极值组合

32个人组 clubs:

odd:

(1) each club has an even number of members

(2) every pair of clubs share even number of members

(3) club与club不能相同.

maximal nums of clubs? (containing a club with 0 members)

even:

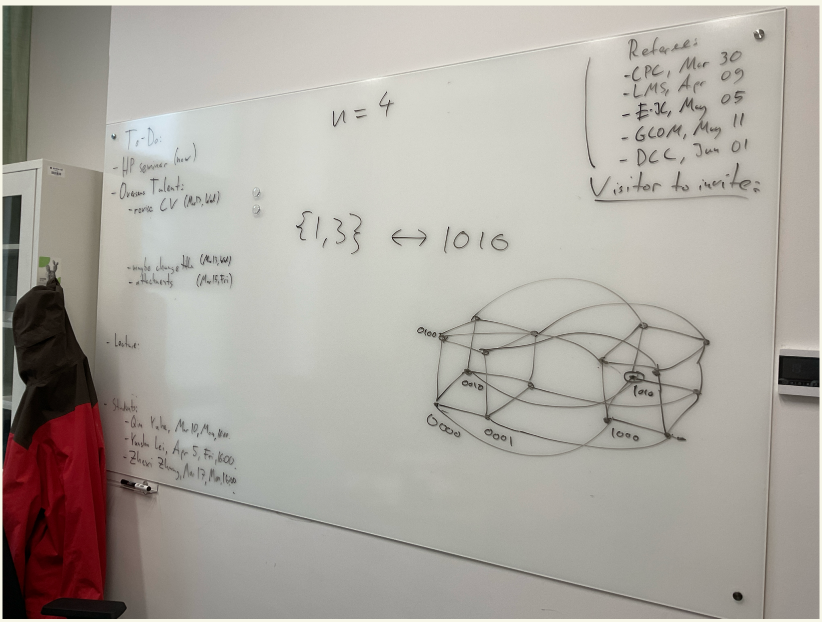
(1) each club has an odd number of members

(2) every pair of clubs share even number of members

maximal nums of clubs?

若#j 公民 $\in C_i$, 那 v_i 的第 j 位是 1.

若#j $\notin C_i$, 那 v_i 的第 j 位是 0.



examples sets ⊆ E
purpose

Lecture Notes for [1, § 5.5, 5.6].

Q (Hadwiger, 1944):

> What is the minimum number $c(n)$ s.t. $\mathbb{R}^n$ can be divided into $c(n)$ subsets $\mathbb{R}^n = S_1 \cup \cdots \cup S_{c(n)}$ s.t. no pair of points within the the same S_i is at unit distance?

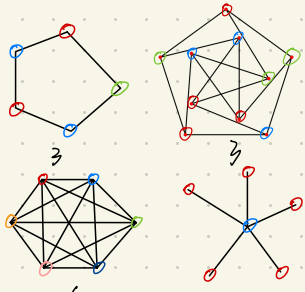
To solve the problem, firstly rephrasing it in graph theory language:

Def. The distance-δ graph in $\mathbb{R}^n$ has the (infinite) set $\mathbb{R}^n$ as its vertex set (how to describe it better?); two points are adjacent if their (Euclidean) distance is δ. The unit-distance graph corresponds to $\delta = 1$.

Now the number $c(n)$ Hadwiger asks us to determine is the chromatic number of the unit-distance graph.

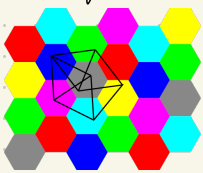
the smallest number of colors needed to label the graph's vertices with colors s.t. no two vertices sharing the same edge have the same color

Eg.



When $n=2$ (Considering the problem in the plane):

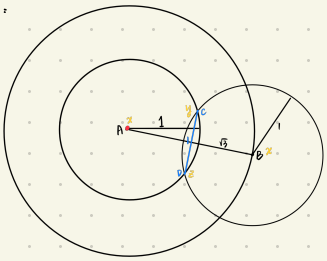
Exe. 5.5.1



From the existence of tessellation of the plane by regular hexagons, with diameters slightly less than one.

$\therefore c(2) \le 7$

Exe. 5.5.2



$\therefore c(2) \ge 4$

$\forall A \in \mathbb{R}^2$, suppose the color of A is x. Make two circles of radius 1 and $\sqrt{3}$ by A as the origin. $\forall B \in O(A, \sqrt{3})$. Make a circle of radius 1 by B as the origin.

Then we have $C, D \in O(A,1) \cap O(B,1)$ and $d(C,D) = 1$.

Thus, the color of A, C, D and B, C, D must be different. Suppose the color of C is y and the color of D is z. Then the color of B is x.

By induction, $\forall P \in O(A, \sqrt{3})$, the color of P is x, but must $\exists P_1, P_2 \in O(A, \sqrt{3})$ s.t. $d(P_1, P_2) = 1$. $\lightning$

For general n:

Exe. 5.5.3 $c(n) \le n^{\frac{n}{2}}$. (the chromatic number is finite)

the longest distance inside a cube with diameter d is $\sqrt{nd^2}$.

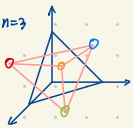
we wanna divide them with the longest distance less than 1.

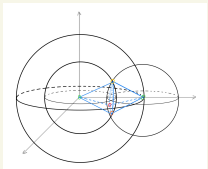
$\sqrt{nd^2} = 1$, $nd^2 = 1$, $d = \frac{1}{\sqrt{n}}$. We can divide a cube with diameter 1 into $(\frac{1}{\sqrt{n}})^n = n^{\frac{n}{2}}$ small cubes with diameter $\frac{1}{\sqrt{n}}$. And paint them with $n^{\frac{n}{2}}$ different colors

The simplex with unit sidelength shows that we need at least $n+1$ colors. And by the idea of Exe. 5.5.2 can be adapted to improve this lower bound to $n+2$.

when $n=2$

when $n=3$





$c(n) \geq cn^2$ for some constant $c>0$ and all sufficiently large n

1972, Larman and Rogers gives the first nonlinear lower bound $\Omega(n^2)$ and an upper bound of $(2\sqrt{2}+o(1))^n$. (Exe. 5.5.4.) And conjectured that the true rate of growth of this function is exponential

◇**Ex. 5.5.4.*** Prove: a simply exponential number (C^n for some constant C) of colors suffices for the n-space for every n.

Hint. Color $\mathbb{R}^n$ by 9^n colors. Use a sphere packing argument: pick a maximal set of points at distance $\geq 1/2$ apart; color these points so that no two of them at distance ≤ 2 receive the same color.

Take an (infinite) set $H \subset \mathbb{R}^n$, maximal w.r.t. distance between any two of its points is $\geq \frac{1}{2}$.

Let $H(r)$ denote the union of open balls of radius r about each point in H. Observe that $H(\frac{1}{2}) = \mathbb{R}^n$.

Let now G be the (infinite) graph with vertex set H, and two points adjacent if their distance is < 2.

Since the open balls of radius $\frac{1}{4}$ about the points of H are disjoint, and at most 9^n such balls fit inside a ball of radius $(\frac{9}{4})^n$.

Use this we color G by $\leq 9^n$ colors. Finally, for $\forall u \in \mathbb{R}^n$, find a point $h(u) \in H$ within distance $< \frac{1}{2}$ from u, and assign u the color of $h(u)$. Since the open balls of radius $\frac{1}{4}$ about the points of H are disjoint, points at unit distance recieve different colors.

