CS395T Pseudorandomness and Combinatorial Constructions
Lecturer: Prof. David Zuckerman, Presenter: Peiyush Jain

1 An Explicit Construction of Large Ramsey Graphs

Given a number t, we wish to construct a graph G on N vertices with no clique or an independent of size t such that N is as large as possible.

Erdős showed the existence of such a graph with $N = 2^{t/2}$.
Nagy gave an explicit construction with $N = O(t^3)$.

We will look at a construction which gives $N = t^{\omega(t)}$ where $\omega(t) \to \infty$ as $t \to \infty$. The approach is to construct the graphs via intersection theorems.

2 Non Uniform Modular RW Theorem

First we need some definitions.

Definition 1 *A family of sets $\Im = \{A_1, A_2, \cdots, A_m\}$ of subsets of a set of n elements is k-*uniform *if*

$$|A_i| = k \quad \forall i \in [m]$$

Definition 2 *Let L be set of s integers. A family of sets $\Im = \{A_1, A_2, \cdots, A_m\}$ of subsets of a set of n elements is L-*intersecting *if*

$$|A_i \cap A_j| \in L \quad \forall\ i \neq j$$

Definition 3 *For a set $L \subset \mathbf{Z}$ and integers r, t we shall say*

$$t \in L \pmod{r}$$

if $t \equiv l \pmod{r}$ *for some $l \in L$. The negation of this statement will be written as* $t \notin L \pmod{r}$

Definition 4 *A polynomial is multilinear if it has degree ≤ 1 in each variable.*

Definition 5 *A monic multilinear polynomial is the product of distinct variables.*

Every multilinear polynomial of degree $\leq s$ can be written as a linear combination of monic multilinear polynomials of degree $\leq s$. There are exactly $\binom{n}{k}$ monic multilinear polynomials in n variables of degree k. Before we move onto the main result of this section, we will need the following Lemma.

Lemma 1 *(***Multilinearization***) Let $\mathbf{F}$ be a field and $\Omega = \{0,1\}^n \subseteq \mathbf{F}^n$. If f is polynomial of degree $\leq s$ in n variables over $\mathbf{F}$ then there exists a multilinear polynomial $\tilde{f}$ of degree $\leq s$ in the same variables such that*

$$f(x) = \tilde{f}(x) \quad \forall x \in \Omega$$

Proof: Just expand f and use the identity ${x_i}^2 = x_i$, valid over Ω. $\square$

Now the main result.

Theorem 1 (Non Uniform modular RW theorem) (Deza-Frankl-Singhi,1983) *Let p be a prime and L a set of s integers. Assume $\Im = \{A_1, A_2, \cdots, A_m\}$ is a family of subsets of $[n]$ such that*

1. $|A_i| \notin L \pmod p \quad \forall i \in [m]$
2. $|A_i \cap A_j| \in L \pmod p \quad \forall i \neq j$

Then,

$$|\Im| = m \leq \sum_{k=0}^{s} \binom{n}{k}$$

Proof: (Alon-Babai-Suzuki, 1991)
Consider the polynomial $F(x, y)$ in 2n variables; with $x, y \in \mathbf{F}_p^n$, such that

$$F(x, y) = \prod_{l \in L} (x \cdot y - l)$$

where $x \cdot y = \sum_{i=1}^{n} x_i y_i$ is the standard inner product in $\mathbf{F}_p^n$.
Let $v_i \in \mathbf{F}_p^n$ be the incidence vector of A_i, i.e $v_i = (x_1, x_2, \cdots, x_n)$ where $x_r = 1$ if $r \in A_i$ and $x_r = 0$ if $r \notin A_i$. Now consider the n-variable polynomials $f_i(x) := F(x, v_i)$. It is clear from the conditions that,

$$f_i(v_j) = \begin{cases} \neq 0 & \text{if} \quad i = j; \\ = 0 & \text{if} \quad i \neq j. \end{cases}$$

