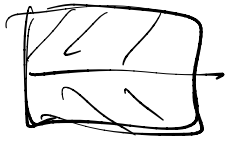
5.2. Communication Complexity : Log-rank conjecture

$$K(C) \quad \hookrightarrow \quad \text{rank } C$$

Lemma: $K(C) \geq \log_2 rk(C)$.

Proof: Suppose $K(C) = t$.
Induction on t.

If $t=0$, then it is trivial.
If $t>0$,
C can be partitioned into 2 matrices C_1, C_2 such that
$K(C_1) \leq t-1$, $K(C_2) \leq t-1$.



By the induction hypothesis

$$rk\, C_1 \leq 2^{t-1}$$
$$rk\, C_2 \leq 2^{t-1}$$

$$rk\, C \leq rk\, C_1 + rk\, C_2 \leq 2^{t-1} + 2^{t-1} = 2^t$$

We remark: Göös, Pitassi, Watson if $K(C) \geq \tilde{\Omega}(\log^2 rk(C))$

Example (Equality Problem)

{Alice, Bob} ⇐⇒ both got a 0-1 string of length n.

Q: Are they identical?

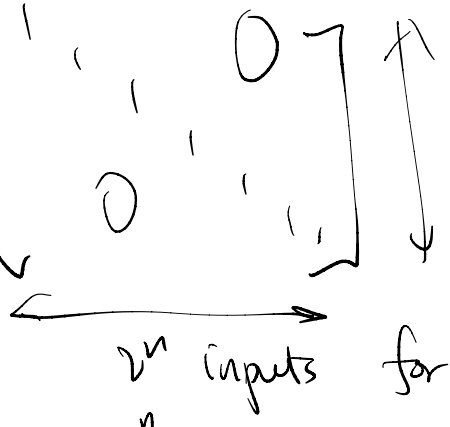
states of Alice = 2^n

Trivial Protocal

$$\Rightarrow K(C) \le \lceil \log_2 2^n \rceil = n$$

C = Communication complexity

$=$



$$rk(C) = 2^n$$

$$K(C) \ge \log_2 rk(C) = n.$$

$$\Rightarrow K(C) = n$$

Example 2 (Disjointness)

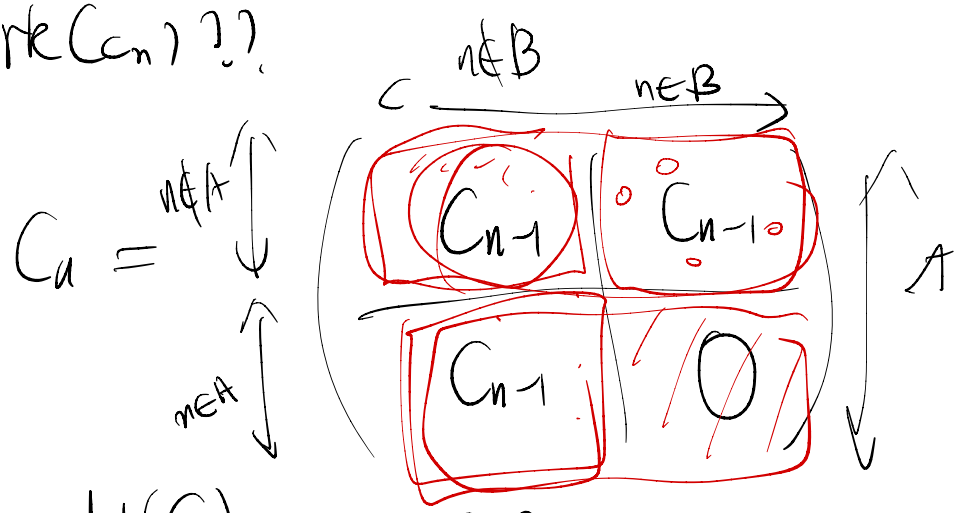
Alice: $A \subseteq \{1, 2, \ldots, n\}$

Bob: $B \subseteq \{1, 2, \ldots n\}$

Q: $A \cap B = \phi$?

C_n = Communication matrix.