It was confirmed by Frankl and Wilson in 1981, as a rather direct sequence of their modular version of the RW Theorem (Thm 7.15).

1981, Frankl and Wilson confirmed

Thm. For large n, the chromatic number of the unit-distance graph on $\mathbb{R}^n$ is greater than 1.2^n.

(both $= c(n)$)

pf. Unit-distance graph and the distance-δ graph on $\mathbb{R}^n$ are isomorphic for $\forall \delta > 0$, so their chromatic number is the same.

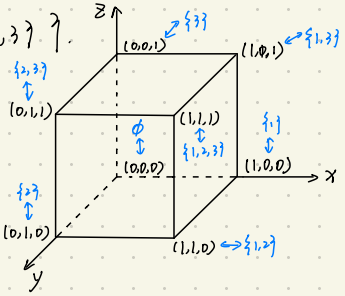
Claim: The distance-δ graph of some subset S of the unit cube $\Omega = \{0,1\}^n$ has exponentially large chromatic number for some $\delta > 0$. where δ depends on n.

Each subset $S \subseteq \Omega$ corresponds to a set system $\mathcal{H} \subseteq 2^{[n]}$.

Eg. when $n=3$. $2^{[n]} = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$.

the vertices are $\Omega = \{0,1\}^3$.

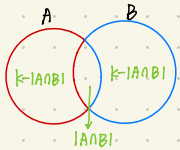
We write $S = S(\mathcal{H})$ to indicate the inverse of this correspondence: $S(\mathcal{H})$ consists of the incidence vectors of the members of $\mathcal{H}$.



Let $d(A,B)$ denote the (Euclidean) distance of the incidence vectors of the sets $A, B \in \mathcal{H}$.

Clearly, $d(A,B)^2$ is the size of the symmetric difference of A and B. (the square of the difference of different elts is 1 while common

elts is 0)



Assume henceforth that $\mathcal{H}$ is k-uniform. Then $d(A,B)^2 = 2(k-|A\cap B|)$ (determined by the intersection sizes)

Then we can use ↓ Avoiding a particular distance amounts to avoiding a particular intersection size.

Corollary 5.18 (Omitted Intersection Theorem). *Let p be a prime number and $\mathcal{F}$ a $(2p-1)$-uniform family of subsets of a set of $4p-1$ elements. If no two members of $\mathcal{F}$ intersect in precisely $p-1$ elements, then*

$$|\mathcal{F}| \le 2\cdot\binom{4p-1}{p-1} < 1.7548^{4p-1}. \tag{13}$$

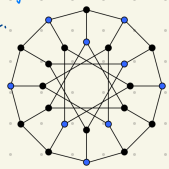
Assume for now that $n=4p-1$ for some prime p. Set $k=2p-1$. Then the intersection size to be avoided should be $p-1$, this corresponds to distance $\delta^2 = 2(2p-1-(p-1)) = 2p$, $\delta=\sqrt{2p}$. With this choice of parameters, the graph G_p we examine has vertex set $\mathcal{H}_p = \binom{[4p-1]}{2p-1}$ (we assume it is $(2p-1)$-uniform; dimension of the space $= 4p-1$)

and two sets $A, B \in \mathcal{H}_p$ are adjacent if $|A\cap B| = p-1$.

We shall prove an exponential lower bound on the chromatic number $\chi(G_p)$. Our strategy is to prove an upper bound on $\alpha(G_p)$, the size of the largest independent set.

An independent set in G is a subset $W\subseteq V$ which induces an empty subgraph (deleting vertices (and their incident edges))

Eg.



the 9 blue vertices form a maximum independent set for the Generalized Peterson Graph $GP(12,4)$, its size is 9.

The size of the largest independent set in G is denoted by $\alpha(G)$.

Actually, Cor 5.18 tells us that $\alpha(G_p) = |\mathcal{F}| \le 2\binom{4p-1}{p-1}$

Indeed, by the definition of adjacency in G_p, no two members of $\mathcal{F}$ intersect in precisely $p-1$ elts; hence Cor 5.18 applies.

Our final step is an application of Prop 2.35.

Proposition 2.35. *Let $\mathcal{G}$ be a graph with n vertices. The following relation holds between the chromatic number $\chi(\mathcal{G})$ and the independence number $\alpha(\mathcal{G})$:*

$$\chi(\mathcal{G}) \ge n/\alpha(\mathcal{G}). \tag{47}$$

Indeed, every color class in a legal coloring is an independent set, so $\chi(\mathcal{G})$ sets each of size $\le \alpha(\mathcal{G})$ add up to the set of vertices of $\mathcal{G}$.

Thus, we have $\chi(G_p) \ge \frac{|\mathcal{H}_p|}{\alpha(G_p)} \ge \frac{\binom{4p-1}{2p-1}}{2\cdot\binom{4p-1}{p-1}} = \frac{\frac{(4p-1)(4p-2)\cdots(2p+1)}{(2p-1)!}}{2\cdot\frac{(4p-1)\cdots(2p+1)}{(p-1)!}} = \frac{3p(3p-1)\cdots(2p+1)}{(p+1)\cdots(2p-1)2p} = \frac{(3p)!\,p!}{((2p)!)^2}$

By Stirling $n! \sim \sqrt{2\pi n}\left(\frac{n}{e}\right)^n$,

We have $\frac{(3p)!\,p!}{((2p)!)^2} \sim \frac{\sqrt{2\pi(3p)}\left(\frac{3p}{e}\right)^{3p}\sqrt{2\pi p}\left(\frac{p}{e}\right)^{p}}{\sqrt{2\pi(2p)}\left(\frac{2p}{e}\right)^{2p}} = \frac{\sqrt{3}}{2}\cdot\left(\frac{27}{16}\right)^p$. (*)

$\frac{27}{16} = 1.688$, and $\left(\frac{27}{16}\right)^{\frac{1}{4}} = 1.13975\cdots$. As $\frac{\sqrt{3}}{2} = 0.866025\cdots$, close to $\left(\frac{16}{27}\right)^{\frac{1}{4}} = 0.877382\cdots$

$\therefore$ We have $\frac{(3p)!\,p!}{((2p)!)^2} > 1.1397^{4p-1}$ (when p is sufficiently large)

That is $\chi(G_p) > 1.1397^{4p-1}$ (when p is sufficiently large)

This means the chromatic number of the distance-$\sqrt{2p}$ graph of the set $S(\mathcal{H}_p)\subset\mathbb{R}^{4p-1}$ is greater than 1.1397^{4p-1}

(when p is large enough). It follows $c(n) > 1.1397^n$ for all $n = 4p-1$, p prime and large enough.

By the density of prime numbers, extends this result to proving that $c(n) > 1.139^n$ for all sufficiently large n.

♢**Ex. 5.5.5.** Extend the lower bound $c(4p-1) > 1.139^{4p-1}$ to a bound $c(n) > 1.139^n$, valid for all sufficiently large n.

The Prime Number Theorem asserts for $\forall\, \varepsilon > 0$ and sufficiently large x, the number of primes not larger than x is between the bounds $(1+\varepsilon)\frac{x}{\ln x}$.

Let p be the largest prime s.t. $n > 4p-1$. By thm, $\forall\, \varepsilon > 0$, and every sufficiently large x, $\exists$ prime number p between $(1-\varepsilon)x$ and x.

