Alegbraic Methods 2

In this chapter, We will continue the discussion of applying algebraic methods. Different from the contents in last semester some more advanced tools will be applied.

1 Bollobás Systems

We start with the original Bollobás's theorem.

Theorem 1 Suppose $A_1, \cdots, A_m$ are r-element sets and $B_1, \cdots, B_m$ are s-element sets, such that

- $A_i \cap B_i = \varnothing$, for every $i \in [m]$;
- $A_i \cap B_j \neq \varnothing$, for every $i, j \in [m]$ with $i \neq j$.

Then we have $m \leqslant \dbinom{r+s}{r}$.

We'll give three different proof here. The first proof is the traditional proof, which use probalistic method:

Proof 1. Put $X = \bigcup_{i=1}^m (A_i \cup B_i)$, and consider a random order π of X. For each i, $1 \leq i \leq m$. Let X_i be the event that all the elements of A_i precede all those of B_i in this order. Clearly, $P(X_i) = \frac{1}{\binom{r+s}{r}}$. It is also easy to check that the events X_i are pairwise disjoint. Indeed, assume this is false, and let π be an order in which all the elements of A_i precede those of B_i and all the elements of A_j precede those of B_j. Without loss of generality, we may assume that the last element of A_i does not appear after the last element of A_j. But in this case, all elements of A_i precede all those of B_j, contradicting the fact that $A_i \cap B_j \neq \varnothing$. Therefore, all the events X_i are pairwise disjoint, as claimed. It follows that

$$1 \geq P\left(\bigcup_{i=1}^m X_i\right) = \sum_{i=1}^m P(X_i) = \frac{m}{\dbinom{r+s}{r}},$$

completing the proof.

The second proof will use some polynomial methods.

Proof 2. Without loss of generality we may assume $A_i, B_i \subset \mathbb{R}$ for every i. Consider

$$A_i(x) := \prod_{a \in A_i} (x-a), \qquad B_i(x) := \prod_{b \in B_i} (x-b),$$

then $A_i, B_i \in \mathbb{R}[x]$, $\deg A_i = r$, and $\deg B_i = s$ for every $i \in [m]$. Moreover, A_i and B_j have a common factor if and only if $i \neq j$.

Now consider polynomials in $\mathbb{R}[b_0, \cdots, b_{s-1}]$ as

$$f_i(b_0, \cdots, b_{s-1}) = \operatorname{Res}(A_i, b_0 + b_1 x + \cdots + b_{s-1}x^{s-1} + x^s, x).$$

If we identify polynomial B_j and the corresponding coefficient vector $\left([x^0]B_j, [x^1]B_j, \cdots, [x^{s-1}]B_j\right)$, then definitely

$$f_i(B_j) \begin{cases} \neq 0, & i = j \\ = 0, & i \neq j \end{cases}.$$

We conclude that $f_1, \cdots, f_m$ are indeed linearly independent. Note that each f_i has s variables and is of degree at most r by definition of resultant, they live in a space of dimension $\dbinom{r+s}{r}$. Thus we see that $m \leqslant \dbinom{r+s}{r}$, as desired.

Now consider abut the third proof with wedge product methods.

Proof 3. Set $W=\mathbb{R}^{r+s}$ and associate a vector $w_x \in W$ for each $x \in (\cup_{i=1}^m A_i) \cup (\cup_{i=1}^m B_i)$, such that any $r+s$ of the associated vectors are linearly independent. This is achievable because the union of any $r+s-1$ hyperplanes cannot cover the whole space, which is a well-known fact from linear algebra.

For every set X (A_i or B_i), associate

$$w_X = \bigwedge_{x\in X} w_x \in \bigwedge\nolimits^{r+s} \mathbb{R}^{r+s}.$$

Note that different orders can only change it by the sign, which doesn't matter for our proof. We claim that $w_{A_1}, \cdots, w_{A_m}$ are linearly independent in $\bigwedge^r \mathbb{R}^{r+s}$. Suppose we have an $\mathbb{R}$-dependence

$$c_1 w_{A_1} + \cdots + c_m w_{A_m} = 0.$$

Then by taking wedge product with w_{B_i}, we have $c_i = 0$, which is a contradiction. Thus, the claim is true and we conclude that $m \leqslant \dim \bigwedge^r \mathbb{R}^{r+s} = C_{r+s}^r$.

