方程式の解に関する組合せ論の紹介

徳重 典英（琉球大学教育学部）

1　はじめに

指定された連立方程式の解を含まないような集合に関する組合せ論を紹介する。極値集合論の典型的な問題は、有限集合 Ω の部分集合 S が指定された構造 Q を含まないとき、S の最大サイズを問う。最大値を知ることが難しい場合は（たいてい難しい）S の最大値の $|\Omega| \to \infty$ における漸近的挙動を捉えようとする。

例えば $\Omega = [n] := \{1, 2, \ldots, n\}$ で、Q が 3-AP (3-term arithmetic progression) すなわち $\{x, x+d, x+2d\}$ の場合を考えよう。ただし公差 d は 0 でないとする。つまり $\{x, x, x\}$ は等差数列とはみなさない。Erdős と Turán [9] は次の問題を提起した。

問題 1　$S \subset [n]$ が 3-AP を含まないとき、$\max |S|$ は何か？

ここで 3-AP $\{x, y, z\}$ は一次方程式 $X - 2Y + Z = 0$ の解である。解 (x, x, x) を「自明な解」と呼べば、上の問題は「非自明な解を含まない集合 S はどれくらい大きくなれるか」というものだ。本稿では構造 Q が「（連立）一次方程式の非自明な解」で Ω が $[n]$ または $\mathbb{F}_p^n$ (p 元体上の n 次元ベクトル空間、p は奇素数) の場合を扱う。

問題 1 の最大値 $\max |S|$ を $r(n)$ と書こう。Behrend [1] は下界 $r(n) > ne^{-c/\sqrt{\log n}}$ をみたす S の構成法を与えた。Roth [19] は上界 $r(n) < cn/(\log\log n)$ を示した。その後、Heath-Brown, Szemerédi, Bourgain, Sanders などにより（主に上界の）評価が改善され、最近 Bloom と Sisask [2] は $r(n) < n/(\log n)^{1+c}$ を得た。もっと荒いレベルで見ると $r(n) = o(n)$ であるが、3-AP 以外にも同様の評価が得られるものがある。一般に加法の定義された集合 X において k-AP とは $x, x+d, \ldots, x+(k-1)d \in X$ であって $d \neq 0$ のものをいう。

定理 1（Szemerédi [24]） 任意の正整数 $k \geq 3$ に対して、$S \subset [n]$ が k-AP を含まないとき、$\max|S| = o(n)$ である。

この定理は等差数列の高次元版ともいえる組合せ直線の結果に拡張できる。ここで $x_1, x_2, \ldots, x_k \in [k]^n$ が組合せ直線であるとは、分割 $[n] = V \sqcup W$ と $y_v \in [k], v \in V$ が存在して、各 $x_i = (x_{i1}, x_{i2}, \ldots, x_{in})$ は $j \in V$ ならば $x_{ij} = y_j$, $j \in W$ ならば $x_{ij} = i$ となることをいう。例えば $\{(1,3,1,2,2),(2,3,2,2,2),(3,3,3,2,2)\}$ は $[3]^5$ の組合せ直線であり、この例では $V = \{2,4,5\}, W = \{1,3\}$ である。つまり V の座標の値は固定されていて、W の座標の値が順に増える。次の結果は Hales–Jewett の定理 [13] の密度版とよばれ、最初に Furstenberg と Katznelson [10] によってエルゴード理論を用いて証明され、その後 DHJ Polymath [17] によってずっと簡潔な組合せ論的な証明が与えられた。

定理 2（density HJ） $S \subset [k]^n$ が組合せ的直線を含まないとき、$\max|S| = o(k^n)$ である。

上の定理から次の結果がしたがう。すなわち、任意の正整数 $k \geq 3$ に対して、$S \subset \mathbb{F}_p^n$ が k-AP を含まないとき、$\max|S| = o(p^n)$ である。しかしこれは定理 1 の有限体版とはみなしにくい。もっと強い結果が期待できるかもしれないからだ。

問題 2 任意の正整数 $k \geq 3$ に対して、ある定数 $c = c(k) < 1$ が存在して、$S \subset \mathbb{F}_p^n$ が k-AP を含まないならば、$|S| < p^{cn}$ であるか？

この問題の答は $k = 3$ のとき肯定的であるが、$k \geq 4$ については未解決である。

定理 3（Ellenberg–Gijswijt [6]） $S \subset \mathbb{F}_p^n$ が 3-AP を含まなければ、$|S| < p^{cn}$ となる定数 $c = c(p) < 1$ がとれる。特に $p = 3$ のとき、$c = 0.924$ がとれる。

問題 3 $S \subset \mathbb{F}_p^n$ が 4-AP を含まなければ、$|S| < p^{cn}$ となる $c < 1$ がとれるか？

4-AP は連立方程式 $x_1 - 2x_2 + x_3 = 0, x_2 - 2x_3 + x_4 = 0$ の非自明な解である。一般

に k-AP は k 変数、$k-2$ 本の連立一次方程式の非自明な解である。

定理 1 は $\mathbb{N}$ の密な部分集合は任意の長さの等差数列を含むことを主張する。どの程度「密」なら大丈夫なのか。Erdős は逆数の和が発散する程度でよいか、と問う。

問題 4（Erdős） $S \subset \mathbb{N}$ が $\sum_{x \in S} \frac{1}{x} = \infty$ を満たせば、S は k-AP を含むか。

これは加法的数論の有名な未解決問題で、最近になってようやく $k=3$ の場合が Bloom と Sisask [2] によって肯定的に解決された。一方、逆数の和が発散する重要な例として素数の集合がある。

定理 4（Green–Tao [12]） 任意の正整数 $k \geq 3$ に対して、素数の集合は k-AP を含む。

この方向のさらなる一般化として「数体の素元星座定理」が東北大チーム（2020 年当時に東北大学に所属していた甲斐亘、見村万佐人、宗政昭弘、関真一朗、吉野聖人の五氏のこと）によって得られた [14]。また関氏は定理 4 の証明を自己完結的に再構成し、その成果が出版される。これは数論にかかわる正則化の手法について、その初歩から最先端までを学べる世界初の成書となろう。

