The Symmetric Formulation of Ellenberg-Gijwijt's Bound on Capset Problem

Terrence Tao

January 4, 2024

Notations

Throughout this presentation,

- n is a fixed positive integer,
- q is a prime power, and $\mathbb{F}_q$ the finite field of order q,
- $\alpha, \beta, \gamma \in \mathbb{F}_q$ are such that $\alpha + \beta + \gamma = 0$.

Definition

A set $A \subseteq \mathbb{F}_q^n$ is called a capset if the only solutions $(\mathbf{x}, \mathbf{y}, \mathbf{z}) \in A^3$ to the equation

$$\alpha\mathbf{x} + \beta\mathbf{y} + \gamma\mathbf{z} = 0$$

are trivial solutions: $\mathbf{x} = \mathbf{y} = \mathbf{z}$.

Remark

The traditional definition for a capset takes $\alpha = \beta = 1$ and $\gamma = -2$ i.e. a capset is a set the does not contain a 3-term arithmetic progression.

The Problem and Our Goal

Problem (Capset Problem)

Does there exist a constant $c < q$ such that

$$|A| = O(c^n)$$

where A is the largest capset of $\mathbb{F}_q^n$?

The answer turns out to be positive, proven by Ellenberg and Gijwijt in 2017 using the Croot-Lev-Pach polynomial method. The main goal of this presentation is to prove the following theorem:

Theorem (Ellenberg, Gijwijt)

Let $A \subseteq \mathbb{F}_q^n$ be a capset. Then,

$$|A| \leq 3N$$

where N is the number of monomials $x_1^{d_1} x_2^{d_2} \dots x_n^{d_n}$ such that $d_i \leq q - 1$ for each $i \in \{1, \dots, n\}$ and $d_1 + \cdots + d_n \leq (q-1)n/3$.

Terry's Reformulation

We will use the symmetric reformulation of the proof written by Terrence Tao on his blogpost. First of all, note the following trivial preposition:

Preposition

A set $A \subseteq \mathbb{F}_q^n$ is a capset if and only if

$$\delta_{\mathbf{0}}(\alpha\mathbf{x} + \beta\mathbf{y} + \gamma\mathbf{z}) = \sum_{\mathbf{a}\in A} \delta_{\mathbf{a}}(\mathbf{x})\delta_{\mathbf{a}}(\mathbf{y})\delta_{\mathbf{a}}(\mathbf{z}) \qquad (\star)$$

for all $(\mathbf{x}, \mathbf{y}, \mathbf{z}) \in A^3$.

$(\star)$ can be thought of as identity of functions $A^3 \to \mathbb{F}_q$. We will come up with a notion of 'rank ' so that rank of RHS is $|A|$ and that of LHS is $\leq 3N$.

Defining rank-one

From now on, $k \geq 2$ is a positive integer.

Definition

For a set $A \subseteq \mathbb{F}_q^n$, a non-zero function $\varphi : A^k \to \mathbb{F}_q$ is called slice-rank-one if it has the form:

$$\varphi(\mathbf{x_1}, \ldots, \mathbf{x_k}) = f(\mathbf{x_1}, \ldots, \mathbf{x_{i-1}}, \mathbf{x_{i+1}}, \ldots, \mathbf{x_k}) g(\mathbf{x_i})$$

for some $1 \leq i \leq k$ and functions $f : A^{k-1} \to \mathbb{F}_q$, $g : A \to \mathbb{F}_q$.

Example

- The function $(\mathbf{x}, \mathbf{y}, \mathbf{z}) \mapsto (x_1 y_2 + x_2^3 y_1^2) z_1^2 z_2^3$ is slice-rank-one.
- The function
$$(\mathbf{x}, \mathbf{y}, \mathbf{z}) \mapsto \delta_{\mathbf{a}}(\mathbf{x}) \delta_{\mathbf{a}}(\mathbf{y}) \delta_{\mathbf{a}}(\mathbf{z})$$
  is slice-rank-one.

Slice-rank-one is same as matrix rank one

Example

For $k = 2$, the function $\varphi : A^2 \to \mathbb{F}_q$ can be thought of as an $|A| \times |A|$ matrix

$$\begin{bmatrix} \varphi(\mathbf{a}_1, \mathbf{a}_1) & \varphi(\mathbf{a}_1, \mathbf{a}_2) & \cdots & \varphi(\mathbf{a}_1, \mathbf{a}_{|A|}) \\ \varphi(\mathbf{a}_2, \mathbf{a}_1) & \varphi(\mathbf{a}_2, \mathbf{a}_2) & \cdots & \varphi(\mathbf{a}_2, \mathbf{a}_{|A|}) \\ \vdots & \vdots & \ddots & \vdots \\ \varphi(\mathbf{a}_{|A|}, \mathbf{a}_1) & \varphi(\mathbf{a}_{|A|}, \mathbf{a}_2) & \cdots & \varphi(\mathbf{a}_{|A|}, \mathbf{a}_{|A|}) \end{bmatrix}$$

