# スライスランク法とその周辺の話題

琉球大学教育学部　徳重 典英
Norihide Tokushige
College of Education, Ryukyu University

## 1. はじめに

講演でも述べたとおり、本稿は見村万佐人氏との共同研究に基づくものです。以下は講演内容に文献情報と多少の証明を加えました。

正整数 $n$ に対して $[n]=\{1,2,\dots,n\}$ とおく。部分集合 $X\subset[n]$ が長さ 3 の等差数列（以下、3-AP と略記）を含まないとき、$|X|$ はどのくらい大きくなれるだろうか。ただし 3-AP とは、$x,x+d,x+2d$ と表示できる 3 数で公差 $d$ は 0 でないものとする。つまり

$$r(n):=\max\{|X|:X\subset[n]\text{ は 3-AP を含まない }\}$$

を評価したい。この問題は Erdős と Turán [12] によって提起された。Behrend[4] は下界について、Roth[20] は上界について

$$n^{1-c/\sqrt{\log n}}<r(n)<\frac{c'n}{\log\log n}$$

を示した。その後、上界については Heath-Brown, Szemerédi, Bourgain, Sanders, Bloom らの研究があり、$O((\log\log n)^4 n/\log n)$ まで改善された（例えば [6] 参照）。これを $O(n/\log n)$ まで改善できるか、そして逆数の和が発散する整数の部分集合は 3-AP を含むか（等差数列に関する Erdős–Turán 予想の一番簡単な場合）は未解決である。

上記の問題は $[n]$ のかわりに $\mathbb{Z}/n\mathbb{Z}$ で考えても本質的な違いはない。そこでもっと一般にアーベル群 $G$ を指定して 3-AP を含まない $G$ の部分集合の最大サイズ $r(G)$ は何か、という問題を考えてみよう。本稿では主に $G=\mathbb{F}_p^n$ の場合をとりあげる。ここで $p$ は素数とし、$\mathbb{F}_p^n$ は $p$ 元体 $\mathbb{F}_p$ 上の $n$ 次元ベクトル空間である。特に $p=3$ の場合は、後述するひまわりの問題や高速行列積の exponent（例えば [5] 参照）との関連もあって関心を集めた。Edel[8] は構成により $r(\mathbb{F}_3^n)$ の下界として $2.21^n$ を得た。一方、上界については既に 1982 年には $o(3^n)$ であることが Brown と Buhler によって示され、その後のいくつかの研究を経て、Bateman と Katz[3] によって $O(3^n/n^{1+\varepsilon})$ まで改善された。しかし定数 $c<3$ を用いて $r(\mathbb{F}_3^n)<c^n$ と評価できるかどうかは全く不明だった。

この問題に大きな進展を与えたのは Croot, Lev, Pach[7] の研究である。彼らは $G=(\mathbb{Z}/4\mathbb{Z})^n$ の場合に $r(G)<3.61^n$ を示した。その証明はいわゆる「多項式の手法」による。同様の手法はすぐに Ellenberg と Gijswijt[9] によって $G=\mathbb{F}_p^n$ の場合に（独立に）応用された。その $p=3$ の場合として次の結果が得られた。

**定理 1** (Ellenberg–Gijswijt)**.** $G=\mathbb{F}_3^n$ のとき、$r(G)<2.76^n$ が成り立つ。

Tao[24] は、Croot–Lev–Pach および Ellenberg–Gijswijt の証明を検討しスライスランクを導入した。本稿ではこのスライスランクについて解説し、それを用いて定理 1 を証明した後、関連する応用例や周辺の話題について紹介する。

## 2. スライスランクと定理 1 の証明

**2.1. 定義と Tao の補題.** $X$ を有限集合、$\mathbb{F}$ を体とする。関数 $f : X^3 \to \mathbb{F}$ がスライス関数であるとは、$f$ が次の形のいずれかに表示できることである。

$$f(x,y,z) = a(x)b(y,z) \text{ または } a(y)b(x,z) \text{ または } a(z)b(x,y).$$

ここで $f$ のスライスランクを次のように定義する。

$$\mathrm{sr}(f) := \min\left\{ r : f = \sum_{i=1}^{r} g_i, \text{ 各 } g_i \text{ はスライス関数} \right\}.$$