本稿では次節以降、$[n]$ または $\mathbb{F}_p^n$ において指定された方程式の解を含まない集合のサイズを評価するいろいろな手法を紹介する。まず 2 節では $r(n)$ の上界を与える Ruzsa–Semerédi のアイデア（正則化の手法）と、$r(n)$ の下界を与える Behrend の構成法を紹介する。3 節ではスライスランクを導入し、定理 3 を証明する。また 3-AP 以外の問題にスライスランク法を適用するときに生じる問題点について説明する。さらに 4 節では Sidon 集合の大きさを sumset を利用して評価する Ruzsa のアイデアについて、最後の 5 節では $\mathbb{F}_p^n$ における非退化解を含まない集合のサイズに関する最近の結果を紹介する。

2　3-AP を含まない $[n]$ の部分集合

2.1　正則化手法による上界

X という世界で、与えられた性質をもつ Y を数えたい。これを次の 2 つのステップを通しておこなう。

1. X をランダムな X' で近似する。
2. ランダムな X' で Y を数える。

1. の X から X' を得ることを正則化という。2. の結果を利用して例えば除去補題などが得られ、そこから例えば Szemerédi の定理などがしたがう。

Szemerédi のグラフ正則化補題は、密なグラフを密なランダムグラフで近似する。その際、近似は例外部分を除いた範囲で、一定の精度のもとにおこなわれる。この例外部分の大きさと近似の精度は、パラメタ ϵ を用いて量的に明示される。ここでは定理の正確な statement を述べるかわりに、正則化で何が得られるかを説明する。まず、ごく小さい正数 ϵ が与えられると、そこから巨大な正整数 $T = T(\epsilon)$ が定まる。次に十分大きい $n \gg T$ をとる。任意[1] の n 頂点グラフ G をとり、これを正則化しよう。これは G の頂点集合 V の分割 $V = V_1 \sqcup V_2 \sqcup \cdots \sqcup V_t$ でよい性質をもつものを与えることである。ただし $t \leq T$ であり[2] 、簡単のため $|V_1| = \cdots = |V_t| = n/t$ であるとしよう。この頂点集合の分割が、G のランダムグラフへの近似を与える。その意味は次のとおりである。もし V_i と V_j の頂点のペアについて確率 p で一様独立に辺を与えるならば、$A \subset V_i$ と $B \subset V_j$ の間を結ぶ辺の本数（の期待値）は、$p|A||B|$ である。G はこのように作られたグラフではないが、G において実際に A と B の間を結ぶ辺の本数と $p|A||B|$ との誤差が（ϵ に応じて）小さい[3]というのである。このことを V_i, V_j 間は確率 p のランダムグラフで近似される、ということにしよう。同様に $V_{i'}, V_{j'}$ 間もランダムグラフで近似されるが、その確率 p' は先の p と異なってよい。このように、V_i たちのペアごとに辺の密度は異なってよいが、それぞれの密度でランダムグラフのように振る舞うのである。以上が G がランダムグラフで近似されるということの意味であるが、残念ながら $\binom{t}{2}$ 個ある V_i たちのペアが、すべてランダムグラフで近似できるとは

1） G に制限はないが、正則化補題が実質的な意味を持つのは G の辺数が n^2 オーダの密なグラフである。
2） n はいくらでも大きくとってよいが、T は n をとる前に確定した定数であることが重要である。
3） もちろん $|A| = |B| = 1$ のような場合は、G において A, B 間には辺があるかないか、つまり本数は 1 か 0 しかないので、p と近いとはいえない。そこで A, B はある程度の大きさをもつ部分集合でなければならないが、その大きさの程度も ϵ で記述される。

限らない。そこで少数の例外（その量も ϵ で定まる）ペアたちはランダムグラフで近似されないこと[4]も認める。まとめると、n 頂点グラフ G の正則化とは、頂点集合を $V = V_1 \sqcup \cdots \sqcup V_t$ のように等分して、少数の例外を除いて V_i, V_j 間がランダムグラフで近似される状態にすることである。このような頂点分割が可能であることを保証するのが Szemerédi 正則化補題である。ちなみに V_i たちの内部にも辺があるだろう。正則化補題の応用において、それら内部の辺たちは使用されない。

グラフ G が正則化されると、V_i たちのペアのほとんどがランダムグラフで近似される。例えば、V_1, V_2, V_3 の間が全部そうであるとして、V_i, V_j 間が確率 p_{ij} のランダムグラフとみなせるとしよう。このとき V_1, V_2, V_3 の中にある三角形（3 頂点完全グラフ K_3 のこと）の個数は $|V_1||V_2||V_3|p_{12}p_{23}p_{13} = (n/t)^3 p_{12}p_{23}p_{13}$ で近似され、誤差も ϵ を用いて評価できる。このように正則化はグラフの部分構造の数え上げを容易にする土台を与える。次の結果はこの仕組みを利用して得られる。これは三角形の除去補題の一種[5] である。

定理 5（Ruzsa–Szemerédi [21]）　n 点グラフのどの辺もちょうど一つの三角形に含まれるならば、辺の本数は $o(n^2)$ である[6]。

証明の概略　仮定をみたすグラフの辺数が cn^2 だったとしよう。このグラフには $cn^2/3$ 個の三角形がある。パラメタ ϵ を c に比べて十分小さくとり、このグラフを正則化して分割 $V = V_1 \sqcup \cdots \sqcup V_t$ を得る。V_i たちのうち、ランダムグラフで近似できないペア間の辺、辺の密度が低いペア間の辺、V_i 内部の辺をすべて除去する。定数をうまく選ぶことで、除去後のグラフにまだ $c'n^3$ 個の三角形が残ることがわかり、矛盾が生じる。 □

除去補題を用いて Roth の定理にグラフ理論的な証明を与えることができる。

4）　実際、どのように分割してもそのような例外が必要となる例がある。

5）　除去補題の原型というべきかもしれない。除去補題は通常、次の形の言明を指す。「任意の $\epsilon > 0$ に対して、ある $\delta > 0$ が存在して、n 頂点グラフ G が高々 δn^3 個の三角形を含めば、G から高々 ϵn^2 辺の除去で三角形のないグラフが得られる。」この言明は自然にハイパーグラフに拡張され、そこから Szemerédi の k-AP に関する定理が得られる。