$rk(C_n)$??



$$\det(C_n) = \det\begin{pmatrix} C_{n-1} & C_{n-1} \\ C_{n-1} & 0 \end{pmatrix} = \pm(\det(C_{n-1}))^2$$

$$C_1 = \begin{array}{c|cc} & \phi & \{1\} \\ \hline \phi & 1 & 1 \\ \{1\} & 1 & 0 \end{array} \qquad \det C_1 = -1 \neq 0.$$

$\Rightarrow \det C_n = \pm 1$ for all n.

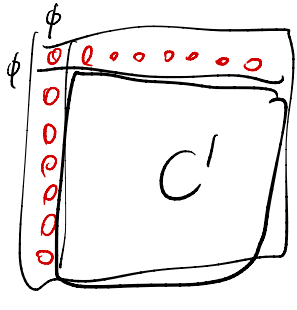
$\Rightarrow rk\, C_n = 2^n$.

$$K(C_n) \geq \log_2 rk(C_n) = n$$
$$K(C_n) \leq \lceil \log_2 2^n \rceil = n .$$
$$\Rightarrow K(C_n) = n . \qquad \square$$

Example 3. (The parity problem)

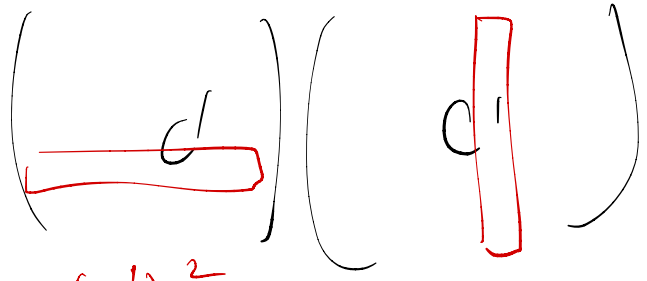
Alice : $X \subseteq \{1, \dots, n\}$
Bob : $Y \subseteq \{1, \dots, n\}$.
Q : Determine whether $|X \cap Y|$ is odd.

Let C be the communication matrix



Let C' be the submatrix of C obtained by deleting the row and the column indexed by ϕ.

C' : symmetric.

$(C')^2 =$ 

X, Y entry of $(C')^2$

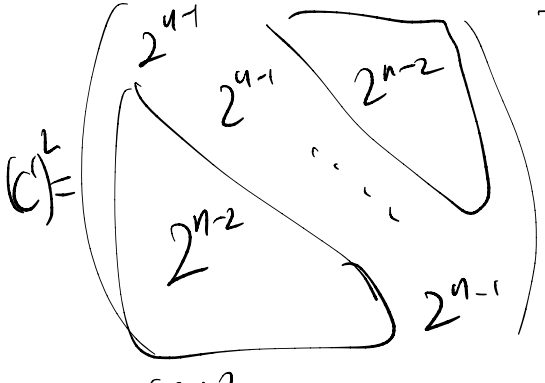
= # subsets $Z \subseteq \{1, \ldots, n\}$ such that $|X \cap Z|$ is odd and $|Y \cap Z|$ is odd.

If $X = Y$, then

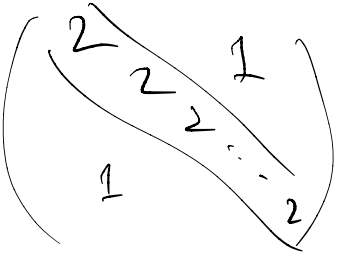
$2^{|X|-1} 2^{n-|X|} = 2^{n-1}$ sets Z having $|X \cap Z|$ odd.

If $X \neq Y$,

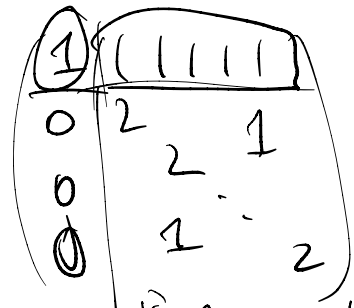
$2^n \frac{1}{2} \frac{1}{2} = 2^{n-2}$



$(C')^2$ is nonsingular

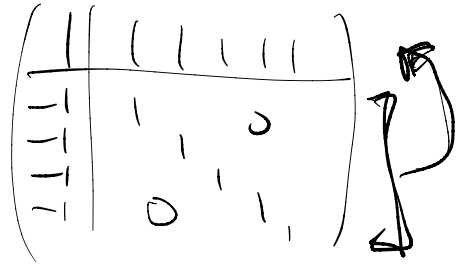


$$\begin{pmatrix} 2 & 1 & & \\ 2 & 2 & & \\ & 2 & 2 & \\ & 1 & 2 & \end{pmatrix}$$ is nonsingular $\Leftrightarrow$

