Linear Algebra Methods in Combinatorics

Arjun Khandelwal, Joshua Xiong

Mentor: Chiheon Kim

MIT-PRIMES Reading Group

May 17, 2015

Eventown and Oddtown

There are n inhabitants of **Even/Odd**town numbered $1, \ldots n$. They are allowed to form clubs according to the following rules:

- Each club has an **even** number of members
- Each pair of clubs share an even number of members
- No two clubs have identical membership

- Each club has an **odd** number of members
- Each pair of clubs share an even number of members
- No two clubs have identical membership

What is the maximum number of clubs that can be formed?

Eventown and Oddtown

There are n inhabitants of **Even/Odd**town numbered $1, \ldots n$. They are allowed to form clubs according to the following rules:

- Each club has an **even** number of members
- Each pair of clubs share an even number of members
- No two clubs have identical membership

- Each club has an **odd** number of members
- Each pair of clubs share an even number of members
- No two clubs have identical membership

What is the maximum number of clubs that can be formed?

$$2^{\lfloor n/2 \rfloor}.$$

Eventown and Oddtown

There are n inhabitants of **Even/Odd**town numbered $1, \ldots n$. They are allowed to form clubs according to the following rules:

- Each club has an **even** number of members
- Each pair of clubs share an even number of members
- No two clubs have identical membership

- Each club has an **odd** number of members
- Each pair of clubs share an even number of members
- No two clubs have identical membership

What is the maximum number of clubs that can be formed?

$2^{\lfloor n/2 \rfloor}$.

n.

Introduction

Vector space

- Set of vectors V over a field $\mathbb{F}$.

Example: $\mathbb{R}^2$ is a plane

Dot product / inner product

- If $v_1 = (a_1, \ldots, a_n)$ and $v_2 = (b_1, \ldots, b_n)$, then

$$v_1 \cdot v_2 = a_1 b_1 + a_2 b_2 + \ldots a_n b_n$$

Introduction

Basis

- A minimal set of vectors B that can be used to represent any vector $\mathbf{v}$ in a vector space V as the sum of scalar multiples of the elements in B.

Dimension

- Maximum number of linearly independent vectors in a vector space

Introduction

Linear independence

- Vectors v_1, . . . , v_m are linearly independent if

$$\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_m v_m = 0 \implies \lambda_i = 0 \quad \forall\, i$$

Theorem (Linear Algebra Bound)

If $v_1, \ldots, v_m \in \mathbb{F}^n$ are linearly independent, $m \leq n$.

Eventown and Oddtown

Proof for Oddtown:

- Each club can be associated with an incidence vector: $v_i = (a_1, \ldots, a_n)$, where $a_i = 1$ if person i is a club member.
- Note that $v_i \cdot v_j$ gives the intersection size of the vectors
  - $v_i \cdot v_j = 0$ iff $i \neq j$

Theorem

The incidence vectors are linearly independent in $\mathbb{F}_2$

- Suppose $\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_n v_n = 0$
- $v_i \cdot (\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_n v_n) = 0$
- $\lambda_i v_i \cdot v_i = 0 \implies \lambda_i = 0$

Polynomial Independence Criterion

The space of polynomials with degree $\leq d$ over a field $\mathbb{F}$ is a vector space like any other.
For a fixed d (in the single-variable case), take as a basis $1, x, x^2, \ldots, x^d$.

Theorem

Given polynomials $f_1, f_2, ..., f_m$ over a field $\mathbb{F}$ with elements of $\mathbb{F}$ $x_1, x_2, ..., x_m$ such that

$$f_i(x_i) \neq 0 \iff i = j$$

the f_i are linearly independent.

Polynomial Independence Criterion

Proof

- Suppose $\lambda_1, \lambda_2, ..., \lambda_m$ are scalars such that $\lambda_1 f_1(x) + \lambda_2 f_2(x) + ... + \lambda_m f_m(x) = 0$
- For an arbitrary $1 \leq j \leq m$, let $x = x_j$
- As $f_i(x_j) = 0$ if $i \neq j$, we are left with $\lambda_j f_j(x_j) = 0$
- As $f_i(x_i) \neq 0$, $\lambda_j = 0$

Nonuniform Modular Ray-Chaudhuri-Wilson Theorem

Theorem

Let p be a prime number and L a set of s elements of $\mathbb{Z}_p$. Suppose $F = \{A_1, A_2, \ldots, A_m\}$ is a family of subsets of [n] such that the following conditions hold.

