DD2442 AUTUMN 2014 LECTURE 3

RI

Frank P Ramsey (1903-1930)
British mathematician
Died already at the age of 26 but produced work in a wide range of areas.
Among other things, founded what is now called RAMSEY THEORY

Loosely put, studies order in complex systems
Metastatement: "Complete disorder is impossible"
Here is a classic example

PROP 1 Among any six people, there are three people all of whom are friends or three people such that none of them are friends.

(This is assuming friendship is a symmetric relation)

Just a graph-theoretic statement

$G = (V, E)$ undirected graph, edges $E \subseteq V \times V$

$U \subseteq V$ is a CLIQUE if $\forall u,v \in V, u \neq v, (u,v) \in E$
$U \subseteq V$ is an INDEPENDENT SET if $\forall u \neq v \in U\ (u,v) \notin E$

PROP 1' Any graph on 6 vertices has a clique or independent set of size 3.

Proof Fix any vertex $v \in V$. Two cases:

1) $\deg(v) \geq 3$. Let x, y, z be neighbours of v. If any two of them are friends, say x, y, then $\{v, x, y\}$ is a triangle / 3-clique. Otherwise $\{x, y, z\}$ is an independent set.

2) $\deg(v) \leq 2$. Let x, y, z be non-neighbours of v. If x, y, z are all friends, then they form a triangle. Otherwise, if, say, x, y are not friends, then $\{v, x, y\}$ is an independent set. $\boxed{\text{E}}$

Graph on n vertices with edges and non-edges

$\Updownarrow$

Complete graph K_n with 2-colouring of edges

Is there a monochromatic clique of a certain size?

DEF2 The RAMSEY NUMBER $R(s,t)$ is the minimum number n such that any graph on n vertices contains either an independent set of size s or a clique of size t.

The Ramsey number $R_k(s_1, \ldots, s_k)$ is the minimum number n such that any colouring of the edges of K_n with k colours contains a clique of size s_i in colour i for some i.

We will focus on $R(s,t)$.

First we have to argue that $R(s,t)$ is well-defined, i.e., that it is not ∞

We saw $R(3,3) \leq 6$; can prove $= 6$.

$R(4,4) = 18$ [1955]

$R(5,5)$ between 43 and 49 [1989], [1995]

$R(6,6)$ between 102 and 165 [1965], [~~165~~ 1994]

Erdős: If an alien force, vastly more powerful than us, lands on earth and demands to know the value of $R(5,5)$ or they will destroy our planet, then we should marshal all our computers and mathematicians and attempt to find the value. But if they ask about $R(6,6)$, we should attempt to destroy the aliens.

Let us prove that $R(s,t)$ is indeed finite.

<u>THM 3</u> (Ramsey's theorem*)
For any $s, t \in \mathbb{N}^+$ it holds that $R(s,t) \leq \binom{s+t-2}{s-1}$

*) stronger than Ramsey's original bound.

<u>Proof</u> By induction (and generalizing proof of Prop 1).

<u>Base case</u>: If $s=1$ or $t=1$, $R(s,t) = 1 = \binom{s+t-2}{s-1}$
(Every graph contains a clique and an independent set of size 1).

<u>Induction</u>: Let $n = R(s-1,t) + R(s,t-1)$ and consider any graph $G=(V,E)$ on n vertices. Fix some $v \in V$. We have two cases:

1) $\underline{\deg(v) \geq R(s,t-1)}$ Look at subgraph induced by neighbours of v. By induction, contains s-independent set or $(t-1)$-clique. In latter case, add v to get t-clique

2) $\underline{\deg(v) < R(s,t-1)} = n - R(s-1,t)$
Look at subgraph of size $\geq R(s-1,t)$ induced by non-neighbours. Contains either $(s-1)$-independent set or t-clique. In former case, can add v to get s-indep set.

