

目次

第 1 章	グラフ理論と確率論の基礎	4
第 2 章	ホフマン限界	5
2.1	独立数とホフマン限界	5
2.2	ホフマン限界の測度版	6
2.2.1	重みグラフ	7
2.2.2	重みグラフの隣接行列	7
2.2.3	重みグラフにおける頂点部分集合の測度	8
2.2.4	重みグラフのホフマン限界	9
2.3	ハイパーグラフのホフマン限界	10
2.3.1	核となるアイデア	10
2.3.2	重み 3 グラフと独立集合	11
2.3.3	リンクグラフと 3 グラフのホフマン限界	11
2.4	極値集合論への応用	13
2.4.1	Erdős–Ko–Rado の定理	13
2.4.2	Erdős–Ko–Rado の定理の測度版	15
2.4.3	3 重交差族の Erdős–Ko–Rado	20
2.4.4	互いに交差する部分空間族とコーシー・シュワルツ法	22
2.4.5	2 交差属の測度版 Erdős–Ko–Rado	24
参考文献		28
第 3 章	加法的組合せ論の話題から	30
3.1	Szemerédi–Trotter の定理とその応用	30
3.1.1	点と直線の接続関係	30
3.1.2	和の集合、積の集合	34
3.2	数列の組合せ論	37

2 目次

3.3	有限アーベル群上のフーリエ変換	38
3.3.1	指標と双対群	38
3.3.2	フーリエ変換	40
3.4	Meshulam の定理	42
3.5	Roth の定理	45
3.6	スライスランク法	49
3.6.1	スライスランクと Tao の補題	49
3.6.2	長さ 3 の等差数列ふたたび	51
3.6.3	ひまわり	53
3.7	長さ 3 の等差数列を含まない部分集合の構成	54
参考文献		57
第 4 章 正則化の手法		59
4.1	正則化補題	59
4.1.1	正則化補題の定式化と指数の性質	59
4.1.2	正則化補題の証明	62
4.2	数え上げ補題と除去補題	64
4.2.1	数え上げ補題	64
4.2.2	除去補題	66
4.3	To be written	69
参考文献		70
第 5 章 確率手法		71
5.1	確率手法の基本アイデア	71
5.1.1	独立数の下界	71
5.1.2	内周と染色数が大きいグラフ	72
5.1.3	2 着色可能性	73
5.2	Lovász の局所補題	75
5.2.1	局所補題とその証明	75
5.2.2	局所補題の応用	78
5.2.3	Moser–Tardos アルゴリズム	81

		3
5.3	測度の集中	82
5.3.1	裾評価の不等式	83
5.3.2	立方体の測度集中	84
5.3.3	エクスパンダグラフの測度集中	86
5.3.4	球面の測度集中	87
5.3.5	Johnson–Lindenstrauss の平坦化補題	91
5.3.6	マルチンゲールと置換の測度集中	94
参考文献		98

第 1 章

グラフ理論と確率論の基礎

第2章

ホフマン限界

組合せ論の問題は、しばしばグラフの独立数を評価する問題として記述できる。ホフマン限界はグラフの固有値から独立数の上界を与える。本章では基本的な隣接行列のホフマン限界から出発して、その測度版やハイパーグラフへの拡張を紹介し、極値組合せ論の問題へ応用する。

2.1 独立数とホフマン限界

グラフ $G = (V, E)$ に対して、頂点の部分集合 $U \subset V$ が独立集合であるとは、 U のどの2頂点も隣接しないことである。独立集合の最大サイズを独立数といい、 $\alpha(G)$ であらわす。ホフマン限界 (Hoffman's ratio bound) は隣接行列の固有値を用いて独立数の上界を与えるものである。

定理 2.1. G は n 頂点 d 正則な単純グラフとする。 G の最小固有値を λ とすると、

$$\frac{\alpha(G)}{n} \leq \frac{-\lambda}{d - \lambda}$$

が成り立つ。

例 2.1. ペテルセングラフは 10 頂点 3 正則グラフで、その固有値は $3, 1, -2$, 対応する重複度は $1, 5, 4$ である。ホフマン限界 $\frac{-(-2) \cdot 10}{3 - (-2)} = 4$ は、独立数と一致する。□

定理 2.1 の証明. G の隣接行列 A の (i, j) 成分は頂点 i と j が隣接すれば 1, そうでなければ 0 と定義された。 A は対称行列だから重複度も込めて n 個の固有値をもつ。 G は d 正則だから A の行和はどの行でも d であり、

$$A\mathbf{1} = d\mathbf{1} \tag{2.1}$$

が成り立つ。 G にループがないことから対角成分はすべて 0 であり、固有値の和も 0 となるから、最小固有値 λ は負であることがわかる。

行列 B を $B = A - \lambda I$ と定める。 B の固有値はすべて非負だから、これは半正定値行列である。独立集合 U のサイズを α とし、 U の特性ベクトルを \mathbf{u} とする。さらに $\mathbf{w} = \mathbf{u} - \frac{\alpha}{n}\mathbf{1}$ とおく。 B が半正定値であることから $\mathbf{w}^T B \mathbf{w} \geq 0$ が成り立つ。この左辺を展開してまとめ直すと目標の不等式が得られる。その際、 \mathbf{u} が独立集合の特性ベクトルであることから

$$\mathbf{u}^T A \mathbf{u} = \sum_{i,j} (A)_{i,j} u_i u_j = 0 \quad (2.2)$$

が成り立つこと、および $\mathbf{u} \cdot \mathbf{u} = \mathbf{u} \cdot \mathbf{1} = \alpha$, $\mathbf{1} \cdot \mathbf{1} = n$ を用いる。 \square

この証明は Godsil と Newman[1] による。この定理の歴史的経緯については Haemers による [2] が詳しい。

ホフマン限界を基本的な形で述べたが、その証明では (2.1) と (2.2) が重要であった。実はこの二つの条件をみたすように隣接行列を拡張できる。そこで n 次対称行列 A が n 頂点単純グラフの擬隣接行列であるとは、頂点 i と j が非隣接ならば $(A)_{i,j} = 0$ であり、行和が正の定数 d であること、と定めよう。この擬隣接行列についても定理 2.1 は成り立つ。通常の隣接行列では隣接ペアの値は 1 であるが、擬隣接行列では 1 以外の値を割り当ててよい。一般に隣接行列のホフマン限界は独立数に一致するとは限らない。そのような場合でも、うまく擬隣接行列を構成するとホフマン限界が独立数に一致することがある。Wilson による Erdős–Ko–Rado の定理の証明 [3] はそのような例である。

2.2 ホフマン限界の測度版

グラフ理論の問題は、与えられた条件をみたす頂点や辺の個数を数える問題に帰着されることがある。その場合、単に個数を数えるかわりに、頂点や辺に重みをつけてその和を考えることが有効なこともある。

グラフの独立数は独立集合の頂点数であったが、これを拡張して各頂点に重みを与え、独立集合の重みの最大値を評価しよう。これは極値集合論に直接の応用があり、またホフマン限界をハイパーグラフに拡張する土台となる。以下の定式化は Filmus, Golubev, Lifshitz[4] による。

2.2.1 重みグラフ

重みグラフ $G = (V, \mu_2)$ を定義する。まず、 $\mu_2 : V \times V \rightarrow \mathbb{R}$ は対称な測度、すなわち、任意の $x, y \in V$ について $\mu_2(x, y) = \mu_2(y, x)$ で、 $\sum_{x \in V} \sum_{y \in V} \mu_2(x, y) = 1$ をみたすとする。次に μ_2 の周辺測度 μ_1 を $\mu_1(x) := \sum_{y \in V} \mu_2(x, y)$ と定義し、これが $\mu_1 > 0$ 、つまり任意の $x \in V$ について $\mu_1(x) > 0$ をみたすとする。このように μ_2 が対称な測度で、その周辺測度が $\mu_1 > 0$ であるとき、 $G = (V, \mu_2)$ を重みグラフという。

$\mu_2(x, y)$ は頂点 x から y への有向辺の重みをあらわし、 $\mu_1(x)$ は x の次数に相当する。 μ_2 が対称であることから実質的には無向グラフを考えている。ただし $\mu_2(x, y)$ は負でもよいし、 $\mu_2(x, x)$ は非零でもよい（ループがあってもよい）。定義から $\sum_{x \in V} \mu_1(x) = \sum_{x \in V} \sum_{y \in V} \mu_2(x, y) = 1$ が成り立つ。

例 2.2. $G_0 = (V, E)$ が通常の単純グラフのとき、 μ_2 を

$$\mu_2(x, y) := \begin{cases} 1/(2|E|) & x \sim y \text{ のとき,} \\ 0 & \text{その他} \end{cases}$$

と定めると、周辺測度 $\mu_1(x)$ は x の次数で、 $G = (V, \mu_2)$ は重みグラフである。□

2.2.2 重みグラフの隣接行列

重みグラフ $G = (V, \mu_2)$ の隣接行列 T を

$$(T)_{x,y} := \frac{\mu_2(x, y)}{\mu_1(x)}$$

と定める。このとき (2.1) と同様に

$$T\mathbf{1} = \mathbf{1} \tag{2.3}$$

が成り立つ。実際、 $(T\mathbf{1})_x = \sum_{y \in V} \frac{\mu_2(x, y)}{\mu_1(x)} = 1$ である。一般には T は対称行列ではないが、以下に述べるように適切な内積を導入することで自己共役作用素となり、その固有値から定理 2.1 を含むホフマン限界が得られる。

重みグラフ $G = (V, \mu_2)$ の隣接行列 T を調べるために、 μ_1 に関する内積を

$$\langle f, g \rangle_{\mu_1} := \sum_{x \in V} \mu_1(x) f(x) g(x)$$

8 第2章 ホフマン限界

と定義する。このとき $\langle f, g \rangle_{\mu_1} = \langle g, f \rangle_{\mu_1}$ であり、 $\langle \mathbf{1}, \mathbf{1} \rangle_{\mu_1} = \sum_x \mu_1(x) = 1$ と規格化されている。この内積に関して T は自己共役作用素、すなわち

$$\langle f, Tg \rangle_{\mu_1} = \langle f, Tg \rangle_{\mu_1}$$

が成り立つ。これを確かめるため V 上の実数値関数 $f, g : V \rightarrow \mathbb{R}$ に対して、

$$\mathbb{E}_{\mu_2}[f, g] := \sum_{x \in V} \sum_{y \in V} \mu_2(x, y) f(x) g(y)$$

と定めると、 μ_2 が対称なことから $\mathbb{E}_{\mu_2}[f, g] = \mathbb{E}_{\mu_2}[g, f]$ である。そこで

$$\langle f, Tg \rangle_{\mu_1} = \mathbb{E}_{\mu_2}[f, g] \tag{2.4}$$

が示せれば、

$$\langle f, Tg \rangle_{\mu_1} = \mathbb{E}_{\mu_2}[f, g] = \mathbb{E}_{\mu_2}[g, f] = \langle g, Tf \rangle_{\mu_1} = \langle Tf, g \rangle_{\mu_1}$$

から T が自己共役作用素であることがわかる。さて (2.4) であるが、

$$(Tg)(x) = \sum_{y \in V} (T)_{x,y} g(y) = \sum_{y \in V} \frac{\mu_2(x, y)}{\mu_1(x)} g(y)$$

を用いると、

$$\begin{aligned} \langle f, Tg \rangle_{\mu_1} &= \sum_{x \in V} f(x) (Tg)(x) \mu_1(x) \\ &= \sum_{x \in V} f(x) \sum_{y \in V} \frac{\mu_2(x, y)}{\mu_1(x)} g(y) \mu_1(x) \\ &= \sum_{x \in V} \sum_{y \in V} f(x) g(y) \mu_2(x, y) = \mathbb{E}_{\mu_2}[f, g] \end{aligned}$$

からしたがう。

2.2.3 重みグラフにおける頂点部分集合の測度

重みグラフ $G = (V, \mu_2)$ において、部分集合 $U \subset V$ の測度を定めよう。まず一般に $f : V \rightarrow \mathbb{R}$ に対して

$$\mathbb{E}_{\mu_1}[f] := \sum_{x \in V} \mu_1(x) f(x)$$

とおく。部分集合 U の特性関数を $\mathbf{1}_U : V \rightarrow \{0, 1\}$ とする。これを $|V|$ 次元ベクトルとみなすこともある。 U の測度を $\mathbb{E}_{\mu_1}[\mathbf{1}_U]$ と定義する。これは二通りの内積表示をもつ。すなわち

$$\mathbb{E}_{\mu_1}[\mathbf{1}_U] = \langle \mathbf{1}_U, \mathbf{1} \rangle_{\mu_1} = \langle \mathbf{1}_U, \mathbf{1}_U \rangle_{\mu_1} \quad (2.5)$$