実際、どんな $f : X^3 \to \mathbb{F}$ も高々 $|X|$ 個のスライス関数の和にかける。特に $\mathrm{sr}(f) \le |X|$ である。

**補題 2** (Tao の補題 [24])**.** 関数 $f : X^3 \to \mathbb{F}$ が「対角条件」すなわち

$$f(x,y,z) \neq 0 \Longleftrightarrow x = y = z$$

をみたすと仮定する。このとき $\mathrm{sr}(f) = |X|$ が成り立つ。

上記補題の日本語による解説は例えば [25] にある。

**2.2. 定理 1 の証明.** Tao[24] にしたがって、$\mathbb{F}_3^n$ の部分集合 $X$ が 3-AP を含まないと仮定し、ある正定数 $c < 3$ が存在して $|X| < c^n$ であることを示そう。そのために次の二つの条件を満たす関数 $f : X^3 \to \mathbb{F}$ を見つけたい。

(C1) $f$ は対角条件をみたす。
(C2) $\mathrm{sr}(f) < c^n$.

このとき Tao の補題から $|X| = \mathrm{sr}(f) < c^n$ が従う。

条件を満たす $f$（のひとつ）を具体的に表示できる。そのために $\mathbb{F}_3^n$ の元を $x = (x_1, \ldots, x_n)$ のように表記し、$f : X^3 \to \mathbb{F}_3$ を次のように定める。

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

実はこの $f$ は (C1) と (C2) をみたし、$c = 2.76$ ととれる。以下、このことを確かめよう。

まず (C1) をみるために、$f$ と 3-AP の関係を調べよう。もし $x,y,z \in \mathbb{F}_3^n$ がこの順に 3-AP をなすならば、$x + z = 2y$, あるいは同じことだが $x + y + z = 0$ である。逆に $x,y,z \in \mathbb{F}_3^n$ が $x + y + z = 0$ をみたせば、これらは 3-AP をなすか、または $x = y = z$ である。したがって任意の $x,y,z \in X$ に対して $x + y + z = 0$ と $x = y = z$ は同値である。また、$g \in \mathbb{F}_3$ が $g^2 \neq 1$ となるのは $g = 0$ のとき、かつそのときに限る。これらのことに注意すると、$x,y,z \in X$ について次のことがわかる。

$$\begin{aligned} f(x,y,z) \neq 0 &\Longleftrightarrow (x_i + y_i + z_i)^2 \neq 1 \text{ for all } i \\ &\Longleftrightarrow x_i + y_i + z_i = 0 \text{ for all } i \\ &\Longleftrightarrow x + y + z = 0 \\ &\Longleftrightarrow x = y = z, \end{aligned}$$

つまり $f$ は (C1) をみたす。

次に (C2) を確かめるために、$f$ のスライスランクを定義に従って評価しよう。そのために $f$ をなるべく少ない個数のスライス関数の和に書きたい。$f$ の定義式 (1) の右辺を展開すると、各項は

$$(\text{係数}) \times x_1^{i_1} \cdots x_n^{i_n} \times y_1^{j_1} \cdots y_n^{j_n} \times z_1^{k_1} \cdots z_n^{k_n}$$

の形の単項式で、次数和は $i_1 + \cdots + k_n \le 2n$ をみたす。つまり平均でみると $x$ に関する次数 $i_1 + \cdots + i_n$ は $2n/3$ 以下であり、同じことが $y, z$ についてもいえる。そこで $f$ の単項式たちのうち $x$ の次数が $2n/3$ 以下のものの和を $f_x$ とし、$f - f_x$ の単項式で $y$ の次数が $2n/3$ 以下のものの和を $f_y$ とすると、$f_z := f - f_x - f_y$ の単項式の $z$ の次数は $2n/3$ 以下である。このようにして

$$f = f_x + f_y + f_z$$

と表すと、$f_x$ は $x$ の次数が $2n/3$ 以下のスライス関数の和であり（つまり $f_x = \sum a(x)b(y,z)$ とみる）、$f_y$ と $f_z$ も同様である。したがって

$$\mathrm{sr}(f) \le \mathrm{sr}(f_x) + \mathrm{sr}(f_y) + \mathrm{sr}(f_z) \le 3\mathrm{sr}(f_x)$$

