Algebraic Methods in Computer Science	November 12, 2014
Lecture: 3	
Lecturer: *Amir Shpilka*	Scribe: *Nadav Trumer*

Intersecting Families

In this lecture we will prove classical results regarding intersecting families of sets. As an application we will give a better construction of a Ramsey graph (a graph containing no large cliques) and prove a lower bound on the chromatic number of the unit distance graph in n dimensions. The results today will use an extension of the algebraic proofs that we gave when we gave an upper bound on the number of points in the plane with only two distances.

The family of theorems that we will proved are called Ray-Chaudhuri–Wilson type theorems. In what follows we denote $x \in_p L$ whenever the value of x modulo p is in L. Similarly, we will denote $x =_p y$ and $x \neq_p y$ when $x = y$ modulo p and $x \neq y$ modulo p respectively.

In this lecture we will study L-intersecting families. Let $\mathcal{F} \subseteq \mathcal{P}([n])$ be a family of subsets of $[n]$. We say that $\mathcal{F}$ is L-intersecting if for any two sets in $\mathcal{F}$, $A \neq B \in \mathcal{F}$, it holds that $|A \cap B| \in L$. We will also consider a modular version of this notion. For a prime p we say that $\mathcal{F}$ is L intersecting modulo p if for any two sets $A \neq B \in \mathcal{F}$, it holds that $|A \cap B| \in_p L$. We will distinguish the case where all the sets in $\mathcal{F}$ have the same size k, in which case we say that $\mathcal{F}$ is k-uniform, and the case where not all sets in $\mathcal{F}$ have the same size, in which case we will say that $\mathcal{F}$ is not uniform.

The classic Ray-Chaudhuri–Wilson theorem gives an upper bound on the size of L intersecting families. Their theorem speaks about the non-uniform modular case.

Theorem 1 (Ray-Chaudhuri–Wilson)**.** *Let $\mathcal{F} \subseteq \mathcal{P}([n])$ be a family of subsets of $[n]$ and $L \subseteq \mathbb{N}$ such that $\forall A_i \neq A_j \in \mathcal{F}$, $|A_i \bigcap A_j| \in_p L$. Then $|\mathcal{F}| \leq \binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{|L|}$.*

For the proofs we will consider spaces of *multilinear* polynomials. A polynomial is multilinear if no variable appears with degree larger than 1. I.e., those are the polynomials that are spanned by the set of monomials $X_I = \prod_{i \in I} x_i$, where I ranges over all subsets of $[n]$. We first prove the following elementary fact.

Fact 2. *1. The dimension of the space of multilinear polynomials is 2^n. The dimension of the space of all multilinear polynomials of degree at most s is $sum_{i=0}^{s}\binom{n}{i}$.*

2. For every function $f : \{0,1\}^n \to D$ there exists an n-variate multilinear polynomial $f_M : \{0,1\}^n \to D$ that is equal to f. Furthermore, if f is a polynomial then $\deg(f_M) \leq \deg(f)$.

Proof. We first prove (2). Define $\forall v \in \{0,1\}^n$, $g_v(x) = \prod_{i=1}^{n}(x_i - (1 - v_i))$. Observe that

$$g_v(x) = \begin{cases} 0 & \text{if } x \neq v \\ \pm 1 & \text{if} x = v \end{cases}.$$

Hence, if we define

$$f_M(x_1, \ldots, x_n) \triangleq \sum_{v \in \{0,1\}^n} g_v(x) \cdot g_v(v) \cdot f(v)$$

then we have that f_M is a multilinear polynomial and for all $u \in \{0,1\}^n$ it holds that, $f_M(u) = \sum_{v\in\{0,1\}^n} g_v(u) \cdot g_v(v) \cdot f(v) = g_u(u) \cdot g_u(u) \cdot f(u) = f(u)$.

For the furthermore part, if f is a polynomial then replace each occurrence of x_i^k, for some $k > 1$ with x_i. It is clear that the value of each monomial remains the same on inputs from the Boolean cube.

