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）

2022 早稲田整数論研究集会

問題設定と関連する結果

極値組合せ論 (extremal combinatorics)

- 有限集合 Ω の部分集合 S が、構造 Q を含まないとき、$\max|S|$ は？ 特に $|\Omega| \to \infty$ では？

例 $\Omega = [n] := \{1, 2, \ldots, n\}$,
Q: 3-AP つまり $\{x, x+d, x+2d\}$ $(d \neq 0)$

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

3-AP $\{x, y, z\}$ は一次方程式 $X - 2Y + Z = 0$ の解。
(ただし「自明な解」(x, x, x) は除く)

今日の話 Q が「一次方程式の解」で、Ω が $[n]$ or $\mathbb{F}_p^n$

その前に、ちょっと歴史とか背景とか。。。

問題 (Erdős–Turán 1930') $S \subset [n]$ が 3-AP を含まないとき、$\max|S| =: r(n)$ は？

- Behrend (1946) $ne^{-c/\sqrt{\log n}} < r(n)$
- Roth (1953) $r(n) < cn/(\log\log n)$
- Heath-Brown, Szemerédi, Bourgain, Sanders, ...
- Bloom-Sisask (2020) $r(n) < n/(\log n)^{1+c}$

とにかく $r(n) = o(n)$.

定理 (Szemerédi 1975) $S \subset [n]$ が k-AP を含まないとき、$\max|S| = o(n)$.

定理 (density HJ) $S \subset [k]^n$ が組合せ的直線を含まないとき、$\max|S| = o(k^n)$.
(Hales–Jewett '63, Furstenberg–Katznelson '91, DHJ Polymath 2012)

定理 (Green–Tao 2008) 素数の集合は k-AP を含む。

問題 (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。(3-AP は OK. Bloom–Sisask 2020)

定理（東北大チーム 2020） 数体の素元星座定理

甲斐亘 見村万佐人 宗政昭弘 関真一郎 吉野聖人

関氏の本 Green–Tao の定理の証明（正則化の手法）

- $\mathbb{F}_p^n$ 内の k-AP とは、$\{x, x+d, x+2d, \ldots, x+(k-1)d\}$ をみたす $x, d \in \mathbb{F}_p^n$ で $d \neq 0$ のもの。
- $S \subset \mathbb{F}_p^n$ が k-AP を含まなければ、$|S| = o(p^n)$ であることが density Hales–Jewett からしたがう。

定理 (Ellenberg–Gijswijt 2016) (the cap set problem)
$S \subset \mathbb{F}_3^n$ が 3-AP を含まなければ、$|S| < (2.76)^n = 3^{0.924n}$.

- $S \subset \mathbb{F}_p^n$ 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。

問題　$S \subset \mathbb{F}_p^n$ が 4-AP を含まなければ、$|S| < p^{cn}$ となる $c < 1$ がとれるか？　$p = 5$ では？

4-AP は連立方程式 $x_1 - 2x_2 + x_3 = 0, x_2 - 2x_3 + x_4 = 0$ の解。

3-AP を含まない集合の上界
正則化の手法

正則化の手法　X の中で Y を数えたい。

- X をランダムな X' で近似する。（正則化）
- ランダムな X' で Y を数える。（数え上げ、除去）

グラフ正則化補題 (Szemerédi) 密なグラフは（例外部分を除いて）密なランダムグラフで（適切な誤差で）近似できる。

三角形除去補題　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、辺の本数は $o(n^2)$.

三角形除去補題から Roth の定理 $r(n) = o(n)$ がしたがう。

グラフ正則化補題 (Szemerédi) 密なグラフは（例外部分を除いて）密なランダムグラフで（適切な誤差で）近似できる。

三角形除去補題　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、辺の本数は $o(n^2)$.

証明のアイデア

（背理法）n 点グラフの G どの辺もちょうど一つの三角形に含まれるのに、辺の本数は cn^2 と仮定。

G の三角形の個数は $cn^2/3$.

G を正則化し、よく観察すると $c'n^3$ 個の三角形が見つかる。

Roth の定理

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

証明

頂点集合 $X = Y = Z = \mathbb{Z}/(2n+1)\mathbb{Z}$ の 3 部グラフ G を

$x \sim y \Leftrightarrow y - x \in S$,

$y \sim z \Leftrightarrow z - y \in S$,

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

と定める。

G の頂点数を N とすると、辺数は $3N|S|$.

各辺はちょうど 1 個の三角形に含まれ、辺数は $o(N^2)$.

以上から $|S| = o(N)$.