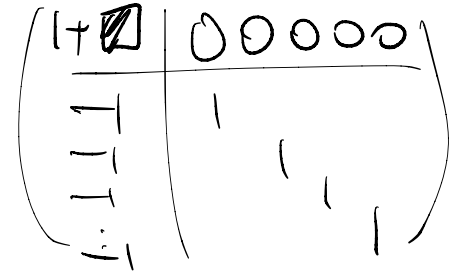


is nonsingular

$\Leftrightarrow$



$\Leftrightarrow$



is nonsingular

So, $(C')^2$ is nonsingular

$$\det(C')^2 = (\det(C'))^2$$

$\Rightarrow \det C' \neq 0$

$\Rightarrow C'$ is nonsingular

$\Rightarrow rk(C') = 2^n - 1$

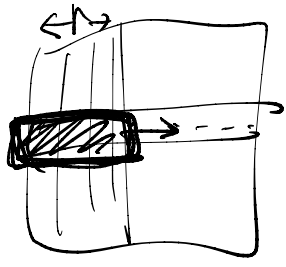
$rk\, C = 2^n - 1$

$K(C) \geq \lceil \log_2(2^n - 1) \rceil = n$ $\quad K(C) \leq n$

$\therefore K(C) = n$ ∎

Prop. $K(C) \leq rk(C)$

Proof. If a 0-1 matrix has rank r, then it has at most 2^r distinct rows



$$K(C) \leq \lceil \log_2 (2^r) \rceil = r$$

Conjecture (Lovász, Saks 1993)
<log-rank Conjecture>
There exist $\alpha > 0$, $\beta > 1$ such that

$$K(C) \leq \alpha \cdot (\log rk(C))^{\beta}$$

for all non-zero 0-1 matrices C.

Best upper bound

Thm (Lovett 2016) $K(C) \leq O(\sqrt{rk(C)} \log_2 rk(C))$

5.3 Communication Complexity : Randomized Protocol.

A randomized communication protocol is a probability distribution over a set of possible (deterministic) protocols.

The complexity of a randomized communication protocol
= expected number of transmitted bits
in order for Alice or Bob
to determine the answer.
(almost)

A randomized protocol $R(x,y)$
has one-sided error
if the following holds:

- If the answer is No, then the protocol always output No.
- If the true answer is Yes
then $P(\text{the protocol outputs Yes}) \geq \frac{1}{2}$.

Problem: (Different?)
Alice: n bits $A \subseteq \{1, \dots, n\}$
Bob: n bits $B \subseteq \{1, \dots, n\}$
Q: Are they different? $A \neq B$?

Pick a prime p $\boxed{2n \le p \le 4n}$

$a_0, a_1, \ldots, a_{n-1} \in \{0,1\}$ Inputs for Alice

$b_0, b_1, \ldots b_{n-1} \in \{0,1\}$ Inputs for Bob

$A(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1}$

$B(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_{n-1} x^{n-1}$.

$A, B : \in \mathbb{F}_p[x]$

$\mathbb{F}_p \to \{0, \ldots, p-1\}$

Protocol: Alice picks a number $r \in \mathbb{F}_p$ randomly.

Send r and $A(r)$ to Bob.

Bob computes $B(r)$.

If $A(r) \neq B(r)$, Bob outputs 1.

If $A(r) = B(r)$, Bob outputs 0.

$$P(A(r) = B(r)) \le \frac{\deg(A-B)}{p}$$

Schwartz-Zippel Lemma

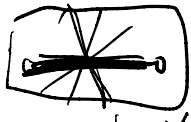
$$\le \frac{n-1}{p} < \frac{1}{2}$$

Complexity $\log_2(4n) + \log_2(4n) = O(\log n)$. □

5.4. KAKEYA'S PROBLEM IN FINITE FIELDS

KAKEYA'S PROBLEM

1917: What is the smallest area of a body on the plane such that one can rotate a needle of length 1 360°?



Kakeya set

In $\mathbb{R}^n$, a set X is a Kakeya set if it contains a line segment of length 1 in every direction.