By the Multilinearization Lemma, these equations remain valid if we replace f_i by the corresponding multilinear polynomials $\tilde{f}_i$. We now show that these $\tilde{f}_i$ are linearly independent.
Suppose,

$$\sum_{i=1}^{n} \lambda_i f_i(x) = P(x) \equiv 0$$

say $\lambda_r \neq 0$. Then we have that, $P(v_r) = \lambda_r f_r(v_r)$, since $f_r(v_r) \neq 0$ it follows that $\lambda_r = 0$, a contradiction.
Notice that each $\tilde{f}_i$ is of degree $\leq |L| = s$. Each $\tilde{f}_i$ is a linear combination of monic multilinear polynomials of degree $\leq s$. Now these monic multilinear polynomials form the basis of a space of dimension $\sum_{k=0}^{s} \binom{n}{k}$. Hence we have that,

$$|\Im| = m \leq \sum_{k=0}^{s} \binom{n}{k}$$

$\square$

We will also need the following result.

Corollary 1 *Let L be a set of s integers and $\Im$ an L-intersecting k-uniform family of subsets of a set of n elements. Then*

$$|\Im| \leq \sum_{i=0}^{s} \binom{n}{i}$$

Proof: Since $\Im$ is k-uniform, all pairwise intersections have $\leq (k-1)$ elements, so we may assume that $k \notin L$. Now choose a prime $p > k$ and apply the previous theorem. $\square$

For $s \leq n/4$, it can be proved that

$$\sum_{k=0}^{s} \binom{n}{k} \; < \; 2 \cdot \binom{n}{s}$$

This inequality will be useful in the next section.

3 The Construction

Let p be a prime and let $n > 2p^2$. Set

$$V = \binom{[n]}{p^2-1},$$

the set of all subsets of $[n]$ of cardinality $p^2 - 1$. We construct a graph $G(n,p)$ on the vertex set V. We join two vertices $A, B \in V$ if

$$|A \cap B| \not\equiv -1 \pmod{p}$$

For $p = 2$, this graph becomes precisely the graph of Nagy.

We now show an upper bound on the size of a clique or independent set in $G(n,p)$.

Theorem 2 *The graph $G(n,p)$ has $\binom{n}{p^2-1}$ vertices and has no clique or independent set of size more than $2 \cdot \binom{n}{p-1}$.*

Proof: Assume $\Im = \{A_1, A_2, \cdots, A_m\}$ is the vertex set of a clique. Then we must have that $|A_i \cap A_j| \not\equiv -1 \pmod{p}$ for any $i \neq j$. Now $\Im$ is a set system satisfying the conditions of Theorem 1 with $s = p-1$ and $L = \{0, 1, \cdots, p-2\}$. Hence

$$m \leq \sum_{k=0}^{p-1} \binom{n}{k}$$

Since $s = p - 1 \leq n/4$, we have that

$$m \leq 2 \cdot \binom{n}{p-1}$$

Now Suppose that $\Im$ is the vertex set of an independent set. Then we have that, for every $i \neq j$, $|A_i \cap A_j| \in L$ where $L = \{p-1, 2p-1, \cdots, p^2-p-1\}$. Also, the size of each A_i is $p^2 - 1$. By Corollary 1, it follows that

$$m \leq 2 \cdot \binom{n}{p-1}$$

$\square$

Corollary 2 *Let $\omega(t) = \ln t/(4 \ln\ln t)$. For every $\epsilon > 0$ and sufficiently large t, one can construct an explicit graph on more than*

$$t^{(1-\epsilon)\omega(t)}$$

vertices with no clique or independent set of size more than t.

Proof: We just have to select suitable n and p. Let $n = p^3$. Select p to be largest prime such that $\binom{p^3}{p-1} < t$. For every $\delta > 0$ and large enough t, this prime will be between $(1 \pm \delta) \ln t/(2 \ln\ln t)$, using the Prime Number Theorem and elementary estimates of the binomial coefficients. A calculation of $\binom{n}{p^2-1}$ using this p gives us the result. $\square$