Math 554

Hemanshu Kaul

kaul@iit.edu

k-distance set is a set of points in $\mathbb{R}^n$ such that distances between pairs of points belong to set of atmost k numbers.

1-distance set How many distinct points can we place in $\mathbb{R}^n$ such that all points will be equidistant?

$n=2$: 3 pt.s / corners of equilateral Triangle.

$n=3$: 4 corners of a tetrahedron.

$n+1$ corners of a regular simplex in $\mathbb{R}^n$.

k-distance set is a set of points in $\mathbb{R}^n$ such that distances between pairs of points belong to set of atmost k numbers.

1-distance set How many distinct points can we place in $\mathbb{R}^n$ such that all points will be equidistant?

$n=2$: 3 pt.s / corners of equilateral Triangle.

$n=3$: 4 corners of a tetrahedron.

$n+1$ corners of a regular simplex in $\mathbb{R}^n$.

2-distance set $X \subseteq \mathbb{R}^n$ is a 2-distance set if $\exists\, d_1, d_2 > 0$ s.t. $\|x-y\| \in \{d_1, d_2\}$ $\forall x \neq y$ in X.

Let $m(n)$ be the max # points in such a set.

2-distance sets in $\mathbb{R}^n$

$m(1) \geqslant$

$m(2) \geqslant$

2-distance sets in $\mathbb{R}^n$

$m(1) \geq 3$ 

$m(2) \geq 5$  corners of a regular pentagon

Let $S \subseteq \mathbb{R}^{n+1}$ be set of $\binom{n+1}{2}$ binary vectors containing exactly 2 ones.
This is a 2-distance set with only 2 & $\sqrt{2}$ as possible distances.
All points of S belong to the n-dim hyperplane $x_1 + x_2 + \ldots + x_{n+1} = 2$
This hyperplane can be projected down to $\mathbb{R}^n$ while preserving distances (isometrically) to get a 2-distance set S' of $\binom{n+1}{2}$ points in $\mathbb{R}^n$.

$$m(n) \geq \binom{n+1}{2} = \frac{n^2}{2} + \Theta(n)$$

Upper Bound ?

2-distance sets in $\mathbb{R}^n$

Theorem [Larman–Rogers–Seidel 1977]

Every 2-distance set in $\mathbb{R}^n$ has size at most $\frac{(n+1)(n+4)}{2}$

2-distance sets in $\mathbb{R}^n$

Theorem [Larman–Rogers–Seidel 1977]
Every 2-distance set in $\mathbb{R}^n$ has size at most $\frac{(n+1)(n+4)}{2}$

Proof Let $S = \{v^{(1)}, v^{(2)}, \dots, v^{(m)}\}$ be a 2-distance set in $\mathbb{R}^n$.
Let λ_1, λ_2 be the two distances allowed.

Define $f_i(x) = (\|x - v^{(i)}\|^2 - \lambda_1^2)(\|x - v^{(i)}\|^2 - \lambda_2^2)$ for $i = 1, \dots, m$

2-distance sets in $\mathbb{R}^n$

Theorem [Larman–Rogers–Seidel 1977]

Every 2-distance set in $\mathbb{R}^n$ has size at most $\frac{(n+1)(n+4)}{2}$

Proof Let $S = \{v^{(1)}, v^{(2)}, \dots, v^{(m)}\}$ be a 2-distance set in $\mathbb{R}^n$

Let λ_1, λ_2 be the two distances allowed.

Define $f_i(x) = \left(\|x - v^{(i)}\|^2 - \lambda_1^2\right)\left(\|x - v^{(i)}\|^2 - \lambda_2^2\right)$ for $i = 1, \dots, m$

Then $f_i(v^{(j)}) = 0$ if $i \neq j$

$f_i(v^{(i)}) = \lambda_1^2 \lambda_2^2 \neq 0$ in $\mathbb{R}$.

$\therefore$ $F = \{f_1(x), f_2(x), \dots, f_m(x)\}$ is lin. ind. in $\mathbb{R}[x_1, x_2, \dots, x_n]$.

2- distance sets in $\mathbb{R}^n$

Theorem [Larman – Rogers – Seidel 1977]

Every 2-distance set in $\mathbb{R}^n$ has size at most $\frac{(n+1)(n+4)}{2}$

Proof Let $S = \{v^{(1)}, v^{(2)}, \ldots, v^{(m)}\}$ be a 2-distance set in $\mathbb{R}^n$

Let λ_1, λ_2 be the two distances allowed.

Define $f_i(x) = (\|x - v^{(i)}\|^2 - \lambda_1^2)(\|x - v^{(i)}\|^2 - \lambda_2^2)$ for $i = 1, \ldots, m$

Then $f_i(v^{(j)}) = 0$ if $i \neq j$

$f_i(v^{(i)}) = \lambda_1^2 \lambda_2^2 \neq 0$ in $\mathbb{R}$.

$\therefore F = \{f_1(x), f_2(x), \ldots, f_m(x)\}$ is lin. ind. in $\mathbb{R}[x_1, x_2, \ldots, x_n]$.

Let $W = \text{span}(F)$, then $m \leq \dim W$

So, to get an upper bound on m, we need an u.b. on $\dim W$ which can found by a "small" spanning set for F.

2-distance sets in $\mathbb{R}^n$

Theorem [Larman–Rogers–Seidel 1977]

Every 2-distance set in $\mathbb{R}^n$ has size at most $\frac{(n+1)(n+4)}{2}$

Proof Let $S=\{v^{(1)}, v^{(2)}, \dots, v^{(m)}\}$ be a 2-distance set in $\mathbb{R}^n$

Let λ_1, λ_2 be the two distances allowed.

Define $f_i(x) = (\|x - v^{(i)}\|^2 - \lambda_1^2)(\|x - v^{(i)}\|^2 - \lambda_2^2)$ for $i = 1, \dots, m$

Expand the expression of each $f_i(x_1, x_2, \dots, x_n)$ to get the monomial terms of the expansion:

degree 4 term : $\left(\sum_{k=1}^{n} x_k^2\right)^2$ # possibilities : ?

degree 3 term : $x_j \sum_{k=1}^{n} x_k^2$ # possibilities : ?

degree 2 term : $x_i x_j$ # possibilities : ?

degree 1 term : x_i # possibilities : ?

degree 0 term : 1 # possibilities : ?

2-distance sets in $\mathbb{R}^n$

Theorem [Larman–Rogers–Seidel 1977]

Every 2-distance set in $\mathbb{R}^n$ has size at most $\frac{(n+1)(n+4)}{2}$

Proof Let $S = \{v^{(1)}, v^{(2)}, \ldots, v^{(m)}\}$ be a 2-distance set in $\mathbb{R}^n$.

Let λ_1, λ_2 be the two distances allowed.

Define $f_i(x) = \left(\|x - v^{(i)}\|^2 - \lambda_1^2\right)\left(\|x - v^{(i)}\|^2 - \lambda_2^2\right)$ for $i = 1, \ldots, m$

Expand the expression of each $f_i(x_1, x_2, \ldots, x_n)$ to get the monomial terms of the expansion:

degree 4 term : $\left(\sum_{k=1}^{n} x_k^2\right)^2$	# possibilities : 1
degree 3 term : $x_j \sum_{k=1}^{n} x_k^2$	# possibilities : n
degree 2 term : $x_i x_j$	# possibilities : $\binom{n}{2} + n = \frac{n(n+1)}{2}$
degree 1 term : x_i	# possibilities : n
degree 0 term : 1	# possibilities : 1

2-distance sets in $\mathbb{R}^n$

Theorem [Larman–Rogers–Seidel 1977]

Every 2-distance set in $\mathbb{R}^n$ has size at most $\frac{(n+1)(n+4)}{2}$

Proof Let $S = \{v^{(1)}, v^{(2)}, \dots, v^{(m)}\}$ be a 2-distance set in $\mathbb{R}^n$

Let λ_1, λ_2 be the two distances allowed.