Applying this to $x = \frac{n}{4}$, we find a prime number s.t. $(1-\varepsilon)n < 4p < n$, therefore

$$c(n) > c(4p-1) > 1.1397^{4p-1} > 1.1397^{(1-\varepsilon)n} > 1.139^n$$

when ε is small enough. □

Actually, we can achieve the lower bound 1.2^n (Exe. 5.5.7.)

Ex. 5.5.6. Let $\Omega(n,k) \subset \mathbb{R}^n$ denote the set of incidence vectors of the k-subsets of $[n]$. Prove: for any prime $p < n/2$, the chromatic number of the distance-$\sqrt{2p}$ graph on $\Omega(n, 2p-1)$ is at least

$$\binom{n}{2p-1} \Big/ \binom{n}{p-1}. \tag{20}$$

♢**Ex. 5.5.7.** In order to improve the lower bound on the chromatic number of the unit-distance graph in $\mathbb{R}^n$, maximize, for fixed n, the quantity (20).

Hint. Use the "entropy function" estimate for the binomial coefficients (Ex. 5.4.4).

Ex. 5.4.4. For $0 < \alpha < 1$, let

$$\widetilde{H}(\alpha) = \frac{1}{\alpha^\alpha (1-\alpha)^{1-\alpha}}. \tag{15}$$

($H(\alpha) = \log_2 \widetilde{H}(\alpha) = -\alpha \log_2 \alpha - (1-\alpha)\log_2(1-\alpha)$ is the "entropy function.") Derive the following asymptotic estimate for binomial coefficients not too close to either tail. Assume αn is an integer.

$$\binom{n}{\alpha n} = \frac{1+o(1)}{\sqrt{2\pi\alpha(1-\alpha)}} \cdot \frac{1}{\sqrt{n}} \cdot (\widetilde{H}(\alpha))^n. \tag{16}$$

Here, the $o(1)$ notation indicates a quantity that tends to zero as $n \to \infty$ (cf. p. xiii), assuming $\gamma < \alpha < 1-\gamma$ for some constant γ (which does not depend on n).

Hint. Use Stirling's formula: $n! = (n/e)^n \sqrt{2\pi n}(1+o(1))$.

Setting $\alpha = \frac{p-1}{n}$, $\beta = \frac{2p-1}{n}$, we have to maximize

$$\frac{\alpha^\alpha (1-\alpha)^{1-\alpha}}{\beta^\beta (1-\beta)^{1-\beta}}.$$

Noting that $\beta \approx 2\alpha$, set $\beta = 2\alpha$, we have $\dfrac{\alpha^\alpha (1-\alpha)^{1-\alpha}}{4^\alpha \alpha^{2\alpha} (1-2\alpha)^{1-2\alpha}} = \dfrac{(1-\alpha)^{1-\alpha}}{(4\alpha)^\alpha (1-2\alpha)^{1-2\alpha}}$ reaches its maximum when $\alpha = \frac{2-\sqrt{2}}{4}$.

And its maximal value is $1.20\overline{7}\cdots$.

By the Prime Number Theorem, we can select a prime $p = (1+o(1))\alpha n$. So for large n, the chromatic number of the distance-$\sqrt{2p}$ graph of the unit cube is $> 1.2^n$, and thereby $c(n) > 1.2^n$.

$$c(n) \geq \frac{\binom{n}{\geq p-1}}{\binom{n}{p-1}} = \frac{\frac{1+o(1)}{\sqrt{2\pi\beta(1-\beta)}} \cdot \frac{1}{\sqrt{n}} \cdot \left(\alpha^\alpha (1-\alpha)^{1-\alpha}\right)^n}{\frac{1+o(1)}{\sqrt{2\pi\alpha(1-\alpha)}} \cdot \frac{1}{\sqrt{n}} \cdot \left(\beta^\beta (1-\beta)^{1-\beta}\right)^n} \leq 1.20\overline{7}^n \sqrt{\frac{\alpha(1-\alpha)}{\beta(1-\beta)}} \approx 1.20\overline{7}^n \sqrt{\frac{(1-\alpha)}{2(1-2\alpha)}}$$

($\approx 0.77688\cdots$ when $\alpha = \frac{2-\sqrt{2}}{4}$). □

Hadwiger's question for $\mathbb{Q}^n$

- the same upper bound remains valid
- the lower bound for $\frac{1}{\sqrt{2p}}\Omega$ are a set of points with irrational coordinates not in $\mathbb{Q}^n$

By Exe 5.8.3, when n is divisible by 4, $\mathbb{Q}^n$ contains an isometric copy of $\frac{1}{\sqrt{2p}}\Omega$.

Theorem 5.22 (Babai, 1992). *For large n, the chromatic number of the unit-distance graph on $\mathbb{Q}^n$ is greater than 1.2^n.*

◇Ex. 5.5.16. Show that the result of the preceding exercise holds in any dimension, divisible by 4.

Create a $4k \times 4k$ matrix consisting of 4×4 diagonal blocks $\begin{pmatrix} \alpha & \beta & \gamma & \delta \\ \beta & -\alpha & \delta & -\gamma \\ \gamma & -\delta & -\alpha & \beta \\ \delta & \gamma & -\beta & -\alpha \end{pmatrix}$ as zero else where. Each row of the matrix has norm $\sqrt{\alpha^2+\beta^2+\gamma^2+\delta^2}$, and the rows are pairwise orthogonal.

◇Ex. 5.5.18. Prove the lower bound 1.2^n for the chromatic number of the unit-distance graph in $\mathbb{Q}^n$ (Theorem 5.22).

Hint. Read the paragraph before Theorem 5.22.

pf. First, let $n = 4l + \varepsilon$ where $0 \leq \varepsilon \leq 3$, $l \in \mathbb{Z}$. As the solution of Ex 5.5.7, set $\alpha = \frac{2-\sqrt{2}}{4} = 0.1464\cdots$

Select a prime number p closed to $\alpha \cdot 4l$,

By Ex 5.5.6, the chromatic number of the distance-$\sqrt{2p}$ graph on $\Omega(4k, 2p-1)$ is greater than $1.20\overline{7}^{4k}$.

By Ex. 5.5.16, an isometric copy T of $\frac{1}{\sqrt{2p}}\Omega(4k, 2p-1)$ resides in $\mathbb{Q}^{4k} \subseteq \mathbb{Q}^n$.

The unit-distance graph on T is isomorphic to the distance-$\sqrt{2p}$ graph on $\Omega(4k, 2p-1)$; therefore the chromatic number of the unit distance graph on $\mathbb{Q}^n$ is greater than $1.20\overline{7}^{4k} > 1.2^n$ (for large n).

In 1981, Frankl and Wilson extended their modular P.W thm to prime power moduli and replaced by an odd power of 2 in § 5.9. Their result is a "1.15" lower bound. This way $\sqrt{2p}$ became a rational number and the pf above went through. The reason their bound became slightly weaker is that the odd powers of 2 do not populate the set of integers as densely as prime numbers do.

Borsuk conjectured that *every set of diameter 1 in $\mathbb{R}^d$ can be partitioned into $d+1$ sets of smaller diameter.*

Verified for centrally symmetric bodies, bodies with smooth surfaces, bodies in dimension 3 and 2.