6）　この結果は (6.3) 問題として知られる次の問題に $o(n^2)$ の上界を与える。$[n]$ の 3 点部分集合の集まり $\{T_1, T_2, \ldots, T_e\}$ $(T_i \in \binom{[n]}{3})$ において、3 個の T_i たちを含むような 6 点がないとき、e の最大値は何か。同様に、4 個の T_i たちを含むような 7 点がないときも $e = o(n^2)$ と予想されている ($(7,4)$ 予想) が、これは未解決である。

定理 6（Roth [19]）　$S \subset [n]$ が 3-AP を含まないとき、$\max |S| = o(n)$ である。

証明　3 部グラフ G の頂点集合を $\mathbb{Z}/(2n+1)\mathbb{Z}$ の 3 個のコピー $X \sqcup Y \sqcup Z$ とし、辺を

$$x \sim y \Leftrightarrow y - x \in S, \quad y \sim z \Leftrightarrow z - y \in S, \quad x \sim z \Leftrightarrow (z-x)/2 \in S$$

と定める。$y-x, (z-x)/2, z-y$ はこの順に 3-AP をなすか、そうでなければ三者はすべて等しい。S は 3-AP を含まないので、x, y, z が G において三角形をなすことと $y - x = (z-x)/2 = z - y$ は同値である。G において $x \sim y$ ならば $s := y - x \in S$ であるが、このとき $z := y + s$ と定めると $y \sim z$, $x \sim z$ である。つまり辺 xy を含む三角形 xyz が一意に定まる。よって G の各辺はちょうど 1 個の三角形に含まれるから、G の頂点数を N とすると定理 5 により辺数は $o(N^2)$ である。一方、$N = 3(2n+1)$ と辺数が $3N|S|$ であることから $|S| = o(n)$ がしたがう。 □

2.2　Behrend による下界の構成

ユークリッド空間の球面上の格子点は 3-AP を含まない。これをうまく $\mathbb{Z}$ にうつすことで 3-AP を含まない $\mathbb{Z}$ の部分集合を構成しよう。

定理 7（Behrend [1]）　十分大きい n に対して 3-AP を含まない $S \subset [n]$ で $|S| > n/11^{\sqrt{\log n}}$ のものを構成できる。

証明　一辺の長さが k の d 次元立方体の格子点の集合 $\{0, 1, \dots, k-1\}^d$ には k^d 個の点がある。これらを $d(k-1)^2 + 1$ 組に分割する。すなわち、球面

$$x_1^2 + \cdots + x_d^2 = t, \quad t = 0, 1, \dots, d(k-1)^2$$

を考え、立方体の格子点を対応する球面の t の値で分割する。鳩の巣原理からある球面上に $k^d/(dk^2)$ より多くの格子点があり、その集合を A とおく。A は球面上の集合であるから 3-AP を含まない。

写像 $f : A \to \mathbb{Z}$ を

$$f(x_1, \dots, x_d) := x_1 + x_2(2k) + x_3(2k)^2 + \cdots + x_d(2k)^{d-1}$$

と定める。つまり A の点の各成分を $2k$ 進数表記[7] の対応する桁の数字と考える。この写像[8] は単射で $f(a+b)=f(a)+f(b)$ をみたす。特に $x,y,z\in A$ に対して $x+z=2y$ と $f(x)+f(z)=2f(y)$ は同値であり、A に 3-AP がないことから $f(A)$ にも 3-AP はない。

ここで $\max_{a\in A} f(a)\le f(k-1,\dots,k-1)<(2k)^d$ に注意して $n:=(2k)^d$ とおくと $f(A)\subset[n]$ であり、さらに A の選び方から $|f(A)|=|A|>k^d/(dk^2)$ である。そこで $S:=f(A)$ が目標の評価をみたすことを確かめよう。$d\sim c\sqrt{\log n}$ とおくと

$$|S|>\frac{k^d}{dk^2}=\frac{n}{(2^c e^{2/c})^{\sqrt{\log n}}\,\frac{c}{4}\sqrt{\log n}}$$

であり、$2^c e^{2/c}$ が最小になるように c を決めると $c=\sqrt{2/\log 2}\approx 1.7$, このとき $2^c e^{2/c}\approx 10.5$ だから、n が十分大きければ $|S|>n/11^{\sqrt{\log n}}$ がしたがう。 $\square$

3　スライスランク法

3.1　3-AP を含まない $\mathbb{F}_p^n$ の部分集合の上界

対角成分がすべて非零の対角行列は full rank をもつ。この行列の添字集合が X で、成分が体 $\mathbb{F}$ の要素ならば、この行列に対応する関数 $f:X^2\to\mathbb{F}$ を

$$f(x,y)\neq 0 \iff x=y$$

と定め、その rank を $|X|$ と定義するのは妥当と思われる。これをふまえてスライスランクを導入しよう。

有限集合 X と体 $\mathbb{F}$ が与えられたとき、$f:X^3\to\mathbb{F}$ がスライス関数であるとは、$f(x,y,z)$ が

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

の形に表示できる[9] ことをいう。f のスライスランク $\mathrm{sr}(f)$ とは、f をスライス関数の

7） base を $2k$ にするのは 2 数の足し算で wraparound を避けるため。

8） Frieman 2-isomorphism

9） よくある設定は X が $\mathbb{F}$ 上の n 次元ベクトル空間の場合で、このとき $a(x)$ は n 変数の関数 $a(x_1,\dots,x_n)$ である。

和に書いたとき、必要なスライス関数の個数の最小値である。次の結果はスライスランクを利用する際の基本となる。

補題 1（Tao [25]） $f : X^3 \to \mathbb{F}$ が「対角条件」すなわち

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

をみたせば、$\mathrm{sr}(f) = |X|$ である[10]。

上の補題は Tao のブログ[11]にある。彼の動機は、次の定理の証明、およびそのアイデアの元となった Croot, Lev, Pach [3] の証明をより対称的な形に定式化することだった。