としてよい。以下、$f_x$ に現れるスライス関数を評価する。

スライス関数の和で $f_x = \sum a(x)b(y,z)$ と書いたとき、$a(x) = (\text{係数}) \times x_1^{i_1} \cdots x_n^{i_n}$ に現れる $(i_1, \ldots, i_n)$ は次の集合

$$I := \{(i_1, \ldots, i_n) \in \{0,1,2\}^n : i_1 + \cdots + i_n \le 2n\} \tag{2}$$

の要素だから、$\mathrm{sr}(f_x) \le |I|$ である。そこで $|I|$ を上から評価しよう。ここで $(i_1, \ldots, i_n) \in I$ と $u = 0,1,2$ に対して $a_u := |\{i_l : i_l = u\}|$ とおけば、

$$\text{(P)} \quad a_0 + a_1 + a_2 = n, \qquad \text{(Q)} \quad a_1 + 2a_2 \le 2n$$

が成り立つ。逆に条件 (P), (Q) をみたす $(a_0, a_1, a_2)$ を固定すると、それに対応する $(i_1, \ldots, i_n) \in I$ の個数は

$$\binom{n}{a_0}\binom{n-a_0}{a_1}\binom{n-a_0-a_1}{a_2} = \frac{n!}{a_0!a_1!a_2!}$$

である。したがって

$$|I| = \sum \frac{n!}{a_0!a_1!a_2!},$$

ただし和は (P) と (Q) をみたす非負整数の組 $(a_0, a_1, a_2)$ についてとる。

ここで関数 $g:(0,1)\to\mathbb{R}$ を $g(t)=t^{-2/3}(1+t+t^2)$ として導入しよう。$(g(t))^n$ を多項展開して (P), (Q) および $t\in(0,1)$ であることを考慮すると

$$\begin{aligned}(g(t))^n &= t^{-\frac{2n}{3}}(1+t+t^2)^n\\ &= \sum_{(\mathrm{P})}\frac{n!}{a_0!a_1!a_2!}t^{a_1+2a_2-\frac{2n}{3}}\\ &> \sum_{(\mathrm{P}),(\mathrm{Q})}\frac{n!}{a_0!a_1!a_2!}t^{a_1+2a_2-\frac{2n}{3}}\\ &> \sum_{(\mathrm{P}),(\mathrm{Q})}\frac{n!}{a_0!a_1!a_2!}=|I|.\end{aligned}$$

つまり $(g(t))^n>|I|$ が任意の $t\in(0,1)$ について成り立つ。$g$ の微分の計算から $g(t)$ は $t=\alpha:=\frac{1}{8}(\sqrt{33}-1)$ で最小値 $g(\alpha)=\frac{3}{8}(33\sqrt{33}+207)^{\frac{1}{3}}<2.76$ をとる。したがって

$$\mathrm{sr}(f_r)\le|I|<(2.76)^n$$

である。ここから $\mathrm{sr}(f)<3(2.76)^n$ がわかる。さらに power trick により $\mathrm{sr}(f)<(2.76)^n$ と改善できる（例えば [14] の Lemma 9.2 参照）。これと Tao の補題から目標の結果が得られた。 □

## 3. スライスランク法の応用

スライスランク法の直接の応用によって得られた結果をふたつ紹介する。

3.1. **ひまわり.** はじめの例は有限集合族における応用である。いくつか記号を導入しよう。$2^{[n]}=\{F:F\subset[n]\}$, $\binom{[n]}{k}=\{F\subset[n]:|F|=k\}$ とおく。相異なる三つの部分集合 $A,B,C\subset[n]$ は、$A\cap B=B\cap C=C\cap A$ をみたすとき（花びら 3 枚の）ひまわりであるという。