である。次にこれらの内積を隣接行列の固有値であらわそう。

G の隣接行列を T とすると、これは自己共役作用素だから $N := |V|$ 個の実固有値をもつ。(2.3) も考慮してこれらを $\lambda_0 = 1, \lambda_1, \dots, \lambda_{N-1}$ とおき、 G の固有値とよぶ。対応する固有ベクトルを内積 $\langle \cdot, \cdot \rangle_{\mu_1}$ に関する正規直交基底にとり、 $\mathbf{v}_0 = \mathbf{1}, \mathbf{v}_1, \dots, \mathbf{v}_{N-1}$ とする。この基底で $\mathbf{1}_U$ を

$$\mathbf{1}_U = \sum_{i=0}^{N-1} \hat{\phi}_i \mathbf{v}_i \quad (2.6)$$

とフーリエ展開すると、フーリエ係数は $\hat{\phi}_i = \langle \mathbf{1}_U, \mathbf{v}_i \rangle_{\mu_1}$ で与えられる。この展開表示を用いると

$$\begin{aligned} \langle \mathbf{1}_U, \mathbf{1} \rangle_{\mu_1} &= \left\langle \sum_{i \geq 0} \hat{\phi}_i \mathbf{v}_i, \mathbf{v}_0 \right\rangle_{\mu_1} = \hat{\phi}_0, \\ \langle \mathbf{1}_U, \mathbf{1}_U \rangle_{\mu_1} &= \left\langle \sum_{i \geq 0} \hat{\phi}_i \mathbf{v}_i, \sum_{i \geq 0} \hat{\phi}_i \mathbf{v}_i \right\rangle_{\mu_1} = \sum_{i \geq 0} \hat{\phi}_i^2 = \hat{\phi}_0^2 + \sum_{i \geq 1} \hat{\phi}_i^2 \end{aligned}$$

を得る。これと (2.5) から

$$\mathbb{E}_{\mu_1}[\mathbf{1}_U] = \hat{\phi}_0 = \hat{\phi}_0^2 + \sum_{i \geq 1} \hat{\phi}_i^2 \quad (2.7)$$

がしたがう。特に $\hat{\phi}_0 \geq 0$ である。

2.2.4 重みグラフのホフマン限界

ここまでの準備をもとに定理 2.1 の測度版を示そう。重みグラフ $G = (V, \mu_2)$ において、 $U \subset V$ が独立集合であるとは、任意の $x, y \in U$ について $\mu_2(x, y) = 0$ であることと定義する。

定理 2.2. 重みグラフ $G = (V, \mu_2)$ の最小固有値を λ とおく。 μ_1 を μ_2 の周辺測度とし、 $U \subset V$ を独立集合、 $\mathbf{1}_U$ をその特性関数とすると、

$$\mathbb{E}_{\mu_1}[\mathbf{1}_U] \leq \frac{-\lambda}{1 - \lambda}$$

が成り立つ。

証明. 独立集合 U の特性関数を $\mathbf{1}_U$ とかく。(2.2) と同様に

$$\mathbb{E}_{\mu_2}[\mathbf{1}_U, \mathbf{1}_U] = \sum_{x \in V} \sum_{y \in V} \mathbf{1}_U(x) \mathbf{1}_U(y) \mu_2(x, y) = \sum_{x \in V} \sum_{y \in V} \mu_2(x, y) = 0 \quad (2.8)$$

である。一方、(2.4) により

$$\mathbb{E}_{\mu_2}[\mathbf{1}_U, \mathbf{1}_U] = \langle \mathbf{1}_U, T\mathbf{1}_U \rangle_{\mu_1}$$

とあらわせる。この右辺を計算するために $\mathbf{1}_U$ を (2.6) のように展開する。このとき $T\mathbf{1}_U = T \sum_{i \geq 0} \hat{\phi}_i \mathbf{v}_i = \sum_{i \geq 0} \hat{\phi}_i \lambda_i \mathbf{v}_i$ より

$$\langle \mathbf{1}_U, T\mathbf{1}_U \rangle_{\mu_1} = \left\langle \hat{\phi}_i \mathbf{v}_i, \sum_{i \geq 0} \hat{\phi}_i \lambda_i \mathbf{v}_i \right\rangle_{\mu_1} = \hat{\phi}_0^2 + \sum_{i \geq 1} \hat{\phi}_i^2 \lambda_i \geq \hat{\phi}_0^2 + \lambda \sum_{i \geq 1} \hat{\phi}_i^2$$

である。(2.7) から $\sum_{i \geq 1} \hat{\phi}_i^2 = \hat{\phi}_0 - \hat{\phi}_0^2$ と $\hat{\phi}_0 = \mathbb{E}_{\mu_1}[\mathbf{1}_U]$ に注意すると

$$\mathbb{E}_{\mu_2}[\mathbf{1}_U, \mathbf{1}_U] \geq \mathbb{E}_{\mu_1}[\mathbf{1}_U]^2 + \lambda (\mathbb{E}_{\mu_1}[\mathbf{1}_U] - \mathbb{E}_{\mu_1}[\mathbf{1}_U]^2) \quad (2.9)$$

である。これと (2.8) から目標の不等式がしたがう。 \square

(2.8) が成り立つのは U が独立集合であるからだが、(2.9) は任意の部分集合 $U \subset V$ で成り立つ。この観察は次節において役に立つ。

単純グラフを例 2.2 のように重みグラフにして定理 2.2 を適用すると定理 2.1 が得られる。この意味で定理 2.2 は定理 2.1 の拡張になっている。次節では定理 2.2 がハイパーグラフの場合にも一般化できることを紹介する。

2.3 ハイパーグラフのホフマン限界

2.3.1 核となるアイデア

この節では 3 グラフのホフマン限界を扱う。 V 上の 3 グラフは、 $\binom{V}{3}$ の部分集合とみなすことが多いが、ここでは $V \times V \times V$ の部分集合を考える。なおこの節の結果を一般の k グラフに拡張することは、記号が煩雑になるだけで難しくはない。

グラフの固有値は隣接行列から定まったが、3 グラフ H においてこれに対応するものは何だろうか。グラフの場合、頂点 i と j が隣接するかどうか、つまり $\{i, j\}$ が辺であるかどうかによって、2 次元の表の (i, j) の位置に対応する値 (0 または

1) を書き込んだものが通常の隣接行列であった。これを素朴に拡張すると、3 グラフの場合には、頂点 i, j, k に対してこの 3 点が辺 (hyperedge) であるかどうかによって 3 次元の箱 T の $(i, j, k) \in V \times V \times V$ の位置に、対応する値 $t_{i,j,k}$ を書き込んだものを扱うことになるだろう。これはこのままでは行列ではないが、この箱を $|V|$ 段の行列を x 軸方向に積み上げたものと考えよう。つまり i 段目の行列は $T_i = \{t_{i,j,k} : (j, k) \in V \times V\}$ である。これを隣接行列にもつグラフ G_i は、頂点 j, k が $\{i, j, k\}$ が G の辺であるときに隣接する。また $\sum_i T_i$ を隣接行列にもつグラフ G は、頂点 k, j がこの 2 点を含む G の辺の個数だけ重みをつけた辺であると解釈できる。グラフ G_i たちおよび G は 3 グラフ H の構造を反映しているから、これらのグラフの固有値から H の独立集合の大きさを評価できるだろう。これが Filmus らによるホフマン限界 [4] の基本アイデアである。

2.3.2 重み 3 グラフと独立集合

重み 3 グラフ $H = (V, \mu_3)$ を定義しよう。このため $\mu_3 : V \times V \times V \rightarrow \mathbb{R}$ は対称な測度、すなわち $\mu_3(x, y, z)$ は x, y, z の並べ替えで同じ値をとり、 $\sum_{x \in V} \sum_{y \in V} \sum_{z \in V} \mu_3(x, y, z) = 1$ であるとする。 μ_3 の周辺測度 μ_2 を $\mu_2(x, y) := \sum_{z \in V} \mu_3(x, y, z)$ と定めると、これは対称な測度である。さらに $\mu_2 > 0$ であるとき、 $H = (V, \mu_3)$ を重み 3 グラフという。このとき $\mu_1(x) := \sum_{y \in V} \mu_2(x, y)$ は対称な測度で $\mu_1 > 0$ をみたす。したがって H が重み 3 グラフならば、 $G = (V, \mu_2)$ は重みグラフである。

重み 3 グラフ $H = (V, \mu_3)$ において、 $U \subset V$ が独立集合であるとは任意の $x, y, z \in U$ について $\mu_3(x, y, z) = 0$ をみたすことである。このとき U は $G = (V, \mu_2)$ の独立集合になるとは限らないことに注意する。したがって (2.8) とは違って $\mathbb{E}_{\mu_2}[\mathbf{1}_U, \mathbf{1}_U] > 0$ かもしれない。しかし (2.9) は U が G において独立かどうかにかかわらず成り立つ。そこで $\mathbb{E}_{\mu_2}[\mathbf{1}_U, \mathbf{1}_U]$ を上から押さえたい。このためにリンクグラフを導入する。

2.3.3 リンクグラフと 3 グラフのホフマン限界

重み 3 グラフ $H = (V, \mu_3)$ の頂点 x におけるリンクグラフ $G_x = (V, \mu_{2,x})$ を定義しよう。このため

$$\mu_{2,x}(y, z) := \frac{\mu_3(x, y, z)}{\mu_1(x)}$$

と定める。このとき

$$\mu_{1,x}(y) := \sum_{z \in V} \mu_{2,x}(y, z) = \sum_{z \in V} \frac{\mu_3(x, y, z)}{\mu_1(x)} = \frac{\mu_2(x, y)}{\mu_1(x)} > 0$$

より $\mu_{1,x} > 0$ だから、 G_x は重みグラフである。

ここで H の独立集合 $U \subset V$ をとる。もし $x \in U$ ならば U は G_x においては独立集合である。実際、 $y, z \in U$ ならば $\mu_{2,x}(y, z) = \frac{\mu_3(x, y, z)}{\mu_1(x)} = 0$ である。したがって $x \in U$ ならば G_x に定理 2.2 が適用できて

$$\mathbb{E}_{\mu_{1,x}}[\mathbf{1}_U] \leq \frac{-\lambda_x}{1 - \lambda_x}$$

が成り立つ。ただし λ_x は G_x の最小固有値である。この評価を用いて $\mathbb{E}_{\mu_2}[\mathbf{1}_U, \mathbf{1}_U]$ を上から押さえることができる。すなわち

$$\begin{aligned} \mathbb{E}_{\mu_2}[\mathbf{1}_U, \mathbf{1}_U] &= \sum_{x \in V} \sum_y \mathbf{1}_U(x) \mathbf{1}_U(y) \mu_2(x, y) \\ &= \sum_{x \in V} \mathbf{1}_U(x) \mu_1(x) \sum_{y \in V} \mathbf{1}_U(y) \frac{\mu_2(x, y)}{\mu_1(x)} \\ &= \sum_{x \in V} \mathbf{1}_U(x) \mu_1(x) \sum_{y \in V} \mathbf{1}_U(y) \mu_{1,x}(y) \\ &= \sum_{x \in V} \mathbf{1}_U(x) \mu_1(x) \mathbb{E}_{\mu_{1,x}}[\mathbf{1}_U] \\ &\leq \mathbb{E}_{\mu_1}[\mathbf{1}_U] \max_{x \in V} \mathbb{E}_{\mu_{1,x}}[\mathbf{1}_U] \\ &\leq \mathbb{E}_{\mu_1}[\mathbf{1}_U] \max_{x \in V} \frac{-\lambda_x}{1 - \lambda_x}, \end{aligned}$$

さらに $\lambda' = \min_{x \in V} \lambda_x$ とおけば

$$\mathbb{E}_{\mu_2}[\mathbf{1}_U, \mathbf{1}_U] \leq \mathbb{E}_{\mu_1}[\mathbf{1}_U] \frac{-\lambda'}{1 - \lambda'} \quad (2.10)$$

である。(2.9) と (2.10) から直ちに次の結果がしたがう。

定理 2.3 (Filmus–Golubev–Lifshitz). 重み 3 グラフ $H = (V, \mu_3)$ から得られる $G = (V, \mu_2)$ の最小固有値を λ , $G_x = (V, \mu_{2,x})$ の最小固有値を λ_x とし、 $\lambda' = \min_{x \in V} \lambda_x$ とおく。また $U \subset V$ を H の独立集合、 $\mathbf{1}_U$ をその特性関数とする。このとき

$$\mathbb{E}_{\mu_1}[\mathbf{1}_U] \leq 1 - \frac{1}{(1 - \lambda)(1 - \lambda')}$$