We prove the original version of Bollobás's theorem above. By modifying the conditions slightly we can get another stronger version:

Theorem 2 Suppose $A_1, \cdots, A_m$ are r-element sets and $B_1, \cdots, B_m$ are s-element sets, such that

- $A_i \cap B_i = \varnothing$, for every $i \in [m]$;
- $A_i \cap B_j \neq \varnothing$, for every $i, j \in [m]$ with $i < j$.

Notice that we can prove theorem 2.2 by only modifying the last paragraph of the third proof :

Modification. Then by taking wedge product with w_{B_m}, we have $c_m = 0$; by taking wedge product with $w_{B_{m-1}}$, we have $c_{m-1} = 0$. Inductively processing from w_{B_m} to w_{B_1}, we get $c_m = c_{m-1} = \cdots = c_1 = 0$. Thus, the claim is true and we conclude that $m \leqslant \dim \bigwedge^r \mathbb{R}^{r+s} = \binom{r+s}{r}$.

Remark. For the skew version, no one knows another proof without using the exterior power argument up to now.

2 Saturated Number

We apply Bollobás's results to a graph theory study.

Definition 3. Given graph F, a graph G is called *F-saturated*, if G is free of copies of F, yet adding any edge to G creates a copy of F. We denote $\mathrm{sat}(n, F)$ as $\min\{|E(G)| : G \text{ is } F\text{-saturated with } n \text{ vertices}\}$ which would be referred to as *saturated number*.

In general, to determine the saturated number of some graph is insane. However, for complete graphs, amazing sharp result can be attained by Bollobás's theorem.

Theorem 4 For complete graph $K_r (r \in \mathbb{N})$, we have

$$\mathrm{sat}(n, K_r) = \binom{n}{2} - \binom{n-r+2}{2}.$$

Proof. Suppose G is a K_r-saturated graph and $e_1, \cdots, e_m$ are the non-edges of G, and let $H_1, \cdots, H_m$ be the corresponding copies of K_r, that are created once we add $e_1, \cdots, e_m$ in to the graph. Note that if there are multi-choices of H_i, just choose anyone would be fine.

By considering e_i, H_i as subsets of the vertices, then it is easily seen that $\{(e_i, H_i) : i \in [m]\}$ forms a Bollobás's system, and hence $m \leqslant \dbinom{n-r+2}{2}$.

Besides, considering a K_{r-2} and a complement of K_{n-r+2}, with all the edges between them added we have $m \geqslant \dbinom{n-r+2}{2}$, completing the proof.

In fact, we may the following modified problem to explore the power of skew Bollobás's theorem.

Definition 5. Given graph F, a graph G is called *weakly F-saturated*, if there is a all the non-edges of G can be made a $e_1, \cdots, e_m$, such that adding them in order increases the number of copies of F in G at each step. We shall denote $\mathrm{wsat}(n, F)$ as $\min\{|E(G)| : G \text{ is weakly } F\text{-saturated with } n \text{ vertices}\}$ which would be referred to as *weakly saturated number*.

Theorem 6. For complete graph $K_r (r \in \mathbb{N})$, we have

$$\mathrm{wsat}(n, K_r) = \binom{n}{2} - \binom{n-r+2}{2}.$$

Proof. Suppose G is a weakly K_r-saturated graph and $e_1, \cdots, e_m$ are the non-edges of G, and let $H_1, \cdots, H_m$ be the corresponding copies of K_r, that are created once we add $e_1, \cdots, e_m$ in to the graph. Note that if there are multi-choices of H_i, just choose anyone would be fine.

By considering e_i, H_i as subsets of the vertices, then it is easily seen that $\{(e_i, H_i) : i \in [m]\}$ forms a skew Bollobás's system, and hence $m \leqslant \binom{n-r+2}{2}$. And the result is also sharp, shown by considering the same construction as before.

