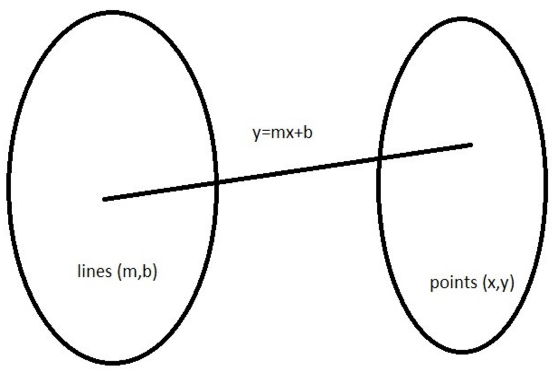
Lecture 10: Linear Algebra Methods

Combinatorial Methods (Winter 2023)
University of Toronto
Swastik Kopparty
Scribes: Yuxi Wang and William Groff

1 Projective Plane

Let p be prime, consider $\mathbb{F}_p^2$. Recall:



Point of infinity: if two lines are parallel, they intersect at a "point of infinity".

Example 1. $\mathbb{F}_p^3 \backslash \{0\}$/*scaling: ({1,1,2}={2,2,4})*

$\left\|\mathbb{F}_p^3 \backslash \{0\}/scaling\right\| = \frac{p^3-1}{p-1} = p^2+p+1$. *Note: the $p+1$ points are extra points at infinity.*

Also: $\left\|\{(x,y,1) : x,y \in \mathbb{F}_p\} \cup \{(x,1,0) : x \in \mathbb{F}_p\} \cup (1,0,0)\right\| = \left\|\mathbb{F}_p^2\right\| + \left\|\mathbb{F}_p\right\| + 1 = p^2+p+1$.
(a,b,c) represents line $ax+by+c=0$.

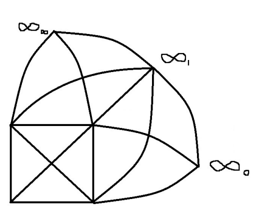
Given a line (a,b,c), how many points are on the line? That is,
how many $(x,y,z) \in \mathbb{F}_p^3 \backslash \{0\}$/scaling s.t. $ax+by+cz=0$?

p points from $\mathbb{F}_p^2$, 1 point from $\mathbb{F}_p$, 0 or 1 point from $(1,0,0)$.

Note: without scaling, p^2 points satisfy $\langle (a,b,c),(x,y,z)\rangle = 0$ (the orthogonal plane).

Observation 2. *Every line has $p+1$ points; every point on $p+1$ lines (of slopes $0,1,\ldots,\infty$); in total there are p^2+p+1 points and p^2+p+1 lines.*

Fano plane: the smallest finite projective plane



2 Oddtown

A town has n people. The people form clubs (sets of people). The size of each club is odd. In any 2 clubs, the size of the intersection is even. What is the maximum number of clubs you can form?

Observation 3. *the clubs must be an anti-chain (otherwise there is odd intersection);*
Lower bound: $\{\{i\} : i \in [n]\}$.

Consider a projective plane with p odd, the lines are sets of size $p+1$ (even), intersections has size 1 (odd) points $\sim$ people, lines $\sim$ clubs, so there can be n clubs.

Claim 4. *The number of clubs is at most n.*

Proof. For each club c_i:

create vector $v_i \in \mathbb{F}_2^n$ s.t. $v_{ij} = \begin{cases} 0 & \text{if person j not in club } c_i \\ 1 & \text{if person j is in club } c_i \end{cases}$

Note that $\langle v_i, v_j \rangle = 0 \bmod 2$ if $i \neq j$; $\langle v_i, v_i \rangle = 1 \bmod 2$. (an "orthonormal basis" of size n).

Then, let $M = [v_1 \ v_2 \ \dots \ v_m]$. M is an $n \times m$ matrix, and $M^\top M = I_M$.

We know $rank(AB) \leq max(rank(A), rank(B))$, so m cannot be greater than n.