Standard identity

$$\underbrace{\binom{n}{k}}_{\text{\# ways to choose } k \text{ elems}} = \underbrace{\binom{n-1}{k}}_{\text{\# ways to choose } k \text{ non-blue elems}} + \underbrace{\binom{n-1}{k-1}}_{\text{\# ways to choose blue elem} + k-1 \text{ other}}$$

Consider set of n elements; colour one of them blue

Using this, we get

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

$$\leq \binom{s+t-3}{s-2} + \binom{s+t-3}{s-1} = \binom{s+t-2}{s-1} \quad \boxed{\text{Lm}}$$

Asymptotic bounds on diagonal Ramsey numbers are something like

$$(\sqrt{2})^s \lessapprox R(s,s) \lessapprox 4^s$$

$$2^{s/2} \lessapprox R(s,s) \lessapprox 2^{2s}$$

Random graph on n vertices: No clique or IS significantly larger than $\log n$

Hence, given s, should be possible to construct Ramsey graph (graph without s-clique or s-independent set) on $\exp(\Omega(s))$ vertices.

AFAIK, state of the art nowhere near this.

Want to take a look at two nontrivial constructions (using algebra, of course)

Recall:

ODD-TOWN THEOREM
Let $\mathcal{F}$ family of subsets of $[n]$ s.t.
$\forall A \in \mathcal{F}$ $|A|$ odd, $\forall A, B \in \mathcal{F}, A \neq B$, $|A \cap B|$ even.
Then $|\mathcal{F}| \leq n$.

FISHER'S INEQUALITY
Let $\mathcal{F}$ family of non-empty subsets of $[n]$ s.t. $\forall A, B \in \mathcal{F}, A \neq B$, it holds that $|A \cap B| = k$ for some fixed k. Then $|\mathcal{F}| \leq n$.

Use this to construct Ramsey graph on $\Omega(s^3)$ vertices that doesn't contain clique or independent set of size s. (Not great, but still nontrivial)

<u>THM 4</u> For $s \in \mathbb{N}^+$, let G_s be the graph with vertices v labelled by triples $A_v = \{a, b, c\}$, $a, b, c \in [s]$, $a \neq b \neq c \neq a$ and edges between u and v if $|A_u \cap A_v| = 1$. Then G_s has $\Omega(s^3)$ vertices but does not contain any clique or IS larger than s.

RVI

Proof Number of vertices = # triples = $\binom{s}{3} = \Omega(s^3)$.
Suppose that $U \subseteq V(G)$ is a clique.
Then $\{A_u \mid u \in U\}$ is a family of subsets of $[s]$ s.t. $|A_u \cap A_v| = 1$. By Fisher's inequality, we have $|U| \leq s$

Suppose instead U independent set. Then $\{A_u \mid u \in U\}$ is a family s.t. $|A_u| = 3$ odd ~~but~~ and $|A_u \cap A_v| = 0$ or 2 even.
By Odd-town theorem, $|U| \leq s$. $\boxed{\checkmark}$

Want to do better - get Ramsey graph of size at least super polynomial in s.
To do so, back to extremal combinatorics (and algebra).

Last time considered 0/1 vectors.
For set $A \subseteq [n]$ 1_A vector s.t.

$$i\text{th coord of } 1_A = \begin{cases} 1 & \text{if } i \in A \\ 0 & \text{otherwise} \end{cases}$$

Could instead represent A by linear form

$$f_A(\vec{x}) = \sum_{i \in A} x_i$$

and reason in terms of linearly independent linear forms. Can go from linear forms to higher-degree (multivariate) polynomials

Polynomials of fixed total degree $\leq d$ form vector space
(One basis consists of monomials $x_1^{d_1} x_2^{d_2} \dots x_n^{d_n}$ of total degree $d_1 + d_2 + \dots + d_n \leq d$).
Then do same (simple) arguments as before about dimension and linear independence.

Some notation

Set of subsets of $[n]$ = powerset of $[n]$ = $2^{[n]}$
Set of all subsets of $[n]$ with k elements $\binom{[n]}{k}$

Consider family of sets $\mathcal{F} \subseteq 2^{[n]}$
Let $\mathcal{L} \subseteq \{0, 1, \dots, n\}$

We say that $\mathcal{F}$ is $\mathcal{L}$-INTERSECTING if $\forall A, B \in \mathcal{F}$, $A \neq B$, it holds that $|A \cap B| \in \mathcal{L}$.