Surprisingly, for $\varepsilon > 0$, there is a Kakeya set of area $< \varepsilon$.

KAKEYA SET OVER A FINITE FIELD

Proposed by Wolff 1999.

For a finite field $\mathbb{F}$, a Kakeya set in $\mathbb{F}^n$ is a subset $E \subseteq \mathbb{F}^n$ containing at least one affine line parallel to every direction in $\mathbb{F}^n - \{0\}$.

In other words,
E is a Kakeya set
$\Leftrightarrow$ for all $v \in \mathbb{F}^n - \{0\}$, there is $c \in \mathbb{F}^n$ such that $\{c + tv : t \in \mathbb{F}\} \subseteq E$.

Conj: (Wolff) If K is a Kakeya set in $\mathbb{F}^n$ then $|K| \geq C_n |\mathbb{F}|^n$.

Partial result: $|K| \geq C_n |\mathbb{F}|^{\frac{n+1}{2}}$ (Wolff)

Thm (Dvir 2009)
If K is a Kakeya set in $\mathbb{F}^n$, then
$$|K| > \binom{|\mathbb{F}|+n-1}{n} \geq \frac{|\mathbb{F}|^n}{n!}$$

Lemma: Let $f \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ be a polynomial of degree $\leq q-1$ over $\mathbb{F}$
$|\mathbb{F}| = q$

Let K be a Kakeya set in $\mathbb{F}^n$.
If $f(x) = 0$ for all $x \in K$
then $f \equiv 0$.

Proof. Suppose not.
Let $f(x_1, \ldots, x_n) = \sum_{i=0}^{d} f_i(x_1, \ldots, x_n)$
where d is the degree of f
f_i = homogeneous polynomial of deg i.
(or $f_i \equiv 0$)
Since $f \not\equiv 0$ and $f(x) = 0$ for all $x \in K$,
$d > 0 \Rightarrow f_d \not\equiv 0$

Let $v \in \mathbb{F}^n - \{0\}$.

$\Rightarrow$ There is $w \in \mathbb{F}^n$ such that $\{w + tv : t \in \mathbb{F}\} \subseteq K$

$\Rightarrow$ $f(w+tv) = 0$ for all t.

Let $g_{w,v}(t) = f(w+tv) \in \mathbb{F}[t]$

degree of $g_{w,v} \leq d < q$

$g_{w,v}(t) = 0$ for all $t \in \mathbb{F}$.

$\Rightarrow$ $g_{w,v} \equiv 0$

$\Rightarrow$ The coefficient of t^d in $g_{w,v} = 0$

$\| f_d(0+1\cdot v) = f_d(v)$

So, $f_d(v) = 0$ for all $v \in \mathbb{F}^n - \{0\}$.

$f_d(v) = 0$ for all $v \in \mathbb{F}^n$.

$d < q$ By Schwartz-Zippel,

$f_d \equiv 0$ or $(\#\text{roots of } f) \leq \frac{d}{q} q^n = dq^{n-1}$

$f_d(v) = 0 \Rightarrow$ #roots $= q^n$

$\therefore f_d = 0$ Contradiction.

Lemma If $E \subseteq \mathbb{F}^n$, $|E| < \binom{n+d}{d}$ then there exists a (non-zero) polynomial $f(X_1, \dots, X_n)$ of degree $\leq d$ such that $f(x) = 0$ for all $x \in E$.

Proof The vector space V_d of polynomials in $\mathbb{F}[X_1, X_2, \dots, X_n]$ of degree $\leq d$ has dimension $\binom{n+d}{d}$

($x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$ $\quad$ $a_1 + a_2 + \cdots + a_n = d$, $a_i \geq 0$)

(d 1's, n +'s)

Let $T : V_d \to \mathbb{F}^E$ be a linear transformation such that

$$T(f) = \big(f(a)\big)_{a \in E}$$

$|E| < \binom{n+d}{d} \Rightarrow \dim \mathbb{F}^E = |E| < \dim(V_d)$

$\Rightarrow \ker(T)$ is non-trivial.

$(\dim \ker(T) > 0)$

$\Rightarrow$ There is $f \neq 0$ such that $T(f) = 0$. ∎

Proof of Dvir's thm:

Let K be a Kakeya set.

