Asymptotic Bounds for AP-Free Sets in Vector Spaces over Finite Fields

UROP Presentation

Aung Hein Thant, Leung Ka Lun

The Chinese University of Hong Kong

January 3, 2024

What we concern

Combinatorists like to deduce structure from information about density. What we concern today starts with the following question:

Question

Let $A \subseteq \mathbb{Z}_{\geq 1}$ and define its density to be $\rho_n(A) = |[1,n] \cap A|/n$. If we know that $\rho_n(A)$ is large (for example, $\rho_n(A) \geq \delta > 0$), can we guarantee that A contains an arithmetic progression?

To make things precise, we introduce the following definition:

Definition (Capset)

A set $A \subseteq \mathbb{Z}_{\geq 1}$ is called a *capset* if

$$x - y = y - z \quad \Longrightarrow \quad x = y = z$$

for any x, y and $z \in A$. For any $X \subseteq \mathbb{Z}_{\geq 1}$, let $r_3(X)$ be the size of the largest capset in X. Our question is about knowing the size of $r_3(\{1, 2, \ldots, n\})$.

Why this is concerned

Theorem (Green and Tao [2008])

The set of primes P (in $\mathbb{Z}_{\geq 1}$) contains arbitrarily long arithmetic progressions.

It is believed that Green-Tao theorem is not about primes and that conclusion holds simply because $\rho_n(P) \sim 1/\log(n)$.

Conjecture

Let $A \subseteq \mathbb{Z}_{\geq 1}$ and suppose

$$\sum_{n \in A} \frac{1}{n}$$

diverges. Is it true that such a set A contains an arbitrarily long arithmetic progression?

Contents

Discussion about capsets can be done in any abelian group G. Today's presentation will mainly focus on the asymptotic bounds of $r_3(\mathbb{F}_3^n)$ and only remarks for $r_3(\{1, 2, \ldots, n\})$. We will proceed in the following order:

(1) Introduction

(2) Some Results on Upper Bounds

(3) Product Construction and the Lower Bound

Our work deals with the last part which will be explained by Kalun.

Roth's Theorem and Improvements

Theorem (Roth [1953])

$r_3(\{1, 2, \ldots, n\}) = o(n)$. *In other words, if* $A \subseteq \mathbb{Z}_{\geq 0}$ *and* $\limsup \rho_n(A) > 0$, *then* A *contains an arithmetic progression.*

The bound $o(n)$ has constantly been improved. Current world record was achieved by Thomas Bloom on 2020 achieved by applying Fourier analytic techniques.

Theorem (Bloom and Sisask [2020])

There is an absolute constant $c > 0$ *such that*

$$r_3(\{1, 2, \ldots, n\}) = O\left(\frac{n}{(\log n)^{1+c}}\right).$$

In particular, this implies that primes contain infinitely many arithmetic progressions of length 3.

Croot-Lev-Pach-Ellenberg-Gijswijt

For the case $\mathbb{F}_q^n$, Ellenberg and Gijwijt established a breakthrough with the following result:

Theorem (Ellenberg and Gijswijt [2017])

There is a constant $c_q < q$ such that

$$r_3(\mathbb{F}_q^n) = O(c_q^n).$$

The constant c_q was explicitly computed in Ellenberg and Gijwijt's remarkable 2-page long proof. But the task of finding the smallest such c_q is still open. Here, I will present the sketch of their proof for $q = 3$ following the exposition of Tao [2016].

Note that in $\mathbb{F}_3^n$, A is a capset if and only if $x + y + z = 0$ implies $x = y = z$. This can be captured by the following identity:

Proposition

Let $A \subseteq \mathbb{F}_3^n$. Then A is a capset if and only if the following identity holds for all $x, y, z \in A$

$$\delta_0(x + y + z) = \sum_{a \in A} \delta_a(x)\delta_a(y)\delta_a(z) \qquad (*)$$

where δ_k is Kronecker delta function of $k \in \mathbb{F}_3^n$.

We will define a notion of *rank* on functions $A^3 \to \mathbb{F}_3$ so that the rank of the LHS $(*)$ is small, but that of RHS is $|A|$.

2. Defining Slice-rank

We first define what it means to have slice-rank 1.

Definition (Slice-rank One)

Let A be a finite set and $k \geq 2$. A function $f : A^k \to \mathbb{F}_3$ is called *slice-rank one* if there exist an index $i \in \{1, \ldots, k\}$ and functions $g : A^{k-1} \to \mathbb{F}_3$ and $h : A \to \mathbb{F}_3$ such that

$$f(x_1, \ldots, x_n) = g(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n)h(x_i).$$

For the case $k = 2$, f can be identified with an $|A| \times |A|$ matrix M_f in a natural way. Then, $f \neq 0$ is slice-rank one if and only if M_f has rank 1.

