Algebraic Methods in Computer Science October 29, 2014

Lecture: 1

Lecturer: *Amir Shpilka* Scribe: *Saleet Klein*

1 Information

Email: shpilka at post dot tau dot ac dot il
Office: Schreiber 118

1.1 Grade

50 points - exam
40 points - 4 problem sets
10 points - grading homework
10 points - scribe

1.2 Linear Algebra and its Applications

We shall see applications of linear algebra to the following areas.

- Geometry
- Intersecting Families
- Expender Graph
- Error correcting codes
- Derandomization
- Proving lower bound
- Fourier transform
- Machine learning

We will see examples of the following the tools and techniques:

- Translating combinatoric problem into algebraic problem ($\mathbb{R}$)
- Translation into a question about polynomials
- Eigenvalues of a matrix
- Combinatorial Nullstelensatz
- Lower bound by linear potential functions
- Fourier transform

1.3 Reference Books

1. Linear Algebra Methods in Combinatorics with Applications to Geometry and Computer Science. L. Babai and P. Frankl
2. Extremal Combinatorics. S. Jukna.
3. Algebraic Methods in Combinatorics. O. Pikhurko. http://www.math.cmu.edu/ pikhurko/AlgMet.ps
4. Combinatorial Nullstellensatz. N. Alon.

1.4 Moto

"We can forgive a man for making a useful thing as long as he doesn't admire it. The only excuse for making a useless thing is that one admire it intensely." (Oscar Wilde)

2 Lindstrom's Theorem

We start by giving a combinatorial theorem that relies only on the basic fact that $n+1$ vectors in an n-dimensional space are linearly dependent.

Theorem 1 (Lindstrom's Theorem, weak version). *Let $A_1, A_2, ..., A_{n+1}$ be non-empty subsets of $[n] = \{1, 2, ..., n\}$, then there exists non-empty disjoint subsets $S_1, S_2 \subseteq [n+1]$ such that*

$$\bigcup_{i \in S_1} A_i = \bigcup_{i \in S_2} A_i$$

Proof. Let $v_i \in \{0,1\}^n \subseteq \mathbb{R}^n$ be the indicator vector of A_i ($k \in A_i \iff (v_i)_k = 1$).
Example: If $n = 5$ *and* $A_1 = \{1, 2, 4\}$ then $v_1 = (1, 1, 0, 1, 0)$.
We have $n+1$ vectors in a vector space with dimension $n \implies \exists \alpha_1, ..., \alpha_{n+1} \in \mathbb{R}$ not all zero such that $\sum_{i=1}^{n+1} \alpha_i v_i = 0$.
Denote $S_1 = \{i \mid \alpha_i > 0\}$ and $S_2 = \{i \mid \alpha_i < 0\}$, from $\sum_{i=1}^{n+1} \alpha_i v_i = 0$ we conclude that:

$$\sum_{i \in S_1} \alpha_i v_i = \sum_{i \in S_2} \mid \alpha_i \mid v_i$$

Since, for $j \in \{1, 2\}$ all the α_i such that $i \in S_j$ have the same sign, and the vectors v_i have nonnegative coordinates, it follows that the support of the vector $\sum_{i \in S_1} \alpha_i v_i$ is $\cup_{i \in S_1} A_i$ and that the support of the vector $\sum_{i \in S_2} \mid \alpha_i \mid v_i$ is $\cup_{i \in S_2} A_i$ (recall that the support of the vector $u = (u_1, ..., u_n)$ is $\text{supp}(u) = \{i \mid u_i \neq 0\}$). Therefore S_1, S_2 are non-empty disjoint subset of $[n+1]$ as desired. □

By concatenating to each vector its complement we are able to argue simultaneously about the union and the intersection.