Fisher's inequality: $|\mathcal{L}| = 1 \Rightarrow |\mathcal{F}| \leq n$.
This can be generalized

THM 5 (Frankl & Wilson 1981)
If $\mathcal{F} \subseteq 2^{[n]}$ is $\mathcal{L}$-intersecting, then

$$|\mathcal{F}| \leq \sum_{k=0}^{|\mathcal{L}|} \binom{n}{k}$$

REMARK All subsets of size $\leq \ell$ is an $\mathcal{L}$-intersecting family for $\mathcal{L} = \{0, 1, \dots, \ell - 1\}$ so Thm 5 is tight.

Proof Let $\mathcal{F} \subseteq 2^{[n]}$, $\mathcal{L} \subseteq \{0,1,\ldots,n\}$, $|\mathcal{L}| = s$. For all $A \neq B \in \mathcal{F}$ $|A \cap B| \in \mathcal{L}$ by assumption.
For every A we define a polynomial $f_A \in \mathbb{R}[x_1, x_2, \ldots, x_n]$ by

Yes! the real numbers!

$$f_A(x) = \prod_{\substack{l \in \mathcal{L} \\ l < |A|}} \left(\sum_{i \in A} x_i - l \right)$$

Total degree $\leq |\mathcal{L}|$.
We claim that $\{f_A \mid A \in \mathcal{F}\}$ are linearly independent. Suppose that $\sum_{A \in \mathcal{F}} \alpha_A f_A = 0$. $(*)$

Evaluate the polynomials on $1_A \in \mathbb{R}^n$

※ Start with set A of largest size.
For $B \neq A$ we get

$$f_A(1_B) = \prod_{\substack{l \in \mathcal{L} \\ l < |A|}} (|A \cap B| - l) = 0$$

$A \not\subseteq B$ because A largest size

because $|A \cap B| = l < |A|$ for some $l \in \mathcal{L}$.
For 1_A we get

$$f_A(1_A) = \prod_{\substack{l \in \mathcal{L} \\ l < |A|}} (|A| - l) = k_A > 0.$$

Thus, we can evaluate $p = \sum_{A' \in \mathcal{F}} \alpha_{A'} f_{A'}$ on 1_A to get

$$p(1_A) = \sum \alpha_{A'} f_{A'}(1_A) = \alpha_A k_A$$

which forces $\alpha_A = 0$ if p is to be the zero polynomial.
Now repeat from ※ for next set of largest size. In this way prove $\alpha_A = 0$ for all coeff.

Now we need to look at the dimension of the vector space. But here is a trick: Suppose we have a monomial

$$x_1 x_2^3 x_3^2$$

Since we only evaluated on $\{0,1\}^n$ above we can multilinearize to

$$x_1 x_2 x_3$$

removing higher powers

Consider multilinear polynomials

$$\{ \tilde{f}_A \mid A \in \mathcal{F} \}$$

These are also all linearly and form a vector space independent by the same argument. This means that

$\{ \tilde{f}_A \mid A \in \mathcal{F} \}$ is a lin indep set of vectors in vector space spanned by monomials $\prod_{i \in I} x_i \quad |I| \leq s = |L|$

Dimension of this space $\leq$ (in fact, $=$)
# of such monomials
$= \sum_{k=0}^{s} \binom{n}{k}$. The theorem follows. $\boxed{}$

By instead moving back to the finite fields that we will prefer to work with in this course, we can get a "modular version" of Thm 5.

THM 6 Let p be a prime and let $\mathcal{L} \subseteq \mathbb{F}_p$. Assume $\mathcal{F} \subseteq 2^{[n]}$ family of sets s.t.