Definition (Slice-rank)

The slice-rank of a function $f : A^k \to \mathbb{F}_3$ is the minimum number m of slice-rank one functions $f_1, \ldots, f_m : A^k \to \mathbb{F}_3$ such that $f = f_1 + \cdots + f_m$.

Note that for $k = 2$ and $f \neq 0$, rank of M_f is the same with slice-rank of f.

3. Slice-rank of Diagonal Tensors

Recall our identity:

$$\delta_0(x+y+z) = \sum_{a \in A} \delta_a(x)\delta_a(y)\delta_a(z) \qquad (*)$$

Regard RHS of $(*)$ as a function $f : A^3 \to \mathbb{F}_3$. Then, f is a "diagonal tensor" in a sense that $f(x, y, z) = 0$ whenever x, y, z are not identical.

Proposition

Let $f : A^k \to \mathbb{F}_3$ be such that $f(x_1, \ldots, x_k) = 0$ whenever $x_1, \ldots, x_k$ are not identical. Then, slice-rank of f is the same as number of tuples $(x_1, \ldots, x_n)$ for which $f(x_1, \ldots, x_n) \neq 0$.

Proof.

This is just induction plus standard linear algebra arguments. □

Thus, slice-rank of RHS of $(*)$ is exactly $|A|$.

4. The Main Idea

Now, let $f(x, y, z) = \delta_0(x + y + z)$. We desire an upper bound for slice-rank of f. So, we write f in terms of as little number of slice-rank one functions as possible. This can be done explicitly:

$$\delta_0(x + y + z) = \prod_{i=1}^{n} \left(1 - (x_i + y_i + z_i)^2\right)$$

The RHS is a polynomial of degree $2n$ in $x_1, \ldots, x_n, y_1, \ldots, y_n, z_1, \ldots, z_n$ where each term looks like

$$x_1^{i_1} \cdots x_n^{i_n} y_1^{j_1} \cdots y_n^{j_n} z_1^{k_1} \cdots z_n^{k_n}$$

where each exponent is from $\{0, 1, 2\}$ and $i_1 + \cdots + k_n \leq 2n$.

4. The Main Idea (continued)

$$x_1^{i_1} \cdots x_n^{i_n} y_1^{j_1} \cdots y_n^{j_n} z_1^{k_1} \cdots z_n^{k_n}$$

where each exponent is from $\{0, 1, 2\}$ and $i_1 + \cdots + k_n \leq 2n$.
By pigeonhole principle, one of $i_1 + \cdots + i_n$, $j_1 + \cdots + j_n$ and $k_1 + \cdots + k_n$ is at most $2n/3$. So, we may regroup the terms into at most $3N$ functions of slice-rank one where

$$N = \#\left\{(i_1, \ldots, i_n) \in \{0, 1, 2\}^n : i_1 + \cdots + i_n \leq 2n/3\right\}.$$

This gives us the bound:

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

5. Final Touch-up

It only remains to show that

$$N = \sum_{\substack{a,b,c \geq 0 \\ a+b+c=n \\ b+2c \leq 2n/3}} \frac{n!}{a!b!c!} = O(C^n)$$

for some constant $C < 3$. For any $0 \leq x \leq 1$, we have

$$Nx^{2n/3} \leq \sum_{\substack{a,b,c \geq 0 \\ a+b+c=n \\ b+2c \leq 2n/3}} \frac{n!}{a!b!c!} x^{b+2c} \leq (1 + x + x^2)^n.$$

Hence,

$$N \leq \inf_{x \in [0,1]} \left(\frac{1 + x + x^2}{x^{2/3}} \right)^n < (2.756)^n.$$

Main Theorem

In 2022, Fred Tyrrell Tyrrell [2022] made an improvement to the lower bound on the size of a maximal cap set, by showing the following result:

Theorem (Fred Tyrrell, 2022)

There is a cap set in $\mathbb{F}_3^{56232}$ *of size*

$$\binom{11}{7}^{141} \cdot 6^{572} \cdot 12^{572} \cdot 112^{8800} \cdot 37 \cdot 142$$

and hence, for large n, there is a cap set $A \subseteq \mathbb{F}_3^n$ *of size* $(2.218021\ldots)^n$.