が成り立つ。

2.4 極値集合論への応用

2.4.1 Erdős–Ko–Rado の定理

部分集合族 $\mathcal{F} \subset \binom{[n]}{k}$ は、任意の $F, F' \in \mathcal{F}$ について $F \cap F' \neq \emptyset$ であるとき交差族であるという。サイズ最大の交差族はどんなものだろうか。例えば $n = 4, k = 2$ のとき、 $\binom{[4]}{2}$ を次のように補集合の組に分けてみよう。

$$\begin{aligned} &\{1, 2\} \quad \{3, 4\} \\ &\{1, 3\} \quad \{2, 4\} \\ &\{1, 4\} \quad \{2, 3\} \end{aligned}$$

もし $\mathcal{F} \subset \binom{[4]}{2}$ が交差族ならば、 \mathcal{F} は各行の部分集合を高々ひとつしか含まない。ここから $|\mathcal{F}| \leq 3$ がわかる。また各行から任意にひとつずつ部分集合を選ぶと、サイズ 3 の交差族が得られる。したがってサイズ 3 の交差族は 8 種類ある。一般に $n = 2k$ で $\mathcal{F} \subset \binom{[n]}{k}$ が交差族ならば、 $|\mathcal{F}| \leq \frac{1}{2} \binom{n}{k} = \binom{n-1}{k-1}$ であり、サイズ最大の交差族は $2^{\binom{n-1}{k-1}}$ 種類あることが同様の議論からしたがう。

もし $n < 2k$ ならば、 $\binom{[n]}{k}$ 自身が交差族である。 $n \geq 2k$ のときは、

$$\left\{ F \in \binom{[n]}{k} : 1 \in F \right\}$$

はサイズ $\binom{n-1}{k-1}$ の交差族である。

定理 2.4 (Erdős–Ko–Rado). $n \geq 2k$ で $\mathcal{F} \subset \binom{[n]}{k}$ が交差族ならば、

$$|\mathcal{F}| \leq \binom{n-1}{k-1} \quad (2.11)$$

である。さらに $n > 2k$ で $|\mathcal{F}| = \binom{n-1}{k-1}$ ならば、ある $i \in [n]$ が存在して

$$\mathcal{F} = \left\{ F \in \binom{[n]}{k} : i \in F \right\}$$

である。

例 2.3. $n = 5, k = 2$ のときに (2.11) をホフマン限界を利用して確かめよう。そのため頂点集合 $V = \binom{[5]}{2}$ 上のグラフ G を $x, y \in V$ に対して

$$x \sim y \iff x \cap y = \emptyset \quad (2.12)$$

と定義する。このとき $U \subset V$ が G の独立集合であることと交差族であることは同値だから、(2.11) を示すには $\alpha(G) \leq \binom{4}{1} = 4$ をいえばよい。

G は 10 頂点 3 正則グラフ (実はペテルセングラフ) である。実際 $|V| = \binom{5}{2} = 10$ であり、頂点 x の次数は $|\binom{[5] \setminus x}{2}| = \binom{3}{2} = 3$ である。 G の隣接行列を A とおく。 $(A^2)_{x,y}$ は x と y の共通近傍のサイズだから、 G の定義により

$$(A^2)_{x,y} = \begin{cases} 3 & x = y \text{ のとき} \\ 1 & x \neq y \text{ かつ } x \not\sim y \text{ のとき} \\ 0 & x \neq y \text{ かつ } x \sim y \text{ のとき} \end{cases}$$

である。したがって

$$A^2 + A - 2I = J \quad (2.13)$$

が成り立つ。 G は 3 正則だから $\mathbf{1}$ は固有値 3 の固有ベクトルである。そこで固有値 $\lambda \neq 3$ の固有ベクトル \mathbf{v} を $\mathbf{1}$ と直交するようにとると、 $A\mathbf{v} = \lambda\mathbf{v}$ と $J\mathbf{v} = \mathbf{0}$ である。これと (2.13) から $\lambda^2 + \lambda - 2 = 0$, すなわち $\lambda = 1, -2$ を得る。つまり G の最小固有値は -2 で、定理 2.1 より $\alpha(G) \leq 4$ がしたがう。□

一般の場合の (2.11) も例 2.3 と同様に証明できる。つまり頂点集合 $V = \binom{[n]}{k}$ 上のグラフ G を (2.12) で定義して、その独立数をホフマン限界で評価すればよい。このグラフは Kneser グラフとよばれ、固有値は

$$\left\{ (-1)^i \binom{n-k-i}{k-i} : i = 0, 1, \dots, k \right\}$$

で、対応する重複度は $\binom{n}{i} - \binom{n}{i-1}$ である (7 章参照)。特に G は $\binom{n-k}{k}$ 正則で、最小固有値は $-\binom{n-k-1}{k-1}$ であり、これに定理 2.1 を適用すると $\alpha(G) \leq \binom{n-1}{k-1}$ が得られる。

t を正整数とする。部分集合族 $\mathcal{F} \subset \binom{[n]}{k}$ は、任意の $F, F' \in \mathcal{F}$ について $|F \cap F'| \geq t$ であるとき t 交差族であるという。任意の $n \geq k \geq t$ を固定したとき、サイズ最大の t 交差族は Ahlswede と Khachatrian によって完全に決定されている [5, 6]。特に $n > (t+1)(k-t+1)$ の場合は、最大サイズは $\binom{n-t}{k-t}$ であり、最大サイズを達成する t 交差族は固定された t 点集合を含む k 点集合全体に限られる。この結果には Wilson によるホフマン限界を利用する証明 [3] が知られている。その概略は次の通りである。頂点集合 $V = \binom{[n]}{k}$ 上にグラフ G を $x, y \in V$ に対して

$$x \sim y \iff |x \cap y| < t$$

と定義する。このグラフの独立集合は t 交差族に対応するから $\alpha(G) \leq \binom{n-t}{k-t}$ を示せばよい。しかし通常の (成分が 0, 1 の) 隣接行列に定理 2.1 を適用して目標の不等式が得られるのは $t = 1$ の場合だけである。そこで Wilson は $x \sim y$ のとき、隣接行列の (x, y) 成分を $|x \cap y|$ の値に応じて「うまく」調整した擬隣接行列を構成した。例えば $n = 8, k = 3, t = 2$ の場合は、行列の (x, y) 成分の値を $|x \cap y| = 0$ のときは $\frac{1}{2}$, $|x \cap y| = 1$ のときは $\frac{3}{2}$ と定める。一般の場合の Wilson の行列の定義は 7 章で紹介するが、それが Bose–Mesner 代数の行列であることから固有値が計算できて (実際、行和 (最大固有値) は $\binom{n}{k} \binom{n-t}{k-t}^{-1} - 1$, 最小固有値は -1 である)、定理 2.1 から $\alpha(G) \leq \binom{n-t}{k-t}$ が得られる。

$n < (t+1)(k-t+1)$ の場合に、Ahlsvede–Khachatrian の定理にホフマン限界、あるいはその拡張による証明を与えることは未解決の問題である。

2.4.2 Erdős–Ko–Rado の定理の測度版

定理 2.4 では k 点部分集合の交差族を考えたが、サイズを制限しない部分集合の交差族を考え、サイズに応じた重みを与えて交差族の大きさを測ることも考えられる。そこで正整数 n と実数 $0 < p < 1$ に対して、 $2^{[n]}$ 上の測度 $\mu_p : 2^{2^{[n]}} \rightarrow [0, 1]$ を集合族 $\mathcal{F} \subset 2^{[n]}$ に対して

$$\mu_p(\mathcal{F}) = \sum_{F \in \mathcal{F}} p^{|F|} (1-p)^{n-|F|}$$

と定める。また \mathcal{F} が交差族であるとは、任意の $F, F' \in \mathcal{F}$ について $F \cap F' \neq \emptyset$ であるとき交差族であるという。このとき定理 2.4 の測度版として次が成り立つ。

定理 2.5 (測度版 EKR). $p \leq \frac{1}{2}$ で $\mathcal{F} \subset 2^{[n]}$ が交差族ならば、

$$\mu_p(\mathcal{F}) \leq p \quad (2.14)$$

である。さらに $p < \frac{1}{2}$ で $\mu_p(\mathcal{F}) = p$ ならば、ある $i \in [n]$ が存在して

$$\mathcal{F} = \{F \in 2^{[n]} : i \in F\}$$

である。

定理 2.4 と定理 2.5 はよく似ているが、特に (2.11) を $|\mathcal{F}| / \binom{n}{k} \leq \frac{k}{n}$ と書き直して (2.14) と比べると $\frac{n}{k}$ と p が対応する。これは p と十分大きな n を固定したとき、 $\mu_p(\binom{[n]}{k})$ は k が pn の付近に集中することを反映している。

定理 2.5 を定理 2.2 を利用して証明する Friedgut[7] の手法を紹介する。これはグラフの積と隣接行列のテンソル積を対応させる手法の典型例である。 $n = 1$ の場合、定理の主張は自明だが、この場合の重みグラフを詳しく調べる。実は $n = 1$ の場合を処理できれば、一般の場合の重みグラフは容易に構成できて、定理 2.2 から定理 2.5 が直ちにしたがう。

定理 2.5 の証明. $q = 1 - p$ とおく。

まず $n = 1$ の場合である。 $V = 2^{[1]} = \{\emptyset, \{1\}\}$ 上の重みグラフ $G = (V, \mu_2)$ を

$$\mu_2(\emptyset, \emptyset) = q - p, \quad \mu_2(\emptyset, \{1\}) = \mu_2(\{1\}, \emptyset) = p, \quad \mu_2(\{1\}, \{1\}) = 0$$

と定義する。このとき $\mu_1(\emptyset) = q$, $\mu_1(\{1\}) = p$ で $p, q > 0$ だから μ_2 は確かに重みグラフを定める。隣接行列 T は $(T)_{x,y} = \frac{\mu_2(x,y)}{\mu_1(x)}$ と定義されるから、 $c = \sqrt{p/q}$ とおくと

$$T = \begin{bmatrix} 1 - c^2 & c^2 \\ 1 & 0 \end{bmatrix}$$

である。ただし行、列の並び順は $\emptyset, \{1\}$ とする。ここで

$$C = \begin{bmatrix} 1 & c \\ 1 & -1/c \end{bmatrix}, \quad D = \begin{bmatrix} 1 & 0 \\ 0 & -c^2 \end{bmatrix}, \quad (2.15)$$

とおくと

$$TC = CD$$

が成り立つ。つまり T の固有値は

$$\lambda_0 = 1, \quad \lambda_1 = -c^2 = -\frac{p}{q}$$

で、対応する固有ベクトルとして C の 1 列目、2 列目、すなわち

$$\mathbf{v}_0 = \mathbf{1}, \quad \mathbf{v}_1 = [c, -1/c]^\top$$

をとれる。この固有ベクトルは内積 $\langle \cdot, \cdot \rangle_p$ に関して正規直交基底になっている。特に最小固有値が $\lambda_1 = -p/q$ であることから、 $U \subset V$ が G の独立集合であるとき、その特性関数 $\mathbf{1}_U$ は定理 2.2 により $\mathbb{E}_{\mu_1}[\mathbf{1}_U] \leq \frac{p/q}{1+p/q} = p$ をみたす。 $(\mu_2$ の定義を天下りに与えたが、どのように μ_2 を見つけたのだろうか。実は、定理 2.2 のホフマン限界が p となるような最小固有値 λ を求め、1 と λ が固有値で、1 の固有ベクトルが $\mathbf{1}$ であるような隣接行列 T を reverse engineering した。これと μ_p が周辺

測度 μ_1 と一致するように、 $p_1(\emptyset) = q$, $p_1(\{1\}) = p$ を要請すると μ_2 が定まる。つまりホフマン限界が正しい値になるように μ_2 を逆算したのだ。）

さて U が G の独立集合であることと U が交差族であることは同じであり、また $\mathbb{E}_{\mu_1}[\mathbf{1}_U] = \mu_p(U)$ である。つまり $U \subset 2^{[1]}$ が交差族ならば $\mu_p(U) \leq p$ が示された。なお U が独立集合であるのは $U = \{\{1\}\}$ の場合だが、このとき $\mathbf{1}_U = [0, 1]^T = p\mathbf{v}_0 - \sqrt{pq}\mathbf{v}_1$ と表示できる。