**定理 3.** ある $c<2$ と $n_0$ が存在して、$n>n_0$ ならばひまわりを含まない $\mathscr{F}\subset 2^{[n]}$ は $|\mathscr{F}|<c^n$ をみたす。

この結果は Erdős と Szemerédi [11] によって予想されたもので、Alon, Shpilka, Umans[2] により定理 1 から従うことが知られていた。したがって定理 1 が得られた時点でこの予想も定理となったわけだが、さらに Naslund と Sawin [18] はスライスランク法を用いて直接の証明を与えた。彼らの証明は現状で最良の $c$ を与える。その概略を紹介する。

部分集合 $F\subset[n]$ の特性ベクトル $x\in\{0,1\}^n$ を $i\in F$ なら $x_i=1$, $i\notin F$ なら $x_i=0$ と定義する。集合族 $\mathscr{F}\subset 2^{[n]}$ がひまわりを含まないとし、$X\subset\{0,1\}^n$ を $\mathscr{F}$ の特性ベクトルの集合とする。各 $0\le k\le n$ について $\mathscr{F}_k=\mathscr{F}\cap\binom{[n]}{k}$ とおき、対応する特性ベクトルの部分集合を $X_k\subset X$ とする。このとき $x\in X_k$ ならば $\sum_i x_i=k$ である。

ひまわりがないという条件は、$X_k$ において次の条件に翻訳される：どんな 3 個のベクトル $x,y,z\in X_k$ もそれが同一のベクトルでなければ、$w:=x+y+z$ とおくとき $w_i=2$ となる $i$ がある。（ここが微妙なところでこの条件は $X_k$ で正しいが、$X$ では一般には成立しない。）そこで関数 $f:X_k^3\to\mathbb{R}$ を

$$f(x,y,z)=\prod_{i=1}^{n}(x_i+y_i+z_i-2).$$

と定義すると、$f$ は対角条件を満たし Tao の補題から $\mathrm{sr}(f) = |X_k|$ である。一方、この関数のスライスランクについては 3-AP のときと同様の議論で $\mathrm{sr}(f) < 3(1.89)^n$ がわかる。ここから $|\mathscr{F}| = \sum_{k=0}^{n} |X_k| < 3(n+1)(1.98)^n < c^n$ が従う。

3.2. **単色単位正三角形を含まない $n$ 次元空間の着色.** 次の例は離散幾何における応用である。$n$ 次元ユークリッド空間 $\mathbb{R}^n$ を $r$ 色で塗って、一辺の長さが 1 の単色正則 $k$ 単体がないようにしたい。このような着色が可能な $r$ の最小値を $\chi_k(\mathbb{R}^n)$ とかく。例えば $\chi_1(\mathbb{R}^2)$ は、距離がちょうど 1 だけ離れた 2 点が必ず異なる色となるように平面を着色できる最小の色の数（つまり $\mathbb{R}^2$ を頂点集合とする単位距離グラフの染色数）であり、$5 \leq \chi_1(\mathbb{R}^2) \leq 7$ が知られている。一般に（$k$ を固定して $n \to \infty$ のとき）

$$\left(1 + \frac{1}{2^{2^{k+4}}} + o(1)\right)^n \leq \chi_k(\mathbb{R}^n) \leq \left(1 + \left(2 + \frac{2}{k}\right)^{\frac{1}{2}} + o(1)\right)^n$$

などが知られている（例えば [22] を見よ）。$k = 2$ のとき、すなわち単色の単位正三角形がないような着色については、$\chi_2(\mathbb{R}^n) > (1 + c + o(1))^n$ であるが、Sagdeev[22] はこの定数について具体的に $c = 0.00085$ ととれることを示した。Naslund[17] はスライスランク法を用いてもっと短い手順で $c = 0.01446$ を得た。

## 4. スライスランク法の弱点

4.1. **連立方程式.** ここまでスライスランク法がうまく適用できる場面を紹介したが、もちろんスライスランク法がいつでもうまく機能するわけではない。スライスランク法の最初の応用は 3-AP を含まない集合のサイズの上界を与えるものだった。同様の議論は 4-AP についても通用するだろうか。集合 $X \subset \mathbb{F}_p^n$ が 3-AP を含まないことは、任意の $x, y, z \in X$ について

$$x - 2y + z = 0 \quad \Longrightarrow \quad x = y = z$$

と言い換えられる。同様に $X$ が 4-AP を含まないことは、任意の $x, y, z, w \in X$ について

$$\begin{cases} x - 2y + z = 0 \\ y - 2z + w = 0 \end{cases} \quad \Longrightarrow \quad x = y = z = w \tag{3}$$