Theorem 2 (Lindstrom's Theorem, strong version). *Let $A_1, A_2, ..., A_{n+2}$ be non-empty subsets of $[n] = \{1, 2, ..., n\}$, then there exists non-empty disjoint subsets $S_1, S_2 \subseteq [n+2]$ such that*

$$\bigcup_{i \in S_1} A_i = \bigcup_{i \in S_2} A_i \text{ and } \bigcap_{i \in S_1} A_i = \bigcap_{i \in S_2} A_i$$

Remark 1. De Morgan's laws implies that $\cap_{i\in S_1} A_i = \cap_{i\in S_2} A_i \iff \cup_{i\in S_1} A_i^c = \cup_{i\in S_2} A_i^c$.

Proof. Denote $\chi_A \in \{0,1\}^n$ the indicator vector of A_i namely $k \in A_i \iff (\chi_{A_i})_k = 1$.
Let $v_i \in \{0,1\}^{2n} \subseteq \mathbb{R}^{2n}$ be $v_i = (\chi_{A_i}, \chi_{A_i^c})$, note that $v_i = (\bar{0}, \bar{1}) + (\chi_{A_i}, -\chi_{A_i})$.
Let us look at the linear map $f : \mathbb{R}^{2n} \to \mathbb{R}^n$ defined as follow $f((x,y)) = (x+y)$ where $x, y \in \mathbb{R}^n$ and $x+y = (x_1+y_1, ..., x_n+y_n)$. Note that the kernel of f is $\text{Ker}(f) = \{(u, -u) \mid u \in \mathbb{R}^n\}$ and the image of f is $\text{Img}(f) = \mathbb{R}^n$ (taking all vectors of the form $(v, \bar{0})$ where $v, \bar{0} \in \mathbb{R}^n$). Therefore $dim(\text{Img}(f)) = n$, which implies, from rank-nullity theorem, that $dim(\text{Ker}(f)) = n$ (Recall rank-nullity theorem: $dim(\text{Ker}(f)) + dim(\text{Img}(f)) = dim(V)$ *where* $f : V \to W$). Hence, the dimension of the vector space $\text{Span}\{(\bar{1}, \bar{0}), (u, -u) \mid \bar{1}, \bar{0}, u \in \mathbb{R}^n\}$ is $n+1$. Each of the $n+2$ vectors v_i is in this vector space of dimension $n+1$. So we can apply the same technique we used in previous proof. □

It is interesting to note that the algebraic proof is the only proof we currently know for Theorem 2.

3 Helly's Theorem

We shall now see that the same observation over the real numbers yields Radon's lemma. We will then use this lemma to deduce Helly's theorem. Both are basic results in convexity theory.

Definition 1 (Convex set)**.** A convex set is a set C such that $\forall v, u \in C$ and $\forall 0 \leq \lambda \leq 1$ $\lambda v + (1-\lambda)u \in C$

Definition 2 (Convex hull)**.** A convex hull (or convex envelope) of a finite set $S = \{v_1, ..., v_n\}$ is the smallest convex set that contains S. Formally

$$\text{conv}(S) = \left\{ \sum_{i=1}^{|S|} \lambda_i v_i \mid v_i \in S,\ 0 \leq \lambda_i \leq 1 \text{ and } \sum_{i=1}^{|S|} \lambda_i = 1 \right\}.$$

Theorem 3 (Helly's Theorem)**.** *If $C_1, ..., C_m$ are convex sets in $\mathbb{R}^n$ such that any $n+1$ of them have a nonempty intersection, then $\cap_{i=1}^m C_i \neq \emptyset$.*

The proof of Theorem 3 is based on the following lemma:

Lemma 4 (Radon's lemma)**.** *Every set $S \subseteq \mathbb{R}^n$ of $n+2$ or more points can be partitioned into two disjoint sets $S_1, S_2 \subseteq S$ such that the convex halls of S_1 and S_2 intersect.*