Define $f_i(x) = (\|x - v^{(i)}\|^2 - \lambda_1^2)(\|x - v^{(i)}\|^2 - \lambda_2^2)$ for $i = 1, \dots, m$

$F = \{f_1(x), \dots, f_m(x)\}$ lin. ind. in $\mathbb{R}[x_1, \dots, x_n]$

and F has a spanning set with $1 + n + \frac{n(n+1)}{2} + n + 1$ monomials

$\therefore \quad m \leq \dim(\operatorname{span}(F)) \leq 1 + n + \frac{n(n+1)}{2} + n + 1 = (n+1)(2 + \frac{n}{2}) = \frac{(n+1)(n+4)}{2}$

$\blacksquare$

Polynomial / Lin. Algebra Method

To show $|S| \leq n$

Step1. Define a polynomial associated with each element of S.

Step2. Show these polynomials are lin. ind.

Step3. Show these polynomials are spanned by a set of n (simpler) polynomials.

Polynomial / Lin. Algebra Method

To show $|S| \le n$

Step 1. Define a polynomial associated with each element of S.
say, $S = \{s_1, s_2, \ldots, s_m\}$ & $s_i \to P_i$, $i = 1, \ldots, m$

Step 2. Show these polynomials are lin. ind.
$\{P_1, \ldots, P_m\}$ lin. ind.

Step 3. Show these polynomials are spanned by a set of n (simpler) polynomials.

$\operatorname{span}(\{P_1, \ldots, P_m\}) \subseteq \operatorname{span}(\{r_1, r_2, \ldots, r_n\})$, so $m \le n$

Polynomial / Lin. Algebra Method (Improvement)

To Show $|S| \leq n$

Step 1. Define a polynomial associated with each element of S.

say, $S = \{s_1, s_2, \dots, s_m\}$ & $s_i \to P_i$, $i = 1, \dots, m$

Step 2. Show these polynomials are lin. ind.

$\{P_1, \dots, P_m\}$ lin. ind. Include some extra polynomials $q_1, \dots, q_k$ s.t. $\{P_1, \dots, P_m, q_1, \dots, q_k\}$ lin. ind.

Step 3. Show these polynomials are spanned by a set of n (simpler) polynomials.

$\mathrm{span}(\{P_1, \dots, P_m\}) \subseteq \mathrm{span}(\{r_1, r_2, \dots, r_n\})$, so $m \leq n$

Ensure $\mathrm{span}(\{P_1, \dots, P_m, q_1, \dots, q_k\}) \subseteq \mathrm{span}(\{r_1, \dots, r_n\})$

so, $m + k \leq n$, i.e., $\underbrace{m \leq n - k}_{\text{improvement}}$

Applying this method, $m(n) \leq \frac{(n+1)(n+4)}{2}$ can be improved to $\frac{(n+1)(n+4)}{2} - (n+1)$

i.e. $(n+1)(n+2)/2$ [Blokhuis 1981]

L-intersecting Family of sets

As we have seen, a classic problem in combinatorics is to count the #sets in an intersecting family, where pairwise intersections satisfy some constraints.

Defn Let $L \subseteq \mathbb{N} \cup \{0\}$.
An L-intersecting family of sets is a family $\mathcal{F}$ such that
$|A \cap B| \in L \quad \forall A, B \in \mathcal{F},\ A \neq B.$

L-intersecting Family of sets

As we have seen, a classic problem in combinatorics is to count the #sets in an intersecting family, where pairwise intersections satisfy some constraints.

Defn Let $L \subseteq \mathbb{N} \cup \{0\}$.
An L-intersecting family of sets is a family $\mathcal{F}$ such that $|A \cap B| \in L$ $\forall A, B \in \mathcal{F}$, $A \neq B$.

- $\mathcal{F} \subseteq \binom{[n]}{k}$
  family of k-subsets of $[n]$

$L = \{0, 1, \dots, k-1\} \Rightarrow |\mathcal{F}| \leq$?

$L = \{1, 2, \dots, k-1\} \Rightarrow |\mathcal{F}| \leq$?

L-intersecting Family of sets

As we have seen, a classic problem in combinatorics is to count the #sets in an intersecting family, where pairwise intersections satisfy some constraints.

Defn Let $L \subseteq \mathbb{N} \cup \{0\}$.
An L-intersecting family of sets is a family $\mathcal{F}$ such that $|A \cap B| \in L \quad \forall A, B \in \mathcal{F},\ A \neq B$.

- $\mathcal{F} \subseteq \binom{[n]}{k}$
  family of k-subsets of [n]

$L = \{0, 1, \dots, k-1\} \Rightarrow |\mathcal{F}| \leq \binom{n}{k}$

$L = \{1, 2, \dots, k-1\} \Rightarrow |\mathcal{F}| \leq \binom{n-1}{k-1}$
[Erdös-Ko-Rado]

L-intersecting Family of sets

As we have seen, a classic problem in combinatorics is to count the # sets in an intersecting family, where pairwise intersections satisfy some constraints.

Defn Let $L \subseteq \mathbb{N} \cup \{0\}$.
An L-intersecting family of sets is a family $\mathcal{F}$ such that
$|A \cap B| \in L \quad \forall A, B \in \mathcal{F},\ A \neq B$.

- $\mathcal{F} \subseteq \binom{[n]}{k}$
  family of k-subsets of $[n]$

$L = \{0, 1, \dots, k-1\} \Rightarrow |\mathcal{F}| \leq \binom{n}{k}$

$L = \{1, 2, \dots, k-1\} \Rightarrow |\mathcal{F}| \leq \binom{n-1}{k-1}$
[Erdös-Ko-Rado]

- $\mathcal{F} \subseteq 2^{[n]}$
  family of subsets of $[n]$

$L = \{0, 1, \dots, n-1\} \Rightarrow |\mathcal{F}| \leq ?$

$L = \{1, \dots, n-1\} \Rightarrow |\mathcal{F}| \leq ?$

$L = \{0, 1, \dots, m-1\} \Rightarrow |\mathcal{F}| \leq ?$
for $m < n$

L-intersecting Family of sets

As we have seen, a classic problem in combinatorics is to count the # sets in an intersecting family, where pairwise intersections satisfy some constraints.

<u>Defn</u> Let $L \subseteq \mathbb{N} \cup \{0\}$.
An L-intersecting family of sets is a family $\mathcal{F}$ such that $|A \cap B| \in L \quad \forall A, B \in \mathcal{F},\ A \neq B$.