$N = 3(2n+1)$ より $|S| = o(n)$. □

Behrendの構成
3-APを含まない大きな集合

アイデア：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。(Freiman 2-isomorphism)

cube $\{0,1,\ldots,k-1\}^d$ には k^d 個の点があり、これらは球面 $x_1^2+\cdots+x_d^2=t$ $(t=0,1,\ldots,d(k-1)^2)$ の上にある。ある球面上に $>k^d/dk^2$ 個の点がありその集合を A とおく。

A は球面上の集合で、3-AP を含まない。$f:A\to\mathbb{Z}$ を

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

と定めると $x+z=2y\Leftrightarrow f(x)+f(z)=2f(y)$ で
$f(A)$ に 3-AP はない。また $f(k-1,\ldots,k-1)<(2k)^d$.

$n:=(2k)^d$ とおくと $f(A)\subset[n]$ で、k,d を適切に選べば、
$|f(A)|=|A|>k^d/dk^2\sim ne^{-c\sqrt{\log n}}$.

3-APを含まない$S \subset \mathbb{F}_3^n$の上界
スライスランク法

- X: 有限集合、$\mathbb{F}$: 体
- $f : X^3 \to \mathbb{F}$ がスライス関数とは、$f(x, y, z)$ が

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

と表記できること。

- スライスランク $\mathrm{sr}(f)$ は、f をスライス関数の和に書いたとき、必要なスライス関数の個数の最小値。

例 $f(x, y, z) = (x + y + z)^2 - 1.$

$$f = x^2 + 2x(y + z) + ((y + z)^2 - 1)$$

よって $\mathrm{sr}(f) \leq 3.$

- X: 有限集合、$\mathbb{F}$: 体
- $f : X^3 \to \mathbb{F}$ がスライス関数とは、$f(x, y, z)$ が

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

  と表記できること。
- スライスランク $\mathrm{sr}(f)$ は、f をスライス関数の和に書いたとき、必要なスライス関数の個数の最小値。

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

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

をみたせば、$\mathrm{sr}(f) = |X|$.

定理 (E-G) $X \subset \mathbb{F}_3^n$ が 3-AP を含まなければ、$|X| < 3\,(2.8)^n$.

証明　$f : X^3 \to \mathbb{F}_3$ で

- f は対角条件 ($f(x,y,z) \neq 0 \Leftrightarrow x = y = z$) をみたし
- $\mathrm{sr}(f) < 3\,(2.8)^n$

のものを見つける。実際

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

が条件をみたす。 □

スライスランク法の欠点

$S \subset \mathbb{F}_p^n$ が 4-AP を含まない。$\Longleftrightarrow$ S が

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

の非自明な解 ((x, x, x, x) でない解) を含まない。

スライスランク法を k 変数、m 本の連立方程式に（直接）適用して、よい上界を得られるのは

$$k \geq 2m + 1$$

のとき。

4-AP は $k = 4,\ m = 2$ なのでうまくいかない。

$S \subset [n]$ が 3-AP を含まない。
$\iff S$ が $x - 2y + z = 0$ の非自明な解を含まない。

ここで自明な解は (x, x, x). (singleton solution)
自明でない解 (x, y, z) は 3 個の異なる値をとる。(非退化解)

方程式が $x_1 - x_2 + x_3 - x_4 = 0$ の場合は？

この設定ではスライスランク法を（直接は）適用できない。

スライスランク法を直接適用して、よい上界を得られるのは

(1) 除外する解が singleton solution のみで、かつ

(2) 変数の個数が方程式の個数より十分大きい場合。

今までに (1) の制限を緩める工夫が見つかったが、
(2) の制限を克服する方法はわかっていない。

$\mathbb{F}_p^n$ で非退化解を持たない集合
最近の話題から

定理 (Sauermann 2019) $p \geq 5$ とし、$S \subset \mathbb{F}_p^n$ が
$x_1 + x_2 + \cdots + x_p = 0$ の非退化解（p 個の異なる値をとる解）を含まなければ、$|S| < C_p\,(2\sqrt{p})^n$.

下界：$|S| > 2.08^n$ (Elsholts)
(非退化) を (singleton solution でない) に替えると $|S| \leq 4^n$.

問題　ある定数 c が存在して $|S| < c^n$ ？

上の定理は Erdős–Ginzberg–Ziv の問題に応用がある。
$s(\mathbb{F}_p^n)$ は、$\mathbb{F}_p^n$ の要素からなるどんな s 項の列からもうまく p 項を選んでその和が 0 となるような最小の s である。

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

$\mathbb{F}_p^n$ が property D をもてば、$s(\mathbb{F}_p^n) \leq (p-1)4^n + 1$ (Naslund)

定理 (Mimura-T 2019) $S \subset \mathbb{F}_p^n$ 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、
$|S| < 2(\lambda^{2/3} p^{1/3})^n$.