If $|K| < \binom{|\mathbb{F}|+n-1}{n}$

then there is a non-zero polynomial f such that $f(x)=0$ for all $x \in K$ and degree of $f \leq |\mathbb{F}|-1$,

Contradicting the 1st lemma.

So, $|K| \geq \binom{|\mathbb{F}|+n-1}{n} = \frac{(|\mathbb{F}|+n-1)(|\mathbb{F}|+n-2)\cdots(|\mathbb{F}|)}{n!}$

$$\geq \frac{|\mathbb{F}|^n}{n!}$$

□

6. SLICE RANK

6.1. CAP SET PROBLEM.

(A set A of $\mathbb{F}_3^n$ is called a cap set if it contains no line.

$\{a+tb : t \in \mathbb{F}_3\}$, $a, b \in \mathbb{F}_3^n$. $b \neq 0$.

SET game:

Find a line in 12 cards (distinct) from $\mathbb{F}_3^n$)

Q: How large can a cap set in $\mathbb{F}_3^n$ be?

1982 Brown, Buhler $o(3^n)$

1995 Meshulam $O(3^n/n)$

2012 Bateman, Katz $O(3^n/n^{1+\varepsilon})$

2016 Big breakthrough!

May 5 (arXiv) Croot, Lev, Pach

(A subset of $\mathbb{F}_4^n$ without a 3-term arithmetic progression has size $\leq O(3.61^n)$

May 12 Ellenberg

May 15 $\downarrow$

cap set in $\mathbb{F}_3^n$ has size $O(c^n)$ $c < 3$.

Gijswit.

May 30 Ellenberg, Gijswit arXiv paper
Every cap set has size $o(2.756^n)$.

Annals of Math. 2017. 4 pages.

Let $\mathbb{F}$ be a finite field, $q = |\mathbb{F}|$
M_n = set of monomials
$$x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$$
where $0 \le i_1, i_2, \ldots, i_n \le q-1$.

S_n = Subspace of $\mathbb{F}[x_1, x_2, \ldots, x_n]$
spanned by M_n.

S_n^d = Subspace of S_n
consisting of polynomials of degree $\le d$.

Lemma $\mathbb{F}$: finite field. $A \subseteq \mathbb{F}^n$.
$f \in S_n^d$

If $f(a+b) = 0$ for all $a, b \in A$, $a \neq b$,
then
the number of $x \in A$ with $f(2x) \neq 0$
is at most $\le 2|M_n^{d/2}|$

(M_n^d is a subset of M_n consisting of
monomials of degree $\le d$.)

Proof By expanding we have

$$f(x+y) = \sum_{m, m' \in M_n^d} C_{m,m'}\, m(x)\, m'(y)$$

degree $\le d$

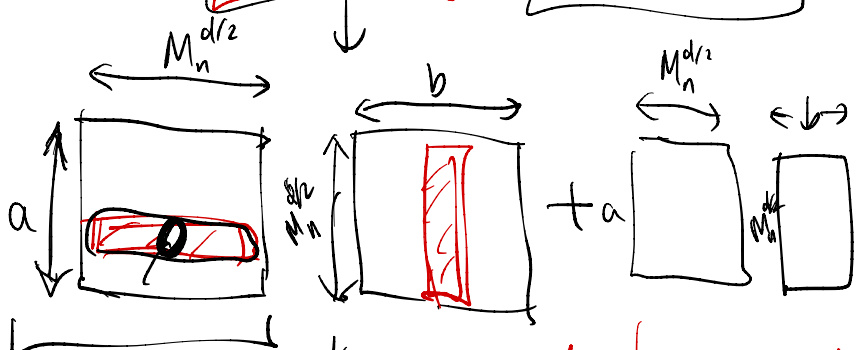
$\Rightarrow$ For each summand either $m(x)$ has degree $\le \frac{d}{2}$ or $m'(y)$ has degree $\le \frac{d}{2}$.

$$f(x+y) = \sum_{m \in M_n^{d/2}} m(x)\, F_m(y) + \sum_{m' \in M_n^{d/2}} m'(y)\, G_{m'}(x)$$

Let B be an $A \times A$ matrix $B = (B_{ab})_{a \in A,\, b \in A}$ whose a,b entry is $f(a+b)$.

$$B_{a,b} = f(a+b) = \sum_{m \in M_n^{d/2}} m(a)\, F_m(b) + \sum_{m \in M_n^{d/2}} G_m(a)\, m(b)$$