と同値である。すなわち、この場合には連立方程式の解を扱う必要が生じる。実際、2 節の議論は自然に連立方程式の場合に拡張できて、スライスランクから $|X|$ の上界を得られる。しかし上記の連立方程式の場合に素直にスライスランク法を適用して得られる上界は $p^n$ という自明なものになる。一方、Hales–Jewett の定理より $|X| = o(p^n)$ が得られるから、目標としてはある定数 $0 < c < 1$ に対して

$$|X| < (cp)^n \tag{4}$$

という評価が得られるかどうかを見極めたい。

ここで、$r$ 個の変数からなる $l$ 本の連立方程式があって、$r_1$ 個の変数は一本の方程式にのみ現れ、$r_2 := r - r_1$ 個の変数は少なくとも 2 本以上の方程式に現れるとしよう。さらにこの連立方程式の $X \subset \mathbb{F}_p^n$ における解は、すべての変数の値が等しいものに限られると仮定する。Mimura–Tokushige[15] では、さらにもし

$$\frac{r_1}{2} + \frac{r_2}{e} > l \tag{5}$$

であれば、$|X|$ の非自明な上界が得られることを示した。残念ながら (3) の場合は $r_1 = r_2 = l = 2$ なので (5) をみたさない。4-AP を含まない $X \subset \mathbb{F}_p^n$ が (4) をみたすかどうかは多くの関心を集めている問題だが、スライスランク法を用いるにしても何か新しい工夫が必要だろう。

4.2. **非自明解をどうとらえるか.** Tao の補題は「集合 $X$ と関数 $f$ が対角条件をみたせば $X$ のサイズは $f$ のスライスランクと一致する」ことを主張する。これが 3-AP を含まない集合 $X \subset \mathbb{F}_p^n$ にうまく適合する理由は、$x,y,z \in X$ に対して

$$x - 2y + z = 0 \quad \Longrightarrow \quad x = y = z$$

が成り立ち、$f : X^3 \to \mathbb{F}_p^n$ を

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

で定めると対角条件がみたされるからだ。この $X$ には方程式 $x - 2y + z = 0$ の非自明な解はない。ただしここで「自明な解」とは一点に縮退しているもの ($x = y = z$) のことである。

スライスランク法を別の（連立）方程式に適用しようとするとき、上記の意味の自明解の条件が一般には強すぎることが問題となる。例えば、任意の $x,y,z,w \in X$ に対して

$$x + y - z - w = 0 \quad \Longrightarrow \quad x = y = z = w \tag{6}$$

という条件を考えよう。もし $a,b \in X, a \neq b$ とすると

$$a + b - a - b = 0$$

なので条件に反する。つまり (6) をみたすなら $|X| \leq 1$ となってしまう。

そこで $X$ が $x + y - z - w = 0$ の「非自明解」を含まないとき、$|X|$ を評価するという問題が意味を持つには、「自明な解」の解釈を拡げる必要がある。代表的な二つの選択肢として、$x,y,z,w \in X$ ならば

$$x + y - z - w = 0 \quad \Longrightarrow \quad \{x,y\} = \{z,w\}$$

あるいは

$$x + y - z - w = 0 \quad \Longrightarrow \quad \#\{x,y,z,w\} < 4$$

が考えられる。前者の $X$ は weak Sidon set, 後者は Sidon set とよばれる。$X \subset [n]$ の場合には、Ruzsa[21] によって詳しく調べられており、前者でも後者でも $|X|$ の最大サイズは $\Theta(\sqrt{n})$ である。彼の議論は $X \subset \mathbb{F}_p^n$ の場合にも翻訳できて、同様の結果が得られる（スライスランク法は用いない）。最近、Sauermann は自明解の範囲を拡げる設定でスライスランク法を適用することに成功した。これについては次節で述べる。