Conjecture was disproved by an accidental counterexample. (Also indicates the futility of low dimensional attacks)

Kahn and Kalai showed: some bodies needed to be split into exponentially many ($1.2^{\sqrt{d}}$) pieces if the diameter of each piece was to be reduced.

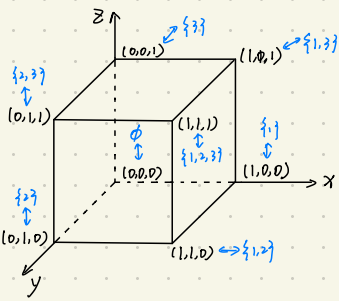
Thm (Kahn-Kalai, 1992) Let $f(d) :=$ the minimal number s.t. $\forall$ set of diameter 1 in $\mathbb{R}^d$ can be partitioned into $f(d)$ pieces of smaller diameter. Then $f(d) > 1.2^{\sqrt{d}}$.

In the other direction, we have $f(d) < 2^d$. (Schramm 1988, $\forall \varepsilon > 0$, sufficiently large d, $f(d) < (\sqrt{\frac{3}{2}}+\varepsilon)^d$)

$f(d)$ might be closed to an exponential function of the form C^d for some constant $C > 1$.

Consider a subset S of the unit cube $\Omega = \{0,1\}^d$. Such a subset corresponds to a set system $\mathcal{F} \subseteq 2^{[d]}$, and we write $S = S(\mathcal{F}) \subset \mathbb{R}^d$ to denote the set of incidence vectors of the members of $\mathcal{F}$. If $\mathcal{F}$ is l-uniform, we obtain $d^2(A,B) = 2(l - |A \cap B|)$ for any $A, B \in \mathcal{F}$. (the maximal $d(A,B)$ occurs when the minimal $|A \cap B|$)

Revision:



Let $\mu(\mathcal{F}) = \min\{|A \cap B| : A, B \in \mathcal{F}\}$

A partition of $S(\mathcal{F})$ into sets of smaller diameter means $\mathcal{F} = \mathcal{F}_1 \cup \cdots \cup \mathcal{F}_t$, $\forall j$, $\max\{d(A,B) : \forall A,B \in \mathcal{F}\}$ of $\mathcal{F}_j$ $> \max\{d(A,B) : \forall A,B \in \mathcal{F}\}$ of $\mathcal{F}$ s.t. $\mu(\mathcal{F}_j) > \mu(\mathcal{F})$ for $\forall j$.

Let $g(\mathcal{F})$ denote the smallest t s.t. it possible. Then $f(d) \geq g(\mathcal{F})$ for any $\mathcal{F} \subset 2^{[d]}$.

Or we can associate G with the set system $\mathcal{F}$ in the following way: the members of $\mathcal{F}$ are the vertices of G and $A, B \in \mathcal{F}$ are adjacent if $|A \cap B| = \mu(\mathcal{F})$. Thus $g(\mathcal{F})$ is the chromatic number $\chi(G)$ (graphs represented by systems)

We shall construct the set system $\mathcal{F}$ s.t. the Graph G it represents according to our "minimum intersection size" adjacent rule will be isomorphic to the graph G_p of the preceding section. (represented there by a set system with the

"intersection size = p-1" adjacent rule.) Therefore the strong lower bound on the chromatic number of G_p

$$\chi(G_p) \geq \frac{|\mathcal{H}_p|}{\alpha(G_p)} \geq \frac{\binom{4p-1}{2p-1}}{\binom{4p-1}{p-1}} > 1.1397^{4p-1} \text{ (eq. (*))} \quad \text{Cor 5.18, Prop 2.35}$$

will apply to our graph G.

Assume for now that d is of the form $\binom{4p-1}{2}$ for some prime number p. We set $n=4p-1$, $k=2p-1$, and $\mathcal{H}_p = \binom{[n]}{k}$. Let $X = \binom{[n]}{2}$; So $|X| = \binom{n}{2} = d$. Our set system $\mathcal{F} \subset 2^X$

We shall associate a set $\Phi(A) \subset 2^X$ with each $A \in \mathcal{H}_p$. Then $\mathcal{F} = \{\Phi(A) : A \in \mathcal{H}_p\}$.

Goal: Make correspondence $A \mapsto \Phi(A)$ s.t. $|A \cap B| = p-1$ iff $|\Phi(A) \cap \Phi(B)| = \mu(\mathcal{F})$, $\forall A, B \in \mathcal{H}_p$

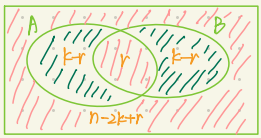
A simple construction: $\Phi(A) = \{\{x,y\} : x \in A,\ y \in [n] \setminus A\}$ $\Phi(A)$ is the set of those pair elements from $[n]$ which are split by A.

So we have $\Phi(A) \subset X$ and $\mathcal{F} = \{\Phi(A) : A \in \mathcal{H}_p\}$ is ℓ-uniform with $\ell = k(n-k)$.

$A \mapsto \Phi(A)$ is 1-1.

Claim: $A \mapsto \Phi(A)$ preserves adjacency.

Assume: $|A \cap B| = r$ $(A, B \in \mathcal{H}_p)$



Then $|\Phi(A) \cap \Phi(B)| = r(n-2k+r) + (k-r)^2 = 2\left(r - (k - \frac{n}{4})\right)^2 - 8\left(k - \frac{n}{4}\right)^2 + k^2$

The minimum of $|\Phi(A) \cap \Phi(B)|$ is attained when r is as closed to $k - \frac{n}{4} = 2p-1 - \frac{1}{4}(4p-1) = p - \frac{3}{4}$, i.e. when $r = p-1$. adjacent

So $G \cong G_p$. Then we have $g(\mathcal{F}) = \chi(G) = \chi(G_p) \geq \frac{|\mathcal{H}_p|}{\alpha(G_p)} \geq \frac{\binom{4p-1}{2p-1}}{\binom{4p-1}{p-1}} > 1.1397^{4p-1} = 1.1397^n$ ↙ holds when p is sufficiently large.

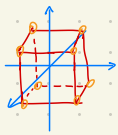
Since $n > \sqrt{2d}$, $f(d) \geq g(\mathcal{F}) > 1.1397^{\sqrt{2d}} > 1.203^{\sqrt{d}}$, completing the pf for all d of the form $d = \binom{4p-1}{2} = (4p-1)(2p-1)$

Using the Prime Number Theorem, we can extend it to all dimensions of d. □

Lecture Notes for [3].

C^n: { vertices of the standard n-dimensional cube of edge length 2 and centered at the origin.

↳ $\{(\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_n) : \varepsilon_i = \pm 1, \forall i\}$



Orthogonal $P=(\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_n)$ & $Q=(\delta_1, \delta_2, \cdots, \delta_n)$: $\sum_{i=1}^{n} \varepsilon_i \delta_i = 0$

Problem 1. (1972, Larman & Rogers) Determine or estimate the maximum number $m(n)$ of vertices of C^n s.t. no two are orthogonal.

Case 1. n is odd ($\exists k \in \mathbb{N}, n=2k+1$). $m(2k+1) = 2^{2k+1}$. (the biggest set)

pf: $\sum_{i=1}^{2k+1} \varepsilon_i \delta_i$ must be the sum of odd number of 1 and even number of -1 or even number of 1 and odd number of -1.