To prove (1) we note that by definition the space of multilinear polynomials is spanned by the 2^n monomials X_I. To prove they are linearly independent we observe that the polynomials g_v defined above are linearly independent. Indeed, for $v, u \in \{0,1\}^n$, $g_v(u) \neq 0$ if and only if $v = u$. Thus, the dimension of the space of multilinear polynomials is at least 2^n and hence equal to 2^n. It follows that the X_I are linearly independent. The claim about the dimension of polynomials of degree at most s now follows by counting the number of monomials X_I of degree at most s and observing that it equals the number of subsets of $[n]$ of size $|I| \leq s$. □

We note that the above fact holds over any field. That is, f can be a polynomial from $\mathbb{F}_p$ to $\mathbb{F}_p$ and if we define f_M as above then we will get that when restricted to $\{0,1\}^n \subseteq \mathbb{F}_p^n$, f and f_M agree.

The first theorem that we prove is by Deza, Frankl and Singhi. It gives a modular (over $\mathbb{F}_p$) and non-uniform (not all sets have the same size) version of Ray-Chaudhuri–Wilson theorem.

Theorem 3 (modular, non-uniform R-W)**.** *Let p be a prime number and L a subset of the integers such that $|L| = s$. Let $\mathcal{F} = A_1, \ldots, A_m \subseteq \mathcal{P}([n])$ be a family of subsets of $[n]$ such that the following conditions hold:*

1. $\forall i,\ |A_i| \notin_p L$.
2. $\forall i \neq j,\ |A_i \cap A_j| \in_p L$.

Then, $|F| \leq \sum_{i=0}^{s} \binom{n}{i}$.

The idea of the proof is to construct, for every element $A \in \mathcal{F}$ a polynomial f_A such that if v is the characteristic vector of some set in $\mathcal{F}$ then $f_A(v) \neq 0$ if and only if v is the characteristic vector of A. This implies that the f_A are linearly independent. The construction will have the additional property that all the polynomials f_A have low degree. Since we only care about inputs from $\{0,1\}^n$ we can consider the multilinearization of each f_A. The result then follows by computing the dimension of the space of multilinear polynomials of small degree.

Proof. Let v_i be the characteristic vector of A_i, i.e., $(v_i)_j = 1 \iff j \in A_i$. It is clear that $\langle v_i, v_j \rangle = |A_i \bigcap A_J|$. Let $f_i(x) = \prod_{\ell\in L} (\langle x, v_i\rangle - \ell)$ be a polynomial over $\mathbb{F}_p$. Denote with f_i' the multilinearization of f_i (as a polynomial in the variables $x = (x_1, \ldots, x_n)$). We note that for $i \neq j$, $\prod_{\ell\in L} (\langle v_j, v_i\rangle - \ell) = 0$. In addition, since $|A_i| \notin_p L$ and p is prime, we conclude $\prod_{\ell\in L} (\langle v_i, v_i\rangle - \ell) \neq 0$. Therefore,

$$f_i(v_j) = \begin{cases} =_p 0 & i \neq j \\ \neq_p 0 & i = j \end{cases}.$$

This implies that the polynomials $\{f_i\}_{i=1}^m$ are linearly independent. Furthermore, as the evaluation points where taken from $\{0,1\}^n$ we conclude that the same is true for $\{f_i'\}_{i=1}^m$. This means $|\mathcal{F}| = \dim(\mathrm{Span}\{f_1', \ldots, f_m'\})$. Moreover, since $\deg(f_i') \leq \deg(f_i) = |L| = s$, we get that $\dim(\mathrm{Span}\{f_1', \ldots, f_m'\}) \leq \sum_{i=0}^{s} \binom{n}{i}$. This concludes the proof. □

As immediate corollary we get the following non-modular and uniform weak-version of R-W theorem. We call such a result weak as we shall later see that in the uniform case one only needs the term $\binom{n}{s}$ in the upper bound on $\mathcal{F}$.