□

Question: what if the club size must be even?

Consider: 1 and 2 always join clubs together, so as 3 and 4, ..., $2k+1, 2k+2$.

Then, we can construct $2^{n/2}$ clubs.

Let $V = \{v_i : i \in [m]\}$. For all $v, w \in V$, $\langle v, w \rangle = 0$.

Let $V^\perp = \{w : \langle v, w \rangle = 0, vv \in V\}$. Then, $dim(V^\perp) = n - dim(V)$.

Also, $V \subseteq V^\perp$, so $dim(V) \leq dim(V^\perp) = n - dim(V)$. So $dim(V) \leq n/2$.

Note: in this case, $M^\top M$ has all zeros on the diagonal, so the rank is $n-1$.

Summary:

size	intersection	maximum club number
odd	even	n
even	even	$2^{n/2}$
even	odd	n or $n+1$
odd	odd	$\approx 2^{n/2}$

3 Fisher's Inequality

Proposition 5. *$A_1, \ldots, A_m \subseteq [n]$ are non-empty. $|A_i \cap A_j| = \lambda$ for all $i \neq j$, $(\lambda \in [n])$. Then, $m \leq f(n) = n$.*

Proof. Let $v_1, \ldots, v_m$ be indicator vectors of $A_i \in \mathbb{F}^n/2^n$.
Then, $\langle v_i, v_j \rangle = \lambda$ for $i \neq j$.

Let $M = [v_1 \ \ldots \ v_m]$. M is an $n \times m$ matrix, and $M^\top M$ is an $m \times m$ matrix with λ in all entries off the diagonal.

At most 1 set A_i^* has size λ.
If so, $\lambda \neq 0$, all other sets must contain it and are disjoint after taking away A_i^*.
So there are $\leq n - \lambda$ other sets.
The total number of sets is $\leq (n - \lambda) + 1 \leq n$.

Case 2: all sets have size $> \lambda$.

Note: matrix $A = \begin{bmatrix} > \lambda & \lambda & \ldots & \lambda \\ \lambda & > \lambda & \ddots & \vdots \\ \vdots & \ddots & > \lambda & \lambda \\ \lambda & \ldots & \lambda & > \lambda \end{bmatrix} - [\lambda]$ has full rank.

So the rank of the first matrix above is $\geq m - 1$, so $m \leq n + 1$.

For $x \in \mathbb{R}^m$, if $x \neq 0$,

$$\begin{aligned} x^\top A x &= \sum_{i,j} x_i A_{ij} x_j \\ &= \sum_i (a_i - \lambda) x_i^2 + \sum_{i,j} \lambda x_i x_j \\ &= \sum_i (a_i - \lambda) x_i^2 + \lambda \left(\sum_i x_i \right)^2 > 0. \end{aligned}$$

So A has full rank.

□

4 2-Distance Sets

Let Δ be the Euclidean Distance

Let $S \subset R$ such that $\exists a, b$ such that $\forall x, y \in S$ with $x \neq y$

$\Delta(x, y) \in \{a, b\}$

Example

$S = \{x \in \{0,1\}^n$ with exactly two ones$\}$
Then $|S| = \mathcal{O}(n^2)$

We claim that this is the best we can do.

To show this we first define a polynomial $P(x_1, ..., x_n, y_1, ...y_n)$ in the following way

$P(\overrightarrow{x}, \overrightarrow{y}) = (||\overrightarrow{x} - \overrightarrow{y}||^2 - a)(||\overrightarrow{x} - \overrightarrow{y}||^2 - b)$

Then if we take x, y $\in S$

$$P(x, y) = \begin{cases} 0 & \text{if } x \neq y \\ ab & \text{if } x = y \end{cases}$$

Now for each $x \in S$ consider the polynomial
$Q_x(y_1, ..., y_n) \in \mathbb{R}[y_1, ..., y_n]$ such that
$Q_x(y) = P(x, y)$