定理 8（Ellenberg–Gijswijt [6]） $X \subset \mathbb{F}_3^n$ が 3-AP を含まなければ、$|X| \leq 3\lambda^n$ である[12]。すなわち $r(n) \leq 3\lambda^n$, ただし $\lambda = \frac{3}{8}(33\sqrt{33} + 207)^{\frac{1}{3}} < 2.76$ である。

証明 対角条件をみたす $f : X^3 \to \mathbb{F}_3$ で $\mathrm{sr}(f) < 3\lambda^n$ のものを見つければよい。実際

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

がそれらをみたす。まず X が 3-AP を含まないことから対角条件の成立を確認できる。

スライスランクの評価には少し計算が必要となる。上記 f の右辺を展開して単項式の和に書いたとき、各単項式の次数は高々 $2n$ であり、例えば x に関する次数 ($x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$ としたときの $i_1 + \cdots + i_n$) は平均して $2n/3$ 以下である。そこで f の単項式で x に関する次数が $2n/3$ 以下のものの和を f_x, 残りの単項式のうち y に関する次数が $2n/3$ 以下のものの和を f_y, 最後に残った単項式（必然的に z に関する次数が $2n/3$ 以下）の和を f_z として $f = f_x + f_y + f_z$ と表せる。一般性を失わず $\mathrm{sr}(f) \leq 3\,\mathrm{sr}(f_x)$ として

10） この補題は定義域を X^k に一般化しても同様に成り立ち、それを k に関する帰納法で（線形代数で）確認できる。

11） この時点では、スライス関数は rank one function とよばれている。

12） $|X| \leq 3\lambda^n$ が示せると、係数の 3 は 1 に落とせる。実際、$X \subset \mathbb{F}_3^n$ が 3-AP を含まなければ、任意の正整数 m に対して $X^m \subset (\mathbb{F}_p^n)^m = \mathbb{F}_p^{mn}$ も 3-AP を含まない。したがって $|X^m| \leq 3\lambda^{mn}$, つまり $|X| \leq 3^{1/m}\lambda^n$. ここで $m \to \infty$ として $|X| \leq \lambda^n$ を得る。この議論を power trick という。

よいから、$\mathrm{sr}(f_x) \le \lambda^n$ を示したい。このため f_x を x の多項式と見て、x の単項式が何種類現れるか数えよう。つまり集合 $I := \{(i_1,\dots,i_n) \in \{0,1,2\}^n : i_1+\cdots+i_n \le 2n/3\}$ のサイズを上から評価する。ここで $i_1,\dots,i_n$ を $\{0,1,2\}$ に値を一様独立にとる確率変数だと考え、$0<t<1$ を固定してマルコフの不等式を使うと

$$\mathbb{P}[i_1+\cdots+i_n \le \tfrac{2n}{3}] = \mathbb{P}[t^{i_1+\cdots+i_n} \le t^{\frac{2n}{3}}] \le \frac{\mathbb{E}[t^{i_1+\cdots+i_n}]}{t^{\frac{2n}{3}}}$$

である。これと

$$\mathbb{E}[t^{i_1+\cdots+i_n}] = \mathbb{E}[t^{i_1}]\cdots\mathbb{E}[t^{i_n}] = \left(\frac{1+t+t^2}{3}\right)^n$$

から

$$\mathbb{P}[i_1+\cdots+i_n \le \tfrac{2n}{3}] \le \left(\frac{1+t+t^2}{t^{\frac{2}{3}}}\right)^n \frac{1}{3^n} \tag{2}$$

を得る。右辺が最小となるように $t=\frac{1}{8}(\sqrt{33}-1)$ を選ぶと、右辺は $\frac{\lambda^n}{3^n}$ となり、$\mathrm{sr}(f_r) \le |I| \le \lambda^n$ がわかった。 $\square$

Edel [5] は 3-AP を含まない $\mathbb{F}_3^n$ の大きな部分集合を構成し、$r(n) > 2.2^n$ を示した。

3.2 スライスランク法の欠点

以下、扱う方程式は係数の和が 0 のものに限る。

S が 3-AP を含まないことと、S が $x-2y+z=0$ の非自明な解を含まないことは同値であった。ここで自明な解とは (x,x,x), いわゆる singleton solution のことであり、自明でない解は 3 個の異なる値をとる。一般に、与えられた方程式の非自明解を含まない集合 S について問題にするとき、自明な解を慎重に定義する必要がある。例えば、方程式が

$$x_1 - x_2 - x_3 + x_4 = 0 \tag{3}$$

の場合を考えよう。もし自明な解を (x,x,x,x) に限ると、$|S| \le 1$ でなければならない。なぜなら任意の $x \ne y$ について (x,x,y,y) が非自明な解になってしまうからだ。これではつまらないので、この方程式については (x,x,y,y) と (x,y,x,y) も自明な解と考えたい。この意味での非自明解を含まない集合 S は Sidon 集合という。残念ながらこの設定は対角条件と相性が悪く、直接にはスライスランク法を適用できない。

さらに応用上は方程式 (3) の非自明な解の範囲をもっと制限して、4 個の異なる値をもつ (x_1, x_2, x_3, x_4) としたいこともある。このような解を非退化解と呼ぼう。例えば $(1,1,2,2)$ は自明な解、$(1,2,2,3)$ は非自明だが退化した解、$(1,2,3,4)$ は非退化解である。もちろんスライスランク法は非退化解を含まない集合の評価には（直接には）使えない。

自明な解を singleton solution に限っても、連立方程式にスライスランク法を適用するには制約がある。S が 4-AP を含まないことは、S が 4 変数、2 本の連立方程式

$$x_1 - 2x_2 + x_3 = 0, \quad x_2 - 2x_3 + x_4 = 0$$

の singleton solution を含まないことと同値である。実はスライスランク法を k 変数、m 本の連立方程式に適用したとき、singleton solution を含まない集合 $S \subset \mathbb{F}_p^n$ のサイズについて意味のある評価が得られるのは

$$k \geq 2m + 1 \tag{4}$$

のときである[13)]。4-AP の問題にスライスランク法を（普通に）適用しても $|S| \leq p^n$ のような自明な評価しか得られない。

スライスランク法を直接適用して有効な結果が得られるのは (i) 除外する解が singleton solution のみで、かつ (ii) 変数の個数 k と方程式の個数 m が条件 (4) をみたすときである。今までに (i) の制限を緩める工夫がいくつか見つかっているが、(ii) の制限を突破する方法はわかっていない。