Proof. Let $S = \{v_1, ..., v_m\}$ where $m \geq n+2$ define $u_i = (v_i, 1) \in \mathbb{R}^{n+1}$. We defined $m \geq n+2$ vectors in $\mathbb{R}^{n+1}$ (dimension $n+1$), so $u_1, ..., u_m$ are linearly dependent, namely there exist $\lambda_1, ..., \lambda_m$ not all zero such that $\sum_{i=1}^m \lambda_i u_i = 0$. Denote $S_1 = \{i \mid \lambda_i > 0\}$ and $S_2 = \{i \mid \lambda_i \leq 0\}$, from $\sum_{i=1}^m \lambda_i u_i = 0$ we conclude that:

$$\sum_{i\in S_1} \lambda_i u_i = \sum_{i\in S_2} \mid \lambda_i \mid u_i$$

Recall that $u_i = (v_i, 1)$, therefore

$$\sum_{i\in S_1} \lambda_i u_i = \sum_{i\in S_2} \mid \lambda_i \mid u_i \iff \sum_{i\in S_1} \lambda_i v_i = \sum_{i\in S_2} \mid \lambda_i \mid v_i \quad \text{and} \quad \sum_{i\in S_1} \lambda_i = \sum_{i\in S_2} \mid \lambda_i \mid$$

Denote $\lambda = \sum_{i\in S_1} \lambda_i = \sum_{i\in S_2} \mid \lambda_i \mid$ ($\lambda \neq 0$ since S_1 defined to be the set of points with positive coefficients). Dividing $\sum_{i\in S_1} \lambda_i v_i = \sum_{i\in S_2} \mid \lambda_i \mid v_i$ by λ yields

$$w = \sum_{i\in S_1} \frac{\lambda_i}{\lambda} v_i = \sum_{i\in S_2} \frac{\mid \lambda_i \mid}{\lambda} v_i.$$

Notice that we have that $\sum_{i\in S_1} \frac{\lambda_i}{\lambda} = \sum_{i\in S_2} \frac{|\lambda_i|}{\lambda} = 1$, and, by definition $0 \leq \frac{\lambda_i}{\lambda} \leq 1$ for $i \in S_1$. Similarly, $0 \leq \frac{|\lambda_i|}{\lambda} \leq 1$ for $i \in S_2$. Thus, w is in the convex hull of both $\{v_i \mid i \in S_1\}$ and $\{v_i \mid i \in S_2\}$. Since S_1 and S_2 are disjoint sets (by their definition) this proves the claim. □

Now we will prove Helly's Theorem (Theorem 3).

Proof. The proof is by induction on m. The base case being $m = n + 2$.

For $m = n + 2$: Define points $v_1, ..., v_m$ s.t. $v_i \in \cap_{j\neq i} C_j$ (any $n + 1$ sets intersect, so there exist such points v_i). By Radon's lemma (Lemma 4), there exist disjoint sets $S_1, S_2 \subseteq \{v_1, ..., v_m\}$, whose convex hulls intersect. That is, there exists $w \in \text{conv}(S_1) \cap \text{conv}(S_2)$. We will show that $\forall i\ w \in C_i$. Assume, w.l.o.g., $v_i \notin S_1$. Any $v_j \in S_1$ is in C_i (by definition, for every $j \neq i$, $v_j \in C_i$), namely $S_1 \subseteq C_i$. C_i is a convex set, and therefore $\text{conv}(S_1) \subseteq C_i$. Since $w \in \text{conv}(S_1)$ also $w \in C_i$. As i was arbitrary this proves the case of $m = n + 2$.

The induction step: we assume the claim is true for $m = k$ ($k \geq n + 2$) and prove it for $m = k + 1$. Define a new collection of convex sets $\forall i\ C'_i = C_i$ ($1 \leq i \leq m - 2$) and define $C'_{m-1} = C_{m-1} \cap C_m$. Since intersection of convex sets is convex set, $C'_1, ..., C'_{m-1}$ is a collection of convex sets, moreover in this collection any $n + 1$ sets intersect (the induction base case implies that any $n+2$ sets among $\{C_i\}_{i=1}^{m}$ have a nonempty intersection, therefore any $n+1$ sets of $\{C'_i\}_{i=1}^{m-1}$ intersect). The inductive hypothesis therefore applies, and shows that the new collection $\{C'_i\}_{i=1}^{m-1}$ has nonempty intersection. This implies the same for the original collection, and completes the proof. □

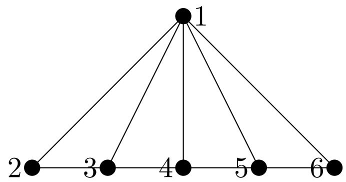
4 Rank of inclusion matrix

Next we will show several examples in which the rank of the inclusion matrix of a family of subsets gives a useful information.