- $|A_i| \mod p \notin L$
- $|A_i \cap A_j| \mod p \in L$ *if* $i \neq j$

Then

$$m \leq \binom{n}{s} + \binom{n}{s-1} + \cdots + \binom{n}{1} + \binom{n}{0}$$

Note that setting $P = 2$ and $L = \{0\}$ gives us the (slightly worse) bound of $m \leq n + 1$ for the Oddtown problem.

Nonuniform Modular Ray-Chaudhuri-Wilson Theorem

Proof

- Consider a polynomial $G(x, y)$, with $x, y \in \mathbb{F}_p^n$.
- We set $G(x, y) = \prod_{\ell \in L} (x \cdot y - \ell)$
- Now consider the n-variable polynomials $f_i(a) = G(x_i, a)$, where x_i is the incidence vector corresponding to A_i.
- Note that $f_i(x_j) \neq 0 \iff i = j$; thus, the f_i are linearly independent by our previous proposition.

Nonuniform Modular Ray-Chaudhuri-Wilson Theorem

Proof (Cont.)

- Still need to find a basis for the polynomials $G(x_i, a)$
- Each term in the expansion will be of the form $ca_1^{e_1}a_2^{e_2}\dots a_n^{e_n}$, with c constant and $e_1 + e_2 + \cdots + e_n \leq s$
- Thus, we have $m \leq \binom{n+s}{n}$
- Using the technique of multilinearization, we can obtain the better bound $m \leq \binom{n}{s} + \binom{n}{s-1} + \cdots + \binom{n}{1} + \binom{n}{0}$

Nonuniform Modular Ray-Chaudhuri Wilson Theorem

A Corollary

Corollary

Let L be a set of s integers and F a family of k-element subsets of a set of n elements with all pairwise intersection sizes in L. Then,

$$|F| \leq \binom{n}{s} + \binom{n}{s-1} + \cdots + \binom{n}{1} + \binom{n}{0}$$

As the size of the pairwise intersections is at most $k-1$ (as F is a k-uniform family), take a prime $p > k$ and apply the Nonuniform Modular Ray-Chaudhuri-Wilson Theorem.

Applications to Ramsey Graphs

Introduction

Graph Theory Basics

- A *graph* G consists of a vertex set V and an edge set E
- An *independence set* is a set of vertices of which no two members have an edge between them
- A *clique* is a set of vertices of which any two members have an edge between them

Ramsey Theory

- An r-Ramsey graph is a graph on n vertices with no clique or independent set of size $\geq r$.
- Question: given a certain r, how large can we make n?

Applications to Ramsey Graphs

Explicit Construction

We consider a graph G on $\binom{n}{p^2-1}$ vertices, with $n > 2p^2$, where we associate each vertex V_i with a p^2-1-subset A_i of $[n]$.
V_i and V_j are adjacent iff $|A_i \cap A_j| \neq -1 \mod p$.

Theorem

G is a $(2\binom{n}{p-1}+1)$-Ramsey graph on $\binom{n}{p^2-1}$ vertices.

Applications to Ramsey Graphs

Explicit Construction

Clique Size

- Assume $F = \{B_1, B_2, ..., B_m\}$ is the vertex set of a clique
- F is a family of k-element subsets of n elements
- F satisfies the conditions of the Modular RCW-theorem with $L = \{0, 1, 2, ..., p-2\}$ and $s = p - 1$
- $|F| \leq \binom{n}{s} + \binom{n}{s-1} + \cdots + \binom{n}{1} + \binom{n}{0} \leq 2\binom{n}{p-1}$

Applications to Ramsey Graphs

Explicit Construction

Independent Set Size

- Assume $F = \{B_1, B_2, ..., B_m\}$ is the vertex set of an independent set
- F is a family of k-element subsets of n elements
- F satisfies the conditions of the corollary of the Modular RCW-theorem with $L = \{p-1, 2p-1, ..., p^2-p-1\}$ and $s = p-1$.
- $|F| \leq \binom{n}{s} + \binom{n}{s-1} + \cdots + \binom{n}{1} + \binom{n}{0} \leq 2\binom{n}{p-1}$

Applications to Ramsey Graphs

Conclusion

Corollary

Let $\omega(t) = \frac{\ln t}{4 \ln \ln t}$. *Then, for every* $\epsilon > 0$ *one can construct a t-Ramsey graph on more than*

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

- We have just constructed a Ramsey graph of size superpolynomial in t – this is currently the best known bound
- The emphasis in this problem is on explicit constructibility rather than existence
- Still an open problem to figure out how to improve the bound

Acknowledgements

Special thanks to:

- Our mentor Chiheon Kim, for an extraordinary amount of patience, knowledge, and time
- The MIT-PRIMES Program, Head Mentor Dr. Khovanova, Dr. Gerovitch, and Prof. Etingof for an excellent opportunity
- Our families for perpetual support