- $\mathcal{F} \subseteq \binom{[n]}{k}$
  family of k-subsets of $[n]$

$L = \{0, 1, \dots, k-1\} \Rightarrow |\mathcal{F}| \leq \binom{n}{k}$

$L = \{1, 2, \dots, k-1\} \Rightarrow |\mathcal{F}| \leq \binom{n-1}{k-1}$

[Erdös-Ko-Rado]

- $\mathcal{F} \subseteq 2^{[n]}$
  family of subsets of $[n]$

$L = \{0, 1, \dots, n-1\} \Rightarrow |\mathcal{F}| \leq 2^n$

$L = \{1, \dots, n-1\} \Rightarrow |\mathcal{F}| \leq 2^{n-1}$

$L = \{0, 1, \dots, m-1\}$ for $m < n$ $\Rightarrow \underbrace{|\mathcal{F}| \leq \binom{n}{0} + \binom{n}{1} + \dots + \binom{n}{m}}_{\text{To be Proved.}}$

Theorem [Frankl-Wilson 1981]

If $\mathcal{F}$ is an L-intersecting family of subsets of $[n]$, where $|L|=s$ then $|\mathcal{F}| \leq \sum_{i=0}^{s} \binom{n}{i}$

Note this is sharp. Take $\mathcal{F}$ = all subsets of $[n]$ of size atmost s

Theorem [Frankl-Wilson 1981]

If $\mathcal{F}$ is an L-intersecting family of subsets of $[n]$, where $|L| = s$ then $|\mathcal{F}| \leq \sum_{i=0}^{s} \binom{n}{i}$

Proof [Babai 1988; also see Alon-Babai-Suzuki 1991]

Let $\mathcal{F} = \{A_1, \dots, A_m\}$ be indexed in such a way that $|A_1| \leq |A_2| \leq \dots \leq |A_m|$

Let v_i be the incidence vector of A_i, $i = 1, \dots, m$.

Let $L = \{l_1, l_2, \dots, l_s\}$

Define $f_1, \dots, f_m$ as $\quad f_i(x) = \prod_{k : l_k < |A_i|} (\overbrace{x \cdot v_i}^{\text{"size of intersection"}} - l_k)$

Theorem [Frankl–Wilson 1981]

If $\mathcal{F}$ is an L-intersecting family of subsets of $[n]$, where $|L| = s$ then $|\mathcal{F}| \leq \sum_{i=0}^{s} \binom{n}{i}$

Proof [Babai 1988; also see Alon–Babai–Suzuki 1991]

Let $\mathcal{F} = \{A_1, \ldots, A_m\}$ be indexed in such a way that $|A_1| \leq |A_2| \leq \cdots \leq |A_m|$

Let v_i be the incidence vector of A_i, $i = 1, \ldots, m$.

Let $L = \{\ell_1, \ell_2, \ldots, \ell_s\}$

Define $f_1, \ldots, f_m$ as $f_i(x) = \prod_{k:\, \ell_k < |A_i|} (\overbrace{x \cdot v_i}^{\text{"size of intersection"}} - \ell_k)$

$\Rightarrow f_i(v_j) = \prod_{k:\, \ell_k < |A_i|} (v_j \cdot v_i - \ell_k) = 0 \quad \forall j < i \quad (\text{since } v_i \cdot v_j = |A_i \cap A_j| < |A_i|)$ distinct sets

$f_i(v_i) = \prod_{k:\, \ell_k < |A_i|} (v_i \cdot v_i - \ell_k) \neq 0 \quad \forall i \quad (\text{since } v_i \cdot v_i = |A_i|)$

By Triangular criterion, $\{f_1, \ldots, f_m\}$ is lin. independent over $\mathbb{R}[x_1, \ldots, x_n]$

Theorem [Frankl–Wilson 1981]

If $\mathcal{F}$ is an L-intersecting family of subsets of $[n]$, where $|L| = s$ then $|\mathcal{F}| \leq \sum_{i=0}^{s} \binom{n}{i}$

Proof [Babai 1988; also see Alon-Babai-Suzuki 1991]

Let $\mathcal{F} = \{A_1, \dots, A_m\}$ be indexed in such a way that $|A_1| \leq |A_2| \leq \dots \leq |A_m|$

Let v_i be the incidence vector of A_i, $i = 1, \dots, m$.

Let $L = \{l_1, l_2, \dots, l_s\}$

Define $f_1, \dots, f_m$ as $\quad f_i(x) = \prod_{k : l_k < |A_i|} (x \cdot v_i - l_k)$

These are lin. ind., so how about a spanning set in $\mathbb{R}[x_1, \dots, x_n]$?

Each f_i is of degree at most s.

So in principle, we are looking at a spanning set of the form:

$1; x_i, x_i^2, \dots, x_i^s; \; x_i^k x_j^{s-k}; \; x_i^{k_1} x_j^{k_2} x_k^{s-k_1-k_2}; \dots \quad \dots\dots\dots \rightarrow$ sum of multinomial coefficients

A polynomial $f \in \mathbb{F}[x_1, \ldots, x_n]$ is called <u>multilinear</u> if f is of the form $\sum_{I \subseteq [n]} \alpha_I \prod_{i \in I} x_i$ where $\alpha_I \in \mathbb{F}$

that is, f has degree at most 1 in each variable.

e.g. $x_1 x_3 x_5 + x_1 x_2 x_4 + x_2 x_3 x_4 + x_4 x_5$ is a multilinear polynomial of degree 3

<u>Observation</u>: Every multilinear polynomial of degree atmost s is a linear combination of multilinear monomials of deg atmost s.

How many?

$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{s} = \sum_{k=0}^{n} \binom{n}{k}$

A polynomial $f \in \mathbb{F}[x_1, \ldots, x_n]$ is called <u>multilinear</u> if f is of the form $\sum_{I \subseteq [n]} \alpha_I \prod_{i \in I} x_i$ where $\alpha_I \in \mathbb{F}$

that is, f has degree at most 1 in each variable.

e.g. $x_1x_3x_5 + x_1x_2x_4 + x_2x_3x_4 + x_4x_5$ is a multilinear polynomial of degree 3

<u>Observation</u>: Every multilinear polynomial of degree atmost s is a linear combination of multilinear monomials of deg atmost s.

<u>Lemma [Multilinearization]</u> Let $\mathbb{F}$ be a field & $\Omega = \{0,1\}^n \subseteq \mathbb{F}^n$
If f is a polynomial of deg atmost s in $\mathbb{F}[x_1, \ldots, x_n]$ then there exists a (unique) multilinear polynomial $\tilde{f}$ of $\deg \leq s$ in $\mathbb{F}[x_1, \ldots, x_n]$ s.t. $f(x) = \tilde{f}(x)$ $\forall x \in \Omega$.

<u>Proof</u> expand f and use the identity $x_i^2 = x_i$ over Ω.
That is, $x_{i_1}^{k_1} x_{i_2}^{k_2} \cdots x_{i_t}^{k_t} \longmapsto x_{i_1} x_{i_2} \cdots x_{i_t}$ over Ω

Theorem [Frankl–Wilson 1981]

If $\mathcal{F}$ is an L-intersecting family of subsets of $[n]$, where $|L| = s$ then $|\mathcal{F}| \leq \sum_{i=0}^{s} \binom{n}{i}$

Proof [Babai 1988; also see Alon-Babai-Suzuki 1991]

Let $\mathcal{F} = \{A_1, \dots, A_m\}$ be indexed in such a way that $|A_1| \leq |A_2| \leq \dots \leq |A_m|$

Let v_i be the incidence vector of A_i, $i = 1, \dots, m$.

Let $L = \{\ell_1, \ell_2, \dots, \ell_s\}$

Define $f_1, \dots, f_m$ as $\quad f_i(x) = \prod_{k : \ell_k < |A_i|} (x \cdot v_i - \ell_k)$

Nothing changes if we replace f_i by $\tilde{f}_i$ using lemma (Multilinearization)

$$\Rightarrow f_i(v_j) = \prod_{k : \ell_k < |A_i|} (v_j \cdot v_i - \ell_k) = 0 \quad \forall j < i \quad (\text{since } v_i \cdot v_j = |A_i \cap A_j| < |A_i|)$$

distinct sets

$$f_i(v_i) = \prod_{k : \ell_k < |A_i|} (v_i \cdot v_i - \ell_k) \neq 0 \quad \forall i \quad (\text{since } v_i \cdot v_i = |A_i|)$$

By Triangular criterion, $\{f_1, \dots, f_m\}$ is lin. independent over $\mathbb{R}[x_1, \dots, x_n]$.