Theorem 5. *For any n distinct points in the plane, that are not collinear, there exists at least n distinct lines, each passing through at least two points from the set.*

Definition 3 (Incidence Matrix)**.** Incidence Matrix is a matrix that shows the relationship between two classes of objects. If the first class is P (points) and the second is L (lines), the matrix has one row for each point in P and one column for each line in L. The entry of row p and column ℓ is 1 if p and ℓ are related (ℓ contains p) and 0 otherwise.

Example. The incidence matrix of the following graph is:



$$\begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

The proof of Theorem 5 is based on the following lemma.

Lemma 6. *The rank of an $n \times n$ matrix of the following form is n:*

$$M = \begin{bmatrix} >1 & 1 & \dots & 1 \\ 1 & >1 & \dots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \dots & >1 \end{bmatrix}$$

Proof. Let $a_{i,i}$ be such that

$$M = \begin{bmatrix} 1 & 1 & \dots & 1 \\ 1 & 1 & \dots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \dots & 1 \end{bmatrix} + \begin{bmatrix} a_{1,1} & 0 & \dots & 0 \\ 0 & a_{2,2} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & a_{n,n} \end{bmatrix}.$$

Clearly, $a_{i,i} > 0$. Note that $(x_1, \dots, x_n) \cdot M \cdot (x_1, \dots, x_n)^t = (\sum_{i=1}^n x_i)^2 + \sum_{i=1}^n a_{i,i} x_i^2$. Thus, if $M \cdot (x_1, \dots, x_n)^t = 0$ then from positivity over $\mathbb{R}$, for every i, $x_i = 0$ (since $a_{i,i} > 0$). Hence M has full rank. □

We will now prove Theorem 5.

Proof. We will prove that the rank of the incidence matrix is at least n. More precisely, we will show that the row rank is at least n, and therefore the column rank is at least n (the column rank is equal to the row rank).

Let A be the incidence matrix (which describe the relations between the points and lines). By looking on the matrix $M = AA^t$ we get an $n \times n$ matrix whose columns and rows are indexed by the points in our set. Indeed, the rows of A are indexed by points and the columns by lines. Observe that M has the following form:

$$M = AA^t = \begin{bmatrix} >1 & 1 & \dots & 1 \\ 1 & >1 & \dots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \dots & >1 \end{bmatrix}.$$

Indeed, $M_{p,q}$ is the number of lines that pass through both p and q thus, if $p \neq q$ then this number is 1 and if $p = q$ then, since the points are not collinear, this number is larger than

1. Lemma 6 implies that $\text{rank}(AA^t) = \text{rank}(M) = n$, therefore[1] $\text{rank}(A) \geq n$ and since there are only n rows $\text{rank}(A) = n$. Thus, the number of columns in A, which is the number of lines, is at least n. □

5 Eventown, Oddtown

There are two towns: Eventown and Oddtown. In each town there are n citizens. The citizens have a habit of forming clubs. Any group of citizens can form a club (we can therefore have 2^n clubs). In order to limit the number of clubs, each town passed rules whose objective is reducing the number of different clubs. The rules require that:

Oddtown	**Eventown**
Each club has an **odd** number of members	Each club has an **even** number of members
Each pair of clubs share an **even** number of members	Each pair of clubs share an **even** number of members
No two clubs are allowed to have identical membership	No two clubs are allowed to have identical membership

Despite the similar rules the two towns had different success.

We first note that in Eventown, citizens can form $2^{n/2}$ different clubs. First, people match into couples. Then, each couple either joins a club together or doesn't join the club at all. A natural question to ask is whether more clubs can be formed.