where $A = \{\mathbf{a}_1, \ldots, \mathbf{a}_{|A|}\}$. When $\varphi(\mathbf{x}, \mathbf{y}) = f(\mathbf{x})g(\mathbf{y})$, this becomes:

$$\begin{bmatrix} f(\mathbf{a}_1)g(\mathbf{a}_1) & f(\mathbf{a}_1)g(\mathbf{a}_2) & \cdots & f(\mathbf{a}_1)g(\mathbf{a}_{|A|}) \\ f(\mathbf{a}_2)g(\mathbf{a}_1) & f(\mathbf{a}_2)g(\mathbf{a}_2) & \cdots & f(\mathbf{a}_2)g(\mathbf{a}_{|A|}) \\ \vdots & \vdots & \ddots & \vdots \\ f(\mathbf{a}_{|A|})g(\mathbf{a}_1) & f(\mathbf{a}_{|A|})g(\mathbf{a}_2) & \cdots & f(\mathbf{a}_{|A|})g(\mathbf{a}_{|A|}) \end{bmatrix}$$

which has rank 1 as a matrix if φ is non-zero.

What is slice-rank

Motivated by our previous example, we can define the slice-rank for general $k \geq 2$ as follows:

Definition

The slice-rank of a non-zero function $\varphi : A^k \to \mathbb{F}_q$ is the minimum number of slice-rank-one functions $A^k \to \mathbb{F}_q$ whose sum is φ. We write the slice-rank of φ by $r_{sl}(\varphi)$. If $\varphi \equiv 0$, we define $r_{sl}(\varphi) = 0$.

Example

- Slice rank of $\varphi : A^2 \to \mathbb{F}_q$ is the same as rank of the corresponding $|A| \times |A|$ matrix induced by φ.
- Slice rank of

$$(\mathbf{x}, \mathbf{y}, \mathbf{z}) \mapsto \sum_{\mathbf{a} \in A} \delta_{\mathbf{a}}(\mathbf{x}) \delta_{\mathbf{a}}(\mathbf{y}) \delta_{\mathbf{a}}(\mathbf{z})$$

  is $\leq |A|$.

Slice-rank of diagonal 'matrices'

Definition

A function $\varphi : A^k \to \mathbb{F}_q$ is called diagonal if $\varphi(\mathbf{x_1}, \ldots, \mathbf{x_k}) \neq 0$ only if $\mathbf{x_1} = \cdots = \mathbf{x_k}$.

Theorem

For a diagonal function φ, $r_{sl}(\varphi) = |Supp(\varphi)|$. In particular, slice rank of

$$(\mathbf{x}, \mathbf{y}, \mathbf{z}) \mapsto \sum_{\mathbf{a} \in A} \delta_{\mathbf{a}}(\mathbf{x})\delta_{\mathbf{a}}(\mathbf{y})\delta_{\mathbf{a}}(\mathbf{z})$$

is $|A|$.

Proof is standard-linear-algebra flavoured and not very interesting. We will come back later after discussing more interesting stuff...

What's next?

Recall our little identity that checks whether or not $A \subseteq \mathbb{F}_q^n$ is a capset:

Preposition

A set $A \subseteq \mathbb{F}_q^n$ is a capset if and only if

$$\delta_{\mathbf{0}}(\alpha\mathbf{x} + \beta\mathbf{y} + \gamma\mathbf{z}) = \sum_{\mathbf{a} \in A} \delta_{\mathbf{a}}(\mathbf{x})\delta_{\mathbf{a}}(\mathbf{y})\delta_{\mathbf{a}}(\mathbf{z}) \qquad (\star)$$

for all $(\mathbf{x}, \mathbf{y}, \mathbf{z}) \in A^3$.

And also the main theorem we want to prove:

Theorem (Ellenberg, Gijwijt)

Let $A \subseteq \mathbb{F}_q^n$ be a capset. Then,

$$|A| \leq 3N$$

where N is the number of monomials $x_1^{d_1} x_2^{d_2} \dots x_n^{d_n}$ such that $d_i \leq q-1$ for each $i \in \{1, \dots, n\}$ and $d_1 + \dots + d_n \leq (q-1)n/3$.