Theorem [Frankl-Wilson 1981]

If $\mathcal{F}$ is an L-intersecting family of subsets of $[n]$, where $|L|=s$ then $|\mathcal{F}| \leq \sum_{i=0}^{s} \binom{n}{i}$

Proof [Babai 1988; also see Alon-Babai-Suzuki 1991]

Let $\mathcal{F}=\{A_1,\dots,A_m\}$ be indexed in such a way that $|A_1|\leq|A_2|\leq\dots\leq|A_m|$

Let v_i be the incidence vector of A_i, $i=1,\dots,m$.

Let $L=\{l_1, l_2, \dots, l_s\}$

Define $f_1,\dots,f_m$ as $f_i(x)=\prod_{k:\, l_k<|A_i|}(x\cdot v_i - l_k)$

Replace each f_i by $\tilde{f}_i$ (its multilinearization).

As, before $\{\tilde{f}_1,\dots,\tilde{f}_m\}$ are linearly independent as well.

Since, all multilinear polynomials of degree $\leq s$ are spanned by multilinear monomials of degree $\leq s$, i.e. $x_{i_1}\cdots x_{i_k}$ s.t. $i_1+\dots+i_k\leq s$ we have a spanning set of size atmost $\binom{n}{0}+\binom{n}{1}+\dots+\binom{n}{s}$ $\therefore m\leq\sum_{k=0}^{s}\binom{n}{k}$

Modular Intersecting Families

Defn Let p be a prime. For $L \subseteq \mathbb{Z}_p$, we say $t \in L \pmod p$ if $t \equiv l \pmod p$ for some $l \in L$.

Defn Let $L \subseteq \mathbb{Z}_p$, p prime.
we say $\mathcal{F} \subseteq 2^{[n]}$, family of subsets of $[n]$, is a <u>p-modular L-intersecting family</u> if

(i) $|A| \notin L \pmod p$ $\forall A \in \mathcal{F}$,

and (ii) $|A \cap B| \in L \pmod p$ $\forall A \neq B$ in $\mathcal{F}$.

Modular Intersecting Families

<u>Defn</u> Let p be a prime. For $L \subseteq \mathbb{Z}_p$, we say <u>$t \in L \pmod{p}$</u> if $t \equiv l \pmod{p}$ for some $l \in L$.

<u>Defn</u> Let $L \subseteq \mathbb{Z}_p$, p prime.
we say $\mathcal{F} \subseteq 2^{[n]}$, family of subsets of $[n]$, is a <u>p-modular L-intersecting family</u> if
(i) $|A| \notin L \pmod{p}$ $\forall A \in \mathcal{F}$,
and (ii) $|A \cap B| \in L \pmod{p}$ $\forall A \neq B$ in $\mathcal{F}$.

<u>Theorem [Deza-Frankl-Singhi 1983]</u> Let p be a prime. $|L| = s$. If $\mathcal{F}$ is a p-modular L-intersecting family of subsets of $[n]$, then $|\mathcal{F}| \leq \sum_{k=0}^{s} \binom{n}{i}$

<u>Proof</u> [Alon-Babai-Suzuki 1991] <u>HW! Mimic the previous proof.</u>

Theorem [Deza-Frankl-Singhi 1983] Let p be prime. $|L|=s$. If $\mathcal{F}$ is a p-modular L-intersecting family of subsets of $[n]$, then

$$|\mathcal{F}| \le \sum_{k=0}^{s} \binom{n}{k}$$

Cor [Ray-Chaudhari-Wilson 1975: weak form]

If $L \subseteq \mathbb{Z}$, $|L|=s$, $\mathcal{F} \subseteq \binom{[n]}{k}$, family of k-unif. subsets of $[n]$, such that $\mathcal{F}$ is L-intersecting then $|\mathcal{F}| \le \sum_{i=0}^{s} \binom{n}{i}$

Pf. Since $\mathcal{F}$ consists of distinct k-subsets, we may assume $k \notin L$ so apply D-F-S thm with $p \ge k$.

Ray-Chaudhari-Wilson Thm gives the bound $|\mathcal{F}| \le \binom{n}{s}$

Theorem [Deza-Frankl-Singhi 1983] Let p be prime. $|L|=s$. If $\mathcal{F}$ is a p-modular L-intersecting family of subsets of $[n]$, then

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

Cor [Ray-Chaudhuri-Wilson 1975: weak form]
If $L \subseteq \mathbb{Z}$, $|L|=s$, $\mathcal{F} \subseteq \binom{[n]}{k}$, family of k-unif. subsets of $[n]$, such that $\mathcal{F}$ is L-intersecting then $|\mathcal{F}| \leq \sum_{i=0}^{s} \binom{n}{i}$

Pf. Since $\mathcal{F}$ consists of distinct k-subsets, we may assume $k \notin L$ so apply D-F-S thm with $p \geq k$.

Ray-Chaudhuri-Wilson Thm gives the bound $|\mathcal{F}| \leq \binom{n}{s}$

Lemma $\sum_{i=0}^{s} \binom{n}{i} \leq \binom{n}{s}\left(1+\frac{s}{n-2s+1}\right)$

Moreover, for $s \leq n/\ell$, we get $\sum_{i=0}^{s} \binom{n}{i} < \binom{n}{s}\left(1+\frac{1}{\ell-2}\right)$

so, for $s \leq \frac{n}{4}$, $\sum_{i=0}^{s} \binom{n}{i} < 2\binom{n}{s}$

off only by a factor of 2

Theorem [Deza-Frankl-Singhi 1983] Let p be prime. $|L|=s$.
If $\mathcal{F}$ is a p-modular L-intersecting family of subsets of $[n]$, then
$$|\mathcal{F}| \leq \sum_{k=0}^{s} \binom{n}{k}$$

Cor [Ray-Chaudhuri-Wilson 1975: weak form]
If $L \subseteq \mathbb{Z}$, $|L|=s$, $\mathcal{F} \subseteq \binom{[n]}{k}$, family of k-unif. subsets of $[n]$, such that $\mathcal{F}$ is L-intersecting then $|\mathcal{F}| \leq \sum_{i=0}^{s} \binom{n}{i}$

Cor [Generalized Fischer Inequality]
Let $\mathcal{F} \subseteq 2^{[n]}$, family of subsets of $[n]$, s.t. $|A \cap B| = k$ $\forall A \neq B$ in $\mathcal{F}$
Then, $|\mathcal{F}| \leq n+1$.

Sharp using $\mathcal{F} = \{\phi, \{1\}, \{2\}, \ldots, \{n\}\}$ (all intersections are empty)
Disallowing empty set in $\mathcal{F}$, improves the bound to $|\mathcal{F}| \leq n$

Theorem [Deza-Frankl-Singhi 1983] Let p be prime. $|L|=s$. If $\mathcal{F}$ is a p-modular L-intersecting family of subsets of $[n]$, then
$$|\mathcal{F}| \le \sum_{k=0}^{s} \binom{n}{k}$$

Cor [Ray-Chaudhuri-Wilson 1975: weak form]

If $L \subseteq \mathbb{Z}$, $|L|=s$, $\mathcal{F} \subseteq \binom{[n]}{k}$, family of k-unif. subsets of $[n]$, such that $\mathcal{F}$ is L-intersecting then $|\mathcal{F}| \le \sum_{i=0}^{s} \binom{n}{i}$

Cor [Generalized Fischer Inequality]

Let $\mathcal{F} \subseteq 2^{[n]}$, family of subsets of $[n]$, s.t. $|A \cap B| = k$ $\forall A \neq B$ in $\mathcal{F}$

Then, $|\mathcal{F}| \le n+1$.