13） 3-AP の問題でスライスランクを適用する関数 f は (1) で定義された。同様に (7) で定義される k 変数、m 本の連立方程式を $\mathbb{F}_p^n$ で扱う場合は

$$f(x^{(1)}, \ldots, x^{(k)}) = \prod_{j=1}^{m} \prod_{i=1}^{n} \left((a_{j1} x_i^{(1)} + a_{j2} x_i^{(2)} + \cdots + a_{jk} x_i^{(k)})^{p-1} - 1 \right)$$

にスライスランク法を適用するのが自然である。このとき意味のある上限が得られるためには

$$\frac{1 + t + \cdots + t^{p-1}}{t^{(p-1)m/k}}$$

の最小値が p より小さくなければならない（これの $p = k = 3,\ m = 1$ の場合が (2) に相当)。この条件が $k \geq 2m + 1$ である。

4 Sidon 集合

方程式 $x_1 - x_2 - x_3 + x_4 = 0$ の自明な解とは (x, x, y, y) または (x, y, x, y) であり、非退化な解とは 4 個の異なる値をとる解のことであった。この方程式の非自明な解を含まない集合を Sidon 集合、非退化な解を含まない集合を弱 Sidon 集合とよぶ。Sidon 集合における 2 数の和は ($x + y = y + x$ を除いて) すべて異なる。$[n]$ における Sidon 集合、弱 Sidon 集合の最大サイズをそれぞれ $r(n), R(n)$ と書こう。Sidon 集合は弱 Sidon 集合でもあるから $r(n) \le R(n)$ である。Ruzsa は [20] において

$$r(n) \le n^{\frac{1}{2}} + n^{\frac{1}{4}} + 1, \quad R(n) \le n^{\frac{1}{2}} + 4n^{\frac{1}{4}} + 11$$

を示した[14)]。さらに無限に多くの n に対して $r(n) \ge n^{\frac{1}{2}}$ も示した。

同様の評価は $\mathbb{F}_p^n$ における Sidon 集合、弱 Sidon 集合でも得られる (cf. [15])。対応する最大サイズをそれぞれ $r_p(n), R_p(n)$ と書くと、$r_p(2n) \ge p^n$,

$$r_p(n) < p^{\frac{n}{2}} + \tfrac{1}{2}, \quad R_p(n) < p^{\frac{n}{2}} + \tfrac{3}{2} + O(p^{-\frac{n}{2}})$$

が成り立つ。ただし $p \ge 5$ とする。上界はスライスランク法ではなく、Ruzsa による sumset の評価を用いる。

定理 9（Ruzsa [20]） G をアーベル群とし、G の非空の部分集合 A, B に対して $A + B := \{a + b : a \in A, b \in B\}$ とおく。このとき A が弱 Sidon 集合ならば、$|A + B| \ge \frac{|A|^2|B|}{3|A|+|B|-1}$ である。

証明 $u \in G$ に対して $\sigma(u) := \#\{(a, b) \in A \times B : u = a + b\}$ とおく。$\sum \sigma(u)^2$ を二通りに評価しよう。まず、下界を得るために

$$\sum_{u \in G} \sigma(u) = \sum_{u \in A+B} \sigma(u) = |A||B|$$

14) Ruzsa は [20] で一般に一次方程式の自明な解を含まない $[n]$ の部分集合を研究し、特に変数が 4 個の場合については詳細な結果を得ている。

に注意して、$\sigma(u)$ たちの「2 乗の平均」と「平均の 2 乗」を比べると

$$\sum_{u\in G}\sigma^2(u)=\sum_{u\in A+B}\sigma^2(u)\geq\frac{1}{|A+B|}\left(\sum_{u\in A+B}\sigma(u)\right)^2=\frac{|A|^2\,|B|^2}{|A+B|} \tag{5}$$

を得る。次に上界として

$$\sum_{u\in G}\sigma^2(u)\leq|B|\,(|B|-1)+3|A|\,|B| \tag{6}$$

を示そう。これがいえると (5) と (6) から $|A+B|$ に関する目標の不等式を得る。

(6) を示すため、$u\in G$ に対して $\delta(u):=\{(x,y)\in A^2:u=x-y\}$ とおく。$\delta(0)=|A|$ であるが、$u\neq 0$ ならば $\delta(u)\leq 2$ である。これを確かめるため、$u\neq 0$ に対して $\delta(u)\geq 2$ であるとしよう。このとき $u=w-a$, $(w,a)\in A^2$ なる解と、これとは異なる解 $u=x-y$, $(x,y)\in A^2$ がある。もし w,a,x,y が異なる 4 点であれば、これらは $x_1-x_2-x_3+x_4=0$ の非退化解となり、A が弱 Sidon 集合であることに反する。したがって w,a,x,y は高々 3 点で、$y=w$ または $x=a$ であるが、両者が同時に起こると $u=x-y=a-w=-u$ となって $u\neq 0$ に反する。つまり $y=w$ と $x=a$ の片方だけが成り立つ。以上で $\delta(u)\geq 2$ ならば実は $\delta(u)=2$ であり、このとき公差 d の 3-AP がただひとつ ($\{x,y=w,a\}$ または $\{w,a=x,y\}$ のどちらか片方) 定まることがわかった。この 3-AP の中間項を $m(u)$ とおく。$m(u)=m(-u)$ であるが、$v\neq\pm u$ ならば $m(u)\neq m(v)$ である[15)]。これは $U:=\{u\in G:\delta(u)=2\}$ から $A':=\{m(u)\in A:u\in U\}$ への $2:1$ の対応を与えるので $|U|=2|A'|\leq 2|A|$ である。