Theorem 7. *In Eventown there are at most $2^{\frac{n}{2}}$ clubs.*

Proof. Assume there are m clubs. Associate with each club its indicator vector v_i, where $(v_i)_k = 1$ iff citizen k belongs to club i. Notice that because of the rules, the inner product between two such v_i and v_j is always even (every club size is even and every intersection is even):

$$\forall i, j \ \langle v_i, v_j \rangle =_2 \begin{cases} 0 & i \neq j \\ 0 & i = j \end{cases},$$

where we denoted $\langle v, u \rangle = \sum v_i u_i$. For a subspace U denote $U^\perp = \{u \mid \forall v \in U \langle v, u \rangle = 0\}$. We have that $\dim(U) + \dim(U^\perp) = n$.

Denote $V = \text{Span}\{v_1, ..., v_m\}$. Observe that $\forall u, v \in V \ \langle v, u \rangle =_2 0$. Hence, $V \subseteq V^\perp$. Thus,

$$n = \dim(V) + \dim(V^\perp) \geq 2\dim(V) \implies \dim(V) \leq \frac{n}{2} \implies |\{v_1, ..., v_m\}| \leq 2^{\frac{n}{2}}.$$

□

In contrary, Oddtown's municipality did better.

[1] If A is a $n \times m$ matrix and B is a $m \times n$ matrix, then $\text{rank}(AB) \leq min\{\text{rank}(A), \text{rank}(B)\}$; and $\text{rank}(A) = \text{rank}(A^t)$

Theorem 8. *In Oddtown there are at most n clubs.*

Proof. We will use the same technique as in the proof of Theorem 5. Define the inclusion matrix A which describes the relationship between clubs and citizens; $a_{C,p} = 1 \iff p \in c$ where p is a person in Oddtown and C is a club. If the number of clubs is m then A is an $m \times n$ matrix. Therefore $M = AA^t$ is an $m \times m$ matrix whose rows and columns are indexed by clubs, such that $m_{C_1,C_2} = \mid C_1 \cap C_2 \mid$ where C_1, C_2 are two clubs. Oddtown rules imply that this matrix is equivalent, modulo 2, to the identity matrix I_m. Hence, the matrix has a full rank, and it holds that

$$m = \text{rank}(I_m) = \text{rank}(M) = \text{rank}(AA^t) \leq \text{rank}(A) \leq \#\text{columns in } A = n = \#\text{citizens}.$$

□

It is of course possible to have n clubs - each person forms its own club.

5.1 λ rule - Fisher's Inequality

We now give a general "rule" that also limits the number of clubs.

λ-rule: Each pair of clubs share exactly λ members and no two clubs are the same.

Theorem 9. *In a town obeying the λ-rule there can be at most n clubs.*

Proof. As before, define the inclusion matrix A describing the relationship between clubs and citizens ($a_{C,p} = 1 \iff p \in C$ where p is a person and C is a club). Again, we will look on $M = AA^t$ which is an $m \times m$ matrix, where m is the number of clubs.

$$M = AA^t = \begin{bmatrix} \mid C_1 \mid & \lambda & \dots & \lambda \\ \lambda & \mid C_2 \mid & \dots & \lambda \\ \vdots & \vdots & \ddots & \vdots \\ \lambda & \lambda & \dots & \mid C_m \mid \end{bmatrix}.$$

Case 1: There exists a club C such that $\mid C \mid = \lambda$. In this case all clubs should contain C and therefore there are at most n clubs (since they must be disjoint outside C).

Case 2: All clubs have more than λ members. In this case the matrix has full rank (a similar proof to Lemma 6). As before we conclude there are there are at most n clubs:

$$m = \text{rank}(M) = \text{rank}(AA^t) \leq \text{rank}(A) \leq \#\text{columns in } A = n.$$

□

We shall now see an "application" of the results that we've proved so far.