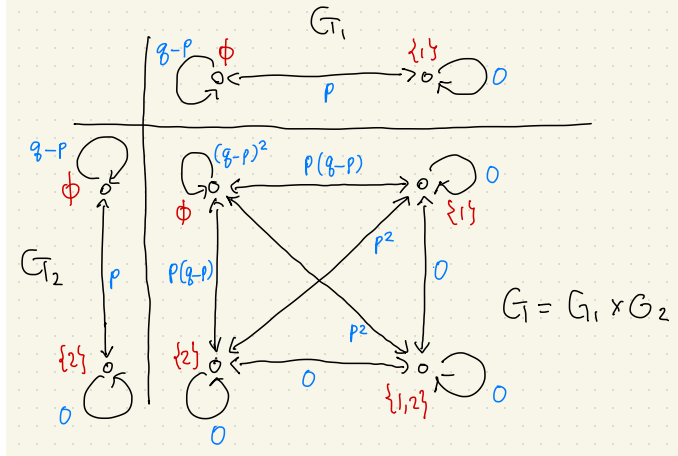
次に $n = 2$ の場合を扱う。 $V = 2^{[2]} = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$ 上の重みグラフ $G_2 = (V, \mu_2)$ を定義する。このため $V^{(1)} = \{\emptyset, \{1\}\}$ とし、 $n = 1$ のとき構成したグラフを $G^{(1)} = (V^{(1)}, \mu_2^{(1)})$ とおく。同様に $V^{(2)} = \{\emptyset, \{2\}\}$ とし、 $G^{(2)} = (V^{(2)}, \mu_2^{(2)})$ とおく。この設定で $V = V^{(1)} \times V^{(2)}$, $\mu_2 = \mu_2^{(1)}\mu_2^{(2)}$, つまり $x, y \in V$ に対して

$$\mu_2(x, y) = \mu_2^{(1)}(x \cap V^{(1)}, y \cap V^{(1)}) \mu_2^{(2)}(x \cap V^{(2)}, y \cap V^{(2)})$$

と定める。このようにして得られる G_2 を $G^{(1)} \times G^{(2)}$ とかく。このとき $\mu_1 = \mu_1^{(1)}\mu_1^{(2)} > 0$ であり、 G_2 は確かに重みグラフである。具体的には

$$\mu_1(\emptyset) = q^2, \quad \mu_1(\{1\}) = \mu_1(\{2\}) = pq, \quad \mu_1(\{1, 2\}) = p^2$$

であり、 μ_1 が μ_p と一致することがわかる。



$G^{(1)}, G^{(2)}$ の隣接行列はどちらも $n = 1$ のときの T であるが、 G_2 の隣接行列 T_2

はテンソル積 $T \otimes T$ で与えられる。すなわち

$$T_2 = \begin{bmatrix} (1-c^2)^2 & c^2(1-c^2) & c^2(1-c^2) & c^4 \\ 1-c^2 & 0 & c^2 & 0 \\ 1-c^2 & c^2 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$

である。また

$$(T \otimes T)(C \otimes C) = (C \otimes C)(D \otimes D)$$

であるから、 T_2 の固有値は $D \otimes D$ の対角成分、つまり

$$\lambda_\emptyset = \lambda_0^2 = 1, \quad \lambda_{\{1\}} = \lambda_{\{2\}} = \lambda_0 \lambda_1 = -p/q, \quad \lambda_{\{1,2\}} = \lambda_1^2 = (p/q)^2$$

で、特に最小固有値は $-p/q$ である。したがって U が G_2 の独立集合ならば、定理 2.2 により $\mu_p(U) \leq p$ を得る。ここまでは $p \leq \frac{1}{2}$ の仮定は使っていない ($n = 1, 2$ の場合は $0 < p < 1$ で (2.14) が成立する)。また T_2 の固有ベクトルは

$$C \otimes C = \begin{bmatrix} 1 & c & c & c^2 \\ 1 & -\frac{1}{c} & c & -1 \\ 1 & c & -\frac{1}{c} & -1 \\ 1 & -\frac{1}{c} & -\frac{1}{c} & \frac{1}{c^2} \end{bmatrix}$$

の列ベクトルで与えられる。この列ベクトルを左から $\mathbf{v}_\emptyset, \mathbf{v}_{\{1\}}, \mathbf{v}_{\{2\}}, \mathbf{v}_{\{1,2\}}$ とおく。 $i = 1, 2$ に対して、 $\mathbf{v}_{\{i\}}$ の x 成分は、 $i \in x$ ならば $-1/c$, $i \notin x$ ならば c であり、成分ごとの積として $\mathbf{v}_{\{1\}}\mathbf{v}_{\{2\}} = \mathbf{v}_{\{1,2\}}$ が成り立つ。さらに $U = \{\{1\}, \{1, 2\}\}$ は $\mu_p(U) = p$ をみたす独立集合で、 $\mathbf{1}_U = [0, 1, 0, 1]^\top = p\mathbf{1} - \sqrt{pq}\mathbf{v}_{\{1\}}$ とあらわせる。

一般の n の場合はもはや明らかであろう。この場合は重みグラフ $G_n = (V, \mu_2)$ を $G^{(1)} \times \dots \times G^{(n)}$ として構成する。このとき μ_1 は μ_p に一致し、対応する隣接行列は $T_n = T^{\otimes n}$ で、固有値は $D^{\otimes n}$ の対角成分、固有ベクトルは $C^{\otimes n}$ の列ベクトルで与えられる。特に $x \in 2^{[n]}$ に対応する固有値は $\lambda_x = (-p/q)^{|x|}$ だから、 $|x| = 1$ のときに最小固有値 $\lambda = -p/q$ をとる。したがって定理 2.2 により、 $U \subset V$ が交差族ならば $\mu_p(U) \leq p$ が成り立つ。ここで $p \leq \frac{1}{2}$ の仮定が使われたことに注意しよう。さらに $p < \frac{1}{2}$ ならば、最小固有値 $\lambda = \lambda_x$ は $|x| = 1$ のときにのみ与えられる。なお x に対応する固有ベクトルは $C^{\otimes n}$ の x の列 \mathbf{v}_x であるが、列ベクトルは

$$\emptyset, \{1\}, \{2\}, \{1, 2\}, \{3\}, \{1, 3\}, \{1, 2, 3\}, \{4\}, \dots \quad (2.16)$$

の順に並べられている。このとき $\mathbf{v}_x = \prod_{i \in x} \mathbf{v}_{\{i\}}$ であり、 $U = \{x \in 2^{[n]} : i \in x\}$ は $\mu_p(U) = p$ をみたす独立集合で $\mathbf{1}_U = p\mathbf{1} - \sqrt{pq}\mathbf{v}_{\{i\}}$ が成り立つ。

最後に極値構造を調べるため、 $\mu_p(U) = p < \frac{1}{2}$ と仮定し、

$$\mathbf{1}_U = \sum_{x \in 2^{[n]}} \hat{\psi}_x \mathbf{v}_x$$

と展開しよう。定理 2.2 で等号が成り立つから (2.9) でも等号が成り立ち、

$$\sum_{x \neq \emptyset} \hat{\psi}_x^2 \lambda_x = \lambda \sum_{x \neq \emptyset} \hat{\psi}_x^2$$

である。ここで $p < \frac{1}{2}$ の仮定により、 $|x| \geq 2$ ならば λ_x は最小固有値ではないため、 $\hat{\psi}_x = 0$ である。さらに $\mathbf{v}_\emptyset = \mathbf{1}$ と (2.7) から $\hat{\psi}_\emptyset = p$ に注意すると

$$\mathbf{1}_U = p\mathbf{1} + \sum_{|x|=1} \hat{\psi}_x \mathbf{v}_x \quad (2.17)$$

とあらわせる。

まず異なる $i, j \in 2^{[n]}$ が存在して、 $\hat{\psi}_{\{i\}}, \hat{\psi}_{\{j\}}$ がともに非零である場合を扱う。つまり

$$\mathbf{1}_U = p\mathbf{1} + \hat{\psi}_{\{i\}} \mathbf{v}_{\{i\}} + \hat{\psi}_{\{j\}} \mathbf{v}_{\{j\}} + \cdots$$

とかける場合である。このとき $\psi^2 : V \rightarrow \{0, 1\}$ を $\psi^2(x) = (\mathbf{1}_U(x))^2$ と定めると、 ψ^2 のフーリエ展開には

$$\hat{\psi}_{\{i\}} \hat{\psi}_{\{j\}} \mathbf{v}_{\{i\}} \mathbf{v}_{\{j\}} = \hat{\psi}_{\{i\}} \hat{\psi}_{\{j\}} \mathbf{v}_{\{i,j\}}$$

という項があらわれる。ここで $\mathbf{v}_{\{i,j\}}$ の係数が非零であることに注意する。一方、 $\mathbf{1}_U$ がブール関数である（値は 0, 1 のみをとる）ことから、 $(\mathbf{1}_U)^2 = \mathbf{1}_U$ である。したがって $\psi^2 = \mathbf{1}_U$ でなければならないが、これは $\mathbf{1}_U$ の一意的なフーリエ展開が (2.17) の形であるという仮定に反する。

そこで (2.17) は、ある $i \in 2^{[n]}$ が存在して

$$\mathbf{1}_U = p\mathbf{1} + \hat{\psi}_{\{i\}} \mathbf{v}_{\{i\}}$$

の形に限定される。このとき $i \neq \emptyset \notin U, i \in [n] \in U$ であるから

$$\begin{aligned} (\mathbf{1}_U)_\emptyset &= 0 = p\mathbf{1} + \hat{\psi}_{\{i\}} c, \\ (\mathbf{1}_U)_{[n]} &= 1 = p\mathbf{1} - \hat{\psi}_{\{i\}}/c \end{aligned}$$

が成り立つ。これを解いて、 $\hat{\psi}_{\{i\}} = -\sqrt{pq}$, つまり $\mathbf{1}_U = p\mathbf{1} - \sqrt{pq}\mathbf{v}_{\{i\}}$ である。これは U が i を含む $[n]$ の部分集合全体であることを意味する。 \square

定理 2.5 は t 交差族に拡張できる。すなわち、 $p \leq \frac{1}{t+1}$ で $\mathcal{F} \subset 2^{[n]}$ が t 交差族ならば、 $\mu_p(\mathcal{F}) \leq p^t$ が成り立つ。この事実は Ahlswede–Khachatrian の定理からしたがうが、Friedgut は定理 2.5 の証明を拡張して、この事実を定理 2.2 から導いた。彼の証明は、Wilson による Erdős–Ko–Rado の定理の証明の測度版とみなせる。定理 2.5 では $n = 1$ の場合の隣接行列のテンソル積で一般の場合の隣接行列が得られたが、 t 交差族で $t \geq 2$ の場合にはテンソル積で得られる行列が隣接行列になるとは限らないため、ここに工夫が必要となる。Friedgut はさらに極値構造の安定性も示した。すなわち \mathcal{F} が t 交差族で $\mu_p(\mathcal{F})$ が p^t に「近い」ならば、 \mathcal{F} は t 点を固定する交差族に「近い」ことを示した。もちろんこのような言明は「近さ」をきちんと定義しなければ意味がないが、これを数量的に定式化して厳密な議論が展開できる。この安定性の証明には Kindler と Safra によるフーリエ解析の深い結果が用いられる。Friedgut の論文 [7] は背後にあるアイデアが詳しく説明されている。

2.4.3 3 重交差族の Erdős–Ko–Rado

部分集合族 $\mathcal{F} \subset \binom{[n]}{k}$ は、任意の $F, F', F'' \in \mathcal{F}$ について $F \cap F' \cap F'' \neq \emptyset$ であるとき 3 重交差族であるという。このとき \mathcal{F} は 2.4.1 節の意味の交差族（これを 3 重交差族と区別したいときは 2 重交差族ともいう）でもあるから、定理 2.5 により $p \leq \frac{1}{2}$ ならば $\mu_p(\mathcal{F}) \leq p$ である。しかし 3 重交差族は 2 重交差族より強い条件をみたすから、定理 2.5 からは得られない結果も期待できるだろう。この違いは $p > \frac{1}{2}$ の場合に生じる。例えば、 $\mathcal{F}_n = \{F \in 2^{[n]} : |F| > \frac{n}{2}\}$ は 2 重交差族であるが、 $p > \frac{1}{2}$ を固定したとき、 $\lim_{n \rightarrow \infty} \mu_p(\mathcal{F}_n) = 1$ である（大数の法則）。つまり n が十分大きいと $\mu_p(\mathcal{F}) > p$ となってしまう。しかし 3 重交差族の場合は $p \leq \frac{2}{3}$ まで測度は p を超えないのである。