さて

$$\begin{aligned}\sum_{u\in G}\sigma(u)^2&=\sum_{u\in G}\#\{(a,b)\in A\times B:u=a+b\}\times\#\{(a',b')\in A\times B:u=a'+b'\}\\&=\sum_{u\in G}\#\{(a,a',b,b')\in A^2\times B^2:u=a+b=a'+b'\}\\&=\sum_{v\in G}\#\{(a,a',c,c')\in A^2\times B^2:v=a-a'=c-c'\}\end{aligned}$$

であるが、右辺最後の和を $v=0$ に対応する和 s_1 と、$v\neq 0$ に対応する和 s_2 に分けよう。$v=0$ のとき、そのような 4 つ組 (a,a,c,c) の個数は $s_1=|A||B|$ である。次

15) もし $m(u)=m(v)$ なら、ふたつの 3-AP $\{m-u,m,m+u\}$ と $\{m-v,m,m+v\}$ から非退化解 $(m-u)-(m+v)-(m-v)+(m+u)=0$ が生じる。

に $v \neq 0$ のとき、$v = c - c'$ となる $(c, c') \in B^2$ をひとつ固定すると、これに対応する $(a, a') \in A^2$ で $v = a - a'$ となるものは高々 2 つである。そこで $i = 1, 2$ に対して $B_i^2 := \{(c, c') \in B^2 : \delta(c - c') = i\}$ とおくと、

$$
\begin{aligned}
|B_1^2| + |B_2^2| &\leq |B^2| - \#\{(b, b) : b \in B\} = |B|(|B| - 1), \\
|B_2^2| &= \sum_{c - c' \in U} 1 \leq |U||B| \leq 2|A||B|
\end{aligned}
$$

である。よって数えるべき 4 つ組 (a, a', c, c') の総数は、

$$
s_2 \leq |B_1^2| + 2|B_2^2| \leq (|B_1^2| + |B_2^2|) + |B_2^2| \leq |B|(|B| - 1) + 2|A||B|
$$

である。以上により、$\sum_{u \in G} \sigma(u)^2 \leq s_1 + s_2$ から (6) を得る。 □

定理 9 を $B = \mathbb{F}_p^n$ に適用すると、$|A + B| = p^n$ より $|A| \leq \frac{1}{2}(\sqrt{4p^n + t} + 3)$ を得る。ここから $R_p(n) < p^{\frac{n}{2}} + \frac{3}{2} + O(p^{-\frac{n}{2}})$ がしたがう。

5 $\mathbb{F}_p^n$ で非退化解を持たない集合

与えられた（連立）方程式の非退化解を含まない集合 S については、スライスランク法を直接には適用できない。しかし方程式によっては適切な前処理と Tao の補題の「多色版」によって S の上界が得られることもある。この種の最初の結果は次のものである。

定理 10（Sauermann [22]） 素数 $p \geq 5$ を固定し、$S \subset \mathbb{F}_p^n$ が $x_1 + x_2 + \cdots + x_p = 0$ の非退化解を含まなければ、$|S| < C_p\,(2\sqrt{p})^n$ である。

下界として $|S| \geq 2^n$ は容易に得られる。実際、$S = \{0, 1\}^n$ は $x_1 + x_2 + \cdots + x_p = 0$ の非退化解を含まない。Elsholts [7] は $|S| > (\sqrt[3]{9})^n \approx 2.08^n$ をみたす S を構成した。一方、定理 10 で非退化解を singleton solution でない解に置き換えると、スライスランク法の直接の適用により $|S| \leq 4^n$ がわかる。

問題 5 絶対定数 c が存在して、定理 10 の S は $|S| < c^n$ をみたすか？

定理 10 は Erdős–Ginzberg–Ziv 定数 [8][16] に応用がある。ここで $s(\mathbb{F}_p^n)$ を、$\mathbb{F}_p^n$ の要素からなるどんな s 項の列からもうまく p 項を選ぶとその和が 0 となるような最小の s と定めよう。この性質を持たない列には、同一要素は高々 $p-1$ 回しか現れない。そこで $(p-1)\,C_p\,(2\sqrt{p})^n+1$ 個の項からなる列で、どの p 項の和も 0 でないものがあったとしよう。このときどの要素も高々 $p-1$ 回しか現れないから、少なくとも $C_p\,(2\sqrt{p})^n+1$ 個の異なる要素がある。しかしこれは定理 10 に矛盾する。つまり次を得た。

定理 11（Sauermann [22]） $s(\mathbb{F}_p^n)<(p-1)\,C_p\,(2\sqrt{p})^n+1.$

$s(\mathbb{F}_p^n)-1$ 項からなる $\mathbb{F}_p^n$ の列が、どの p 項の和も非零であるならば、その列に現れるどの要素もちょうど $p-1$ 回現れる[17] ことを仮定すれば、$s(\mathbb{F}_p^n)\le(p-1)4^n+1$ がしたがう (Naslund [16])。

次の結果は Sauermann の手法を拡張する試みから得られたものだが、その後 random sampling を用いて簡単に示せることがわかった。

定理 12（Mimura-T [15]） $S\subset\mathbb{F}_p^n$ が連立方程式 (W)

$$x_1-x_2-x_3+x_4=0,$$
$$x_2-x_3-x_4+x_5=0$$

の非退化解（5 個の異なる値をとる解）を含まないならば、$|S|<2(\lambda^{2/3}p^{1/3})^n$ である。ただし λ は定理 3 の c を用いて $\lambda:=p^c$ と定義される。

証明 背理法で示すため、S は (W) の非退化解を含まないが $|S|\ge2(\lambda^{2/3}p^{1/3})^n$ であると仮定する。S 内の 3-AP の個数を評価しよう。同じ公差の 3-AP が disjoint に 2 つあるとそこに (W) が生じる。また 5-AP は (W) の非退化解である。したがって S 内に同じ公差の 3-AP は高々 2 個[18] である。また $\mathbb{F}_p^n$ における 3-AP の公差の種類は