Corollary 4 (non-modular, uniform R-W)**.** *Let $\mathcal{F} \subseteq \mathcal{P}([n])$ be a k-uniform family and $L \subseteq \mathbb{N}$ a set of $|L| = s$ integers. Assume that $\mathcal{F}$ is L-intersecting. Then $|\mathcal{F}| \leq \sum_{i=0}^{s} \binom{n}{i}$.*

Proof. Assume w.l.o.g. that $L \subseteq [k-1]$ (since elements of $\mathcal{F}$ are k-uniform, their intersections belong to $\{0, \ldots, k-1\}$). Let p be a large prime number, say, $p > n$. The result now follow from Theorem 3. □

Next we prove a non-modular, non-uniform version.

Theorem 5 (non-modular, non-uniform RW)**.** *Let $\mathcal{F} \subseteq \mathcal{P}([n])$ be L-intersecting for a subset $L \subseteq \mathbb{N}$ of size $|L| = s$. Then $|\mathcal{F}| \leq \sum_{i=0}^{s} \binom{n}{i}$.*

Recall that the crux of the proof of Theorem 3 was showing that the f_i' are linearly independent. One way of interpreting what we did is to consider the matrix

$$M = \begin{array}{c} \\ f_1 \\ f_2 \\ \vdots \\ f_m \end{array} \begin{array}{c} \begin{array}{cccc} A_1 & A_2 & \ldots & A_m \end{array} \\ \begin{pmatrix} f_1(A_1) & f_1(A_2) & \ldots & f_1(A_m) \\ f_2(A_1) & f_2(A_2) & \ldots & f_2(A_m) \\ \vdots & \vdots & \ddots & \vdots \\ f_m(A_1) & f_m(A_2) & \ldots & f_m(A_m) \end{pmatrix} \end{array}.$$

This matrix can be represented as

$$M = \begin{array}{c} \\ f_1 \\ f_2 \\ \vdots \\ f_m \end{array} \begin{array}{c} \begin{array}{cccc} A_1 & A_2 & \ldots & A_m \end{array} \\ \begin{pmatrix} \neq 0 & 0 & \ldots & 0 \\ 0 & \neq 0 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & \neq 0 \end{pmatrix} \end{array}.$$

From this representation it is clear that M has full rank. It is also clear that the rank of M is upper bounded by the dimension of the span of the f_i', which is what we wanted to show. For the proof of Theorem 5 we will have a different matrix M', that again will rise from evaluation of polynomials at characteristic vectors. This matrix will satisfy

$$M' = \begin{pmatrix} \neq 0 & * & \ldots & * \\ 0 & \neq 0 & \ldots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & \neq 0 \end{pmatrix},$$

which also implies that M' has full rank. We obtain such a matrix by defining polynomials f_i that satisfy the condition $f_i(v_j) = 0$ when $i > j$ (we have no control of $i < j$). This is somehow less limiting and this is the main difference from the proof of Theorem 3.

Proof. Assume, w.l.o.g., that $|A_1| \leq |A_2| \leq \cdots \leq |A_m|$, and let $f_i(x) = \prod_{\ell \in L,\, \ell < |A_i|} (\langle x, v_i \rangle - \ell)$. Since $\langle v_i, v_i \rangle = |A_i|$, we obviously get $f_i(v_i) \neq 0$. In addition, for $j < i$, it holds that

$$f_i(v_j) = \prod_{\ell \in L,\, \ell < |A_i|} (|A_i \cap A_j| - \ell) = 0.$$

Indeed, as $|A_j| \leq |A_i|$ and $A_i \neq A_j$ we have that $|A_i \cap A_j| < |A_i|$. For $i < j$ we do not have any information about the size of the intersection, but this does not affect us. We thus get the following matrix representing the value of f_i at point v_j:

$$M = \begin{pmatrix} \neq 0 & * & \dots & * \\ 0 & \neq 0 & \dots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \neq 0 \end{pmatrix}.$$

Clearly, M has full rank, thus $\text{rank}(M) = |\mathcal{F}| = m$. In particular all the polynomials f_i are linearly independent. Since $\deg(f_i) \leq s$, the result follows in the same manner as before. Note that this bound is tight as the example $\mathcal{F} = \{A| \ |A| \leq s\}$ demonstrates. □

Next we prove a stronger version of Corollary 4, which achieves an upper bound of $\binom{n}{s}$ on the size of $\mathcal{F}$, when $\mathcal{F}$ is a uniform family.