Rank of $\delta_{\mathbf{0}}(\alpha\mathbf{x} + \beta\mathbf{y} + \gamma\mathbf{z})$

Lemma

Let $\varphi : A^3 \to \mathbb{F}_q$ *given by*

$$\varphi(\mathbf{x}, \mathbf{y}, \mathbf{z}) = \delta_{\mathbf{0}}(\alpha\mathbf{x} + \beta\mathbf{y} + \gamma\mathbf{z}).$$

Then, $r_{sl}(\varphi) \leq 3N$ *where* N *is the number of monomials* $x_1^{d_1} x_2^{d_2} \dots x_n^{d_n}$ *such that* $d_i \leq q-1$ *for each* $i \in \{1, \dots, n\}$ *and* $d_1 + \dots + d_n \leq (q-1)n/3$.

Proof

We want to rewrite φ as sum of $\leq 3N$ slice-rank-one functions. So, define a polynomial $p \in \mathbb{F}_q[x_1, \dots, x_n, y_1, \dots, y_n, z_1, \dots, z_n]$ by

$$p := \prod_{i=1}^{n} (1 - (\alpha x_i + \beta y_i + \gamma z_i)^{q-1}).$$

Note that p as a function $A^3 \to \mathbb{F}_q$ is the same as φ. Now, we expand p by multiplying everything out and it will look something messy like this:

$$\sum_{\substack{i_1,\dots,k_n \in \mathbb{Z}_{\geq 0} \\ i_\bullet, j_\bullet, k_\bullet \leq q-1 \\ i_1+\cdots+k_n \leq n(q-1)}} C_{i_1 \dots k_n} x_1^{i_1} \dots x_n^{i_n} y_1^{j_1} \dots y_n^{j_n} z_1^{k_1} \dots z_n^{k_n}.$$

Proof (continued)

$$\sum_{\substack{i_1,\dots,k_n \in \mathbb{Z}_{\geq 0} \\ i_\bullet, j_\bullet, k_\bullet \leq q-1 \\ i_1+\cdots+k_n \leq n(q-1)}} C_{i_1\cdots k_n} x_1^{i_1} \dots x_n^{i_n} y_1^{j_1} \dots y_n^{j_n} z_1^{k_1} \dots z_n^{k_n}. \tag{1}$$

Now, we want to regroup the terms. For each term, since $i_1 + \cdots + k_n \leq n(q-1)$, at least one of the following quantities is at most $n(q-1)/3$:

$$i_1 + \cdots + i_n, \quad j_1 + \cdots + j_n, \quad k_1 + \cdots + k_n.$$

So, we can collect the terms into three (not necessarily mutually-exclusive) types:

- terms with $i_1 + \cdots + i_n \leq n(q-1)/3$,
- terms with $j_1 + \cdots + j_n \leq n(q-1)/3$,
- terms with $k_1 + \cdots + k_n \leq n(q-1)/3$.

Proof (continued)

- terms with $i_1 + \cdots + i_n \leq n(q-1)/3$,
- terms with $j_1 + \cdots + j_n \leq n(q-1)/3$,
- terms with $k_1 + \cdots + k_n \leq n(q-1)/3$.

Regrouping the terms according to their types (choose randomly if the term is in more than one type), we would have written (1) as sum of $\leq 3N$ expressions (recall that N is the number of monomials $x_1^{d_1} x_2^{d_2} \dots x_n^{d_n}$ such that $d_i \leq q-1$ for each $i \in \{1, \dots, n\}$ and $d_1 + \cdots + d_n \leq (q-1)n/3$). Since each of these expressions is slice-rank-one and p agrees with φ on A^3,

$$r_{sl}(\varphi) \leq 3N.$$

Why should N be small?

Now that we have $|A| \leq 3N$, we only need to see why $N = O(c^n)$ for some constant $c < q$. **Intuition:** If we uniformly choose a random monomial from

$$S = \{x_1^{d_1} \dots x_n^{d_n} : 0 \leq d_i \leq q-1 \text{ for } i = 1, \dots, n\},$$

then, the expected degree is $n(q-1)/2$ which is far from $n(q-1)/3$. Formally, let $d = \text{Uniform}(\{0, 1, \dots, q-1\})$ be a discrete random variable and d_1, $d_2, \dots$ be i.i.d. copies of d. Then,

$$\mathbb{P}\left(d_1 + \cdots + d_n \leq \frac{n(q-1)}{3}\right) = \frac{N}{q^n}.$$

Note that Law of Large Numbers is already giving us $N = o(q^n)$, but we need to get a more precise bound.