Case 2. $\exists k \in \mathbb{N}$, $n=4k+2$. $m(4k+2) = 2^{4k+1}$

pf: Step 1. $C_{even}^{4k+2} := \{(\varepsilon_1, \varepsilon_2, \cdots \varepsilon_{4k+2}) : \varepsilon_i = 1 \text{ holds an even number of times}\}$.

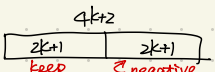
For P in C_{even}^{4k+2}, suppose $\varepsilon_i = 1$ holds $2m$ of times; for Q in C_{even}^{4k+2}, suppose $\varepsilon_i' = 1$ holds $2n$ of times. And they have $\varepsilon_i = \varepsilon_i' = 1$ holds for u times. Then

$$\sum_{i=1}^{4k+2} \varepsilon_i \varepsilon_i' = u - (2m-u) - (2n-u) + (4k+2-2m-2n+u) = u - 2m + u - 2n + u + 4k + 2 - 2m - 2n + u = 4(k+u-m-n) + 2 \neq 0$$

$2m$		$4k+2-2m$	
u	$2m-u$	$2n-u$	$\cdots$
$1 \times 1 = 1$	$1 \times (-1) = -1$	$(-1) \times 1 = -1$	$(-1) \times (-1) = 1$

∴ At least, in C_{even}^{4k+2}, no two vertices are orthogonal.

∴ $m(4k+2) \geq 2^{4k+1}$.



Step 2. For $\vec{\varepsilon} = (\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_{4k+2})$, $\vec{\varepsilon}^* := (\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_{2k+1}, -\varepsilon_{2k+2}, -\varepsilon_{2k+3}, \cdots, -\varepsilon_{4k+2})$

Then obv. $\varepsilon \cdot \varepsilon^* = 0$, and $(\varepsilon^*)^* = \varepsilon$.

Suppose $\mathcal{C} \subset C^{4k+2}$ and there are no orthogonal points in $\mathcal{C}$. Then $\mathcal{C}^* := \{\varepsilon^* : \varepsilon \in \mathcal{C}\}$.

Obv. we have $\mathcal{C}^* \cap \mathcal{C} = \phi$ and $|\mathcal{C}^*| = |\mathcal{C}|$.

∴ $|\mathcal{C}| \leq \frac{1}{2} \cdot 2^{4k+2} = 2^{4k+1}$.

☆ Case 3. $\exists k \in \mathbb{N}$, $n=4k$.

Larman and Rogers: large k, $m(4k) \ll \frac{2^{4k}}{k^2}$

Rödl and P. Frankl: $\exists$ very small $\gamma > 0$ s.t. $m(4k) < (2-\gamma)^{4k}$.

This paper: The exact value of $m(4k)$ when k is the power of an odd prime.

Thm 1.3 Suppose $k=p^\alpha$, $\alpha\geq 1$, $p\geq 3$, p prime, then

$$m(4k)=4\sum_{i=0}^{k-1}\binom{4k-1}{i}<\frac{4^{4k}}{3^{3k}} \text{ holds.} \quad (\star)$$

To give a proof, we need some coding theory vision of problem 1.1:

Def. A (binary) code of length n over the alphabet $\{a,b\}$ is a collection $\mathcal{C}$ of sequences, which are called codewords $\vec{x}=(x_1,x_2,\cdots,x_n)$ $x_i\in\{a,b\}$ $\forall i$.

Def. The (Hamming) distance of two cordwords $\vec{x}$ and $\vec{y}$ is defined by $d(\vec{x},\vec{y})=\#i: x_i\neq y_i$.

Note: • $d(x,y)\in\{0,1,\cdots,n\}$

• $d(x,y)=0 \iff \vec{x}=\vec{y}$.

For $\mathcal{C}\subset C^n$, it can be seen as a code of length n over the alphabet $\{1,-1\}$.

Obv. $\vec{\varepsilon}=(\varepsilon_1,\varepsilon_2,\cdots,\varepsilon_n)$, $\vec{\delta}=(\delta_1,\delta_2,\cdots,\delta_n)$ are orthogonal $\iff$ $d(\vec{\varepsilon},\vec{\delta})=\frac{n}{2}$.

One of the principle problem of coding theory:

Problem 1.4 Given a set $D\subset\{1,2,\cdots,n\}$, determine or estimate the maximum number $m(n,D)$ of codewords in a code $\mathcal{C}$ of length n satisfying $d(\vec{x},\vec{y})\in D$ for all distinct $\vec{x},\vec{y}\in\mathcal{C}$.

A classical result gives: $m(n,D)\leq\sum_{i=0}^{|D|}\binom{n}{i}$.

Then we can say $m(n)=m(n,\{1,2,\cdots,n\}-\{\frac{n}{2}\})$. For even n, we have $m(n)\leq\sum_{i=0}^{2n-1}\binom{n}{i}=\sum_{i=0}^{2n}\binom{n}{i}-1=2^n-1$.

Then we can prove $(\star)$ from the following: (Thm 1.6 we'll prove later)

Thm 1.6 Suppose $k=p^\alpha$, p prime, $p\geq 3$, $\alpha\geq 1$, $\mathcal{C}$ is a code of length l s.t. $k\nmid d(x,y)$ holds for all distinct $\vec{x},\vec{y}\in\mathcal{C}$. Then

$$|\mathcal{C}|\leq\sum_{i=0}^{k-1}\binom{l}{i} \text{ holds.}$$

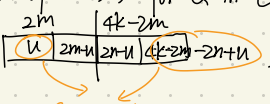
It means $m(l,\{1,2,\cdots,l\}-\{k,2k,\cdots\})\leq\sum_{i=0}^{k-1}\binom{l}{i}$.

Proof of Thm 1.3:

Suppose $\mathcal{C}\subset C^{4k}$ contains no pair of orthogonal points, i.e. $\forall\vec{x},\vec{y}\in\mathcal{C}$, $d(\vec{x},\vec{y})\neq 2k$.

Define $\mathcal{C}_{even}:=\{\vec{x}=(x_1,x_2,\cdots,x_n)\in\mathcal{C}: \#i: x_i=1 \text{ is even}\}$, $\mathcal{C}_{odd}:=\{\vec{x}=(x_1,x_2,\cdots,x_n)\in\mathcal{C}: \#i: x_i=1 \text{ is odd}\}$.

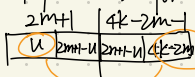
For P in $\mathcal{C}_{even}$, suppose $\varepsilon_i=1$ holds $2m$ of times; for Q in $\mathcal{C}_{even}$, suppose $\varepsilon_i'=1$ holds $2n$ of times. And they have $\varepsilon_i=\varepsilon_i'=1$ holds for u times. Then



$d(P,Q)$ is even.

Sum $=4k-2m-2n+2u$, even.

For P in $\mathcal{C}_{odd}$ suppose $\varepsilon_i=1$ holds $2m+1$ of times; for Q in $\mathcal{C}_{odd}$ suppose $\varepsilon_i=1$ holds $2n+1$ of times. And they have $\varepsilon_i=\varepsilon_i'=1$ holds for u times. Then



$d(P,Q)$ is even.

Sum $= 4k-2m-2n+2u-2$, even.

$\because k$ odd $\therefore d(\vec{x},\vec{y}) \neq k, 2k, 3k$ also holds.