Theorem 6 (uniform non-modular RW)**.** *Let $\mathcal{F} \subseteq \mathcal{P}([n])$ be a k-uniform family that is L-intersecting for a subset $L \subseteq \mathbb{N}$ of size $|L| = s$. Then $|\mathcal{F}| \leq \binom{n}{s}$.*

The idea of the proof is the following: We already proved in Corollary 4 that $|\mathcal{F}| \leq \sum_{i=0}^{s} \binom{n}{i}$. We shall exhibit $\sum_{i=0}^{s-1} \binom{n}{i}$ additional multilinear polynomials that are linearly independent of our f_i, and that have degree at most s. The fact that $\mathcal{F}$ is k-uniform will play an important role in defining these polynomials. In the following proof we denote by $\mathbb{1}_I$ the characteristic vector of a subset $I \subseteq [n]$.

Proof. We can assume w.l.o.g. that $k \notin L$ and $s < k$ (because $\forall A \neq B \in \mathcal{F}$, $|A \cap B| < |A| = k$. Thus we can assume $L \subseteq [k-1]$). As before we denote $\mathcal{F} = \{A_1, \dots, A_m\}$ and let v_i be the characteristic vector of A_i. We also set $f_i = \prod_{\ell \in L} (\langle x, v_i \rangle - \ell)$.

Next we shall define a new set of polynomials. For each subset $I \subseteq [n]$ we have the corresponding monomial $X_I = \prod_{i \in I} x_i$. We note that for $J \in \{0,1\}^n$,

$$X_I(\mathbb{1}_J) = \begin{cases} 1 & \text{if } I \subseteq J \\ 0 & \text{if } I \nsubseteq J \end{cases}.$$

For each $|I| < s$, let $g_I = X_I(\sum_{i=1}^{n} x_i - k)$. It is clear that the number of different g_I corresponds to the number of subsets of size smaller than s, which equals $\sum_{j=0}^{s-1} \binom{n}{i}$.

We shall now show that the set $\{f_i\}_{i=1}^m \cup \{g_I\}_{|I|<s}$ is linearly independent.

Claim 7. *$f_1, \dots, f_m$, $\{g_I\}_{|I|<s}$ are linearly independent as functions over the set $\{0,1\}^n$.*

Proof. Suppose $h = \sum_{i=1}^{m} \alpha_i f_i + \sum_{|I|<s} \beta_I g_I = 0$. Our goal is showing that, for every i, I, $\alpha_i = 0$ and $\beta_I = 0$. Since $h = 0$ we have $h(v_j) = 0$. Thus,

$$0 = \sum_{i=1}^{m} \alpha_i f_i(v_j) + \sum_{|I|<s} \beta_I g_I(v_j).$$

From k-uniformity it follows that $g_I(v_j) = 0$ for all j. This implies that for every j, $\sum_{i=1}^{m} \alpha_i f_i(v_j) = 0$. As before, $\sum_{i=1}^{m} \alpha_i f_i(v_j) = \alpha_j f_j(v_j)$. Since $f_j(v_j) \neq 0$, we obtain $\alpha_j = 0$, for every j. Hence,

$$h = \sum_{|I|<s} \beta_I g_I = 0.$$

Consider the following matrix M whose rows and columns are indexed by subsets of $[n]$ of size smaller than s. In position (I, J) we have $g_I(\mathbb{1}_J)$. Clearly, $M_{I,J} = 0$ if $I \not\subseteq J$, and $M_{I,I} \neq 0$. We shall assume for simplicity that the sets are ordered according to size. We thus have

$$M = \begin{array}{c} \\ g_\emptyset \\ \vdots \\ g_I \\ \vdots \end{array} \begin{array}{c} \begin{array}{cccc} \emptyset & \dots & J & \dots \end{array} \\ \begin{pmatrix} \neq 0 & * & \dots & * \\ 0 & \neq 0 & \dots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \neq 0 \end{pmatrix} \end{array}$$

so clearly M has full rank. In particular, the g_I are linearly independent. As $h = \sum_{|I|<s} \beta_I g_I = 0$ we deduce that $\beta_i = 0$, for every i. This concludes the proof of the theorem. □