## 5. スライスランク法の拡張

5.1. **Sauermann の結果.** $X \subset \mathbb{F}_p^n$ が任意の $x_1,x_2,\ldots,x_p \in X$ に対して

$$x_1 + x_2 + \cdots + x_p = 0 \quad \Longrightarrow \quad x_1 = x_2 = \cdots = x_p$$

をみたせば、スライスランク法により $|X|$ の非自明な上界を直ちに得られる。しかし条件を

$$x_1 + x_2 + \cdots + x_p = 0 \quad \Longrightarrow \quad \#\{x_1,x_2,\ldots,x_p\} < p$$

と変更すると、このままではTaoの補題の対角条件にうまく当てはまらず、スライスランク法を直接には適用できない。それにもかかわらず、Sauermannは適切な前処理を施した後にTaoの補題の‘multi-colored version’（例えば[14]のTheorem 1.2参照）を適用することでスライスランク法を拡張し、次の結果を得た。

**定理 4** (Sauermann [23])**.** $p$ を素数とし、$X \subset \mathbb{F}_p^n$ は方程式

$$x_1 + x_2 + \cdots + x_p = 0$$

の $p$ 個の相異なる根をもたないとする。このとき $n$ に依存しない定数 $C_p$ が存在して

$$|X| < C_p (2\sqrt{p})^n.$$

Mimura–Tokushige[15]ではSauermannのアイデアを連立方程式の非自明解をもたない集合に拡張した。その手法は連立方程式で定義されるいろいろな構造に適用可能であるが、例えば次のことがわかる。

**定理 5.** $p$ を素数とし、$A \subset \mathbb{F}_p^n$ が任意の $x,y,z,u,v \in A$ に対して

$$\begin{cases} x - y + z - u = 0 \\ x - 2z + v = 0 \end{cases} \quad \Longrightarrow \quad \#\{x,y,z,u,v\} < 5$$

をみたすとする。このとき、ある定数 $c < p$ が存在して $|A| < (cp)^n$ が成り立つ。

一方、このような $A$ でサイズが最大ならば、定数 $c' > 0$ に対して $|A| > (c'p)^n$ をみたす。

5.2. **ゼロサムの問題.** Sauermannの研究の動機は次の定理の拡張にある。

**定理 6** (Erdős–Ginzburg–Ziv[10])**.** $2n-1$ 項からなる整数列 $a_1, a_2, \ldots, a_{2n-1}$ の中からうまく $n$ 個を取り出すと、その和 $a_{i_1} + a_{i_2} + \cdots + a_{i_n}$ は $n$ の倍数である。

この定理は複数の証明が知られているが(例えば[1, 26]参照)そのひとつは多項式の手法によるもので次の定理を利用する。

**定理 7** (Chevally–Warning)**.** $j = 1,2,\ldots,n$ について $P_j(x_1,\ldots,x_m)$ は係数を $\mathbb{F}_p$ にもつ $m$ 変数、次数 $r_j$ の多項式で、$\sum_{j=1}^n r_j < m$ をみたす。このとき $P_1,\ldots,P_n$ の共通零点の個数 $N$ は $p$ の倍数である。特に、共通零点がひとつあれば、それ以外にもある。