$B =$



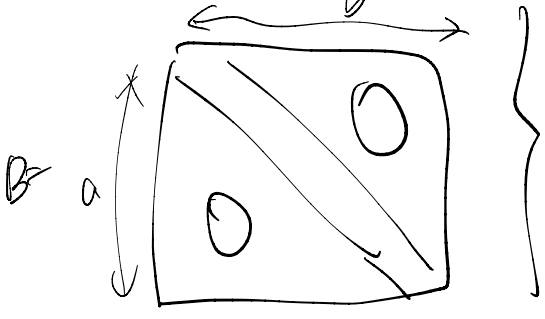
rank $\le |M_n^{d/2}|$ rank $\le |M_n^{d/2}|$ rank $\le |M_n^{d/2}|$

$rk(PQ) \le rk(P)$

$\operatorname{rank}(A+B) \le \operatorname{rank} A + \operatorname{rank} B$

$\therefore \operatorname{rank} B \le 2|M_n^{d/2}|$.

$f(a+b)=0$ for all $a \neq b$, $a, b \in A$.



$\rightarrow$ B is a diagonal matrix.

$\operatorname{rank} B = \#$ non-zero diagonal entries

$\le 2|M_n^{d/2}|$.

(The number of $x \in A$ with $f(2x) \neq 0$)

$\le 2|M_n^{d/2}|$. □

Thm (Ellenberg, Gijswijt 2017)

$A \subseteq \mathbb{F}^n$, $|\mathbb{F}| = q$, $\mathbb{F}$: finite field, $q \ge 2$.

If A has no 3-term arithmetic progression

in other words

$$\left(\begin{array}{c} a_1+a_2=2a_3 \\ a_1, a_2, a_3 \in A \end{array}\right) \Rightarrow \left(a_1=a_2=a_3\right)$$

then $|A| \le 3|M_n^{\frac{(q-1)n}{3}}|$.

Proof. Let $d \le (q-1)n$, $d \ge 0$

Define V as the subspace of S_n^d vanishing on the complement of $2A$.

$$V = \{ f \in S_n^d : f(x) = 0 \text{ for all } x \notin 2A \}$$

$$(2A = \{ 2x : x \in A \})$$

$$\dim V \ge \dim S_n^d - \left(|\mathbb{F}^n| - |2A| \right)$$

$$S_n^d \longrightarrow \mathbb{F}^{|\mathbb{F}^n| - |2A|}$$

$$f \longmapsto (f(x) : x \notin 2A)$$

$$\boxed{\dim V \ge |M_n^d| - q^n + |A|.}$$

$a \neq b$, $a, b \in A$ $\quad f(a+b) = 0$

$\Downarrow$ $a+b \notin 2A$ $\Rightarrow$ $f \in V$

By the previous lemma

$$\#\{x \in A : f(2x) \neq 0\} \le 2 |M_n^{d/2}|$$

for every $f \in V$.

Choose $f \in V$ so that $\Sigma = \{ x \in \mathbb{F}^n : f(x) \neq 0 \}$ is maximal.

$f(x)=0$ if $x \notin 2A$.

$$|\Sigma| = |\{x \in \mathbb{F}^n : f(x) \neq 0\}|$$
$$= |\{2y \in \mathbb{F}^n : f(2y) \neq 0\}|$$
$$= |\{y \in \mathbb{F}^n : f(2y) \neq 0\}| \leq 2|M_n^{d/2}|$$

We claim that $|\Sigma| \geq \dim V$.

If not, then there is a non-zero $g \in V$ such that $g(x)=0$ for all $x \in \Sigma$.

$f, g \Rightarrow f+g \in V$

$\Rightarrow \Sigma' = \{x \in \mathbb{F}^n : f(x)+g(x) \neq 0\}$

Then $\Sigma' \supsetneq \Sigma$.

Contradiction to the choice of f.

This implies that

$$\dim V \leq 2|M_n^{d/2}|$$

$$2|M_n^{d/2}| \geq |M_n^d| - q^n + |A|$$

$$\therefore |A| \leq 2|M_n^{d/2}| + q^n - |M_n^d|$$

$q^n - |M_n^d|$ $\quad q^n \Leftrightarrow$ #monomials $x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$

$0 \leq i_1, i_2 \leq q-1$.