We continue with the proof of the theorem. By taking the multi linearizations f_i', g_I', they are still independent over $\{0,1\}^n$. Also remember that they live in a $\sum_{i=0}^{s} \binom{n}{i}$ dimensional space. By recalling that $|\{g_I\}| = \sum_{j=0}^{s-1} \binom{n}{i}$, we get $|\mathcal{F}| \leq \binom{n}{s}$. Notice this bound is tight: take $L = \{0, \dots, s-1\}$, $\mathcal{F} = \{A \mid |A| = s\}$.

□

Next we state a strong version of the modular R-W theorem. Assuming k-uniformity, one can achieve the same bound as in the non-modular version.

Theorem 8 (Modular Uniform RW:)**.** *Let p be a prime, $L \subseteq \mathbb{N}$, $|L| = s$, s.t. $s \leq p-1$, $\mathcal{F} \subseteq \mathcal{P}([n])$, L-intersecting and k-uniform s.t. $k \notin L \bmod p$, $k + s < n$, Then $|\mathcal{F}| \leq \binom{n}{s}$.*

We shall omit the proof. The high level idea is to first define the usual polynomials f_i, satisfying $f_i(v_j) = \delta_{i,j}$, and then to define another set of polynomials that together with the f_i form an independent set. Exact details can be found at [BF92].

Applications

We will now present some applications of the RW theorems. We will use the RW theorems to get a lower bound of the chromatic number of the unit distance graph, and also to construct Ramsey graphs that (constructively!) show that the Ramsey number grows super-polynomialy.

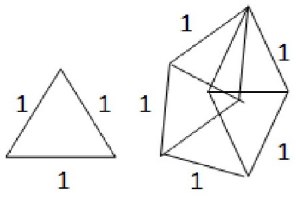

Figure 1: Showing that $\chi(G_2) > 2$, $\chi(G_2) > 3$.

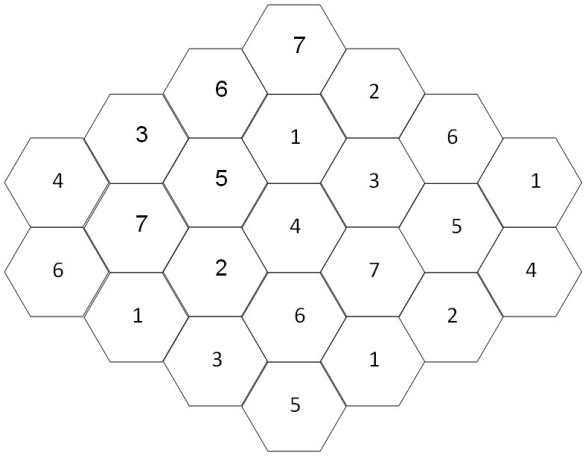

Figure 2: Showing that $\chi(G_2) \leq 7$.

Unit-Distance graph

Consider the unit distance graph in $\mathbb{R}^d$: we connect x and y with an edge if and only if $|x-y| = 1$. We denote this graph with G_d. The question that we are interested in concerns coloring ov the vertices of the infinite graph G_d. Recall that a coloring of a graph G with k colors is a function $c : V(G) \to [k]$ such that any two neighbors get distinct colors, that is, $\forall (v, u) \in E(G)$, $c(v) \neq c(u)$. We denote the chromatic number of G, $\chi(G)$, to be $\chi(G) = \min(\{k \mid G \text{ can be colored by } k \text{ colors}\})$. We ask what is the chromatic number $\chi(G_d)$?

The simplest case is the case $d = 2$, i.e., the unit distance graph in the plane. Figure 1 shows that $\chi(G_2) > 3$. It is also not very difficult to get a coloring of G_2 with 7 colors, by dividing the plane to hexagons (entrapped in unit circles), as Figure 2 shows. Thus $4 \leq \chi(G_2) \leq 7$. It is an intriguing open problem to close the gap. Interestingly, the exact number may depend on the set of axioms of set theory that one works with (see [SS04]).