Reiherは上の定理をうまく使ってErdős–Ginzburg–Zivの定理の2次元版を得た。

**定理 8** (Reiher[19])**.** どんな $4n-3$ 個の平面上の整数格子点に対しても、うまく $n$ 個を選ぶとその平均が整数格子点である。

ここで $s(\mathbb{F}_p^n)$ を次の性質をみたす最小の $s$ と定義する：

$\mathbb{F}_p^n$ の元からなるどんな $s$ 項列からもうまく $p$ 項を取り出してその和を0にできる。

$\mathbb{F}_p^n$ はproperty Dをみたすという予想があり、もし予想が正しければ

$$s(\mathbb{F}_p^n) \le (p-1)4^n + p$$

がスライスランク法からしたがう（例えば[16]を見よ）。しかしこのような付加的な仮定なしに得られた（現状での）最良の結果は次のもので、これは定理4の帰結である。

**定理 9** (Sauermann[23]). $p$ を 5 以上の素数とするとき、$n$ に依存しない定数 $C_p$ が存在して

$$s(\mathbb{F}_p^n) < (p-1)C_p(2\sqrt{p})^n + 1.$$

## 6. ランダムサンプリング法

定理 5 は [13] のアイデアを用いても証明できる。ここで連立方程式

$$\begin{cases} x-y+z-u=0 \\ x-2z+v=0 \end{cases}$$

をみたす異なる 5 点 $\{x,y,z,u,v\}$ からなる構造を W とよぶ。$A \subset \mathbb{F}_p^n$ が W を含まなければ、$|A|$ が小さいことを背理法で示そう。その概略は次の通りである。まず次のことを確かめる。

- $A$ が W を含まなければ $A$ 内の 3-AP の個数は少ない。（したがって $A$ から少数の点を削除して 3-AP がないようにできる。）
- もし $|A|$ が大きければ（背理法の仮定）、$A$ の部分集合 $C$ で 3-AP を含まないがサイズの大きいものがある。

しかしこれは次の定理に矛盾する。

**定理 10** (Ellenberg-Gijswijt[9]). $p$ を素数とし、$C \subset \mathbb{F}_p^n$ が 3-*AP* を含まないとする。このとき $|C| \leq \Lambda^n$ が成り立つ。ただし

$$\Lambda := \min_{0<t<1} t^{-\frac{p-1}{3}}(1+t+\cdots+t^{p-1})$$

とする。

単純な計算で $\Lambda < p$ がわかる。例えば、$p=3$ のとき $\Lambda \approx 2.76$ である。つまり上の定理は定理 1 を一般の素数 $p$ に拡張したものである。

定理 *5* の証明 *(Sauermann* による*).* $X \subset \mathbb{F}_p^n$ が W を含まないにもかかわらず

$$|A| \geq 2(\Lambda^{\frac{2}{3}}p^{\frac{1}{3}})^n$$

であると仮定し、矛盾をみちびく。

5-AP は W の一種だから、$A$ 内に 5-AP はない。

公差 $d \in \mathbb{F}_p^n$ の 3-AP が disjoint に二つ $A$ 内にあれば、例えば $\{x,y,z\}$, $\{x',y',z'\}$（異なる 6 点）とすると、$\{x,x',y,y',z\}$ は W となり矛盾。したがって $A$ 内に公差 $d$ の 3-AP は高々2 個しかなく、2 個あるのは 4-AP のときに限られる。

公差 $d$ の 3-AP と公差 $-d$ の 3-AP は同一視できるから、$A$ 内の 3-AP の可能な公差 $d \neq 0$ は高々 $\frac{p^n-1}{2} < \frac{1}{2}p^n$ 種類である。各 $d$ に対して、対応する $A$ 内の 3-AP は高々2 個しかないから、

$$\#(A \text{ 内の 3-AP}) < \frac{1}{2}p^n \cdot 2 = p^n.$$

$A$ の各点を確率 $q := \left(\frac{\Lambda}{p}\right)^{\frac{n}{3}}$ で一様ランダムに選び、$A$ の random subset $B$ をつくる。$X = |B|$ とおくと、

$$\mathbb{E}[X] = q|A| \geq \left(\frac{\Lambda}{p}\right)^{\frac{n}{3}} \cdot 2(\Lambda^{\frac{2}{3}} p^{\frac{1}{3}})^n = 2\Lambda^n.$$

ここで $Y = \#(B$ 内の 3-AP$)$ とおくと、

$$\mathbb{E}[Y] = \#(A \text{ 内の 3-AP}) \times q^3 < p^n \cdot q^3 = \Lambda^n.$$

したがって $\mathbb{E}[X - Y] > \Lambda^n$ である。つまり $A \setminus B$ に対応する $A$ の部分集合 $C$ が存在して、$C$ は 3-AP を含まないが $|C| > \Lambda^n$ である。これは定理 10 に矛盾する。 □

## References


[1] N. Alon, M. Dubiner. Zero-sum sets of prescribed size. Combinatorics, Paul Erdős is Eighty, Bolyai Society Mathematical Studies 1 (1993) 33–50.