$q^n - |M_n^d| =$ # Monomials $x_1^{d_1} x_2^{d_2} \cdots x_n^{d_n}$

such that $0 \le d_1, d_2, \ldots, d_n \le q-1$

$d_1 + d_2 + \cdots + d_n \ge d+1$

$=$ # monomials $x^{q-1-d_1} x^{q-1-d_2} \cdots x_n^{q-1-d_n}$

$0 \le q-1-d_1 \le q-1$

$\sum((q-1)-d_i) = (q-1)n - \sum d_i$

$\le (q-1)n - d - 1$

$= |M^{(q-1)n-d-1}|$

$\therefore |A| \le 2|M_n^{d/2}| + |M^{(q-1)n-d-1}|.$

Choose d so that

$\frac{d}{2} = (q-1)n - d - 1 \iff \frac{3}{2}d = (q-1)n - 1$

$$d = \frac{2(q-1)n - 2}{3}$$

$|A| \le 3|M_n^{d/2}| \le 3\left(M_n^{\frac{(q-1)n}{3} - \frac{1}{3}}\right) \le 3|M_n^{\frac{(q-1)n}{3}}|$

Thm (Ellenberg, Gijswijt 2017)

If A is a subset of $\mathbb{F}_3^n$ with no 3-term arithmetic progression (A is a cap set), then

$$|A| \leq 3N$$

where

$$N = \sum_{\substack{a,b,c \geq 0 \\ a+b+c=n \\ b+2c \leq 2n/3}} \frac{n!}{a!\,b!\,c!}.$$

Furthermore, $3N \leq o(2.756^n)$.

Proof. Take $q=3$.

Let $N = |M_n^{\frac{2n}{3}}|$ (monomials $x_1^{d_1} x_2^{d_2} \cdots x_n^{d_n}$)

$= \#$ solutions of $d_1 + d_2 + \cdots + d_n \leq \frac{2n}{3}$, $d_i = 0, 1, 2$

$$= \left(\sum_{\substack{0a+1b+2c \leq \frac{2n}{3} \\ a+b+c=n \\ a \geq 0,\ b \geq 0,\ c \geq 0}} \frac{n!}{a!\,b!\,c!} \right)$$

$$(1+x+x^2)^n = (1+x+x^2)(1+x+x^2)\cdots(1+x+x^2)$$

$$= \sum_{i=0}^{2n} \boxed{\quad} x^i$$

$$= \sum_{i=0}^{2n} \left(\sum_{\substack{a+b+c=n \\ b+2c=i}} \frac{n!}{a!b!c!} \right) x^i$$

Take $0 < x < 1$.

$$\frac{(1+x+x^2)^n}{x^{\frac{2n}{3}}} = \sum_{i=0}^{2n} \left(\sum_{\substack{a+b+c=n \\ b+2c=i}} \frac{n!}{a!b!c!} \right) x^{i-\frac{2n}{3}}$$

$$\geq \sum_{i=0}^{2n/3} \sum_{\substack{a+b+c=n \\ b+2c=i}} \frac{n!}{a!b!c!} = N.$$

So, $N \leq (x^{-\frac{2}{3}} + x^{\frac{1}{3}} + x^{\frac{4}{3}})^n$ for all $0 < x < 1$.

Let $f(x) = x^{-\frac{2}{3}} + x^{\frac{1}{3}} + x^{\frac{4}{3}}$

$$f'(x) = -\frac{2}{3}x^{-\frac{5}{3}} + \frac{1}{3}x^{-\frac{2}{3}} + \frac{4}{3}x^{+\frac{1}{3}}$$

$$= x^{-\frac{5}{3}}\left(-\frac{2}{3} + \frac{1}{3}x + \frac{4}{3}x^2\right)$$

$$= -\frac{1}{3}x^{-\frac{5}{3}}(-2+x+4x^2)$$

$f'(x) = 0$

$\Leftrightarrow \quad x = \frac{1 \pm \sqrt{1+32}}{8} = \frac{-1 \pm \sqrt{33}}{8}$

Choose $x = \frac{-1+\sqrt{33}}{8}$

$f(x) \sim 2.75510\ldots$

$\Rightarrow \quad 3N \leq o\left(\left(2.756\ldots\right)^n\right)$

for large N.

□