What about higher values of d? E.g., what is the asymptotic value of $\chi(G_d)$ when d grows? We will prove exponential (in d) upper and lower bounds on $\chi(G_d)$.

First we give an upper bound of order $\exp(d)$ for the d-dimensional case. Assume that $\{x_1, x_2, \dots\}$ is a maximal collection of points in $\mathbb{R}^d$, with respect to inclusion, satisfying $\forall i \neq j \ |x_i - x_j| \geq \frac{1}{2}$. Greedily, we color the open balls of radius $\frac{1}{2}$ around each x_i, which we denote $B(x_i, \frac{1}{2})$. That is, we use a new color only if we cannot color that ball with any color that we already used. Further, if a point was colored already we do not recolor it. It is clear that this is a legal coloring of all points

in the union of those balls. We now wish to estimate the number of distinct colors needed for this greedy coloring.

To bound this number we make a few observations. Given a point x_i, we need to understand the number of balls $B(x_j, \frac{1}{2})$ that may effect the color of the ball around x_i. Consider a point $p_1 \in B(x_i, \frac{1}{2})$. Let p_2 be another point at distance 1 from p_1, that was already colored. In particular, there exists another point x_j such that $p_j \in B(x_j, \frac{1}{2})$. Thus, by the triangle inequality this implies

$$|x_1 - x_2| \leq |x_1 - p_1| + |p_1 - p_2| + |p_2 - x_j| < 2.$$

In particular, all the bad centers x_j belong to the ball $B(x_i, 2)$. Our goal is then to understand how many points x_j belong to that ball. We first note that the open balls with radius $\frac{1}{4}$ around the different x_j, $B(x_j, \frac{1}{4})$, are disjoint. Indeed, otherwise there would be two different centers of distance smaller than $1/2$. It follows that all the balls $B(x_j, \frac{1}{4})$ are contained in the ball $B(x_i, 9/4)$. Thus, a clear upper bound on the number of points x_j that belong to $B(x_i, 2)$ is $\mathrm{vol}(B(x_i, 9/4))/\mathrm{vol}(B(x_j, 1/4)$. Notice that this ratio equals 9^d, for balls in $\mathbb{R}^d$. As x_i it self is one of the points in the ball, we see that 9^d colors suffice for coloring. Indeed, since there will be at most $9^d - 1$ conflicting colors, for each x_i, the greedy algorithm can also find a good color.

We shall now prove an $\exp(d)$ lower bound by applying the R-W theorem. Specifically, we shall prove $\chi(G_d) \geq 1.2^d$

We shall construct a subset of the d-dimensional cube that cannot be colored with fewer than $\exp(d)$ many colors. For the construction we first interpret distances between characteristic vectors in term of size of intersections.

Let $A, B \subset [d]$ be sets of size exactly k, for some $0 \leq k \leq d$. Let$v_A, v_B \in \{0,1\}^d$ be their corresponding characteristic vectors. Then $\|v_A - v_B\|^2 = |A \Delta B| = |A| + |B| - 2|A \cap B| = 2(k - |A \cap B|)$. In particular, the distance between the characteristic vectors only depends on $|A \cap B|$.

Let p be a prime number, $d = 4p - 1$ and $k = 2p - 1$. Instead of looking at the unit distance graph it will be more convenient (for notation reasons) to consider the δ-distance graph for $\delta = \sqrt{2p}$. Indeed, this is isomorphic to the unit-distance graph. Notice that $\delta^2 = \sqrt{2p} = 2(k - (p-1))$. In particular, for two sets of size k, A and B, we have $\|v_A - v_b| = \delta$ if and only if $|A \cap B| = p - 1$.

Let us consider the set of all subsets of d of size k. A coloring of the δ-distance graph with m colors thus corresponds to a partition of $\binom{[d]}{k}$ to m families $\mathcal{F}_1, \ldots, \mathcal{F}_m$, where $\mathcal{F}_i$ is the set of all characteristic vectors that were colored with color i, such that for every $i \in [m]$ and every $A, B \in \mathcal{F}_i$, $|A \cap B| \neq p - 1$ (i.e., there is no edge between same color vectors).