6 Ramsey's Theorem

Theorem 10 (Ramsey's Theorem)**.** *For every two positive integers s and t, there exists a positive integer $R(s,t)$, such that for any $n \geq R(s,t)$ and for any red-blue coloring of the edges of the complete graph K_n, the colored graph either contains a red-clique on s vertices or a blue-clique on t vertices.*

Definition 4 (Ramsey's Numbers)**.** The minimal integer for which the property above holds is called the s-t Ramsey's number and is denoted by $R(s,t)$.

Theorem 11 (Upper Bound)**.** *For all $s,t \in \mathbb{N}$*

$$R(s,t) \leq \binom{s+t-2}{s-1}$$

In particular, $R(3,3) \leq 6$ (in this case there is equality, $R(3,3) = 6$).

The proof of Theorem 11 is based on the following lemma:

Lemma 12. *For all $s,t \in \mathbb{N}$*

$$R(s,t) \leq R(s-1,t) + R(s,t-1).$$

Proof. The proof is by induction on s,t.

For $s=1$ or $t=1$: It is clear from the definition that for all $n \in \mathbb{N}$, $R(n,1) = R(1,n) = 1$ (a 1-clique corresponds to a vertex).

The induction step: Consider a complete graph on $R(s-1,t) + R(s,t-1)$ vertices whose edges are colored with two colours, red and blue. Pick a vertex v from the graph, and partition the remaining vertices into two sets S and T, such that for every vertex w, if (v,w) is red then $w \in S$, and if (v,w) is blue then $w \in T$. Because the graph has $R(s-1,t) + R(s,t-1) =\mid S \mid + \mid T \mid +1$ vertices, it follows that either $\mid S \mid \geq R(s-1,t)$ or $\mid S \mid \geq R(s,t-1)$. In the former case, if S has a blue K_t then so does the original graph and we are finished. Otherwise, S has a red K_{s-1} and so $S \cup \{v\}$ has red K_s by definition of S. The latter case is analogous. □

Now we will prove Theorem 11.

Proof. Again, the proof is by induction on s,t.

For $s=1$ or $t=1$: Every graph contains a clique of size 1, thus $R(s,t) \leq \binom{s+t-2}{s-1}$ (when $s=1$ the right side of the inequality is $\binom{t-1}{0} = 1$).

The induction step: Assume the expression holds for $R(s,t-1)$ and $R(s-1,t)$. Then

$$R(s,t) \overset{(1)}{\leq} R(s-1,t) + R(s,t-1) \overset{(2)}{\leq} \binom{s+t-3}{s-2} + \binom{s+t-3}{s-1} \overset{(3)}{=} \binom{s+t-2}{s-1}$$

(1) By Lemma 12; (2) By induction hypothesis; and (3) By Pascal's rule.[2] (when $k = s-1$ and $n = s+t-2$) □

[2] Pascal's rule $\binom{n-1}{k-1} + \binom{n-1}{k} = \binom{n}{k}$

The first lower bound for Ramsey's numbers was obtained by Paul Erdős using probabilistic method (random coloring).

Theorem 13 (Lower Bound)**.** *For all $t \in \mathbb{N}$*

$$\sqrt{2}^t \leq R(t,t)$$

Proof. Let $n = \sqrt{2}^t$. Consider a random coloring of K_n (each edge of K_n is colored red or blue with probability $\frac{1}{2}$). The number of subgraphs of K_n that equal K_t is exactly $\binom{n}{t}$. Moreover, the probability that a single K_t is monochromatic (containing or using only one color) is $2^{1-\binom{t}{2}}$ (The graph K_t has $\binom{t}{2}$ edges, and since the probabilities for different edges are independent the probability that K_t is red is $2^{-\binom{t}{2}}$. Similarly, the probability that K_t is blue is $2^{-\binom{t}{2}}$, so the probability that K_t is monochromatic is the sum of those, which is $2^{-\binom{t}{2}} + 2^{-\binom{t}{2}} = 2^{1-\binom{t}{2}}$). Therefore, the expected number of monochromatic t-cliques is $\binom{n}{t}2^{1-\binom{t}{2}}$. Hence, by Markov's inequality, the probability that there is at least one monochromatic t-clique, K_t, is at most $\binom{n}{t}2^{1-\binom{t}{2}}$. The following estimate shows that this probability is strictly less then 1

$$\binom{n}{t}2^{1-\binom{t}{2}} < \frac{2n^t}{t!2^{t(t-1)/2}} = \frac{2^{1+t/2}}{t!} < 1.$$