3 Finite Automaton

As a more interesting application of Bollobas's systems, we shall discuss *finite automaton* and the related Černý's conjecture here.

Definition 7. A *finite automaton* $\mathcal{A} = (\Omega, \Sigma, T)$ consists of

- a finite set Ω of states,
- an finite alphabet Σ,
- and a transition function $T : \Omega \times \Sigma \to \Omega$.

Every time, the automaton starts from some initial state $\omega_0 \in \Omega$. Then a string $S = s_1 s_2 \cdots s_m$ where $s_i \in \Sigma$ is inputted, and the transition function iterates for m times to reach

$$\omega_1 = T(\omega_0, s_1), \quad \omega_2 = T(\omega_1, s_2), \quad \cdots \quad, \quad \omega_m = T(\omega_{m-1}, s_m).$$

To make the notations easier, we shall always denote $T(\omega, s)$ by ωs. Moreover, if we have a string $S = s_1 \cdots s_m$ on Σ, then write $\omega S = \omega s_1 s_2 \cdots s_m = (\cdots((\omega s_1)s_2)\cdots)s_m$.

Our main concern would be the *synchronization* problem of finite automatons:

Definition 8 Given a finite automaton $\mathcal{A} = (\Omega, \Sigma, T)$, a string S on Σ is called *synchronizing*, if $\omega S = \omega'$ for some fixed $\omega' \in \Omega$ holds for every $\omega \in \Omega$.

A finite automaton is called *synchronizable*, if there is a synchronizing string. Note that not every finite automaton is synchronizable, for example, when $T(w, s) \equiv w$, it is clear that the finite automaton does not admit a synchronizing string.

We define the *synchronizing constant* $\mathrm{syn}(n)$ as the maximum length of all shortest synchronizing strings, each of a finite automaton among all synchronizable finite automatons on n states. Note that we don't know whether $\mathrm{syn}(n)$ can be ∞ or not yet! Let's see trivial bounds first:

Theorem 9.1 For $n \in \mathbb{N}$, $\mathrm{syn}(n) \leqslant 2^n$.

Proof. Consider the digraph with vertices 2^Ω: For every $s \in \Sigma$ and $W \in 2^\Omega$, define

$$Ws = \{\omega s : \omega \in W\},$$

and add an arc from W to Ws. Then the automaton $\mathcal{A}$ is synchronizable implies that there is a directed path from Ω to some single-element subset of Ω. Since the digraph is on 2^n vertices, the shortest such path is of length at most 2^n, which is $\mathrm{syn}(n) \leqslant 2^n$, as desired.

Theorem 9.2 For $n \in \mathbb{N}$, $\mathrm{syn}(n) \leqslant \frac{1}{2} n^3 (1 - o(1))$.

Proof. We claim that a finite automaton $\mathcal{A} = (\Omega, \Sigma, T)$ is synchronizable, if and only if for every $\omega, \omega' \in \Omega$, there is a string S on Σ such that $\omega S = \omega' S$.

($\Longrightarrow$) direction is trivial by definition. For ($\Longleftarrow$) direction, note that as long as there are still stations $\omega_1 \neq \omega_2$ in ΩS_0, we can find a string S' synchronizing ω_1 and ω_2. Concatenate S_0 and S' and repeat (set $S_0 = S_0 S'$ then), we see that $\mathcal{A}$ is synchronizable. The claim is proved.

Now we show that $\operatorname{syn}(n) \leqslant (n-1)\binom{n}{2}$. The key is that as long as $\mathcal{A}$ is synchronizable, there's always a string no longer than $\binom{n}{2}$ that synchronizes two states as in the claim. The reason is just similar as in trivial bound : Consider the graph of all 1-element and 2-element subsets of Ω, there are $\binom{n}{2}$ of size 2, and hence we can find a directed path of length at most $\binom{n}{2}$ to go from a 2-element subset to a 1-element subset. Note that $\mathcal{A}$ is synchronized after synchronizing $(n-1)$ pairs, we conclude that $\operatorname{syn}(n) \leqslant (n-1)\binom{n}{2} = \frac{1}{2}n^3(1-o(1))$.