定理 2.6 (3 重交差族の測度版 EKR). $p \leq \frac{2}{3}$ で $\mathcal{F} \subset 2^{[n]}$ が 3 重交差族ならば、

$$\mu_p(\mathcal{F}) \leq p \quad (2.18)$$

である。さらに $p < \frac{2}{3}$ で $\mu_p(\mathcal{F}) = p$ ならば、ある $i \in [n]$ が存在して

$$\mathcal{F} = \left\{ F \in 2^{[n]} : i \in F \right\}$$

である。

定理 2.2 から定理 2.4 を証明したのと同様に、定理 2.3 から定理 2.5 が得られる。
以下にその概略を述べる。

証明. $n = 1$ の場合。 $V = 2^{[1]} = \{\emptyset, \{1\}\}$ 上の重み 3 グラフ $H = (V, \mu_3)$ を定義しよう。記述を簡単にするため、 \emptyset を 0, $\{1\}$ を 1 と略記して、例えば $\mu_3(\emptyset, \{1\}, \{1\})$ を $\mu_3(0, 1, 1)$ とかく。 $\mu_3 : V^3 \rightarrow \mathbb{R}$ を

$$\begin{aligned} \mu_3(0, 1, 1) &= \mu_3(1, 0, 1) = \mu_3(1, 1, 0) = \frac{1}{2}p, & \mu_3(0, 0, 0) &= 1 - \frac{3}{2}p, \\ \mu_3(1, 0, 0) &= \mu_3(0, 1, 0) = \mu_3(0, 0, 1) = \mu_3(1, 1, 1) = 0 \end{aligned}$$

と定める。このとき

$$\mu_2(1, 1) = \frac{1}{2}p, \quad \mu_2(1, 0) = \mu_2(0, 1) = \frac{1}{2}p, \quad \mu_2(0, 0) = 1 - \frac{3}{2}p$$

より $\mu_2 > 0$ だから、 $H = (V, \mu_3)$ は確かに重み 3 グラフである。また

$$\mu_1(1) = p, \quad \mu_1(0) = q$$

より $\mu_1 > 0$ だから、 $G = (V, \mu_2)$ は重みグラフである。 G の隣接行列を T , $x \in V$ に対してリンクグラフ G_x の隣接行列を T_x とおくと

$$T = \begin{bmatrix} 1 - \frac{p}{2q} & \frac{p}{2q} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix}, \quad T_\emptyset = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad T_{\{1\}} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

である。定理 2.3 のように λ, λ' を定めて計算すると $\lambda = 1 - \frac{1}{2q}$, $\lambda' = -1$ である。
したがって $U \subset V$ が独立集合ならば、定理 2.3 から $\mathbb{E}_{\mu_1}[\mathbf{1}_U] \leq p$ を得る。

$n \geq 2$ の場合に、重み 3 グラフ H_n を構成しよう。 $n = 1$ のときの $V = 2^{\{i\}}$ 上の 3 グラフを $H^{(i)}$ とおき、 $H_n = H^{(1)} \times H^{(2)} \times \cdots \times H^{(n)}$ と定める。このとき重みグラフの隣接行列は $T^{\otimes n}$ であり、 $x \in 2^{[n]}$ に対応するリンクグラフの隣接行列は $T_{s_n} \otimes \cdots \otimes T_{s_1}$, ただし $s_i = x \cap \{i\}$ である。固有値 λ, λ' を計算すると $n = 1$ の場合と同じ結果が得られ（ここに $p \leq \frac{2}{3}$ が必要）、定理 2.3 により $\mathbb{E}_{\mu_1}[\mathbf{1}_U] \leq p$ を得る。ここで U が独立集合であることと交差族であることは同じだから、 U が交差族ならば $\mu_p(U) \leq p$ である。

極値構造の決定は定理 2.4 の証明と同様にできる。

□

2.4.4 互いに交差する部分空間族とコーシー・シュワルツ法

ここまで扱った交差族は有限集合の部分集合の集まりであったが、交差族はベクトル空間の部分空間の集まりや対称群の置換の集まりなどにも定義できる。交差族を調べる組合せ論的手法はいろいろなものがあるが、ホフマン限界の利点のひとつは交差族を考える世界を取り替えても同様の枠組みが適用できることだろう。この節ではベクトル空間の部分空間族に交差性を定義し、ホフマン限界とコーシー・シュワルツ不等式を併用する手法を紹介する。

有限体 \mathbb{F}_q 上のベクトル空間 V の k 次元部分空間全体を $\begin{bmatrix} V \\ k \end{bmatrix}_q$, または q を固定している場合には単に $\begin{bmatrix} V \\ k \end{bmatrix}$ とかく。 k 次元部分空間族 $\mathcal{F} \subset \begin{bmatrix} V \\ k \end{bmatrix}$ が t 交差族であるとは、任意の $F, F' \in \mathcal{F}$ について $\dim(F \cap F') \geq t$ をみたすことである。部分空間には部分集合にはない構造が入っているため、部分空間の交差族に関する問題は部分集合のそれよりも扱いやすい場合がある（その逆の場合もある）。特に部分空間の t 交差族の構造は、部分集合族の場合よりもずっと単純である。

正整数 n, k, t を固定し、 V を有限体 \mathbb{F}_q 上の n 次元ベクトル空間、 $\mathcal{F} \subset \begin{bmatrix} V \\ k \end{bmatrix}$ を t 交差族とする。Frankl と Wilson[8] はホフマン限界を用いて次のことを示した。 $n > 2k$ ならば $|\mathcal{F}| \leq \begin{bmatrix} n-t \\ k-t \end{bmatrix}$ で、等号は \mathcal{F} が固定された t 次元部分空間を含む k 次元部分空間全体のときにのみ成立し、 $2k - t < n < 2k$ ならば $|\mathcal{F}| \leq \begin{bmatrix} 2k-t \\ k \end{bmatrix}$ で、等号は \mathcal{F} が固定された $2k - t$ 次元部分空間に含まれる k 次元部分空間全体のときにのみ成立する。彼らは $n = 2k$ ならば $|\mathcal{F}| \leq \begin{bmatrix} n-t \\ k-t \end{bmatrix} = \begin{bmatrix} 2k-t \\ k \end{bmatrix}$ であることも示したが、等号成立が上に述べた二種類の構造に限られるかどうか決定できなかった。極値構造がこの二種類のみであることを主張する論文はいくつか出版されたが、正しい証明は田中 [9] によって得られた。

二つの部分空間族 $\mathcal{F}_1, \mathcal{F}_2 \subset \begin{bmatrix} V \\ k \end{bmatrix}$ が互いに t 交差するとは任意の $F_1 \in \mathcal{F}_1, F_2 \in \mathcal{F}_2$ について $\dim(F_1 \cap F_2) \geq t$ が成り立つことである。Frankl-Wilson の結果は互いに t 交差する部分空間族に自然に拡張できる。例えば $n > 2k$ ならば、 $|\mathcal{F}_1||\mathcal{F}_2| \leq \begin{bmatrix} n-t \\ k-t \end{bmatrix}^2$ が成り立つ。このような対象を扱うために、ホフマン限界を拡張しよう。重みグラフ $G = (\Omega, \mu_2)$ に対して、頂点集合の部分集合 $U, W \subset \Omega$ の対 $\{U, W\}$ が独立集合対であるとは、任意の $u \in U$ と $w \in W$ に対して $\mu_2(u, w) = 0$ が成り立つことである。

定理 2.7. 重みグラフ $G = (\Omega, \mu_2)$ の隣接行列 T の 1 以外の固有値のうち、絶対

値最大のものを λ とおく。このとき独立集合対 $\{U, W\}$ について

$$\sqrt{\mathbb{E}_{\mu_1}[\mathbf{1}_U] \mathbb{E}_{\mu_1}[\mathbf{1}_W]} \leq \frac{|\lambda|}{1 + |\lambda|}$$

が成り立つ。

正整数 n, k が $n \geq 2k$ をみたすとする。有限体 \mathbb{F}_q の n 次元ベクトル空間を V とし、 $\Omega = \begin{bmatrix} V \\ k \end{bmatrix}$ とおく。Frankl と Wilson は重みグラフ $G = (\Omega, \mu_2)$ で、次の三条件をみたすものを構成した。(i) $x, y \in \Omega$ が $\dim(x \cap y) \geq t$ をみたせば、 $\mu_2(x, y) = 0$, (ii) $U \subset \Omega$ に対して、 $\mathbb{E}_{\mu_1}[\mathbf{1}_U] = |U| / \begin{bmatrix} n \\ k \end{bmatrix}$, (iii) G の最小固有値は $\lambda = -1 / (\begin{bmatrix} n \\ k \end{bmatrix} \begin{bmatrix} n-t \\ k-t \end{bmatrix}^{-1} - 1)$ で、1 と λ 以外の固有値の絶対値は $-\lambda$ より小さい。この重みグラフに定理 2.7 を適用すると、 $n \geq 2k$ のとき互いに t 交差する $\mathcal{F}_1, \mathcal{F}_2 \subset \begin{bmatrix} V \\ k \end{bmatrix}$ について $|\mathcal{F}_1| |\mathcal{F}_2| \leq \begin{bmatrix} n-t \\ k-t \end{bmatrix}^2$ を得る。

同様の手法は $n \geq 2k > 2l$ で $\mathcal{F}_1 \subset \begin{bmatrix} V \\ k \end{bmatrix}$ と $\mathcal{F}_2 \subset \begin{bmatrix} V \\ l \end{bmatrix}$ が互いに t 交差する場合にも適用できるが、定理 2.7 からは $|\mathcal{F}_1| |\mathcal{F}_2|$ の真の上界は得られない。須田と田中 [10] はこの問題を半正定値計画問題として定式化し、その双対問題の最適解を構成することで、 $t = 1$ の場合の真の上界 $\begin{bmatrix} n-1 \\ k-1 \end{bmatrix} \begin{bmatrix} n-1 \\ l-1 \end{bmatrix}$ を得た。 $t \geq 2$ の場合は未解決である。

定理 2.7 は古くから知られていたようだが、交差族の問題に陽に用いられたのはおそらく Ellis–Friedgut–Pilpel の論文 [11] が最初だと思われる。そこでは対称群における置換の t 交差族が研究されている。交差族の部分構造を詳しく調べようとすると、自然に互いに交差する集合族が出現するのである。

定理 2.7 を証明するために、不等式をひとつ準備する。実数 $a, b \in [0, 1]$ に対して

$$\sqrt{1-a}\sqrt{1-b} \leq 1 - \sqrt{ab} \quad (2.19)$$

が成り立つ。実際、相加相乗平均の不等式を二回用いると、

$$(\text{左辺}) \leq \frac{1}{2}((1-a) + (1-b)) = 1 - \frac{1}{2}(a+b) \leq (\text{右辺})$$

を得る。

定理 2.7 の証明. U, W の特性関数をそれぞれフーリエ展開して

$$\mathbf{1}_U = \sum_{x \in V} \hat{\phi}_x \mathbf{v}_x, \quad \mathbf{1}_W = \sum_{x \in V} \hat{\psi}_x \mathbf{v}_x$$

とおく。ただし $\mathbf{v}_\emptyset = \mathbf{1}$ とする。このとき (2.8) と同様に

$$\mathbb{E}_{\mu_2}[\mathbf{1}_U, \mathbf{1}_W] = 0$$

である。また $x \in V$ に対応する固有値を λ_x とかくと、

$$\begin{aligned} \mathbb{E}_{\mu_2}[\mathbf{1}_U, \mathbf{1}_W] &= \langle \mathbf{1}_U, T \mathbf{1}_W \rangle_{\mu_1} \\ &= \left\langle \sum_{x \in V} \hat{\phi}_x \mathbf{v}_x, \sum_{x \in V} T \hat{\psi}_x \mathbf{v}_x \right\rangle_{\mu_1} \\ &= \hat{\phi}_\emptyset \hat{\psi}_\emptyset + \sum_{x \neq \emptyset} \hat{\phi}_x \hat{\psi}_x \lambda_x \end{aligned}$$

である。したがって (2.7) から $\hat{\phi}_\emptyset, \hat{\psi}_\emptyset$ が非負であることに注意すると

$$\hat{\phi}_\emptyset \hat{\psi}_\emptyset = \left| \sum_{x \neq \emptyset} \hat{\phi}_x \hat{\psi}_x \lambda_x \right| \leq \sum_{x \neq \emptyset} |\hat{\phi}_x \hat{\psi}_x \lambda_x| \leq |\lambda| \sum_{x \neq \emptyset} |\hat{\phi}_x \hat{\psi}_x|$$