Define $\mathcal{C}^+_{even}=\{(x_1,\cdots,x_{n-1}):(x_1,\cdots,x_n)\in\mathcal{C}_{even}, x_n=+1\}$, $\mathcal{C}^-_{even}=\{(x_1,\cdots,x_{n-1}):(x_1,\cdots,x_n)\in\mathcal{C}_{even}, x_n=-1\}$,

$\mathcal{C}^+_{odd}=\{(x_1,\cdots,x_{n-1}):(x_1,\cdots,x_n)\in\mathcal{C}_{odd}, x_n=+1\}$, $\mathcal{C}^-_{odd}=\{(x_1,\cdots,x_{n-1}):(x_1,\cdots,x_n)\in\mathcal{C}_{odd}, x_n=-1\}$.

They are codes of length $4k-1$ and the distance of two distinct codewords is never divisible by k.

$$\therefore |\mathcal{C}| \le 4\sum_{i=0}^{k-1}\binom{4k-1}{i}. \quad (\text{Thm 1.6})$$

And define $\mathcal{D}=\{(\varepsilon_1,\cdots,\varepsilon_{4k})\in C^{4k}: |\{i: 1\le i\le 4k-1, \varepsilon_i=1\}| \text{ is either less than } k \text{ or more than } 3k\}$.

Obv. $\forall \vec{x},\vec{y}\in\mathcal{D}$, $d(\vec{x},\vec{y})<2k$ or $d(\vec{x},\vec{y})>2k$.

$\therefore \mathcal{D}$ contains no two orthogonal vectors.

$\{\#1<k \,\&\, \#1>3k$, common $1<k$, common $-1<k$

Similar for $\#1<k \,\&\, \#1<k$, $\#1>3k \,\&\, \#1>3k$.

$$|\mathcal{D}| = 2\cdot 2\cdot\sum_{i=0}^{k-1}\binom{4k-1}{i}$$

$\uparrow$ ±1 for ε_{4k} $\quad\uparrow$ the case # more than $3k$.

$$\therefore |\mathcal{C}| \ge 4\sum_{i=0}^{k-1}\binom{4k-1}{i}.$$

$$\therefore |\mathcal{C}| = 4\sum_{i=0}^{k-1}\binom{4k-1}{i}.$$

Proof of Thm 1.6

$\forall \vec{x}\in\mathcal{C}$. Define $S(\vec{x})=\{i: x_i=1\}$

Define $M(j)$ a matrix with size of $|\mathcal{C}|\times\binom{l}{j}$. The rows of $M(j)$ are indexed by the codewords of $\mathcal{C}$, and the columns by the j-element subsets of $\{1,2,\cdots,l\}$, which means we can say the position of entries in the matrix as $(\vec{x},A)$. where $\vec{x}\in\mathcal{C}$ and A is a j-elements subset of $\{1,\cdots,l\}$.

Obv we have $\operatorname{rank} M(j)\le\binom{l}{j}$.

And we let the entry in $(\vec{x},A)$ be $(-1)^{|S(x)\cap A|}$.

Then let's compute the general entry of $N(j)=M(j)M(j)^T$, which has the size of $|\mathcal{C}|\times|\mathcal{C}|$ ($l\times l$).

And the rows and columns are both indexed by codewords of $\mathcal{C}$.

$$N_j(\vec{x},\vec{y}) = \sum_{\substack{A\subset\{1,2,\cdots,l\}\\|A|=j}}(-1)^{|S(x)\cap A|}(-1)^{|S(y)\cap A|} = \sum_{\substack{A\subset\{1,2,\cdots,l\}\\|A|=j}}(-1)^{|S(x)\triangle S(y))\cap A|}$$

$(-1)\cdot(-1)=1$.

$\hookrightarrow$ the symmetric difference of $S(x)$ & $S(y)$.

By def, we have $|S(\vec{x}) \triangle S(\vec{y})| = d(\vec{x},\vec{y})$

Note that given $S(\vec{x}) \triangle S(\vec{y})$, there are exactly $\binom{d(\vec{x},\vec{y})}{i}\binom{l-d(\vec{x},\vec{y})}{j-i}$ j element sets which intersect $S(x) \triangle S(y)$ in i elements.

$$\therefore n_j(\vec{x},\vec{y}) = \sum_{i=0}^{j} (-1)^i \binom{d(\vec{x},\vec{y})}{i}\binom{l-d(\vec{x},\vec{y})}{j-i}$$

The right hand of the expression is a polynomial in $d(\vec{x},\vec{y})$ of degree j. This polynomial is a Krawtchouk polynomial in the form $K(l,j,d(\vec{x},\vec{y}))$, which plays an important role in coding theory.

The coefficient of $d(\vec{x},\vec{y})^j$ is $\sum_{i=0}^{j} \frac{(-1)^i}{i!}\frac{(-1)^{j-i}}{(j-i)!} = \frac{(-1)^j}{j!}\sum_{i=0}^{j}\binom{j}{i} = \frac{(-2)^j}{j!}$.

$\binom{z-1}{k-1}$ is a polynomial of degree $k-1$. $p(z)$ can be uniquely written as a linear combination for $0 \le j \le k-1$:

$p(z) = \sum \alpha_j K(l,j,z)$

Consider $N = \sum_{j=0}^{k-1} \alpha_j N(j)$.

$\therefore n(x,y) = p(d(\vec{x},\vec{y})) = \binom{d(\vec{x},\vec{y})-1}{k-1}$.

$\because N(j) = M(j)\,M(j)^T \quad \therefore \operatorname{rank}(N(j)) \le \sum_{j=0}^{k-1} \operatorname{rank}(M(j)) \le \sum_{0\le j\le k-1}\binom{l}{j}$.

Then we are aiming to prove $\operatorname{rank}(N(j)) = |\mathcal{C}|$.

<u>Lemma</u> Suppose $k = p^\alpha$, $\alpha \ge 1$, p prime, d an integer, then $\binom{d-1}{k-1} = \begin{cases} 1 \pmod p & \text{if } k \mid d \\ 0 \pmod p & \text{if } k \nmid d \end{cases}$

pf. Suppose $b = ak-1$ for some integer a. Then $\binom{b}{k-1} = \prod_{i=1}^{k-1}\frac{ak-i}{k-i}$.

$\forall \alpha(i)$ s.t. $p^{\alpha(i)} \mid k-i$, we have $p^{\alpha(i)} \mid ak-i$ since $p^{\alpha(i)} \mid k$.

And since $\frac{\frac{ak-i}{p^{\alpha(i)}}}{\frac{k-i}{p^{\alpha(i)}}} = \frac{\frac{(a-1)k}{p^{\alpha(i)}} + \frac{k-i}{p^{\alpha(i)}}}{\frac{k-i}{p^{\alpha(i)}}} = \frac{(a-1)k}{k-i} + 1 \equiv 1 \pmod p$

$\therefore \binom{b}{k-1} \equiv 1 \pmod p$

Suppose $k = p^\alpha \nmid (b+1)$. Then $\binom{b+1}{k} = \frac{b+1}{k}\binom{b}{k-1}$.