Finally we present the best-known upper bound by now, which turns out to be a cool application of the skew Bollobas's system result.

Theorem 9.3 For $n \in \mathbb{N}$, $\operatorname{syn}(n) \leqslant \dfrac{1}{6}n^3(1-o(1))$.

Proof. Suppose $\mathcal{A} = (\Omega, \Sigma, T)$ is synchronizable with $|\Omega| = n$. The main result we're going to prove is that for any $2 \leqslant r \leqslant n$ and $\Omega' \subset \Omega$ with $|\Omega'| = r$, we can find a word S of length at most $\binom{n-r+2}{2}$, such that $|\Omega' S| < |\Omega'|$.

Let S be a shortest word such that $|\Omega' S| < |\Omega'|$, say $S = s_1 s_2 \cdots s_m$. Definitely there are $\omega, \omega' \in \Omega'$ with $\omega S = \omega' S$. We set $S_i = s_1 s_2 \cdots s_i$, and $A_i = \{\omega S_i, \omega' S_i\}$, $B_i = (\Omega S_i)^c$ for $i = 1, 2, \cdots, m$. Then,

- $|A_i| = 2, |B_i| = n - r$, and (A_i, B_i) are distinct (clear by minimality of S).
- $A_i \cap B_i = \varnothing$, since $A_i = \{\omega, \omega'\}S_i \subset \Omega' S_i$.
- For $i < j$, $A_j \cap B_i \neq \varnothing$. Otherwise, $\{\omega, \omega'\}S_j \subset \Omega' S_i$, which means $\tilde{S} := s_1 \cdots s_i s_{j+1} \cdots s_m$ also satisfies $|\Omega'| > |\Omega' \tilde{S}|$, contradiction with the minimality of S.

Thus, (A_i, B_i) forms a skew Bollobas's system, and hence $m \leqslant \binom{n-r+2}{2}$.

Based on what we have shown,

$$\operatorname{syn}(n) \leqslant \sum_{r=2}^{n} \binom{n-r+2}{2} = \binom{n+1}{3}.$$

So we conclude that $\operatorname{syn}(n) \leqslant \frac{1}{6}n^3(1-o(1))$.

After establishing these upper bounds, let's see the lower bound of synchronizing number through an example given by Ján Černý.

Theorem 10 $\operatorname{syn}(n) \geqslant (n-1)^2$ for every $n \geqslant 2$.

Proof. Consider the following *Černý's automaton* $\mathcal{A} = (\Omega, \Sigma, T)$:

- $\Omega = \mathbb{Z}/n\mathbb{Z}$;
- $\Sigma = \{x, y\}$;
- $x(a) = a$, except $x(0) = 1$, and $y(a) = a + 1$ for every $a \in \mathbb{Z}/n\mathbb{Z}$.

A straightforward check shows that $(xy^{n-1})^{n-2}x$ synchronizes $\mathcal{A}$ and is of length $(n-1)^2$. We're supposed to show that this is the shortest.

Assume word S synchronize $\mathcal{A}$ and is of the shortest length, we claim that $S = (xy^{n-1})^{n-2}x$. The very first observation is that $\Omega S = \{1\}$, and the last bit of S has to be x. Now flip S to get word T (for example, $S = yxyyx$ implies $T = xyyxy$). We shall call some of x's in T as *special*. First, set the beginning x in T as x_1. If x_i is specified, scan from the symbol on the right of x_i in T one by one to the right until we have seen $n-1$ y's, then set the first x we see as x_{i+1}. We call the state space as Ω goes through S and exactly before x_i as Ω_i. The point is that $\Omega_i \subset \{0, 1, \cdots, i\}$ (by operation chasing), and hence there are at least $x_1, x_2, \cdots, x_{n-1}$ in T and between each of consecutive two there are at least $n-1$ y's. We conclude that T, hence S, is of length at least $(n-1)^2$, with the only equality case of $S = (xy^{n-1})^{n-2}x$.

Remark. Historically, Ján Černý proposed the conjecture of $\operatorname{syn}(n) = (n-1)^2$ in 1960s. Now, over 50 years have passed, and this problem is still open.