Pf. Let $\mathcal{F} = \{A_1, \dots, A_m\}$

Case 1. $\exists A_i$ s.t. $|A_i| = k$. WLOG $|A_1| = k$. Then, $A_i \cap A_j = A_1$ $\forall 1 \le i \neq j \le m$

$\therefore$ the sets A_i for $i > 1$ are disjoint outside A_1

So, $m-1 \le n-k$, which is at most n, so $m \le n+1$.

Theorem [Deza-Frankl-Singhi 1983] Let p be prime. $|L|=s$. If $\mathcal{F}$ is a p-modular L-intersecting family of subsets of $[n]$, then

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

Cor [Ray-Chaudhuri-Wilson 1975: weak form]
If $L \subseteq \mathbb{Z}$, $|L|=s$, $\mathcal{F} \subseteq \binom{[n]}{k}$, family of k-unif. subsets of $[n]$, such that $\mathcal{F}$ is L-intersecting then $|\mathcal{F}| \leq \sum_{i=0}^{s} \binom{n}{i}$

Cor [Generalized Fischer Inequality]
Let $\mathcal{F} \subseteq 2^{[n]}$, family of subsets of $[n]$, s.t. $|A \cap B| = k$ $\forall A \neq B$ in $\mathcal{F}$
Then, $|\mathcal{F}| \leq n+1$.

Pf. Let $\mathcal{F} = \{A_1, \dots, A_m\}$

Case 2. $|A_i| > k$ $\forall i$. Show how to apply D-F-S theorem here.
How to pick prime p?
How to choose L?

Ask me if you are stuck.

Applications of D-F-S / Modular Frankl-Wilson Theorem

- Chromatic numbers of unit-distance graph on $\mathbb{R}^d$

  Vertex set $= \mathbb{R}^d$, edge between any two points at unit distance

  for any other fixed number

  [Hadwiger-Nelson problem, 1951] $\chi(\mathbb{R}^2) = ?$

  known: $4 \le \chi(\mathbb{R}^2) \le 7$

  Moser Spindle

  coloring by hexagonal tiling

  Improved in 2019 to 5 : 510-vertex unit-distance graph with no 4-coloring.

What about higher dimensions? $\chi(\mathbb{R}^d) = ?$

What about other vertex sets? $\mathbb{Q}$, $\mathbb{Z}$, etc.

What about other metrics? ℓ_p, p-adic, etc.

What about "nice" colorings? Each color class is measurable, etc.

Applications of D-F-S / Modular Frankl-Wilson Theorem

- **Chromatic number of unit-distance graph on $\mathbb{R}^d$**

Vertex set $= \mathbb{R}^d$, edge between any two points at unit distance

- By a tiling of $\mathbb{R}^d$ by (hyper)cubes: $\mathbb{R}^n = \bigcup_{x \in \mathbb{Z}^n} Q_x$ where

$$Q_x = \{ y \in \mathbb{R}^d : \lfloor y_i \sqrt{n} \rfloor = x_i \ \forall i \}$$

Each Q_x has diameter < 1, so can be monochromatic.

Let G be s.t. $V(G) =$ cubes Q_x & $Q_x Q_y \in E(G)$ if $\exists\, u \in Q_x$ & $v \in Q_y$ s.t. $\|u - v\| = 1$

Proper coloring of G gives a proper coloring of $\mathbb{R}^d$.

$$\therefore \underline{\chi(\mathbb{R}^d)} \leq \chi(G) \leq \Delta(G) + 1 \leq \underline{(10.4)^d}$$

By volumetric argument.

Applications of D-F-S / Modular Frankl-Wilson Theorem

- **Chromatic number of unit-distance graph on $\mathbb{R}^d$**

Vertex set $= \mathbb{R}^d$, edge between any two points at unit distance

Frankl-Wilson 1981 $\chi(\mathbb{R}^d) \geq (1.13)^d$ for suff. large d.

Proof

In Problem #5 of HW, you will use Modular F-W to show, $\exists$ a graph G in $\mathbb{R}^d$ such that

$$\chi(\mathbb{R}^d) \geq \underbrace{\chi(G) \geq \frac{\binom{d}{2p-1}}{\sum_{i=0}^{p-1}\binom{d}{i}}}_{\text{problem \#5}} \geq \frac{\binom{d}{2p-1}}{2\binom{d}{p-1}} \quad \text{for a prime } p.$$

then it can be estimated $\dfrac{\binom{d}{2p-1}}{2\binom{d}{p-1}} \geq (1.13)^d$ for $d = 4p-1$.

Applications of D-F-S / Modular Frankl-Wilson Theorem

- **Borsuk's Conjecture**

Let $X \subseteq \mathbb{R}^d$ be a bounded set.

How many subsets are needed to partition X into subsets of diameter smaller than $\text{diam}(X)$ itself?

Let $f(d) =$ min n s.t. every bounded $X \subseteq \mathbb{R}^d$ has a partition into n subsets $X_1 \sqcup \dots \sqcup X_n$ s.t. $\text{diam}(X_i) < \text{diam}(X)$ $\forall i$.

Applications of D-F-S / Modular Frankl-Wilson Theorem

- **Borsuk's Conjecture**

Let $X \subseteq \mathbb{R}^d$ be a bounded set.

How many subsets are needed to partition X into subsets of diameter smaller than $\mathrm{diam}(X)$ itself?

Let $f(d) =$ min n s.t. every bounded $X \subseteq \mathbb{R}^d$ has a partition into n subsets $X_1 \sqcup \ldots \sqcup X_n$ s.t. $\mathrm{diam}(X_i) < \mathrm{diam}(X)$ $\forall i$.

Borsuk's Conjecture (1933) $f(d) = d+1$

proved true $d = 2, 3$; all balls in $\mathbb{R}^d$; smooth convex bodies, etc.

Applications of D-F-S / Modular Frankl-Wilson Theorem

- **Borsuk's Conjecture**

Let $X \subseteq \mathbb{R}^d$ be a bounded set.

How many subsets are needed to partition X into subsets of diameter smaller than $\mathrm{diam}(X)$ itself?

Let $f(d) = \min n$ s.t. every bounded $X \subseteq \mathbb{R}^d$ has a partition into n subsets $X_1 \sqcup \ldots \sqcup X_n$ s.t. $\mathrm{diam}(X_i) < \mathrm{diam}(X)$ $\forall i$.

Borsuk's Conjecture (1933) $f(d) = d+1$

proved true $d = 2, 3$; all balls in $\mathbb{R}^d$; smooth convex bodies, etc

Kahn-Kalai 1993 $f(d) \geq (1.2)^{\sqrt{d}}$ for all suff. large d.

key ingredient of their proof was Modular F-W thm.

Applications of D-F-S / Modular Frankl-Wilson Theorem

- **Constructive Ramsey Graphs**

We saw earlier $(\sqrt{2})^t < R(t,t) < 4^t$ for large enough t

This based on a probabilistic argument
Can we give an explicit construction?

long history going back to Nagy 1972.

Applications of D-F-S / Modular Frankl-Wilson Theorem

- **Constructive Ramsey Graphs**

We saw earlier $(\sqrt{2})^t < R(t,t) < 4^t$ for large enough t

This based on a probabilistic argument
Can we give an explicit contruction?
long history going back to Nagy 1972.