Before that, the last update was done by Edel Edel [2004] in 2004 with the lower bound being $(2.217389\cdots)^n$.

Underlying Principle

The idea mainly based on the following results:

Proposition (1)

Let $A \subseteq \mathbb{F}_3^m$, $B \subseteq \mathbb{F}_3^n$ be cap sets. Then the direct product $A \times B \subseteq \mathbb{F}_3^{mn}$ is also a cap set of size $|A||B|$.

Proposition (2)

Let $A \subseteq \mathbb{F}_3^n$ be a cap set of size c^n. Then, for any $\epsilon > 0$, there is an M such that for all $m \geq M$, there is a cap set of size greater than $(c - \epsilon)^m$ in F_3^m.

Remark: With Proposition 2, finding an asymptotic lower bound for cap set is equivalent to finding a cap set $A \subseteq \mathbb{F}_3^n$ such that $|A|^{\frac{1}{n}}$ is as large as possible.

Underlying Principle (cont.)

Meanwhile, from the idea of proposition 1, we can always produce more cap sets by taking direct products $A \times B$, given $A \subseteq \mathbb{F}_3^n$ and $B \subseteq \mathbb{F}_3^m$ are both cap sets.

However, since $|A \times B|^{\frac{1}{n+m}} \leq \max(|A|^{\frac{1}{n}}, |B|^{\frac{1}{m}})$, the bound from $A \times B$ will not achieve our goal.

Therefore, apart from taking direct products, we switch to the idea of taking union:
Given a collection of cap sets in same dimension, can we take the union of them and it is still a cap set?

It turns out that this is possible, under some conditions.

Some New Constructions

Definition (Extendable Collection)

Let $A_0, A_1, A_2 \subseteq \mathbb{F}_3^n$ be cap sets. The collection (A_0, A_1, A_2) is called *extendable* if the following two holds:

(1) For all $x, y \in A_0$, $z \in A_1 \cup A_2$, $x + y + z \neq 0$.

(2) For all $x \in A_0$, $y \in A_1$, $z \in A_2$, $x + y + z \neq 0$.

Definition (admissible set)

Let $S \subseteq \{0, 1, 2\}^m$. S is *admissible* if the following two holds:

(1) For all distinct $t, t' \in S$, there are coordinates i and j such that $t_i = 0 \neq t'_i$ and $t_j \neq 0 = t'_j$. (double condition)

(2) For all distinct $t, t', t'' \in S$, there is a coordinate k such that $\{t_k, t'_k, t''_k\} = \{0, 1, 2\}, \{0, 0, 1\}$ or $\{0, 0, 2\}$. (triple condition)

We further write S $= I(m, w)$ if S consists of $\binom{m}{w}$ vectors, each of weight w.

Extended Product Construction

From now on, let $A_0, A_1, A_2 \subseteq \mathbb{F}_3^n$ be cap sets, and $S \subseteq \{0,1,2\}^m$ be an admissible set.
We can extend an extendable collection of cap sets by the following idea:

Lemma (3)

For all $t \in S$, we define

$$t(A_0, A_1, A_2) := A_{t_1} \times A_{t_2} \times \cdots \times A_{t_m} \subseteq \mathbb{F}_3^{nm}$$

Then, the set

$$S(A_0, A_1, A_2) := \bigcup_{t \in S} t(A_0, A_1, A_2) \subseteq \mathbb{F}_3^{nm}$$

is a cap set.

The proof can be done by cases checking.

Special type of admissible set

We introduce a special type of admissible set.

Definition (recursively admissible set)

Let $S \subseteq \{0,1,2\}^m$ be an admissible set. We call S is a *recursively admissible set* if $|S| \geq 2$ and for all distinct pairs $s, s' \in S$, we have at least one of the following holds:

(1) There are coordinates i, j such that $\{s_i, s'_i\} = \{0,1\}$ and $\{s_j, s'_j\} = \{0,1\}$.

(2) There is a coordiate k such that $s_k = s'_k = 0$.

Again, we write $S = \tilde{I}(m,w)$ if S consists of $\binom{m}{w}$ vectors, each of weight w.

This special set helps to enlarge the extendable collection of cap sets:
If (A_0, A_1, A_2) is an extendable collection of cap sets, and S is an recursively admissible set, then $(S(A_0, A_1, A_2), A_1^m, A_2^m)$ is an extendable collection of cap sets.

Sketch of Proof of Main Theorem

Upon Construction: there exists cap sets $A_0, A_1, A_2 \subseteq \mathbb{F}_3^6$, with $|A_1| = |A_2|$, such that (A_0, A_1, A_2) is extendable.