16） [8] の結果は $s(\mathbb{Z}/n\mathbb{Z})=2n-1$, すなわち、$2n-1$ 項の $\mathbb{Z}/n\mathbb{Z}$ の列からうまく n 項を選ぶと、その和が 0 となる。Reiher [18] はその 2 次元版 $s((\mathbb{Z}/n\mathbb{Z})^2)=4n-3$ を示した。つまり、$4n-3$ 個の平面上の整数格子点からうまく n 個を選ぶと、その平均が整数格子点となる。

17） このとき $\mathbb{F}_p^n$ は property D をもつという。$\mathbb{F}_p^n$ が property D をもつかどうかわかっていない。

18） S 内に 3-AP が 2 個あるときは、2 点を共有して 4-AP を生じる。

$\frac{p^n-1}{2} < \frac{p^n}{2}$ である[19)]。以上から $\#\{\text{3-APs in } S\} < p^n$ である。

S の各点を一様独立に確率 $u := (\lambda/p)^{\frac{n}{3}}$ で選び、random subset $T \subset S$ をつくる。確率変数 X を $X = |T|$ と定義すると

$$\mathbb{E}[X] = |S| \cdot u \geq 2(\lambda^{2/3}p^{1/3})^n \cdot (\lambda/p)^{\frac{n}{3}} = 2\lambda^n$$

である。次に確率変数 Y を $Y = \#\{\text{3-APs in } T\}$ と定義すると、

$$\mathbb{E}[Y] = \#(\text{3-APs in } S) \cdot u^3 < p^n \cdot (\lambda/p)^n = \lambda^n$$

である。したがって $\mathbb{E}[X - Y] > \lambda^n$ を得るが、これは T から Y 点除去して 3-AP がないようにしても、まだ λ^n より多くの点が残ることを意味する。しかし定理 3 から 3-AP を含まない集合のサイズは λ^n より小さいから、矛盾が生じた。 □

[15] ではその他のいくつかの連立方程式についても、非退化解を含まない集合 S が定数 $c < 1$ に対して $|S| < p^{cn}$ をみたすことを示した。では、どんな連立方程式がこの性質をもつだろうか？ この問題を定式化するため、k 個の変数からなる m 本の連立方程式 (7) を考える。

$$\begin{aligned} a_{11}x_1 + \cdots + a_{1k}x_k &= 0, \\ \cdots\cdots \\ a_{m1}x_1 + \cdots + a_{mk}x_k &= 0. \end{aligned} \tag{7}$$

ただし次のことを仮定する。

(仮定 1) 係数 a_{ij} は $\mathbb{F}_p$ から、変数 x_i は $\mathbb{F}_p^n$ からとり、その個数は $k \geq 2m+1$ をみたす。
(仮定 2) $m \times k$ の係数行列 $A = (a_{ij})$ は full rank, つまり $\operatorname{rank} A = m$ である。
(仮定 3) 方程式の係数和は 0, つまり任意の $1 \leq i \leq m$ に対して $a_{i1} + a_{i2} + \cdots + a_{ik} = 0$.
(仮定 4) (7) の線形結合に $x_j - x'_j = 0$ は現れない。

k 変数 m 本の連立方程式 (7) に対して、定数 $c < 1$ が存在して非退化解をもたない $S \subset \mathbb{F}_p^n$ が必ず $|S| < p^{cn}$ をみたすとき、方程式 (7) は moderate であるという。例えば 3-AP を定める方程式 $x - 2y + z = 0$ や定理 12 の方程式 (W) は moderate である。

19) 公差は零ベクトルでない。また $z = x + 2d$ のとき、$\{x, x+d, x+2d\}$ と $\{z, z-d, z-2d\}$ は同じ 3-AP を与えるから、この意味で公差 d と $-d$ を同一視できる。

定理 13（Sauermann [23]） $k \geq 3m$ で、A の $m \times m$ の小行列がすべて正則ならば、(7) は moderate である。

上の定理とは対照的に、A が線形従属な列ベクトルのペアをたくさん持つ場合も対応する方程式は moderate である。これを正確に述べるため、係数行列の 2 つの列に対して、片方が他方のスカラー倍であるとき同値であると定義して、列ベクトルを同値類に分割する。同値類のサイズとはその同値類に属する列ベクトルの個数である。零和の同値類とは、その同値類に属する列ベクトルの和が零ベクトルとなることである。

定理 14（van Dobben de Bruyn–Gijswijt [4]） 方程式 (7) の係数行列は、サイズが 1 の同値類を高々 1 個もつとする。このとき、サイズ 2 の零和の同値類がないか、またはすべての同値類が零和であるならば、(7) は moderate である。

方程式 (W) の係数行列 A= $\begin{pmatrix} 1 & -1 & -1 & 1 & 0 \\ 0 & 1 & -1 & -1 & 1 \end{pmatrix}$ の 2 列目、4 列目からなる小行列は正則でないから、定理 13 は適用できない。またこの行列のサイズ 1 の同値類は 3 個ある[20]ため、定理 14 も適用できない。

Gijswijt は非退化解の範囲を制限して、generic な解を定義した。すなわち、連立方程式 (7) の解 $(y_1, \ldots, y_k)$ が generic であるとは、$\sum \mu_i y_i = 0$ かつ $\sum \mu_i = 0$ ならば、$\sum \mu_i x_i = 0$ は (7) の線形結合から得られることをいう。例えば $x_1 - x_2 + x_3 - x_4 = 0$ を $\mathbb{F}_p^2$ $(p \geq 5)$ で考えよう。このとき $(\binom{0}{0}, \binom{1}{0}, \binom{3}{0}, \binom{2}{0})$ は非退化な解だが $x_2 + x_3 - 2x_4 = 0$ をみたし generic な解ではない。一方、$(\binom{0}{0}, \binom{1}{0}, \binom{1}{1}, \binom{0}{1})$ は generic な解である。

方程式 (7) の generic な解をもたない $S \subset \mathbb{F}_p^n$ は必ず $|S| < p^{cn}$ $(c < 1)$ をみたすとき、方程式 (7) は temperate であるという。generic な解は非退化な解なので[21]、(7) が temperate なら moderate である。連立方程式 (7) が tame とは、(7) から得られる m' 個の独立な方程式に $2m' + 1$ 個以上の変数が含まれることをいう。すなわち、(7) の係数行列 $A \in \mathbb{F}_p^{m \times k}$ に行の基本変形と列の交換を施して、$\begin{pmatrix} A' & 0 \\ B & C \end{pmatrix}$ の形で $A' \in \mathbb{F}_p^{m' \times k'}$, $k' \leq 2m'$ をみたすものが得られないことである。定理 12 の (W) および定理 13、定理 14 の (7) はすべて temperate である。したがってこれらの結果はすべて次の定理から

20） 列ベクトルの同値類への分割は $[5] = \{1\} \sqcup \{2, 4\} \sqcup \{3\} \sqcup \{5\}$.