$R(t,t) > 2^{(1-\epsilon)\ln^2 t / 4 \ln\ln t}$ with an explicit construction.

p prime. $n \geq 4p^2$. $V(G) = \binom{[n]}{p^2-1}$, $A_1 A_2 \in E(G)$ iff $|A_1 \cap A_2| \not\equiv -1 \pmod p$

Use Frankl-Wilson Thm to show $\alpha(G) \leq \sum_{k=0}^{p-1} \binom{n}{k}$

Use Modular Frankl-Wilson to show $\omega(G) \leq \sum_{k=0}^{p-1} \binom{n}{k}$

With $n = p^3$, & p largest prime s.t. $\binom{p^3}{p-1} < t$, then $\exists\, G$ with $\binom{p^3}{p^2-1}$ vertices, and $\alpha(G), \omega(G) \leq (1+o(1))\binom{p^3}{p-1} = (1+o(1))t$. Estimate $\binom{p^3}{p^2-1}$ in terms of t using usual bounds.

Theorem [Frankl-Wilson 1981]

If $\mathcal{F}$ is an L-intersecting family of subsets of $[n]$, where $|L|=s$ then $|\mathcal{F}| \leq \sum_{i=0}^{s} \binom{n}{i}$

Conjecture [Frankl-Füredi 1981] If $L=[s]=\{1,2,\ldots,s\}$, then the bound in Frankl-Wilson can be improved to $\sum_{i=0}^{s} \binom{n-1}{s}$

→ Proved by Ramanan in 1997

→ Snevily (2003) proved that conjecture is true even when, all we know about L is $|L|=s$ as long as $0 \notin L$.

We will prove a modular version of this conjecture.

Theorem [Snevily 1994] Let p be prime. $L \subseteq \mathbb{Z}_p$.
If $\mathcal{F}$ is a p-modular L-intersecting family of subsets of $[n]$ with $|L| = s$, then $|\mathcal{F}| \leq \sum_{i=0}^{s} \binom{n-1}{i}$

Notice this is an improvement of Modular F-W thm.

Example Let $L = [s]$, $\mathcal{F} = \{F \subseteq [n] : 1 \in A, |A| \leq s+1\}$

$$|\mathcal{F}| = \sum_{i=0}^{s} \binom{n-1}{i}$$

$$F \cap F' \subseteq L \quad \forall F \neq F' \in \mathcal{F}$$

Theorem [Snevily 1994] Let p be prime. $L \subseteq \mathbb{Z}_p$.
If $\mathcal{F}$ is a p-modular L-intersecting family of subsets of $[n]$ with $|L| = s$, then $|\mathcal{F}| \leq \sum_{i=0}^{s} \binom{n-1}{i}$

Proof We will modify the proof of F-W / modular F-W by including additional $\sum_{i=1}^{s} \binom{n-1}{i-1}$ polynomials with the original polynomials of the form $\prod_{k} (x \cdot v_i - l_k)$, so that all these linearly independent polynomials are still spanned by $\sum_{i=0}^{s} \binom{n}{i}$ monomials.

So the improved upper bound will be

$$\sum_{i=0}^{s} \binom{n}{i} - \sum_{i=1}^{s} \binom{n-1}{i-1} = \sum_{i=0}^{s} \binom{n-1}{i}$$

Theorem [Snevily 1994] Let p be prime. $L \subseteq \mathbb{Z}_p$.
If $\mathcal{F}$ is a p-modular L-intersecting family of subsets of $[n]$ with $|L| = s$, then $|\mathcal{F}| \leq \sum_{i=0}^{s} \binom{n-1}{i}$

Proof. Let $\mathcal{F} = \{A_1, \ldots, A_m\}$ where A_i are indexed in such a way that $A_1, \ldots, A_q$ omit the element 1 and $A_{q+1}, \ldots, A_m$ contain 1.

Let v_i be the incidence vector of A_i, $\forall i$.

Let $f_i(x) = \prod_{\ell \in L} (x \cdot v_i - \ell)$ in $\mathbb{F}_p[x_1, \ldots, x_n]$

Theorem [Snevily 1994]

Let p be prime. $L \subseteq \mathbb{Z}_p$.
If $\mathcal{F}$ is a p-modular L-intersecting family of subsets of $[n]$ with $|L| = s$, then $|\mathcal{F}| \leq \sum_{i=0}^{s} \binom{n-1}{i}$

Proof. Let $\mathcal{F} = \{A_1, \dots, A_m\}$ where A_i are indexed in such a way that $A_1, \dots, A_q$ omit the element 1 and $A_{q+1}, \dots, A_m$ contain 1.

Let v_i be the incidence vector of A_i, $\forall i$.

Let $f_i(x) = \prod_{\ell \in L} (x \cdot v_i - \ell)$ in $\mathbb{F}_p[x_1, \dots, x_n]$

$f_i(v_j) = 0 \quad \forall i \neq j$ (since $v_j \cdot v_i = |A_j \cap A_i| \in L \bmod p$)

$f_i(v_i) \neq 0 \quad \forall i$ (since $v_i \cdot v_i = |A_i| \notin L \bmod p$,
each factor $(v_i \cdot v_i - \ell) \not\equiv 0 \bmod p$
i.e., each factor is not a multiple of p
hence $\prod_{\ell \in L} (v_i \cdot v_i - \ell)$ is not a multiple of p
since ?

Theorem [Snevily 1994] Let p be prime. $L \subseteq \mathbb{Z}_p$.
If $\mathcal{F}$ is a p-modular L-intersecting family of subsets of $[n]$ with $|L| = s$, then $|\mathcal{F}| \leq \sum_{i=0}^{s} \binom{n-1}{i}$

Proof Let $\mathcal{F} = \{A_1, \ldots, A_m\}$ where A_i are indexed in such a way that $A_1, \ldots, A_q$ omit the element 1 and $A_{q+1}, \ldots, A_m$ contain 1.

Let v_i be the incidence vector of $A_i, \forall i$.

Let $f_i(x) = \prod_{l \in L} (x \cdot v_i - l)$ in $\mathbb{F}_p[x_1, \ldots, x_n]$

$f_i(v_j) = 0 \quad \forall i \neq j$ (since $v_j \cdot v_i = |A_j \cap A_i| \in L \bmod p$)

$f_i(v_i) \neq 0 \quad \forall i$ (since $v_i \cdot v_i = |A_i| \notin L \bmod p$, each factor $(v_i \cdot v_i - l) \not\equiv 0 \bmod p$ i.e., each factor is not a multiple of p hence $\prod_{l \in L} (v_i \cdot v_i - l)$ is not a multiple of p since p is a prime)

$\therefore \{f_1, \ldots, f_m\}$ lin. ind.

so, $\{\tilde{f}_1, \ldots, \tilde{f}_m\}$ also lin. ind., where $\tilde{f}_i$ is the multilinear reduction of f_i in $\mathbb{F}_p[x_1, \ldots, x_n]$

Theorem [Snevily 1994] Let p be prime. $L \subseteq \mathbb{Z}_p$.
If $\mathcal{F}$ is a p-modular L-intersecting family of subsets of $[n]$ with $|L| = s$, then $|\mathcal{F}| \leq \sum_{i=0}^{s} \binom{n-1}{i}$

Proof Let $\mathcal{F} = \{A_1, \ldots, A_m\}$ where A_i are indexed in such a way that $A_1, \ldots, A_q$ omit the element 1 and $A_{q+1}, \ldots, A_m$ contain 1.

Let v_i be the incidence vector of $A_i, \forall i$.

$f_i(x) = \prod_{\ell \in L} (x \cdot v_i - \ell)$ are lin. ind. in $\mathbb{F}_p[x_1, \ldots, x_n]$

and the corresponding multilinear reductions $\{\tilde{f}_i : i = 1, \ldots, m\}$ are also lin. ind. in $\mathbb{F}_p[x_1, \ldots, x_n]$

As before, $\{\tilde{f}_1, \ldots, \tilde{f}_m\}$ is spanned by multilinear monomials with at most s variables.

This is the proof that $m \leq \sum_{i=0}^{s} \binom{n}{i}$

Now, let's improve it!