$\because \binom{b+1}{k}$ is an integer, thus p^α divides $(b+1)\binom{b}{k-1}$. $\therefore p \mid \binom{b}{k-1}$. □

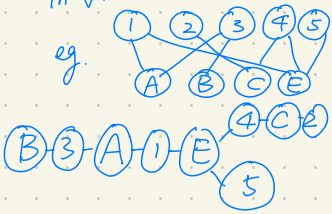
$\therefore$ The diagonal terms of N are equal to $\binom{-1}{k-1} \equiv 1 \pmod p$. However $k \nmid d(\vec{x},\vec{y})$ implies that all the off diagonal terms are divisible by p. $\therefore \det N \equiv 1 \pmod p$, in particular $\det N \neq 0$ holds. $\therefore \operatorname{rank}(N) = |\mathcal{C}|$, we have $|\mathcal{C}| \le \sum_{i=0}^{k-1}\binom{l}{i}$. □

Lecture Notes for [ ].

Def. The orthogonal graph Ω_n has the elements of $\{-1,1\}^n$ as vertices, and two vertices are adjacent if they are orthogonal, in other words, their Hamming distance is $\frac{n}{2}$.

The graph Ω_n is edgeless if n is odd, and is bipartite if $n \equiv 2 \pmod 4$.

A graph whose vertices can be divided into two disjoint sets U and V, and every edge connects a vertex in U to one in V.



For $n \equiv 0 \pmod 4$. Frankl and Galliard construct an independent set of Ω_n:

We can divide it into Ceven and Codd.

$\{(\varepsilon_1, \cdots, \varepsilon_{4k}) \in C^{4k} : |\{i : 1 \le i \le 4k-1,\ \varepsilon_i = 1\}|$ is either less than k or more than $3k\}$. whose size is $a_n := 4\sum_{i=0}^{\frac{n}{4}-1} \binom{n-1}{i}$

Galliard asked in 2001 if the independence number $\alpha(\Omega_n)$ of Ω_n is a_n when $n = 2^k$, $k \ge 2$.

This paper gives us the result by Frankl's method:

Thm. Let $n = 2^k$ for some $k \ge 2$. Then $\alpha(\Omega_n) = a_n$.

pf of the Thm: Let A_j be the 0-1-matrix indexed by the vertices of the hypercube $Q_n = \{-1,1\}^n$ with $(A_j)_{\vec{x}\vec{y}} = 1$ if $\vec{x}$ and $\vec{y}$ have Hamming distance j.

The $(n+1)$-dimensional matrix algebra spanned by $A_0 = I, A_1, \cdots, A_n$ is called the Bose-Mesner algebra of Q_n.

THE INDEPENDENCE NUMBER OF THE ORTHOGONALITY GRAPH IN DIMENSION 2^k

FERDINAND IHRINGER AND HAJIME TANAKA

ABSTRACT. We determine the independence number of the orthogonality graph on 2^k-dimensional hypercubes. This answers a question by Galliard from 2001 which is motivated by a problem in quantum information theory. Our method is a modification of a rank argument due to Frankl who showed the analogous result for $4p^k$-dimensional hypercubes, where p is an odd prime.

1. INTRODUCTION

The *orthogonality graph* Ω_n has the elements of $\{-1,1\}^n$ as vertices, and two vertices are adjacent if they are orthogonal, in other words, if their Hamming distance is $n/2$. The graph Ω_n occurs naturally when comparing classical and quantum communication [3]. In particular, for $n = 2^k$ the cost of simulating a specific quantum entanglement on k qubits can be reduced to determining the chromatic number $\chi(\Omega_n)$ of Ω_n [2, 9]. The graph Ω_n is edgeless if n is odd, and is bipartite if $n \equiv 2 \pmod 4$. For $n \equiv 0 \pmod 4$, Frankl [7] and Galliard [9] constructed an independent set of Ω_n of size

$$a_n := 4 \sum_{i=0}^{n/4-1} \binom{n-1}{i},$$

and Galliard [9] asked in 2001 if this is the independence number $\alpha(\Omega_n)$ of Ω_n when $n = 2^k$, $k \geqslant 2$. Newman [15] and, according to [8, p. 275, Remark], Frankl conjectured that this holds whenever $n \equiv 0 \pmod 4$. See also [4]. Frankl [7] already showed the conjecture in 1986 for all $n = 4p^k$ for $k \geqslant 1$, where p is an odd prime. De Klerk and Pasechnik [13] proved the conjecture for $n = 16$, i.e., that $\alpha(\Omega_{16}) = 2304$, using Schrijver's semidefinite programming bound [16]. Furthermore, Frankl and Rödl [8] showed that $\alpha(\Omega_n) < 1.99^n$ if $n \equiv 0 \pmod 4$. In this note, we apply Frankl's method from [7] to show the following:

Theorem. *Let $n = 2^k$ for some $k \geqslant 2$. Then $\alpha(\Omega_n) = a_n$.*

Together with the discussion in [9, Section 5.5], that is using $\chi(\Omega_n) \geqslant 2^n/\alpha(\Omega_n)$, our result implies an explicit version of Theorem 4 in [2]. Finding such an explicit result is one motivation for Galliard's work. See also [10, 12].

The first author is supported by a postdoctoral fellowship of the Research Foundation — Flanders (FWO).

The second author is supported by JSPS KAKENHI Grant Number JP17K05156.

2. Proof of the Theorem

Let A_j be the 0-1-matrix indexed by the vertices of the hypercube $Q_n = \{-1,1\}^n$ with $(A_j)_{xy} = 1$ if x and y have Hamming distance j. The matrices A_j have $n+1$ common eigenspaces $V_0, V_1, \dots, V_n$, and in the usual ordering of the eigenspaces the eigenvalue of A_j with respect to V_i is given by the Krawtchouk polynomial (see [5, Theorem 4.2])

$$K_j(i) = K_j(i;n) := \sum_{h=0}^{j} (-1)^h \binom{i}{h}\binom{n-i}{j-h}.$$

It is known that the orthogonal projection matrix E_i onto V_i has the entry $(E_i)_{xy} = 2^{-n}K_i(j)$ if x and y are at Hamming distance j [5, Theorem 4.2], so that we have in particular $\operatorname{rank} E_i = \operatorname{trace} E_i = K_i(0) = \binom{n}{i}$. The $(n+1)$-dimensional matrix algebra spanned by $A_0 = I, A_1, \dots, A_n$ is called the *Bose–Mesner algebra* of Q_n.

Assume now that $n = 2^k$, $k \geqslant 3$. (The result is trivial if $k = 2$.) Let C be an independent set of Ω_{2^k}, and let $C^{\pm}_{\mathrm{even}}, C^{\pm}_{\mathrm{odd}} \subseteq \{-1,1\}^{2^k-1}$ be as in [7]: C^{+}_{even} is given by taking all the even-weight elements of C that end with $+1$, followed by truncating at the last coordinate, and the other three are analogous. Let C' be one of these four families. Then the Hamming distances in C' are even and unequal to 2^{k-1}, so they lie in the following set:

$$\{2s : s = 0, 1, \dots, 2^{k-1} - 1,\ s \neq 2^{k-2}\}. \tag{1}$$

Below we work with the Bose–Mesner algebra $\mathscr{A}$ of Q_{2^k-1}. For every $M \in \mathscr{A}$, let $\overline{M}$ denote the principal submatrix corresponding to C'. Consider the polynomial

$$\varphi(\xi) = \binom{\xi/2 - 1}{2^{k-2} - 1} \in \mathbb{R}[\xi],$$

and expand it in terms of the Krawtchouk polynomials $K_i(\xi) = K_i(\xi; 2^k - 1)$:

$$\varphi(\xi) = \sum_{i=0}^{2^{k-2}-1} c_i K_i(\xi). \tag{2}$$

Let

$$X = \sum_{j=0}^{2^k-1} \varphi(j) A_j \in \mathscr{A}.$$

On the one hand, observe that $\overline{X}$ has only integral entries in view of (1), and an easy application of Lucas' theorem (cf. [6]) shows moreover that $\overline{X} \equiv \overline{I} \pmod 2$. In particular, $\overline{X}$ is invertible. On the other hand, from (2) we have

$$X = 2^{2^k-1} \sum_{i=0}^{2^{k-2}-1} c_i E_i.$$

It follows that

$$|C'| = \operatorname{rank} \overline{X} \leqslant \operatorname{rank} X \leqslant \sum_{i=0}^{2^{k-2}-1} \operatorname{rank} E_i = \sum_{i=0}^{2^{k-2}-1} \binom{2^k - 1}{i}.$$