21） 退化解は例えば $x_j - x_{j'} = 0$ をみたすが、これは (仮定 4) により (7) の線形結合からは得られないので generic な解ではない。

したがう[22)]。

定理 15（Gijswijt [11]） (7) が tame ならば、temperate である。さらにこのとき、ある $\delta, c > 0$ が存在して、任意の $\delta' < \delta$ に対して、$S \subset \mathbb{F}_p^n$ が $|S| > p^{(1-\delta')n}$ をみたせば、S には $\Omega(p^{(k-m-c\delta')n})$ 個の解がある[23)]。

問題 6（Gijswijt [11]） (7) は tame でなくても (さらに (仮定 1) の $k \geq 2m+1$ をみたさなくても) temperate か？[24)]

6 文献案内

正則化の手法やスライスランク法なども含む極値組合せ論の入門書としては Yufei Zhao の本 [27] がおすすめ[25)]です。日本語で読みたい人は [28, 29] もどうぞ。加法的数論の幅広い内容を詳しく扱ったものとしては Tao と Vu の本 [26] があります。ガチ勢はこれから出版される関真一朗氏[26)]の本を読みましょう。

参考文献

[1] 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.

[2] T. F. Bloom, O. Sisask. Breaking the logarithmic barrier in Roth's theorem on arithmetic progressions. arXiv:2007.03528

[3] E. Croot, V. F. Lev, P. P. Pach. Progression-free sets in $\mathbb{Z}_n^4$ are exponentially small. Ann. of Math. (2) 185 (2017), no. 1, 331–337.

22) しかしそれぞれの定理の与える上限 $|S| < p^{cn}$ の c の値は、定理 14 の方がずっと悪いかもしれない。

23) この現象を super saturation という。つまり $0 < c < c' < 1$ が存在して、$|S| \leq p^{cn}$ なら S が generic な解を含まないことがあるが、$|S| > p^{c'n}$ なら S は必ず generic な解をたくさん含む。

24) $p = 2, 3$ のとき、つまり $\mathbb{F}_2^n, \mathbb{F}_3^n$ において (7) は temperate である [11]。

25) You Tube の講義もおすすめ。

26) 朝倉数学ライブラリー『グリーン・タオの定理』関真一朗（著）朝倉書店、2023 年 1 月発売予定。

[4] J. van Dobben de Bruyn, D. Gijswijt. On the size of subsets of $\mathbb{F}_q^n$ avoiding solutions to linear systems with repeated columns. arXiv:2111.09879

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

[6] 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.

[7] C. Elsholtz. Lower bounds for multidimensional zero sums. Combinatorica 24 (2004), no. 3, 351–358.

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

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

[10] H. Furstenberg, Y. Katznelson. A density version of the Hales–Jewett theorem. J. Anal. Math. 57 (1991), 64–119.

[11] D. Gijswijt. Excluding affine configurations over a finite field. arXiv:2112.12620

[12] B. Green, T. Tao. The primes contain arbitrarily long arithmetic progressions. Ann. of Math. (2) 167 (2008), no. 2, 481–547.

[13] A. W. Hales, R. I. Jewett. Regularity and positional games. Trans. Amer. Math. Soc. 106 (1963), 222–229.

[14] W. Kai, M. Mimura, A. Munemasa, S. Seki, K. Yoshino. Constellations in prime elements of number fields. arXiv:2012.15669

[15] M. Mimura, N. Tokushige. Solving linear equations in a vector space over a finite field. Discrete Math. 344 (2021), no. 12, Paper No. 112603, 11 pp.

[16] E. Naslund. Exponential bounds for the Erdős–Ginzburg–Ziv constant. J. Combin. Theory Ser. A 174 (2020) 105185, 19 pp.

[17] D. H. J. Polymath. A new proof of the density Hales–Jewett theorem. Ann. of Math. (2) 175 (2012), no. 3, 1283–1327.

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

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

[20] I. Z. Ruzsa. Solving a linear equation in a set of integers I. Acta Arithmetica,

LXV.3, 1993, 259–282.

[21] I. Z. Ruzsa, E. Szemerédi. Triple systems with no six points carrying three triangles. Combinatorics (Proc. Fifth Hungarian Colloq., Keszthely, 1976), Vol. II, pp. 939–945, Colloq. Math. Soc. János Bolyai, 18, North-Holland, Amsterdam-New York, 1978.

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

[23] L. Sauermann. Finding solutions with distinct variables to systems of linear equations over $\mathbb{F}_p$. arXiv:2105.06863

[24] E. Szemerédi, *On sets of integers containing no k elements in arithmetic progression*, Acta Arith. **27** (1975), 199–245, Collection of articles in memory of Juriĭ Vladimirovič Linnik.

[25] T. Tao. A symmetric formulation of the Croot–Lev–Pach–Ellenberg–Gijswijt capset bound, 2016. blog post

[26] T. Tao, Terence; V. H. Vu. Additive combinatorics. Paperback edition. Cambridge Studies in Advanced Mathematics, 105. Cambridge University Press, Cambridge, 2010. xviii+512 pp.

[27] Yufei Zhao. Graph Theory and Additive Combinatorics, 2022^+. pdf

[28] 徳重典英. 例から学ぶ極値組合せ論, 東北大学集中講義, 2019. pdf

[29] 徳重典英. スライスランク法とその周辺の話題. 数理解析研究所講究録 2169（RIMS 共同研究「代数的組合せ論と関連する群と代数の研究」）2020 年 9 月 53–62. pdf