を得る。次にコーシー・シュワルツの不等式と (2.7) から

$$\begin{aligned} \sum_{x \neq \emptyset} |\hat{\phi}_x \hat{\psi}_x| &\leq \sqrt{\sum_{x \neq \emptyset} \hat{\phi}_x^2} \sqrt{\sum_{x \neq \emptyset} \hat{\psi}_x^2} \\ &= \sqrt{\hat{\phi}_\emptyset - \hat{\phi}_\emptyset^2} \sqrt{\hat{\psi}_\emptyset - \hat{\psi}_\emptyset^2} \\ &= \sqrt{\hat{\phi}_\emptyset \hat{\psi}_\emptyset} \sqrt{1 - \hat{\phi}_\emptyset} \sqrt{1 - \hat{\psi}_\emptyset} \end{aligned}$$

であるが、さらに (2.19) を適用すると

$$\hat{\phi}_\emptyset \hat{\psi}_\emptyset \leq |\lambda| \sum_{\emptyset \neq x} |\hat{\phi}_x \hat{\psi}_x| \leq |\lambda| \sqrt{\hat{\phi}_\emptyset \hat{\psi}_\emptyset} \sqrt{1 - \hat{\phi}_\emptyset} \sqrt{1 - \hat{\psi}_\emptyset},$$

これを整理して $\hat{\phi}_\emptyset \hat{\psi}_\emptyset = \mathbb{E}_{\mu_1}[\mathbf{1}_U] \mathbb{E}_{\mu_1}[\mathbf{1}_W]$ と書き直すと目標の不等式を得る。 \square

2.4.5 2 交差属の測度版 Erdős–Ko–Rado

2.2.1 節では、重みグラフ $G = (V, \mu_2)$ を定義するためにまず対称な測度 μ_2 を定め、ここから周辺測度 μ_1 と隣接行列 T を導いた。実際の応用では、目的に応じた μ_1 が最初にあり、うまく隣接行列 T を見つけてそこから逆に μ_2 を定義することが多い。そのような具体例として次の結果を示そう。

定理 2.8. $p \leq \frac{1}{3}$ で $\mathcal{F} \subset 2^{[n]}$ が 2 交差族ならば、

$$\mu_p(\mathcal{F}) \leq p^2$$

である。

ここで $\mathcal{F}_0 = \{F \in 2^{[n]} : [2] \subset F\}$ とおけば、これは 2 交差族で $\mu_p(\mathcal{F}_0) = p^2$ である。また $\mathcal{F}_1 = \{F \in 2^{[n]} : |F \cap [4]| \geq 3\}$ とおくと、これも 2 交差族で $\mu_p(\mathcal{F}_1) = 4p^3(1-p) + p^4$ であり、 $p = \frac{1}{3}$ のとき $\mu_p(\mathcal{F}_0) = \mu_p(\mathcal{F}_1) = p^2$ をみtas。実は定理の不等式で等号をみtas 2 交差族は、 $p < \frac{1}{3}$ ならば \mathcal{F}_0 と同型なものだけ、 $p = \frac{1}{3}$ ならば \mathcal{F}_0 または \mathcal{F}_1 と同型なものだけである。

証明に用いる重みグラフ $G = (V, \mu_2)$ を $V = 2^{[n]}$ 上に構成しよう。独立集合 $U \subset V$ が 2 交差族 \mathcal{F} に対応するには $x, y \in V$ が $|x \cap y| \geq 2$ をみtas とき $\mu_2(x, y) = 0$ であり、 $\mu_1(1_U) = \mu_p(\mathcal{F})$ でなければならない。したがって $x \in V$ に対して

$$\mu_1(x) := p^{|x|}(1-p)^{n-|x|} \quad (2.20)$$

と定める。隣接行列 T には何が要請されるだろうか。(2.3) が成り立つために T の列和は 1、つまり

$$\sum_{y \in V} (T)_{x,y} = 1 \quad (2.21)$$

が必要である。このとき T が定まった後に、

$$\mu_2(x, y) := (T)_{x,y} \mu_1(x) \quad (2.22)$$

と定義すると $\sum_{y \in V} \mu_2(x, y) = \mu_1(x)$ 、すなわち μ_1 は μ_2 の周辺測度となる。さらに μ_2 が対称であるために

$$(T)_{x,y} \mu_1(x) = (T)_{y,x} \mu_1(y) \quad (2.23)$$

も必要である。これは T が自己共役作用素であることに対応する。

逆に、(2.20) によって μ_1 を定めたとき、隣接行列 T が (2.21) と (2.23) をみtas せば、(2.22) によって定まる μ_2 は重みグラフ G を与える。この重みグラフに定理 2.2 を適用して定理 2.8 を得るには、隣接行列 T がさらに次の二つの条件をみtas せばよい。ひとつは、独立集合と 2 交差性の対応から

$$|x \cap y| \geq 2 \text{ ならば } (T)_{x,y} = 0 \quad (2.24)$$

であること、もうひとつは T の最小固有値 λ が

$$\frac{-\lambda}{1-\lambda} = p^2 \quad (2.25)$$

をみたすことである。結局、定理 2.8 の証明は、隣接行列 T で (2.21), (2.23), (2.24), (2.25) をみたすものを探す問題に帰着した。

定理 2.8 の証明. 上に述べた条件をみたす隣接行列 T を構成する。まず $q = 1 - p$, $c = \sqrt{p/q}$ とおいて、2 次行列

$$A = \begin{bmatrix} 1 - c^2 & c^2 \\ 1 & 0 \end{bmatrix}, \quad I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

から

$$A(i, j) = \begin{cases} I & i = j \text{ のとき} \\ S & i \neq j \text{ のとき} \end{cases}$$

と定め、 2^n 次行列 A_n, B_n を

$$A_n = A^{\otimes n}, \quad B_n = \frac{1}{n} \sum_{j=1}^n \bigotimes_{i=1}^n A(i, j)$$

と定義する。例えば $n = 3$ のとき $A_3 = S \otimes S \otimes S$,

$$B_3 = \frac{1}{3} (I \otimes S \otimes S + S \otimes I \otimes S + S \otimes S \otimes I)$$

である。次に実数 a_n, b_n に対して

$$T = a_n A_n + b_n B_n$$

とおく。このとき上で定めた T が (2.21), (2.23), (2.24), (2.25) をみたすように、うまく a_n, b_n を選びたい。

T の行と列は (2.16) のように順序づけられている。このとき $(A_n)_{x,y}$ は $|x \cap y| \geq 1$ ならば 0, $(B_n)_{x,y}$ は $|x \cap y| \geq 2$ ならば 0 であり、 T は (2.24) をみたす。

ここで (2.15) のように C, D を定め $C_n = C^{\otimes n}, D_n = D^{\otimes n}$ とおくと、 $AC = CD$ と $IC = CI$ から

$$A_n C_n = C_n D_n, \quad B_n C_n = C_n Q_n \quad (2.26)$$

を得る。ただし Q_n は

$$D(i, j) = \begin{cases} I & i = j \text{ のとき} \\ D & i \neq j \text{ のとき} \end{cases}$$

とおいて

$$Q_n = \frac{1}{n} \sum_{j=1}^n \bigotimes_{i=1}^n D(i, j)$$

と定めた。

また $\Delta = \begin{bmatrix} q & 0 \\ 0 & p \end{bmatrix}$ とおくと $C^\top \Delta C = I$ であり、 $\Delta_n = \Delta^{\otimes n}$, $I_n = I^{\otimes n}$ とおくと

$$C_n^\top \Delta_n C_n = I_n$$

が成り立つ。つまり C_n の列ベクトルは内積 $\langle \cdot, \cdot \rangle_{\mu_1}$ に関する正規直交基底である。さらに (2.26) より、この列ベクトルは A_n と B_n の共通の固有ベクトルで、 $x \in 2^{[n]}$ に対応する A_n, B_n の固有値はそれぞれ

$$\left(-\frac{p}{q}\right)^{|x|} \text{ および } \left(-\frac{p}{q}\right)^{|x|} \left(1 - \frac{|x|}{pn}\right)$$

である。特に C_n の一列目 ($x = \emptyset$ の列) は $\mathbf{1}$ であり、 $T\mathbf{1} = (a_n + b_n)\mathbf{1}$ を得る。したがって (2.21) をみたすには

$$a_n + b_n = 1 \tag{2.27}$$

が必要である。また T の最小固有値 λ は $|x| = 1$ に対応するものだから

$$\lambda = a_n \left(-\frac{p}{q}\right) + b_n \left(-\frac{p}{q}\right) \left(1 - \frac{1}{pn}\right)$$

であり、これが (2.25) をみたすことと (2.27) とから

$$b_n = \frac{pn}{1+p}, \quad a_n = 1 - b_n$$

を得る。逆に上の a_n, b_n を用いて $T = a_n A_n + b_n B_n$ と定義すると、 T は (2.21), (2.24), (2.25) をみたす。 T が (2.23) をみたすことは $(\Delta_n T)^\top = \Delta_n T$ からしたがう。□

ここで述べた A_n, B_n を用いて T を構成する方法も Friedgut によるもので、[12] に書いてあるように t 交差族の結果に拡張できる。Friedgut の最初の証明 [7] はこれよりやや複雑で、隣接行列を剰余環 $\mathbb{R}[X]/(X^t = 0)$ 上で構成している。

参考文献

- [1] M. W. Newman. Independent sets and eigenspaces, Ph.D. Thesis, University of Waterloo, 2004.
- [2] W. H. Haemers, Hoffman’s ratio bound, *Linear Algebra Appl.* **617** (2021), 215–219; MR4218548
- [3] R. M. Wilson, The exact bound in the Erdős-Ko-Rado theorem, *Combinatorica* **4** (1984), no. 2-3, 247–257; MR0771733
- [4] Y. Filmus, K. V. Golubev and N. Lifshitz, High dimensional Hoffman bound and applications in extremal combinatorics, *Algebr. Comb.* **4** (2021), no. 6, 1005–1026; MR4357784
- [5] R. F. Ahlswede and L. H. Khachatrian, The complete intersection theorem for systems of finite sets, *European J. Combin.* **18** (1997), no. 2, 125–136; MR1429238
- [6] R. F. Ahlswede and L. H. Khachatrian, A pushing-pulling method: new proofs of intersection theorems, *Combinatorica* **19** (1999), no. 1, 1–15; MR1722359
- [7] E. Friedgut, On the measure of intersecting families, uniqueness and stability, *Combinatorica* **28** (2008), no. 5, 503–528; MR2501247
- [8] P. Frankl and R. M. Wilson, The Erdős-Ko-Rado theorem for vector spaces, *J. Combin. Theory Ser. A* **43** (1986), no. 2, 228–236; MR0867648
- [9] H. Tanaka, Classification of subsets with minimal width and dual width in Grassmann, bilinear forms and dual polar graphs, *J. Combin. Theory Ser. A* **113** (2006), no. 5, 903–910; MR2231096
- [10] S. Suda and H. Tanaka, A cross-intersection theorem for vector spaces based on semidefinite programming, *Bull. Lond. Math. Soc.* **46** (2014), no. 2, 342–348; MR3194752
- [11] D. C. Ellis, E. Friedgut and H. Pilpel, Intersecting families of permutations, *J. Amer. Math. Soc.* **24** (2011), no. 3, 649–682; MR2784326

- [12] Y. Filmus, Spectral methods in extremal combinatorics, Ph.D. Thesis, University of Toronto, 2013.