Tyrrell makes use of a recursively admissible set $S = \tilde{I}(6, 5)$ to extend the collection first, then use another admissible set $T \subseteq I(1562, 990)$ where $|T| = 142 \cdot 37 \cdot \binom{11}{7}^{141}$ to create the desired cap set.

The counting can be done with the formula:

$$|S(A_0, A_1, A_2)| = \binom{m}{w} |A_0|^{m-w} |A_1|^w$$

Discussion

However, Tyrrell shows that this is not the best bound. By elementary calculus, he shows that the best admissible sets (according to the (A_0, A_1, A_2) he used) are those of the form $I(m, \frac{28m}{31})$, for large m, with the best asymptotic lower bound $(124^{1/6})^n = (2.23\cdots)^n$.
Yet, the existence and construction of such set is still unknown. Tyrrell make the construction via SAT solver.
This can be done by transforming the requirement of admissible sets into conjunctive normal form and pass this to the solver. However, the time cost is very high when m gets larger (in fact it does not work efficiently when $m > 10$). A conjecture is given according to this:

Conjecture

For any m > w > 0, there always exists an $I(m, w)$ admissible set.

Our small idea

Can we construct those set from a simple (but naive approach)? Recall the recurrence relation of binomial coefficients:

$$\binom{m}{w} + \binom{m}{w+1} = \binom{m+1}{w+1}$$

Imagine we are given the sets $I(m, w)$ and $I(m, w+1)$, can we convert them into potential candidates of $I(m+1, w+1)$ and take the union so that it fulfils the requirements of admissible set?
The idea is as follows:
We need to add one more entry to elements in $I(m, w)$ and $I(m, w+1)$.
We will keep the extra entry at the end of each elements.

Our small algorithm

Assume we are given the two sets $I(m, w)$ and $I(m, w+1)$ to initiate the progress.

(1) Convert $I(m, w+1)$ into $I'(m, w+1)$: For $v \in I(m, w+1)$, we only need to insert one 0 entry at the end.

(2) Convert $I(m, w)$ into $I'(m, w)$: For $v' \in I(m, w)$, we only need to give one more nonzero entry at the end. The choices between "1" and "2" will be given by SAT solver. The decision needs to make the union of two sets fulfils the requirement of admissible sets.

From this, the support of any two vectors of the new set
$P := I'(m, w+1) \cup I'(m, w)$ are distinct and weight of all vectors are $w+1$, so (double condition) is satisfied.
We only need to deal with (triple condition) when employing SAT solver.

Example

We end our discussion by providing a demonstration on a small set.
Our best records: Construct $I(m, w)$ for m up to 6, and for all $w \leq m$.

$$I(4,2) = \Big\{[0,0,1,1],[0,2,0,2],[1,0,0,1],[0,1,1,0],[1,0,2,0],[1,1,0,0]\Big\}$$

$$I(4,3) = \Big\{[0,1,1,1],[1,0,2,2],[1,1,0,2],[1,1,1,0]\Big\}$$

$$I(5,3) = \Big\{[0,0,1,1,1],[0,2,0,2,2],[1,0,0,1,1],[0,1,1,0,2],$$
$$[1,0,2,0,1],[1,1,0,0,1],$$
$$[0,1,1,1,0],[1,0,2,2,0],[1,1,0,2,0],[1,1,1,0,0]\Big\}$$

References

Thomas F Bloom and Olof Sisask. Breaking the logarithmic barrier in roth's theorem on arithmetic progressions. *arXiv preprint arXiv:2007.03528*, 2020.

Yves Edel. Extensions of generalized product caps. *Designs, Codes and Cryptography*, 31:5–14, 2004.

Jordan S Ellenberg and Dion Gijswijt. On large subsets of with no three-term arithmetic progression. *Annals of Mathematics*, pages 339–343, 2017.

Ben Green and Terence Tao. The primes contain arbitrarily long arithmetic progressions. *Annals of mathematics*, pages 481–547, 2008.

Klaus F Roth. On certain sets of integers. *J. London Math. Soc*, 28(104-109):3, 1953.

T Tao. A symmetric formulation of croot-lev-pach-ellenberg-gijwijt capset bound, 2016. URL `https://terrytao.wordpress.com/2016/05/18/a-symmetric-formulation-of-the-croot-lev-pach-ellenberg-gijswij`

Fred Tyrrell. New lower bounds for cap sets. *arXiv preprint arXiv:2209.10045*, 2022.