If a blue K_3 exists, then these 3 vertices and u form a blue K_4. □

Remark 7.3. Notice that the same conclusion holds for any 2-coloring of edges of K_9. If it does not hold, each vertex must be incident to 3 yellow edges and 5 blue edges. But this is impossible.

Now, we introduce the definition of *Ramsey Number* as follows.

Definition 7.4 (Ramsey number)**.** $R(s,t)$ is defined as the smallest n satisfying: Given K_n, for any 2-coloring of edges of K_n, either a yellow K_s or a blue K_t exists.

From above, we already know that $R(3,3) = 6$ and $R(3,4) \leq 9$. We can also find that $R(s,t) \leq R(s-1,t) + R(s,t-1)$ of which the proof is similar to that in Question 7.2.

The key to the above proofs is the *Pigeonhole Principle*.

Theorem 7.5 (Pigeonhole principle)**.** *Let N, R be two finite sets of size $|N| = n > r = |R|$. Consider a mapping $f : N \to R$ and non-negative integers $a_1, a_2, \ldots, a_r$ such that $\sum_{i=1}^{r} a_i < n$. Then, there exists $s \in R$ such that $|f^{-1}(s)| \geq a_s + 1$.*

This is a simple but useful tool to prove existence.

Example 7.6 (Question 0.2)**.** Taking any $n+1$ numbers from $[2n]$,

1. there exists two among them that are relative prime;
2. there exists two among them such that one divides the other.

Example 7.7. Given n integers $a_1, a_2, \ldots, a_n$, there exists consecutive numbers $a_{t+1}, a_{t+2}, \ldots, a_{t+\ell}$ whose sum $\sum_{k=1}^{\ell} a_{t+k}$ is a multiple of n.

Example 7.8. Let f_n be the n-th Fibonacci number. For any $k > 0$, there is n such that f_n ends with k 0's.

Proposition 7.9. *For any $T > 0$, there is $n > 0$ such that $T \mid f_n$.*

Proof. Let $(f_n \bmod T, f_{n+1} \bmod T)$ be the pigeons. There are duplicated pairs when $N = T \times T$. Since $f_n = f_{n+2} - f_{n+1}$, $(f_1, f_0) = (1, 0)$ also appears at some position $k > 0$. □

Example 7.10. A student who has 20 weeks to prepare for ICPC has decided to complete at least one training contest every week, but he only has 30 sets of training problems. Show that no matter how he schedules his training, there exists consecutive weeks during which the student will complete exactly 9 training sets.

7.2 *Happy ending problem*

In 1933, Esther Klein proved the following claim.

> *Claim 7.11.* Any five points in a plane in general position has a subset that forms a convex quadrilateral. General position means that no two points coincide and no three points are collinear.

She also conjectured that for any n, a sufficiently large finite set of points in general position contains a convex polygon of size n. Later, the problem was named the "*happy ending problem*" by Paul Erdős. In 1935, Paul Erdős and George Szekeres proved the conjecture.

Theorem 7.12 (Erdős-Szekeres theorem)**.** *For any positive n, any sufficiently large finite set of points in general position has a subset of n points that forms a convex polygon.*

Remark 7.13. It is a fundamental theorem of combinatorial geometry. Four years later (1937), Esther Klein became Esther Szekeres. (That's why Erdős name it the "happy ending problem"!) During World War II, George and Esther escaped to China and lived in Hongkew, Shanghai. They moved to Australia after the war.

Before giving the proof of this theorem, let's first see another theorem proved by Paul Erdős and George Szekeres at the same time.

Theorem 7.14. *Any sequence of length $mn + 1$ with distinct numbers has either an increasing subsequence of length $n + 1$ or a decreasing subsequence of length $m + 1$.*

We have introduced this theorem in Section 4.2, and proved it by the Mirsky's theorem. Now we give an alternate proof by the pigeonhole principle.

Proof. Define a_i, b_i as the length of the longest increasing, decreasing subsequence that ends at the i-th number, respectively. For any $i < j$,

$a_i \neq a_j$ or $b_i \neq b_j$ holds. (This is because if the i-th number is smaller than the j-th one, then $a_i < a_j$. Otherwise, $b_i < b_j$.)

If the longest increasing subsequence has length at most n and the longest decreasing subsequence has length at most m, then there must exist $i < j$ such that $a_i = a_j$ and $b_i = b_j$ due to the *pigeonhole principle*, which leads to the contradiction. □

Now, let's introduce the proof of Theorem 7.12

Proof. Let's prove that for any $\binom{p+q}{p} + 1$ points in general position, there exists a concave polyline of length $p+1$ or a convex polyline of length $q+1$. (Note that a concave/convex polyline will lead to a convex polygon. If we have proved this, then set $p = q = n-2$ and the whole proof will be completed.)

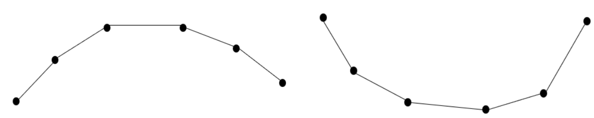

Figure 7.1: The left picture shows a concave polyline of length 5, while the right one shows a convex polyline of length 5.