第3章

加法的組合せ論の話題から

本章では、3.1 節で加法的数論の基本的対象である和の集合、積の集合に関する初等的な結果を紹介し、3.2 節以降では等差数列に関する問題をフーリエ解析やスライスランク法といった手法とともに扱う。

3.1 Szemerédi–Trotter の定理とその応用

3.1.1 点と直線の接続関係

平面上に n 個の点 $P = \{p_1, \dots, p_n\}$ と m 本の直線 $L = \{l_1, \dots, l_m\}$ があるとき、 P と L の接続関係を

$$I(P, L) := \{(p, l) \in P \times L : \text{点 } p \text{ は直線 } l \text{ 上にある}\}$$

と定める。さらに

$$f(n, m) := \max\{|I(P, L)| : |P| = n, |L| = m\}$$

とおく。 $f(n, m)$ を評価し、それを達成する P, L を特徴づけることは、組合せ幾何の基本的な問題である。

(P, L, I) に対応する二部グラフ $B = B(P, L, I)$ を、 $V(B) = P \sqcup L$, $E(B) = I$ と定める。上の問題はこのグラフの最大サイズ ($\max |E(B)|$) を問う。二直線は高々 1 点でしか交わらないから、二部グラフ B には $C_4 = K_{2,2}$ がない。次の結果は Kövári–Sós–Turán[1] による。

定理 3.1. 正整数 n, t は $n \geq 2t$ をみたすとする。 n 頂点グラフ G のサイズが $n^{2-\frac{1}{t}}$ 以上ならば、 G は $K_{t,t}$ を部分グラフとして含む。

証明. グラフ G について $V(G) = \{x_1, \dots, x_n\}$, $|E(G)| \geq s := n^{2-\frac{1}{t}}$ とする。握

手補題^{†1}から

$$2|E| = \sum_{i=1}^n \deg_G(x_i) \geq 2s \quad (3.1)$$

である。次に、新たに二部グラフ H を

$$\begin{aligned} V(H) &:= V(G) \sqcup \binom{V(G)}{t}, \\ E(H) &:= \{\{x, T\} \in V(G) \times \binom{V(G)}{t} : N_G(x) \supset T\} \end{aligned}$$

と定義する。もし H の $\binom{V(G)}{t}$ 側の平均次数が t 以上ならば、 $\deg_H(T) \geq t$ なる $T \in \binom{V(G)}{t}$ が存在する。このとき $y_1, \dots, y_t \in N_H(T)$ とすると、各 i について $N_G(y_i) \supset T$ であり、 $y_i \notin T$ だから $\{y_1, \dots, y_t\} \cap T = \emptyset$ である。したがって $\{y_1, \dots, y_t\} \sqcup T$ が誘導する G の部分グラフは $K_{t,t}$ を含む。

そこで H の $\binom{V(G)}{t}$ 側の平均次数が t 以上であることを示そう。実際、

$$\begin{aligned} |E(H)| &= \sum_{i=1}^n \deg_H(x_i) = \sum_{i=1}^n \binom{\deg_G(x_i)}{t} \\ &\geq n \binom{\frac{1}{n} \sum_{i=1}^n \deg_G(x_i)}{t} \geq n \binom{2s/n}{t} \geq t \binom{n}{t} \end{aligned}$$

である。ここで、最初の不等式は二項係数の凸性から^{†2}、二番目の不等式は (3.1) から、最後の不等式は直接計算^{†3}による。したがって平均次数 $|E(H)|/\binom{n}{t}$ は t 以上である。□

$n = |P|$, $m = |L|$ の場合に得られる二部グラフは頂点数が $n + m$ で $K_{2,2}$ を含まない。そこで上の定理を $t = 2$ で適用して

$$|I(P, L)| \leq (n + m)^{3/2} \quad (3.2)$$

を得る。

\mathbb{F}_q^3 の一次元部分空間全体を P 、二次元部分空間全体を L とすると、 $n := |P| = q^2 + q + 1$, $m := |L| = q^2 + q + 1$ である。 P を要素を点、 L の要素を直線とよび、 $p \in P$ が $l \in L$ の部分空間であるとき、点 p は直線 l 上にあると解釈する。こ

^{†1} グラフの次数和は辺数の 2 倍に等しい。

^{†2} f が凸関数なら $\frac{1}{n} \sum_{i=1}^n f(a_i) \geq f(\frac{1}{n} \sum_{i=1}^n a_i)$ である (Jensen の不等式)。

^{†3} この節の末尾を見よ。

のとき、異なる2点を通る直線が1本定まり、異なる2直線は1点で交わり、一直線上にない4点がある^{†4}。さらにどの点も $q+1$ 本の直線が通り、どの直線上にも $q+1$ 個の点がある。したがって $|I(P, L)| = (q+1)(q^2 + q + 1)$ であり、 $q \rightarrow \infty$ のとき $|I| = \Omega(m+n)^{3/2}$ である。

この例からわかるように「二直線は高々一点で交わる」という条件のみを使って得られる接続関係の最大サイズの評価は（定数倍を除いて）(3.2) が最善である。しかし「 \mathbb{R}^2 上の」点と直線については評価を改善できる。それが次の定理である。

定理 3.2 (Szemerédi–Trotter[2]). \mathbb{R}^2 における n 個の点の集合 P と、 m 本の直線の集合 L の接続関係は、 $|I(P, L)| \leq 4 \left((mn)^{\frac{2}{3}} + m + n \right)$ をみたす。

例えば、一般の位置にある m 本の直線の集合を L とし、 L の二直線の交点として得られる点の集合を P とすると、 $m = |L|$, $n := |P| = \binom{m}{2}$, $|I(P, L)| = 2n = m(m-1)$ である。このとき、(3.2) の上界は $\Theta(m^3)$ であるが、定理 3.2 の上界は $\Theta(m^2)$ であり、係数を除いて最善であることがわかる。

定理 3.2 の証明はどこかで \mathbb{R}^2 に特有の性質を利用しなければならない。ここではグラフの平面描画における交差点数を利用する Székely の証明 [3] を紹介する。形式的には、グラフ G を平面上に描くとは、単射 $f: V(G) \rightarrow \mathbb{R}^2$ で任意の辺 $e = \{x, y\} \in E(G)$ について $f(x)$ と $f(y)$ を結ぶ辺上には x, y 以外の頂点がないようなものを指定することである。平面上に辺の交差なしに描けるグラフを平面グラフという。二辺が交差するとは、端点以外に共有点を持つことをいう。（グラフの頂点ではない）ある点 x を通る辺が r 本あるときには、ここに $\binom{r}{2}$ 個の交差があると数える。つまり交差点数を数えるときは重複を考慮する。グラフ G は平面描画を指定するごとに交差点の個数が定まるが、あらゆる描画を考えてその個数の最小値を G の交差点数とよび、 $\text{Cr}(G)$ とかく。

補題 3.1. 頂点数 v , 辺数 e の平面グラフ G は、 $e \leq 3v - 6$ をみたす。

証明. G は2連結であると仮定してよい^{†5}。2連結平面グラフの面の境界は閉路である。面の個数を f とすると、オイラーの公式から $v + f - e = 2$, また f 個の面の境界の閉路の長さをそれぞれ l_1, \dots, l_f とすると、 $2e = l_1 + \dots + l_f \geq 3f$ であ

^{†4} この構造 (P, L, I) を有限射影平面 $PG(2, q)$ という。

^{†5} 任意の頂点（とその頂点に接続しているすべての辺）を取り除いても連結であるとき、そのグラフは2連結であるという。 G が2連結でなければ、平面性を保ったまま辺を加えて2連結にできる。

る。この二つの条件から f を消去すると目標の不等式が得られる。 \square

定理 3.3 ([4, 5]). 頂点数 v , 辺数 e のグラフ G が $e \geq 4v$ をみたせば、 $\text{Cr}(G) > \frac{e^3}{64v^2}$ が成り立つ。

証明. G の e 本の辺をを 1 本ずつ描いていき、 e' 本目までは辺の交差なしに描けるが、その後は必ず交差が生じるとしよう。このとき $e' \leq 3v - 6$ であり、残りの $e - e'$ 本の辺はどれも、はじめの e' 本と少なくとも一つの交差を持つ。したがって

$$\text{Cr}(G) \geq e - e' \geq e - (3v - 6) > e - 3v$$

が任意の v 頂点、 e 辺グラフで成り立ち、任意の G の部分グラフ H においても

$$\text{Cr}(H) > |E(H)| - 3|V(H)| \quad (3.3)$$

である。

次に $\text{Cr}(G) = t$ とし、この交差点数を実現する G の平面描画を固定する。 G のランダム誘導部分グラフ H を以下の通り構成する。すなわち、 G の各頂点を独立に確率 p で H の頂点とする。このとき H の頂点数と辺数の期待値はそれぞれ pv , p^2e である。一方、 G の各交差は確率 p^4 で H の交差となる。したがってこの平面描画における H の交差点数の期待値は p^4t であるが、この描画は (G では最適でも) H の交差点数を最小化するとは限らないから、 $\mathbb{E}[\text{Cr}(H)] \leq p^4t$ である。(3.3) が任意の H で成り立つため、 $\mathbb{E}[\text{Cr}(H)] > \mathbb{E}[|E(H)|] - 3\mathbb{E}[|V(H)|]$ も成り立ち、

$$p^4t > p^2e - 3pv$$

を得る。これが任意の $0 < p \leq 1$ で成り立つから、 $p = 4v/e$ を代入^{†6}すると $t > \frac{e^3}{64v^2}$ がしたがう。ただし $p = 4v/e \leq 1$ でなければならないが、このために $e \geq 4v$ と仮定した。 \square

定理 3.2 の Székely による証明. \mathbb{R}^2 上に与えられた P と L に対して、グラフ $G = (V, E)$ を次のように定義する。頂点集合は $V := P$ とし、二頂点 $x, y \in V$ はこの二点が、ある直線 $l \in L$ 上で隣り合っているとき (つまり線分 xy 上にこの二点以外の V の頂点がないとき) 辺で結ぶ。このとき $I := I(P, L)$ とおくと、

$$|V| = n, \quad |E| = I - m$$

^{†6} t が最大になるように p を選ぶと $p = 4.5v/e$ で、ここから $t > 4e^3/(243v^2)$ がしたがう。ただし $e \geq 4.5v$ が必要となる。

34 第3章 加法的組合せ論の話題から

である。後者確かめるため、 $L = \{l_1, \dots, l_m\}$ とし、直線 l_i 上に E の辺が e_i 本あるとしよう。すると l_i 上に V の頂点は $e_i + 1$ 個ある。したがって

$$I = \sum_{i=1}^m (e_i + 1) = |E| + m.$$

もし $|E| < 4|V|$ なら、 $I - m = |E| < 4|V| = 4n$ から

$$I < 4n + m \quad (3.4)$$

である。次に $|E| \geq 4|V|$ と仮定し、 G の交差点数 $\text{Cr}(G)$ を評価しよう。定理 3.3 から次の下界が従う。

$$\text{Cr}(G) > \frac{|E|^3}{64|V|^2} = \frac{(I - m)^3}{64n^2}.$$

一方、 G の頂点を平面上に好きなように配置し、辺は線分（直線の一部）で描いたとしよう。二本の線分は高々一点で交わるから、この描画によって生じる交差の個数は高々 $\binom{m}{2}$ である。このことから次の自明な上界を得る。

$$\text{Cr}(G) \leq \binom{m}{2} < \frac{m^2}{2}.$$

上の二つの不等式から $(I - m)^3 < 32m^2n^2$ 、すなわち

$$I < (32)^{\frac{1}{3}}(mn)^{\frac{2}{3}} + m. \quad (3.5)$$

結局 (3.4) または (3.5) が成り立つから、例えば

$$I < (32)^{\frac{1}{3}}(mn)^{\frac{2}{3}} + m + 4n < 4\left((mn)^{\frac{2}{3}} + m + n\right)$$

を得る。 □

3.1.2 和の集合、積の集合

実数の有限部分集合 $A, B \subset \mathbb{R}$ に対して、 A と B の和の集合、積の集合を次のように定める。

$$\begin{aligned} A + B &:= \{a + b : a \in A, b \in B\}, \\ A \cdot B &:= \{ab : a \in A, b \in B\}. \end{aligned}$$

A のサイズを固定したとき、例えば $|A| = n$ であるとき、 $A + A$ や $A \cdot A$ のサイズはどれくらい小さくできるだろうか。 A が等差数列の場合も等比数列の場合も、

$$\min\{|A + A|, |A \cdot A|\} = \Theta(|A|), \quad \max\{|A + A|, |A \cdot A|\} = \Theta(|A|^2)$$

が成り立つ。 A をうまく選べば、 $\max\{|A + A|, |A \cdot A|\}$ をもっと小さくできるだろうか。Erdős と Szemerédi はそうはならないと考えた [6]。すなわち任意の $\epsilon > 0$ に対してある $c = c(\epsilon)$ が存在して

$$\max\{|A + A|, |A \cdot A|\} \geq c|A|^{2-\epsilon}$$

というのが彼らの予想である。Elekes は定理 3.2 を用いて次の評価を得た。

定理 3.4 (Elekes[7]). ある定数 c が存在して、任意の $A \subset \mathbb{R}$ に対して

$$\max\{|A + A|, |A \cdot A|\} \geq c|A|^{\frac{5}{4}}$$

が成り立つ。

証明. 定理 3.2 を利用するため、 A から定まる点の集合 P と直線の集合 L を平面 \mathbb{R}^2 上に定義しよう。点の集合は

$$P := \{(a, b) : a \in A + A, b \in A \cdot A\}$$

と定義する。 $s := |A + A|$, $p := |A \cdot A|$ とおくと $|P| = sp$ である。次に直線の集合を

$$L := \{y = a(x - b) : a, b \in A\}$$

と定める。 $n := |A|$ とおくと、 $|L| = \Theta(n^2)$ である^{†7}。 $a, b \in A$ を固定したとき、方程式 $y = a(x - b)$ で表される L の直線を l とすると、 l 上には少なくとも n 個の P の点がある。実際、

$$\{(b + c, ac) : c \in A\} \subset P$$

であり、左辺の n 個の点は l 上にある。 L の各直線は n 個以上の P の点を通るので、接続関係のサイズについて

$$|I(P, L)| \geq |A||L| = \Theta(n^3)$$

^{†7} $0 \in A$ ならば $|L| = (n - 1)n + 1$, $0 \notin A$ ならば $|L| = n^2$ である。

が成り立つ。一方、定理 3.2 から

$$\begin{aligned} |I(P, L)| &\lesssim (|P||L|)^{\frac{2}{3}} + |P| + |L| \\ &= \Theta\left((spn^2)^{\frac{2}{3}} + sp + n^2\right) \end{aligned}$$