Elementary Proof of $N = O(c^n)$

First, note that

$$N = \left|\{(d_1, \ldots, d_n) : 0 \le d_i \le q-1, \sum_{i=1}^{n} d_i \le \frac{n(q-1)}{3}\}\right|$$

$$= \sum_{\substack{m_0, \ldots, m_{q-1} \\ m_0+m_1+\cdots+m_{q-1}=n \\ m_1+2m_2+3m_3+\cdots+(q-1)m_{q-1} \le n(q-1)/3}} \frac{n!}{m_0! m_1! \cdots m_{q-1}!}.$$

Therefore, for all $0 \le x \le 1$,

$$N x^{\frac{n(q-1)}{3}} \le \sum_{\cdots} \frac{n!}{m_0! m_1! \cdots m_{q-1}!} x^{m_1+2m_2+\cdots+(q-1)m_{q-1}}$$

$$\le (1 + x + x^2 + \cdots + x^{q-1})^n$$

Hence,

$$N \le \inf_{0 \le x \le 1} \left(\frac{1 + x + x^2 + \cdots + x^{q-1}}{x^{(q-1)/3}} \right)^n < c^n.$$

Slice rank of diagonal 'matrices'

Now, let us present the proof of the following theorem:

Theorem

For a diagonal function $\varphi : A^k \to \mathbb{F}_q$,

$$r_{sl}(\varphi) = |Supp(\varphi)|.$$

Proof

We induct on k. Base case $k = 2$ is already done as an example. It suffices to deal with the case where φ is non-zero on the diagonal since slice-rank does not increase under restriction:
If $A_1 \subseteq A$, and $\varphi_1 = \varphi|_{A_1^k}$, then

$$r_{sl}(\varphi_1) \leq r_{sl}(\varphi).$$

Suppose to the contrary that $\varphi : A^k \to \mathbb{F}_q$ can be written as sum of less than $m < |A|$ slice-rank-one functions.

Proof (page 2)

Suppose that $\varphi : A^k \to \mathbb{F}_q$ can be written as sum of m slice-rank-one functions:

$$\varphi = \varphi_1 + \cdots + \varphi_m.$$

Suppose that $\varphi_1, \ldots, \varphi_r$ separates the variable $\mathbf{x}_1$ i.e.

$$\varphi_i(\mathbf{x}_1, \ldots, \mathbf{x}_k) = f_i(\mathbf{x}_2, \ldots, \mathbf{x}_k) g_i(\mathbf{x}_1), \quad i = 1, \ldots, r$$

for some $r \neq 0$ (WLOG), $f_i : A^{k-1} \to \mathbb{F}_q$ and $g_i : A \to \mathbb{F}_q$. Define V to be the 'orthogonal complement' of g_i's i.e.

$$V := \{h : A \to \mathbb{F}_q | \sum_{\mathbf{x}_1 \in A} h(\mathbf{x}_1) g_i(\mathbf{x}_1) = 0 \text{ for all } i = 1, \ldots, r\}.$$

Proof (page 3)

Take $h \in V$ with maximal support, and consider:

$$\sum_{\mathbf{x}_1 \in A} h(\mathbf{x}_1)\varphi(\mathbf{x}_1, \ldots, \mathbf{x}_k) = \sum_{\mathbf{x}_1 \in A} h(\mathbf{x}_i)(\varphi_1 + \cdots + \varphi_r)(\mathbf{x}_1, \ldots, \mathbf{x}_k) + \sum_{\mathbf{x}_1 \in A} h(\mathbf{x}_i)(\varphi_{r+1} + \cdots + \varphi_m)(\mathbf{x}_1, \ldots, \mathbf{x}_k).$$

Now, both sides become functions of $\mathbf{x}_2, \ldots, \mathbf{x}_k$. But,

$$r_{sl}(\text{RHS}) \leq m - r, \quad r_{sl}(\text{LHS}) = |\text{Supp}(h)|.$$

So, it suffices to show that $|\text{Supp}(h)| \geq |A| - r$.

Proof (page 4)

We will show that $|\mathrm{Supp}(h)| \geq \dim V \geq |A| - r$. The latter inequality can be proven by staring at the definition of V:

$$V := \{h : A \to \mathbb{F}_q | \sum_{\mathbf{x}_1 \in A} h(\mathbf{x}_1) g_i(\mathbf{x}_1) = 0 \text{ for all } i = 1, \ldots, r\}.$$

For the former, if $|\dim V| > |\mathrm{Supp}(h)|$, then the linear map $V \to \mathbb{F}_q^{|\mathrm{Supp}(h)|}$ given by evaluation at points of $\mathrm{Supp}(h) \subseteq A$ cannot be injective. Thus, we would be able to find a non-zero $h' \in V$ that vanishes on $\mathrm{Supp}(h)$. In that case,

$$|\mathrm{Supp}(h + h')| > |\mathrm{Supp}(h)|$$

contradicting the maximality.