Therefore, with non-zero probability, there are no monochromatic cliques of size t, and such a coloring implies that $R(t,t) \geq \sqrt{2}^t = n$. □

Concluding, we obtained the following bounds on $R(t,t)$:

$$\sqrt{2}^t \leq R(t,t) \leq \binom{2t-2}{t-1} \approx \frac{4^t}{\sqrt{t}}$$

As one can easily see, there is a large gap between the best known lower bounds and the best known upper bounds. It is a very interesting open problem to improve the lower bound to be of the form $(2+\epsilon)^{t/2}$ for some constant $\epsilon > 0$ and/or to improve the upper bound to $(4-\epsilon)^t$, for some constant $\epsilon > 0$.

6.1 Nagy's Construction

Definition 5 (Ramsey's Graph)**.** We call a coloring of the complete graph K_n with no "large" monochromatic cliques, a Ramsey Graph. Equivalently, we say that an n-vertex graph G is a Ramsey graph if neither G nor its complement G^c have "large" cliques (edges of G correspond to "blue" edges). We say the graph is explicit if there is a polynomial time algorithm that given the name of an edge (the two $\log n$ sequences describing its nodes) outputs its color.

Construction 1 (Nagy's Construction)**.** *Identify the set of vertices of K_n with the set of triplets from $[t] = \{1, ..., t\}$. Formally $V = \{v \subseteq [t] \mid |v| = 3\}$ (subset of size 3). Join two such triplets by a red edge if they have precisely one vertex in common and by a blue edge otherwise. I.e.,*

$$\forall u, v \in V \; color(v,u) = \begin{cases} red & if\ |v \cap u| = 1 \\ blue & otherwise \end{cases}.$$

Theorem 14. *Nagy's construction gives an explicit two coloring of the complete graph on $n = \binom{t}{3}$ vertices, K_n, without a monochromatic K_{t+1} subgraph.*

Proof. Suppose that we have a monochromatic clique on m vertices. Those vertices correspond to m triplets that all edges connecting them have the same color. We shall now prove that $m \leq t$.

red-clique: Let $\{R_1, ..., R_m\}$ be a collection of m triplets that form a red clique. Observe that $\forall i, j \, |R_i \cap R_j| = 1$ (We join two such triplets by red if they have precisely one vertex in common). By considering each triplet as a club we get that $\{R_1, ..., R_m\}$ are m clubs such that each pair of clubs share exactly $\lambda = 1$ members. From Fisher's Inequality (theorem 9) it follows that there are at most t vertices in such a collection. In particular, $m \leq t$, which implies that the size of a red-clique is at most t.

blue-clique: Let $\{R_1, ..., R_m\}$ be a collection of m triplets that form a red clique. Observe that $\forall i, j \, |R_i \cap R_j| \in \{0, 2\}$. Again by considering each triplet as a club we get that $\{R_1, ..., R_m\}$ are m clubs such that each club has an odd number of members (3 members) and each pair of clubs share an even number of members (0 or 2 members). Therefore, Oddtown theorem (Theorem 8) yields that there are at most t vertices in such a collection. In particular, $m \leq t$, which implies that the size of a blue-clique is at most t. □

In the following lectures we will see an improved construction of an explicit Ramsey graph by Frankl and Wilson that is also based on intersection families.

Notes

This lecture is based on the manuscript of Babai and Frankl [BF92].

References

[BF92] László Babai and Péter Frankl, *Linera algebra methods in combinatorics (with applications to geometry and computer science)*, Manuscript, 1992. 1-10