As $|C| = |C^{+}_{\mathrm{even}}| + |C^{-}_{\mathrm{even}}| + |C^{+}_{\mathrm{odd}}| + |C^{-}_{\mathrm{odd}}|$, the theorem follows.

3. Future Work

Schrijver's semidefinite programming bound has been extended to hierarchies of upper bounds; see, e.g., [1, 14]. In view of [13], it is interesting to investigate if these bounds in turn prove the conjecture for other values of n. One of the referees pointed out to us that using next level in the hierarchy, see [11], yields the correct bound of $a_{24} = 178208$ for the case $n = 24$.

Problem. Prove the conjecture for $n = 40$, which is the first open case.

Acknowledgements. We thank the anonymous referee for solving the case $n = 24$.

References

[1] C. Bachoc, D. C. Gijswijt, A. Schrijver, and F. Vallentin, Invariant semidefinite programs, in: Handbook on semidefinite, conic and polynomial optimization (M. F. Anjos and J. B. Lasserre, eds.), Springer, New York, 2012, pp. 219–269; arXiv:1007.2905.

[2] G. Brassard, R. Cleve, and A. Tapp, Cost of exactly simulating quantum entanglement with classical communication, Phys. Rev. Lett. 83 (1999) 1874–1877; arXiv:quant-ph/9901035.

[3] H. Buhrman, R. Cleve, and A. Widgerson, Quantum vs. classical communication and computation, in: Proceedings of the 30th Annual ACM Symposium on the Theory of Computing, Dallas, TX, USA, 1998, pp. 63–68; arXiv:quant-ph/9802040.

[4] P. J. Cameron, Problems from CGCS Luminy, May 2007, European J. Combin. 31 (2010) 644–648.

[5] P. Delsarte, An algebraic approach to the association schemes of coding theory, Philips Res. Rep. Suppl., No. 10, 1973.

[6] N. J. Fine, Binomial coefficients modulo a prime, Amer. Math. Monthly 54 (1947) 589–592.

[7] P. Frankl, Orthogonal vectors in the n-dimensional cube and codes with missing distances, Combinatorica 6 (1986) 279–285.

[8] P. Frankl and V. Rödl, Forbidden intersections, Trans. Amer. Math. Soc. 300 (1987) 259–286.

[9] V. Galliard, Classical pseudo-telepathy and colouring graphs, diploma thesis, ETH Zurich, 2001; available at `http://math.galliard.ch/Cryptography/Papers/PseudoTelepathy/SimulationOfEntanglement.pdf` .

[10] V. Galliard, A. Tapp, and S. Wolf, The impossibility of pseudo-telepathy without quantum entanglement, in: Proceedings 2003 IEEE International Symposium on Information Theory, Yokohama, Japan, 2003; arXiv:quant-ph/0211011.

[11] D. C. Gijswijt, H. D. Mittelmann, and A. Schrijver, Semidefinite code bounds based on quadruple distances, IEEE Trans. Inform. Theory 58 (2012) 2697–2705; arXiv:1005.4959.

[12] C. D. Godsil and M. W. Newman, Coloring an orthogonality graph, SIAM J. Discrete Math. 22 (2008) 683–692; arXiv:math/0509151.

[13] E. de Klerk and D. V. Pasechnik, A note on the stability number of an orthogonality graph, European J. Combin. 28 (2007) 1971–1979; arXiv:math/0505038.

[14] M. Laurent, Strengthened semidefinite programming bounds for codes, Math. Program. 109 (2007) 239–261.

[15] M. W. Newman, Independent sets and eigenspaces, thesis, University of Waterloo, 2004.

[16] A. Schrijver, New code upper bounds from the Terwilliger algebra and semidefinite programming, IEEE Trans. Inform. Theory 51 (2005) 2859–2866.

Department of Mathematics: Analysis, Logic and Discrete Mathematics, Ghent University, Belgium

E-mail address: `ferdinand.ihringer@ugent.be`

Research Center for Pure and Applied Mathematics, Graduate School of Information Sciences, Tohoku University, Japan

E-mail address: `htanaka@tohoku.ac.jp`

5-16 讲座

Thm 19.1 Let (V,a) be a linear space, where V is a v "point's and a is a family of k-elements of V with $|a|=b$ and where any two points appear together in one block. Then $b \geq v$.

Let N be the $v \times b$ incidence matrix.

$NN^T = \begin{bmatrix} k_1 & & & \\ & k_2 & & \\ & & \ddots & \\ & & & k_n \end{bmatrix}_{v \times v} = \begin{bmatrix} k+1 & & & \\ & k+1 & & \\ & & \ddots & \\ & & & k-1 \end{bmatrix} + \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & 1 & \cdots & 1 \\ \vdots & \vdots & & \vdots \\ 1 & 1 & \cdots & 1 \end{bmatrix}$ semipositive $\Rightarrow$ nonsingular

Fisher's Inequality 2-(v,k,λ) design $\begin{cases} v = \#\text{ points} \\ k = \text{block size} \\ \text{any two points in exactly } \lambda \text{ blocks} \end{cases}$

blocks $B_1, B_2, \cdots, B_b$

$a_2 = |B_1 \cap B_2|$, $a_3 = |B_1 \cap B_3|$, $\cdots$, $a_b = |B_1 \cap B_b|$.

$\bar{a} = \text{average}\{a_2, \cdots, a_b\}$

Fisher calculated $\bar{a} = \sum_{i=2}^{b-1} a_i$ and $\sum (a_i - \bar{a})^2$, $\sum_{i=2}^{b} (a_i - \bar{a})^2 \geq 0 \Rightarrow b - v \geq 0 \Rightarrow b \geq v$.

t-(v,k,λ) any t points are in λ blocks (blocks of size k), $b \geq \binom{v}{1}$ when $t=2$

Petrenuk if $t=4$, $b \geq \binom{v}{2}$, if $t=28$, $b \geq \binom{v}{s}$

$X = n$-set, $a =$ family of k-subsets

Assume $|A \cap B| \in \{\mu_1, \mu_2, \cdots, \mu_t\}$, $|B \cap A_1| \in \{3, 10, 24, 45\}$ (subsets of size 100)

R-C-W Thm. $|a| \leq \binom{n}{t}$

Suppose p prime, assume $|A \cap B| \in \{\mu_1, \mu_2, \cdots, \mu_s\}$ (mod p)

take $p=7$