Claim 6. *There exists some linear space V of dimension $\mathcal{O}(n^2)$ such that $Q_x \in V$ for all $x \in S$*

Claim 7. *$\{Q_x : x\}$ are linearly independent*

Proof of claim 3.
$Q_x(y) = (||x - y||^2 - a)(||x - y||^2 - b)$
$= (\sum_i (x_i - y_i)^2 - a)(\sum_j (x_j - y_j)^2 - b)$
$= (\sum_i y_i^2)(\sum_j y_j^2) - \sum_i 2x_i y_i (\sum_j {y_j}^2) - \sum_j 2x_j y_j (\sum_i {y_i}^2) + \sum_{i,j}(2x_i y_i)(2x_j y_j) + (\sum_j {y_j}^2)a + (\sum_i {y_i}^2)b - \sum_i (2x_i y_i)b - \sum_j (2x_j y_j)a$

Therefore $Q_x(y) \in \text{Span}(\{(\sum_i {y_i}^2)(\sum_j {y_j}^2)\} \cup \{y_i(\sum_j {y_j}^2) : i \in [n]\} \cup \{y_i y_j : i, j \in [n]\} \cup \{\sum_j {y_j}^2\} \cup \{y_i : i \in [n]\} \cup \{1\})$

Spanned by $n^2 + \mathcal{O}(n)$ functions □

Proof of claim 4.
Suppose $\sum_x \lambda_x Q_x = 0$

Take any $x' \in S$ and sub it into $\sum_x \lambda_x Q_x$

$\sum_x \lambda_x Q_x(x') = 0$

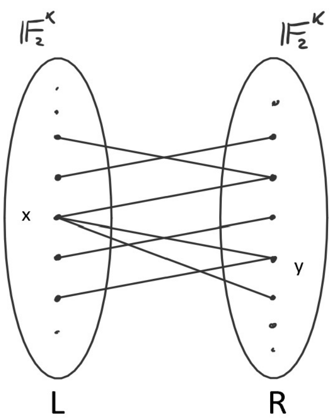
But all of the terms a $Q_x(x') = 0$ except the case where $x = x'$ in that case $Q_{x'}(x') = ab$

Therefore $0 = \sum_x \lambda_x Q_x(x') = \lambda_{x'} ab$

So $\lambda_{x'} = 0$

But this was for any $x' \in S$ so the Q_x are linearly independent □

5 Complete Bipartite Graph



We colour the edge (x,y) Red if $\langle x, y \rangle = 1$ and Blue if $\langle x, y \rangle = 0$

Claim 8. *This graph has no monochromatic* $K_{\mathcal{O}(\sqrt{n}),\mathcal{O}(\sqrt{n})}$

Proof of claim.
Case 1: Monochromatic Blue $K_{\mathcal{O}(\sqrt{n}),\mathcal{O}(\sqrt{n})}$

For any $S \subset L$ and $T \subset R$ with $|S| = \sqrt{n}$ and $|T| = \sqrt{n}$
Suppose $\langle x, y \rangle = 0 \ \forall x \in S$ and $y \in T$

Then span(S) $\perp$ span(T)

Therefore dim(span(S)) + dim(span(T)) $\leq$ k

$|span(S)| \leq 2^{\frac{k}{2}} = \sqrt{n}$ or
$|span(T)| \leq 2^{\frac{k}{2}} = \sqrt{n}$

Case 2: Monochromatic Red $K_{\mathcal{O}(\sqrt{n}),\mathcal{O}(\sqrt{n})}$

For any $S \subset L$ and $T \subset R$ with $|S| > \sqrt{n}$ and $|T| > \sqrt{n}$

Suppose $\langle x, y \rangle = 1 \forall x \in S, y \in T$

Then consider $(1, x), (1, y) \in \mathbb{F}_2^{k+1}$

These are orthogonal sets again so either

$|S|$ or $|T| \leq \sqrt{2^{k+1}} \leq 2\sqrt{n}$

□