[2] N. Alon, A. Shpilka, C. Umans. On sunflowers and matrix multiplication. Comput. Complexity 22 (2013), no. 2, 219–243.

[3] M. Bateman, N. Katz New bounds on cap sets. J. Amer. Math. Soc. 25 (2012): 585–613.

[4] F. Behrend. On sets of integers which contain no three terms in arithmetical progression. Proc. Nat. Acad. Sci. U. S. A., 32 (1946) 331–332.

[5] J. Blasiak, T. Church, H. Cohn, J. Grochow, E. Naslund, W. Sawin, C. Umans. On cap sets and the group-theoretic approach to matrix multiplication. Discrete Anal. 2017, Paper No. 3, 27 pp.

[6] T. Bloom, O. Sisask. Logarithmic bounds for Roth's theorem via almost-periodicity. Discrete Anal. 2019, Paper No. 4,

[7] E. Croot, V. F. Lev, P. P. Pach. Progression-free sets in n4 are exponentially small. Ann. of Math. (2) 185 (2017), no. 1, 331–337.

[8] Y. Edel. Extensions of generalized product caps. Designs, Codes and Cryptography 31 (2004) 5–14.

[9] J. S. Ellenberg, D. Gijswijt. On large subsets of $\mathbb{F}_q^n$ with no three-term arithmetic progression. Ann. of Math. (2) 185 (2017), no. 1, 339–343.

[10] P. Erdős, A. Ginzburg, A. Ziv. A theorem in additive number theory. Bull. Israel Research Council 10F (1961) 41–43.

[11] P. Erdős, E. Szemerédi. Combinatorial properties of systems of sets. J. Combinatorial Theory Ser. A 24 (1978), no. 3, 308–313.

[12] P. Erdős, P. Turán. On Some Sequences of Integers. J. London Math. Soc. 11 (1936) 261–264.

[13] J. Fox, L. Sauermann. Erdős–Ginzburg–Ziv constants by avoiding three-term arithmetic progressions. Electron. J. Combin. 25 (2018), no. 2, Paper 2.14, 9 pp.

[14] L.M. Lovász, L. Sauermann. A lower bound for the $k$-multicolored sum-free problem in $\mathbb{Z}_m^n$. arXiv:1804.08837.

[15] M. Mimura, N. Tokushige. Avoiding a shape, and the slice rank method for a system of equations. arXiv:1909.10509.

[16] E. Naslund. Exponential bounds for the Erdős–Ginzburg–Ziv constant. J. Combin. Theory Ser. A 174 (2020).

[17] E. Naslund. Monochromatic Equilateral Triangles in the Unit Distance Graph. arXiv:1909.09856.

[18] E. Naslund, W. Sawin. Upper bounds for sunflower-free sets. Forum Math. Sigma 5 (2017), e15, 10 pp.

[19] C. Reiher. On Kemnitz' conjecture concerning lattice-points in the plane. Ramanujan J. 13 (2007) 333–337.

[20] K. F. Roth. On certain sets of integers. J. London Math. Soc. 28, (1953) 104–109.

[21] I. Ruzsa. Solving a linear equation in a set of integers I. Acta Arithmetica, LXV.3, 1993, 259–282.

[22] A. Sagdeev. Improved Frankl–Rödl Theorem and Some of Its Geometric Consequences. Problems of Information Transmission 54 (2018) 139–164.

[23] L. Sauermann. On the size of subsets of $\mathbb{F}_p^n$ without $p$ distinct elements summing to zero. arXiv:1904.09560.

[24] T. Tao. A symmetric formulation of the Croot–Lev–Pach–Ellenberg–Gijswijt capset bound. blog post, 2016, http://terrytao.wordpress.com/2016/05/18/a.
[25] 徳重典英. 例から学ぶ極値組合せ論 東北大学集中講義 www.cc.u-ryukyu.ac.jp/〜hide/excomb2019.pdf
[26] 徳重典英. エレガントな解答をもとむ（解答）数学セミナー 2020 年 3 月号 84–87.

琉球大学教育学部 (COLLEGE OF EDUCATION, RYUKYU UNIVERSITY)
*E-mail address*: hide@edu.u-ryukyu.ac.jp