- $|A| \notin \mathcal{L} \pmod p$ for $A \in \mathcal{F}$
- $|A \cap B| \in \mathcal{L} \pmod p$ for $A, B \in \mathcal{F}, A \neq B$

Then
$$|\mathcal{F}| \leq \sum_{k=0}^{|\mathcal{L}|} \binom{n}{k}$$

<u>Notation comment</u>

$|A| \equiv r \pmod p$ for unique $r \in \{0, 1, \dots, p-1\}$

$|A| \in \mathcal{L} \pmod p$ means $r \in \mathcal{L}$ and analogously for $|A| \notin \mathcal{L} \pmod p$

<u>Proof</u> Essentially the same as for Thm 5. Let $\mathcal{F} \subseteq 2^{[n]}$, $\mathcal{L} \subseteq \mathbb{F}_p$. For $A \in \mathcal{F}$ we define $f_A \in \mathbb{F}_p[x]$ by
$$f_A(\vec{x}) = \prod_{\ell \in \mathcal{L}} \left(\sum_{i \in A} x_i - \ell \right)$$

Doing all calculations in $\mathbb{F}_p$ we have
$$f_A(\mathbb{1}_B) = \prod_{\ell \in \mathcal{L}} (|A \cap B| - \ell) = 0$$
because $|A \cap B| \in \mathcal{L} \pmod p$, while
$$f_A(\mathbb{1}_A) = \prod_{\ell \in \mathcal{L}} (|A| - \ell) \neq 0$$
since $|A| \notin \mathcal{L} \pmod p$ (and $\mathbb{F}_p$ doesn't have zero divisors).

This also holds for multilinear versions $\{\tilde{f}_A \mid A \in \mathcal{F}\}$, and these polynomials again live in a vector space generated by $\sum_{k=0}^{|L|} \binom{n}{k}$ monomials. $\boxed{L}$

Before we saw a graph on $n = \binom{s}{3}$ vertices without cliques or independent sets of size larger than s. Now we can improve this to

$$n = s^{\Omega(\log s / \log\log s)}$$

Superpolynomial in s, but still far from $\exp(\Omega(s))$

THM 7 (Frankl & Wilson '81)
For any prime p there is a graph G_p on $n = \binom{p^3}{p^2-1}$ vertices such that any clique or independent set is of size at most $\sum_{i=0}^{p-1} \binom{p^3}{i}$

Standard inequalities

$$\left(\frac{n}{k}\right)^k \le \binom{n}{k} \le \left(\frac{ne}{k}\right)^k$$

yield

$$n \ge p^{p^2}$$

$$s = \sum_{i=0}^{p-1} \binom{p^3}{i} \le p \cdot \binom{p^3}{p} \lessapprox \left(\frac{p^3}{p}\right)^p = p^{2p} \approx p^p$$

Hence

$$n \gtrsim s^p \approx s^{\log s / \log\log s}$$

Proof Let vertices V of G be $\binom{[p^3]}{p^2-1}$, i.e., all subsets of $[p^3]$ of size p^2-1.
For two vertices u, v labelled by $A_u, A_v \in \binom{[p^3]}{p^2-1}$
Let (u,v) be an edge if $|A_u \cap A_v| \not\equiv p-1 \pmod{p}$.

Note that $|A_u| = p^2-1 \equiv p-1 \pmod{p}$.

If $\mathcal{U}$ is a clique, then $\{A_u \mid u \in \mathcal{U}\}$ satisfies

$$|A_u| \equiv p-1 \pmod{p}$$
$$|A_u \cap A_v| \not\equiv p-1 \pmod{p}$$

Setting $\mathcal{L} = \{0, 1, \ldots, p-2\}$ and applying Thm 6, we get $|\mathcal{U}| \leq \sum_{i=0}^{p-1} \binom{p^3}{i}$

If $\mathcal{U}$ is an independent set, then

$$|A_u \cap A_v| \equiv p-1 \pmod{p} \text{ for all } u \neq v \in \mathcal{U}.$$

That is

$$|A_u \cap A_v| \in \{p-1, 2p-1, \ldots, (p-1)p-1\}$$

Then $\{A_u \mid u \in \mathcal{U}\}$ is $\mathcal{L}$-intersecting for $\mathcal{L} = \{p-1, 2p-1, \ldots, (p-1)p-1\}$, $|\mathcal{L}| = p-1$, and Thm 5 yields

$$|\mathcal{U}| \leq \sum_{i=0}^{p-1} \binom{p^3}{i} \qquad \blacksquare$$

AFAIK Frankl Wilson remained
state of the art until Anup Rao 2006
with co-authors (two papers at STOC 2006)
who worked on problems related to
randomness extraction and derandomization