Let $C_1, \ldots, C_t$ be all the sets of size less than s in $[n]$ that omit 1. We index these sets s.t. $|C_1| \leq |C_2| \leq \cdots \leq |C_t|$

Note that $t = \sum_{i=1}^{s} \binom{n-1}{i-1}$.

(note x_1 doesn't occur in any h_j)

Define $h_j(x) = \prod_{r \in C_j} x_r$, $j = 1, \ldots, t$

and $g_j(x) = (x_1 - 1) h_j(x)$, $j = 1, \ldots, t$

Let $C_1, \ldots, C_t$ be all the sets of size less than s in $[n]$ that omit 1. We index these sets s.t. $|C_1| \le |C_2| \le \cdots \le |C_t|$

Note that $t = \sum_{i=1}^{s} \binom{n-1}{i-1}$.

(note x_1 doesn't occur in any h_j)

Define $h_j(x) = \prod_{k \in C_j} x_k$, $j = 1, \ldots, t$

and $g_j(x) = (x_1 - 1) h_j(x)$, $j = 1, \ldots, t$

Since $\deg(h_j) < s$, $\deg(g_j) \le s$ $\forall j$. And the multilinear reduction $\tilde{g}_j$ of g_j is spanned by multilinear monomials of degree at most s.

$\therefore \{\tilde{f}_1, \ldots, \tilde{f}_m\} \cup \{\tilde{g}_1, \ldots, \tilde{g}_t\}$ have the same spanning set as before of size $\sum_{i=0}^{s} \binom{n}{i}$

Let $C_1, \dots, C_t$ be all the sets of size less than s in $[n]$ that omit 1. We index these sets s.t. $|C_1| \le |C_2| \le \dots \le |C_t|$

Note that $t = \sum_{i=1}^{s} \binom{n-1}{i-1}$.

Define $h_j(x) = \prod_{r \in C_j} x_r$, $j = 1, \dots, t$ (note x_1 doesn't occur in any h_j)

and $g_j(x) = (x_1 - 1) h_j(x)$, $j = 1, \dots, t$

Since $\deg(h_j) < s$, $\deg(g_j) \le s$ $\forall j$. And the multilinear reduction $\tilde{g}_j$ of g_j is spanned by multilinear monomials of degree at most s.

$\therefore \{\tilde{f}_1, \dots, \tilde{f}_m\} \cup \{\tilde{g}_1, \dots, \tilde{g}_t\}$ have the same spanning set as before of size $\sum_{i=0}^{s} \binom{n}{i}$

Claim $\{\tilde{f}_1, \dots, \tilde{f}_m\} \cup \{\tilde{g}_1, \dots, \tilde{g}_t\}$ is lin. ind.

If this claim is true, then $m + t \le \sum_{i=0}^{s} \binom{n}{i}$, i.e., $m \le \sum_{i=0}^{s} \binom{n}{i} - \sum_{i=1}^{s} \binom{n-1}{i-1} = \sum_{i=0}^{s} \binom{n-1}{i}$

Claim $\{\tilde{f}_1, \dots, \tilde{f}_m\} \cup \{\tilde{g}_1, \dots, \tilde{g}_t\}$ lin. ind.

By Multilinear lemma, its enough to prove $\{f_1, \dots, f_m\} \cup \{g_1, \dots, g_t\}$ is lin ind.

We already know $\{f_1, \dots, f_m\}$ is lin. ind.

Since $h_j(x)$ are distinct monomials, they are lin. ind. and so $\{g_1, \dots, g_t\}$ are also lin. ind.

$\left[\sum \alpha_i g_i = 0 \Rightarrow (x_1 - 1)(\sum \alpha_i h_i) = 0 \Rightarrow \sum \alpha_i h_i = 0 \Rightarrow \alpha_i = 0 \pmod p \right]$

Claim $\{\tilde{f}_1, \dots, \tilde{f}_m\} \cup \{\tilde{g}_1, \dots, \tilde{g}_t\}$ lin. ind.

By Multilinear lemma, its enough to prove $\{f_1, \dots, f_m\} \cup \{g_1, \dots, g_t\}$ is lin ind.

We already know $\{f_1, \dots, f_m\}$ is lin. ind.

Since $h_j(x)$ are distinct monomials, they are lin. ind. and so $\{g_1, \dots, g_t\}$ are also lin. ind.

$\left[\sum \alpha_i g_i = 0 \Rightarrow (x_1 - 1)(\sum \alpha_i h_i) = 0 \Rightarrow \sum \alpha_i h_i = 0 \Rightarrow \alpha_i = 0 \pmod p \right]$

Let $p(x) = \sum_{i=1}^{m} \alpha_i f_i(x) + \sum_{j=1}^{t} \beta_j g_j(x) = 0$

To Show: $\alpha_i = 0 \ \forall i$ & $\beta_j = 0 \ \forall j$

Claim $\{\tilde{f}_1, \dots, \tilde{f}_m\} \cup \{\tilde{g}_1, \dots, \tilde{g}_t\}$ lin. ind.

By Multilinear lemma, its enough to prove $\{f_1, \dots, f_m\} \cup \{g_1, \dots, g_t\}$ is lin ind.

We already know $\{f_1, \dots, f_m\}$ is lin. ind.

Since $h_j(x)$ are distinct monomials, they are lin. ind.

and so $\{g_1, \dots, g_t\}$ are also lin. ind.

$\left[\sum \alpha_i g_i = 0 \Rightarrow (x_1 - 1)(\sum \alpha_i h_i) = 0 \right.$
$\left. \Rightarrow \sum \alpha_i h_i = 0 \Rightarrow \alpha_i = 0 \pmod p \right]$

Let $p(x) = \sum_{i=1}^{m} \alpha_i f_i(x) + \sum_{j=1}^{t} \beta_j g_j(x) = 0$ To Show: $\alpha_i = 0 \ \forall i$ & $\beta_j = 0 \ \forall j$

Let $A_i' = A_i \cup \{1\} \ \forall i$ and let y_i be incidence vector of A_i'
(note y_i has 1 as its first coordinate)

$p(y_i) = \sum_{i=1}^{m} \alpha_i f_i(y_i) + 0 \quad (\because g_j(y_i) = 0 \ \forall j)$

<u>Claim</u> $\{\tilde{f}_1, \ldots, \tilde{f}_m\} \cup \{\tilde{g}_1, \ldots, \tilde{g}_t\}$ lin. ind.

By Multilinear lemma, its enough to prove $\{f_1, \ldots, f_m\} \cup \{g_1, \ldots, g_t\}$ is lin ind.

We already know $\{f_1, \ldots, f_m\}$ is lin. ind.

Since $h_j(x)$ are distinct monomials, they are lin. ind. and so $\{g_1, \ldots, g_t\}$ are also lin. ind.

$$\left[\begin{array}{l} \sum \alpha_i g_i = 0 \Rightarrow (x_1 - 1)(\sum \alpha_i h_i) = 0 \\ \Rightarrow \sum \alpha_i h_i = 0 \Rightarrow \alpha_i = 0 \pmod p \end{array} \right]$$

$$\text{Let } p(x) = \sum_{i=1}^{m} \alpha_i f_i(x) + \sum_{j=1}^{t} \beta_j g_j(x) = 0$$

To show: $\alpha_i = 0 \ \forall i$ & $\beta_j = 0 \ \forall j$

Let $A_i' = A_i \cup \{1\} \ \forall i$ and let y_i be incidence vector of A_i' (note y_i has 1 as its first coordinate)

$$p(y_i) = \sum_{i=1}^{m} \alpha_i f_i(y_i) + 0 \quad (\because g_j(y_i) = 0 \ \forall j)$$

<u>Note that</u> $A_j' \cap A_i' = A_j \cap A_i \ \forall i \leq j$

(For $j \geq q$, $1 \in A_j$, so $A_j' = A_j$.
For $j < q$, $1 \notin A_j$ and since $i \leq j < q$, $1 \notin A_i$ also)

Claim $\{\tilde{f}_1, \dots, \tilde{f}_m\} \cup \{\tilde{\tilde{g}}_1, \dots, \tilde{g}_t\}$ lin. ind.