$S \subset \mathbb{F}_p^n$ が 3-AP を含まなければ $|S| < \lambda^n$, ただし $\lambda < p$.

証明 1. Sauermann のアイデア＋スライスランク法
証明 2. ランダムサンプリングによる証明

ランダムサンプリングによる証明

(W) を含まない $S \subset \mathbb{F}_p^n$ が $|S| \geq 2\,\lambda^{\frac{2}{3}n} p^{\frac{1}{3}n}$ をみたすと仮定。

S には同じ公差の 3-AP は高々 2 個。

$\mathbb{F}_p^n$ の公差の種類は $(p^n - 1)/2 < p^n/2$.

$\#(\text{3-APs in } S) < 2 \times p^n/2 = p^n$.

S の各点を確率 $q = (\lambda/p)^{\frac{n}{3}}$ で選び
random subset T を作り、$X := |T|$.

$\mathbb{E}[X] = |S|\,q \geq 2\lambda^n$.

$Y := \#(\text{3-APs in } T)$ とおくと
$\mathbb{E}[Y] = \#(\text{3-APs in } S)\,q^3 < \lambda^n$.

$\mathbb{E}[X - Y] > \lambda^n$. ($T$ の各 3-AP から一点ずつ捨てた)
S の subset で 3-AP を含まず、サイズ $> \lambda^n$ のものがある。

定理 (Mimura-T 2019) $S \subset \mathbb{F}_p^n$ 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、
$|S| < p^{cn}$, ただし $c < 1$.

その他、いくつかの連立方程式で非退化解を含まない
$S \subset \mathbb{F}_p^n$ が $|S| < p^{cn}$ $(c < 1)$ をみたすことを示した。

問題 どんな連立方程式でこのような上界が得られるか？

k 個の変数からなる m 本の連立方程式 $(*)$ を考える。

$$a_{11}x_1 + \cdots + a_{1k}x_k = 0$$

$$\cdots\cdots$$

$$a_{m1}x_1 + \cdots + a_{mk}x_k = 0$$

仮定

- $k \geq 2m+1$, $a_{ij} \in \mathbb{F}_p$, $x_i \in \mathbb{F}_p^n$
- $m \times k$ の係数行列 $A = (a_{ij})$ は full rank ($\operatorname{rank} A = m$)
- $a_{i1} + a_{i2} + \cdots + a_{ik} = 0 \quad (1 \leq \forall\, i \leq m)$
- $(*)$ 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 (*) (係数行列 A) を考える。
非退化解をもたない $S \subset \mathbb{F}_p^n$ が必ず $|S| < p^{cn}$ $(c < 1)$ をみたすとき、連立方程式 (*) は moderate であるという。

定理 (Sauermann 2021) $k \geq 3m$ で、A の $m \times m$ の小行列がすべて正則ならば、(*) は moderate.

定理 (van Dobben de Bruyn–Gijswijt 2021) A が線形従属な列ベクトルのペアをたくさん持てば、(*) は moderate.

Mimura–T の (W) は上のどちらの定理にも含まれない。

連立方程式 $(*)$ の解 $(y_1, \ldots, y_k)$ が generic $\Longleftrightarrow \sum \mu_i y_i = 0$ かつ $\sum \mu_i = 0$ ならば、$\sum \mu_i x_i = 0$ は $(*)$ の線形結合。

例 $x_1 - x_2 + x_3 - x_4 = 0$ を $\mathbb{F}_p^2$ $(p \geq 5)$ で考える。

$\left(\begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 3 \\ 0 \end{pmatrix}, \begin{pmatrix} 2 \\ 0 \end{pmatrix} \right)$ 非退化だが $x_2+x_3-2x_4 = 0$ をみたし generic でない。

generic な解をもたない $S \subset \mathbb{F}_p^n$ が必ず $|S| < p^{cn}$ $(c < 1)$ をみたすとき、$(*)$ は temperate であるという。

{generic な解 } $\subset$ { 非退化な解 } なので、
$(*)$ が temperate なら moderate.

定理 (Gijwijt 2021) 『連立方程式 (*) から得られる m' 個の独立な方程式に必ず $2m'+1$ 個以上の変数が含まれる』ならば、(*) は temperate.

この結果は Sauermann 2021, v.D.d.Bruyn–Gijswijt 2021, Mimura–T の結果を含む。

問題 (Gijswijt) 上の定理は『...』の仮定がなくても成り立つか？ さらに $k \geq 2m+1$ でなくても成り立つか？