We will finish the proof by induction on p and q. It obviously holds when $p = 1$ or $q = 1$. Suppose there are $\binom{p+q}{p} + 1$ points in general position and no convex polyline of length $q+1$ exists. By induction hypothesis, a concave polyline of length p exists as $\binom{p+q}{p} + 1 \geq \binom{p+q-1}{p-1} + 1$. Remove the rightmost point of the concave polyline and add the point into a set S. Repeat the process for $\binom{p+q}{p} + 1 - \binom{p+q-1}{p-1} = \binom{p+q-1}{p} + 1$ times. Based on the induction hypothesis, there exists either a concave polyline of length $p+1$, or a convex polyline of length q in S. If there exists a concave polyline of length $p+1$, then we're done. Otherwise there exists a convex polyline of length q in S. In this way, we can find $p+q+1$ points such that the left $p+1$ points form a concave polyline of length p while the right $q+1$ points form a convex polyline of length q. It's easy to show that either the left $p+2$ points form a concave polyline of length $p+1$, or the right $q+2$ points form a convex polyline of length $q+1$, which completes the proof. □

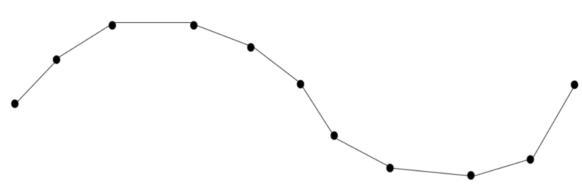

Figure 7.2: The picture shows the case that 11 points form a polyline of length 10, where $p = q = 5$. It is easy to see that left 7 points form a concave polyline of length $p+1 = 6$.

7.3 *Ramsey theory and applications*

In this section, we introduce generalized *Ramsey theorem*.

Theorem 7.15 (Ramsey theorem). *Let $r \geq 1$ and $q_i \geq r$ for $1 \leq i \leq s$. There exists a minimal integer $N = R(q_1, \dots, q_s; r)$ such that for any coloring $f : E(K_N^{(r)}) \to [s]$ of edges of the complete r-uniform hypergraph $K_N^{(r)}$, $\exists i \in [s]$ and a copy of $K_{q_i}^{(r)}$ of color i.*

Proof. □

Denote $R(\overbrace{q, \dots, q}^{s \text{ times}}; r)$ by $R_s(q; r)$.

With this theorem, we can prove *Schur's theorem*.

Theorem 7.16 (Schur's theorem). *Given any positive integer c, there exists $S(c)$ such that no matter how we color $[S(c)]$ with c colors, there exists monochromatic x, y, z that $x + y = z$.*

Proof. Take $S(c) = R_c(3; 2)$. For any edge (i, j) in graph $K_{S(c)}$, color it by $|i - j|$'s color. According to Theorem 7.15, there exists a monochromatic K_3 in graph $K_{S(c)}$. Assume that $u < v < w$ form a monochromatic K_3. Set $x = v - u, y = w - v, z = w - u$. Obviously, x, y, z have the same color and $x + y = z$, which completes the proof. □

Also, we obtain an easier proof of Theorem 7.12.

Proof. $N = R(n, 5; 4)$ points suffice. For any four vertices, if they form a convex quadrilateral, use the first color (let's assume it's blue) to color the corresponding hyperedge. Otherwise, use the second color (let's assume it's yellow). According to Theorem 7.15, there exists a blue $K_n^{(4)}$ or a yellow $K_5^{(4)}$. However, a yellow $K_5^{(4)}$ can never exist based on Claim 7.11, which implies that there exists n points where any 4 of them form a convex quadrilateral. It further yields that these n points form a convex polygon (why?). □

An interesting application of Schur's theorem is to refute the Fermat Last Theorem in finite fields. The well-known 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 7.17. *Suppose $n \geq 1$. 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 $1 \le r \le p-2$. 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 $\varphi(n)$ be the number of integers $1 \le d \le n$ such that $\gcd(d,n) = 1$. For any positive integer N, we have $\sum_{d|N} \varphi(d) = N$ (cf. Proposition 3.7). In particular, $\sum_{d|p-1} \varphi(d) = p-1$.

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 $\psi(d) \le \varphi(d)$.

As $\sum_{d|p-1} \varphi(d) = \sum_{d|p-1} \psi(d)$, we have $\varphi(d) = \psi(d)$ for any $d \mid p-1$. In particular, $\psi(p-1) = \varphi(p-1) > 0$. 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 7.16, 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 $\gcd(q, p) = 1$)

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

We now introduce some generalizations of Schur's theorem. The following theorem is a direct corollary from its proof.

Theorem 7.18 (Folkman's theorem)**.** *For any $c, r > 0$, $\exists\, N = N(c,r)$ 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 7.19 (van der Waerden's theorem)**.** *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.*

Roughly speaking, Ramsey's theorem tells us no matter how we partition an universal structure of size n, there exists a part that contains some desired sub-structures, as long as n is sufficiently large. Sometimes we concern that whether some certain parts contain desired sub-structures. The following theorems give such results on arithmetic progressions.

Theorem 7.20 (Szemerédi's theorem)**.** *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.

A natural question is, how about zero-density subsets? The problem becomes much complicated. A well-known counterexample is that no 4-AP of squares exists, while a long standing and folklore conjecture is that the prime numbers contain infinitely many arithmetic progressions of any length k. In 2004, Ben Green and Terence Tao proved this conjecture.

Theorem 7.21 (Green-Tao theorem)**.** *Let P be any subset of the prime numbers of positive relative upper density, i.e.,*

$$\limsup_{n\to\infty} \frac{|P \cap [n]|}{\pi(n)} > 0\,,$$

where $\pi(n)$ denotes the number of primes less than or equal to n. Then P contains infinitely many arithmetic progressions of length k for all k.

Remark 7.22. The longest known prime AP is of 26 terms.

Conjecture 7.23 (Erdős conjecture on arithmetic progressions)**.** Let S be a subset of $\mathbb{N}_+$. If

$$\sum_{n\in S} \frac{1}{n} = \infty\,,$$

then S contains arithmetic progressions of any length.

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

Theorem 7.24 (Rado's theorem)**.** *Let $E : \sum a_i x_i = 0$ be a linear equation, 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.*