We will show, using the R-W theorem, that for all i, $|\mathcal{F}_i| \leq \binom{d}{p-1}$. This clearly implies

$$m \geq \frac{\binom{d}{k}}{\binom{d}{p-1}} = \exp(d).$$

Tuning the parameters yields the result. We now give the details of the proof.

Proof. Let $\mathcal{F} = \mathcal{F}_i$ for some i. Clearly, $\mathcal{F}$ is a k-uniform family. Let $L = \{0, \ldots, p-2\}$. We have that $|A| = k = 2p - 1 \notin_p L$ and for every $A, B \in F_i$, the intersection satisfies $|A \cap B| \in_p L$, Indeed, the intersection size has to be smaller than $|A| = k = 2p - 1$. Furthermore, it cannot be of size $p - 1$ because of the coloring property - if it was $p - 1$ then A and B have an edge between them and hence cannot belong to the same color class. Thus, $|A \cap B| \in_p L$. Theorem 8 implies that $|\mathcal{F}| \leq \binom{d}{p-1}$. We thus have,

$$m \geq \frac{\binom{d}{k}}{\binom{d}{p-1}} = \frac{\binom{4p-1}{2p-1}}{\binom{4p-1}{p-1}} = \exp(p) = \exp(d).$$

□

Construction of a Ramsey Graph

We shall now see a two-coloring of the complete graph that does not have large monochromatic cliques.

Construction 9 (Frankel-Wilson Construction of Ramsey graph.)**.** *Let p be a prime number and $n = p^3$. We identify the vertices of our graph, V, with all subsets of $[n]$ of size $p^2 - 1$. That is, $V = \binom{[n]}{p^2-1}$. We color the edge (A, B) blue if and only if $|A \cap B| \equiv_p p - 1$. Otherwise we color it red.*

A red clique is a $(p^2 - 1)$-uniform family $\mathcal{F}$ such that for all $A \neq B \in \mathcal{F}$, $|A \cap B| \not\equiv_p p - 1$. In particular, $\mathcal{F}$ is L-intersecting for $L = \{0, \ldots, p - 2\}$. By Theorem 8, $|\mathcal{F}| \leq \binom{n}{p-1}$.

A blue clique is a $(p^2 - 1)$-uniform family $\mathcal{F}$ such that for all $A \neq B \in \mathcal{F}$, $|A \cap B| \equiv_p p - 1$. Thus, it is L-intersecting for $L = \{p - 1, 2p - 1, \ldots, (p - 1)(p - 1)\}$. In particular, $|L| = p - 1$. From Theorem 6 we get $|\mathcal{F}| \leq \binom{n}{p-1}$.

To make better sense of the parameters, denote with t the size of the maximal clique. Hence, $t < \binom{n}{p-1} = \binom{p^3}{p-1} \approx p^{2p}$. Therefore, $p \approx \frac{1}{2} \log t / \log \log t$. Expressing the number of vertices as a function of t we get $|V| = \binom{n}{p^2-1} = \binom{p^3}{p^2-1} \approx p^{p^2} = t^{\Omega(\log t / \log \log t)} = 2^{\Omega(\log^2 t / \log \log t)}$. This is still significantly less than what a random construction gives ($|V| = 2^{\Omega(t)}$) but it is a great improvement to the construction of Nagy for which $|V| = O(t^3)$.

The best known construction is by Barak et al. [BRSW06] who constructed a graph on roughly $2^{2^{\log \log^{1+\epsilon} t}}$ many vertices.

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. 3-5, 3-8

[BRSW06] Boaz Barak, Anup Rao, Ronen Shaltiel, and Avi Wigderson, *2-source dispersers for sub-polynomial entropy and ramsey graphs beating the frankl-wilson construction*, Proceedings of the 38th Annual ACM Symposium on Theory of Computing, Seattle, WA, USA, May 21-23, 2006, 2006, pp. 671–680. 3-8

[SS04] Alexander Soifer and Saharon Shelah, *Axiom of choice and chromatic number: examples on the plane*, J. Comb. Theory, Ser. A **105** (2004), no. 2, 359–364. 3-6