By Multilinear lemma, its enough to prove $\{f_1, \dots, f_m\} \cup \{g_1, \dots, g_t\}$ is lin ind.

We already know $\{f_1, \dots, f_m\}$ is lin. ind.

Since $h_j(x)$ are distinct monomials, they are lin. ind.
and so $\{g_1, \dots, g_t\}$ are also lin. ind.
$\left[\sum \alpha_i g_i = 0 \Rightarrow (x_1 - 1)(\sum \alpha_i h_i) = 0 \Rightarrow \sum \alpha_i h_i = 0 \Rightarrow \alpha_i = 0 \pmod p \right]$

Let $p(x) = \sum_{i=1}^{m} \alpha_i f_i(x) + \sum_{j=1}^{t} \beta_j g_j(x) = 0$ To Show: $\alpha_i = 0 \ \forall i$ & $\beta_j = 0 \ \forall j$

Let $A_i' = A_i \cup \{1\} \ \forall i$ and let y_i be incidence vector of A_i'
(note y_i has 1 as its first coordinate)

$p(y_i) = \sum_{i=1}^{m} \alpha_i f_i(y_i) + 0$ $(\because g_j(y_i) = 0 \ \forall j)$

Note that $\underline{A_j' \cap A_i = A_j \cap A_i \ \text{if } i \leq j}$

$\therefore f_i(y_j) = \Pi(y_j \cdot v_i - \ell) = \Pi(|A_j' \cap A_i| - \ell) = \Pi(|A_j \cap A_i| - \ell) = f_i(v_j)$ for $i \leq j$

We know $f_i(v_j) = 0 \ \forall i \neq j$, so ?

Claim $\{\tilde{f}_1, \ldots, \tilde{f}_m\} \cup \{\tilde{g}_1, \ldots, \tilde{g}_t\}$ lin. ind.

By Multilinear lemma, its enough to prove $\{f_1, \ldots, f_m\} \cup \{g_1, \ldots, g_t\}$ is lin ind.

We already know $\{f_1, \ldots, f_m\}$ is lin. ind.

Since $h_j(x)$ are distinct monomials, they are lin. ind. and so $\{g_1, \ldots, g_t\}$ are also lin. ind. $\left[\sum \alpha_i g_i = 0 \Rightarrow (x_1 - 1)(\sum \alpha_i h_i) = 0 \Rightarrow \sum \alpha_i h_i = 0 \Rightarrow \alpha_i = 0 \pmod{p} \right]$

$$\text{Let } p(x) = \sum_{i=1}^{m} \alpha_i f_i(x) + \sum_{j=1}^{t} \beta_j g_j(x) = 0$$

To Show: $\alpha_i = 0 \ \forall i$ & $\beta_j = 0 \ \forall j$

Let $A_i' = A_i \cup \{1\} \ \forall i$ and let y_i be incidence vector of A_i' (note y_i has 1 as its first coordinate)

$$p(y_i) = \sum_{i=1}^{m} \alpha_i f_i(y_i) + 0 \qquad (\because g_j(y_i) = 0 \ \forall j)$$

Note that $\underline{A_j' \cap A_i' = A_j \cap A_i \ \ \forall i \leq j}$

$\therefore f_i(y_j) = \prod (y_j \cdot v_i - \ell) = \prod(|A_j' \cap A_i| - \ell) = \prod(|A_j \cap A_i| - \ell) = f_i(v_j)$ for $i \leq j$

We know $f_i(v_j) = 0 \ \forall i \neq j$, so evaluating $p(x)$ at $y_m, y_{m-1}, \ldots, y_1$ gives us $\underline{\alpha_m = 0}, \underline{\alpha_{m-1} = 0}, \ldots, \underline{\alpha_1 = 0}$.

Claim $\{\tilde{f}_1, \dots, \tilde{f}_m\} \cup \{\tilde{g}_1, \dots, \tilde{g}_t\}$ lin. ind.

By Multilinear lemma, its enough to prove $\{f_1, \dots, f_m\} \cup \{g_1, \dots, g_t\}$ is lin ind.

We already know $\{f_1, \dots, f_m\}$ is lin. ind.

Since $h_j(x)$ are distinct monomials, they are lin. ind.
and so $\{g_1, \dots, g_t\}$ are also lin. ind.

$$\left[\sum \alpha_i g_i = 0 \Rightarrow (x_1 - 1)\left(\sum \alpha_i h_i\right) = 0 \Rightarrow \sum \alpha_i h_i = 0 \Rightarrow \alpha_i = 0 \pmod p \right]$$

Let $p(x) = \sum_{i=1}^{m} \alpha_i f_i(x) + \sum_{j=1}^{t} \beta_j g_j(x) = 0$ To Show: $\alpha_i = 0 \ \forall i$ & $\beta_j = 0 \ \forall j$

Let $A_i' = A_i \cup \{1\} \ \forall i$ and let y_i be incidence vector of A_i'

$$p(y_i) = \sum_{i=1}^{m} \alpha_i f_i(y_i) = 0$$

Backword substitution

$$p(y_m) = \sum_{i=1}^{m} \alpha_i f_i(y_m) = \alpha_m f_m(y_m) = 0 \Rightarrow \alpha_m = 0,$$ & so on, $\alpha_i = 0 \ \forall i.$

$$\therefore p(x) = 0 + \sum_{j=1}^{t} \beta_j g_j(x) = 0 \Rightarrow \beta_1 = \beta_2 = \dots = \beta_j = 0,$$ since $\{g_1, \dots, g_t\}$ lin. ind

$\blacksquare$

Theorem [Ray-Chaudhuri – Wilson 1975]

Let $n \geq 2s$, $|L| = s$. Suppose $\mathcal{F}$ is an L-intersecting k-uniform family of subsets of $[n]$ $\left(\mathcal{F} \subseteq \binom{[n]}{k}\right)$.
Then $|\mathcal{F}| \leq \binom{n}{s}$

Proof HW problem #2.

Follow the proof of Snevily's Thm.

- Define $f_1, \dots, f_m$. Show they are lin. ind.
- Define $g_1, \dots, g_t$ using $h_1, \dots, h_t$ and $c_1, \dots, c_t$

similar but not the same as in previous proof. (exploit the fact $\mathcal{F}$ is k-uniform here)

(Ques: Can we assume $k \notin L$?)

- Show lin. ind.
- Find spanning set

Similar (& more) results have been proved for intersecting families of vector spaces, lattices, etc.

Theorem [Frankl, Graham 1985]

Let q be a prime power. Let V be a finite-dimensional vector space over $\mathbb{F}_q$. Let $L \subseteq \mathbb{Z}^+ \cup \{0\}$.

Let $\mathcal{F}$ be a family of k-dimensional subspaces of V.

If $\dim(V_1 \cap V_2) \in L$ $\forall V_1 \neq V_2$ in $\mathcal{F}$, then $|\mathcal{F}| \leq \begin{bmatrix} n \\ s \end{bmatrix}_q$

where $$\begin{bmatrix} n \\ s \end{bmatrix}_q = \frac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-s+1}-1)}{(q^s-1)(q^{s-1}-1)\cdots(q-1)}$$ ← q-Gaussian coefficient.