である^{†8}。この二つの不等式から

$$n^3 \lesssim (spn^2)^{\frac{2}{3}} + sp + 2n^2 \quad (3.6)$$

を得る。これを用いて

$$sp \gtrsim n^{\frac{5}{2}} \quad (3.7)$$

を示そう。すると目標の $\max\{s, p\} \gtrsim n^{\frac{5}{4}}$ が従う。

(3.6) の右辺の三つの項のうち、オーダーが一番大きいのはどれだろうか。いま $n \rightarrow \infty$ の状況を考えていて左辺が n^3 だから、右辺三項目の $2n^2$ は無視できる。もし二項目の sp が最大なら $n^3 \lesssim sp$ だから (3.7) が従う。残ったのは一項目が最大の場合で、このとき $n^3 \lesssim (spn^2)^{\frac{2}{3}}$ から (3.7) を得る。□

この節の内容は [8] の 7 章、[9] の 8 章を参考にした。

定理 3.1 の証明の最後の不等式について。目標の不等式は

$$\prod_{i=0}^{t-1} \frac{2n^{1-1/t} - i}{n - i} \geq \frac{t}{n} \quad (3.8)$$

と書ける。これは $t = 1, 2$ のとき正しいことを直接確かめられるので、 $t \geq 3$ とする。さて $\frac{a}{b} \geq \frac{a-1}{b-1}$ と $b \geq a$ は同値である。 $a = 2n^{1-1/t}$, $b = n$ の場合には $b \geq a$ は $2 \leq n^{1/t}$ つまり $t \leq \log_2 n$ と同値である。このとき (3.8) の左辺は $> \left(\frac{2n^{1-1/t}-t}{n-t}\right)^t$ だから、 $\frac{2n^{1-1/t}-t}{n-t} > (t/n)^{1/t}$ すなわち

$$(2n^{1-1/t} - t)n^{1/t} \geq t^{1/t}(n - t)$$

を示せばよい。これは $t = 3$ で正しいので $4 \leq t \leq \log_2 n$ とし、より強く、

$$2n \geq tn^{1/t} + nt^{1/t} \quad (3.9)$$

を示す。上式右辺の一項目 $tn^{1/t}$ は t の関数として $t = \log n$ まで単調減少、その後は単調増加であり、 $t = 4$ のとき $4n^{1/4}$, $t = \log_2 n$ のとき 2 である。つまり一項目について

^{†8} 定数 C が存在して $f(n) \leq Cg(n)$ のとき $f(n) \lesssim g(n)$ と書くことにする。

$\max_{4 \leq t \leq \log_2 n} tn^{1/t} \leq 4n^{1/4}$ である。二項目については $t^{1/t}n \leq 4^{1/4}n < 1.42n$ である。以上のことから (3.9) の右辺は $4n^{1/4} + 1.42n$ より小さい。したがって (3.9) は

$$2n \geq 4n^{1/4} + 1.42n$$

から従うが、これは実際 $n \geq 14$ で正しい。 $4 \leq t \leq \log_2 n$ を仮定していたので $n \geq 16$ で成り立てば十分である。

$2 \geq n^{1/t}$ の場合には (3.8) の左辺は 1 より大きい。一方、左辺 $t/n \leq 1/2 < 1$ なので、この場合も (3.8) が成り立つ。□

3.2 数列の組合せ論

1927 年に van der Waerden は正整数を二つのクラスに分割すると、そのどちらかにはいくらでも長い（つまり項数が任意の有限個の）等差数列があることを示した。これは Schur によって予想されたものであった。van der Waerden の証明を拡張して次のことも示せる。任意の正整数 k と r に対して、十分大きく N をとると、 $[N] := \{1, 2, \dots, N\}$ の r 個のクラスへの任意の分割 $[N] = A_1 \sqcup \dots \sqcup A_r$ において、ある A_i は項数 k の等差数列を含む。ただし、もとの証明からは「どの」 A_i がそのような等差数列を含むかはわからない。Erdős と Turán は、一番密度の高いクラスは必ず長い等差数列を含むはずだと考えた。すなわち、次のことが予想される。任意の k と $\delta > 0$ に対して、十分大きく N をとると、任意の $A \subset [N]$ は $|A| \geq \delta N$ ならば k 項からなる等差数列を含む。1936 年の彼らの論文では $k = 3$ の場合の予想が提起された。1952 年に Roth はこの予想をフーリエ解析を利用して示した。Szemerédi は 1969 年に $k = 4$ の場合を、1974 年に一般の k の場合を組合せ論的な方法で証明した。これは組合せ論の最も重要な結果の一つである。この結果には、1977 年に Furstenberg によって離散力学系のエルゴード理論による証明が与えられた。さらに 2003 年には Gowers および Rödl らによって、ハイパーグラフの正則化手法の帰結としてもこの結果が得られた。

Erdős は、逆数の和が発散する自然数の部分集合には、任意の k に対して k 項からなる等差数列が含まれると予想し、1981 年の論文ではこの予想の解決に 3000 ドルの賞金をつけ、後に 5000 ドルに更新した。逆数の和が発散する部分集合の例として、素数の集合がある。2004 年に Green と Tao は、素数のみからなる任意項数の等差数列があることを証明した。Erdős の予想自体は、 $k = 3$ の場合のみが（肯定的に）解決しており、これは 2020 年の Bloom と Sisask の結果である。さらに 2023 年に Kelly と Meka は次のことを示した。ある定数 $\beta > 0$ が存在して、 $A \subset [N]$ が $|A| \geq N \cdot 2^{-O(\log N)^\beta}$ をみたせば A は 3 項からなる等差数列を含む。一方、1946 年には Behrend によって $|A| = N \cdot 2^{-O(\log N)^{1/2}}$ だが 3 項等差数列を含まない $A \subset [N]$ の存在が示されている。

等差数列に関する問題は、 $[N]$ に限らず和が定義できる集合上で考えられる。特に有限

体 \mathbb{F} 上の有限次元ベクトル空間に問題を設定することを有限体モデルとよぶ。 \mathbb{F}^n はアーベル群であり、またベクトル空間でもあるが、このような構造を備えることによって、問題の解析が $[N]$ における議論より単純になったり、強い結果が得られたりすることがある。そこで以下の節では、フーリエ解析に関する初歩的な準備のあと、まず \mathbb{F}_3^n における3項等差数列の分布を扱い、それをふまえて Roth の定理を証明する。また多項式の手法であるスライスランク法を紹介し、それを等差数列の問題に応用する。最後に球面の凸性を利用して、等差数列を含まない大きな集合を構成する Behrend の結果を紹介する。

ここに等差数列に関する形式的な用語をまとめておく。有限アーベル群 G において、

$$(a, a+d, a+2d, \dots, a+(k-1)d) \in G^k$$

を初項 a 、公差 d 、長さ k の広義等差数列という。公差 $d=0$ の場合は、自明な等差数列という。単に等差数列というときは、 $d \neq 0$ を仮定する。長さ k の（広義）等差数列を（広義） k -AP と書く。 G に含まれる広義 k -AP は、初項と公比で指定されるから、その個数は $|G|^2$ である。例えば $G = \mathbb{F}_3$ のとき、3-AP として、 $(0, 1, 2)$ と $(0, 2, 1)$ は区別する。

3.3 有限アーベル群上のフーリエ変換

3.3.1 指標と双対群

この節ではこの章で扱う離散フーリエ解析の準備として形式的な設定をまとめる。関数解析になじみのある読者は、次節以降の具体例から読み始めて、必要に応じてこの節に戻って定義を確認されたい。なお、この節では G は有限アーベル群とし、 $|G| \geq 2$ を仮定する。

G における群演算は加法 $+$ を用いる。具体的には $G = \mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$ または $G = \mathbb{F}_p^n$ (p は素数) を想定する。 G の単位元を 0 と書く。 $\mathbb{C}^\times := \mathbb{C} \setminus \{0\}$ も複素数の積に関してアーベル群であるが、 \mathbb{C}^\times において群演算は乗法 \cdot (または \cdot を省略) を用いる。 \mathbb{C}^\times の単位元は 1 である。 G から \mathbb{C}^\times への写像 χ が群準同型であるとき、すなわち、任意の $a, b \in G$ について、

$$\chi(a+b) = \chi(a)\chi(b)$$

であるとき、 χ を G の指標という。このとき $\chi(0) = 1$ である。また $|G| = N$ とすると、任意の $a \in G$ は、 $Na = 0$ をみたす。ただし Na は a の N 個の和とする。したがって $1 = \chi(0) = \chi(Na) = \chi(a)^N$ により、 $\chi(a)$ は 1 の N 乗根である。群準同型 $\chi: G \rightarrow \mathbb{C}^\times$ を指標と定義したが、それは $\chi: G \rightarrow \mathbb{T} := \{z \in \mathbb{C} : |z| = 1\}$ に限られる。特に $\chi(-a) = \chi(a)^{-1} = \overline{\chi(a)}$ である (\bar{z} は z の複素共役を表す)。

G の指標全体を \widehat{G} と書き、 G の (ポントリャーギン) 双対という。 $\chi, \xi \in \widehat{G}$ に対して、その積 $\chi\xi: G \rightarrow \mathbb{T}$ を各 $a \in G$ について $\chi\xi(a) := \chi(a)\xi(a)$ と定めると、 \widehat{G} は可換な乗法

群となる。これを G の双対群という。 \widehat{G} の単位元を χ_0 と書く。これは G の各元に 1 を対応させる指標である。 χ_0 を自明な指標（単位指標）という。

G 上の複素数値関数 $f, g: G \rightarrow \mathbb{C}$ に対して、その内積 $\langle f, g \rangle$ を平均（期待値）によって導入しよう。このため、まず一般に $h: G \rightarrow \mathbb{C}$ に対して

$$\mathbb{E}_x h(x) := |G|^{-1} \sum_{x \in G} h(x)$$

とし、さらに

$$\langle f, g \rangle := \mathbb{E}_x f(x) \overline{g(x)}$$

と定める。 $\langle f, g \rangle = 0$ であるとき、 f と g は直交するという。

補題 3.2. 非自明な指標 $\chi \in \widehat{G}$ は $\mathbb{E}_x \chi(x) = 0$ をみたす。また \widehat{G} の異なる指標は直交する。

証明. 非自明な指標 χ に対して、 $\chi(a) \neq 1$ となる $a \in G$ が存在するから、

$$\mathbb{E}_x \chi(x) = \mathbb{E}_x \chi(x+a) = \mathbb{E}_x \chi(x) \chi(a) = \chi(a) \mathbb{E}_x \chi(x),$$

つまり $(1 - \chi(a)) \mathbb{E}_x \chi(x) = 0$ から $\mathbb{E}_x \chi(x) = 0$ を得る。

次に ξ, η を異なる指標とすると、 $\xi \cdot \eta^{-1}$ は非自明な指標だから、

$$0 = \mathbb{E}_x (\xi \cdot \eta^{-1})(x) = \mathbb{E}_x \xi(x) \overline{\eta(x)} = \langle \xi, \eta \rangle$$

がしたがう。 □

G 上の複素数値関数全体 \mathbb{C}^G は、 $f, g \in \mathbb{C}^G$ と $z, w \in \mathbb{C}$ について和とスカラー倍を $(f+g)(z) := f(z) + g(z)$, $(wf)(z) := wf(z)$ と定義することで \mathbb{C} 上のベクトル空間となる。各 $a \in G$ に対して $f_a \in \mathbb{C}^G$ を $f_a(a) := 1$, $f_a(b) := 0$ ($b \neq a$) と定めると、 f_a たちは \mathbb{C}^G の基底をなす。特に \mathbb{C}^G は $|G|$ 次元である。異なる指標は直交するから線形独立であり、 $|\widehat{G}| \leq |G|$ がわかる。さらに「有限アーベル群は巡回群の直積に表せる」という事実を用いると $|\widehat{G}| = |G|$ もわかる。実は G と \widehat{G} は群として同型である^{†9}。特に $G = \mathbb{Z}_n$ または \mathbb{F}_p^n の場合には、同型写像（のひとつ） $G \ni a \mapsto \chi_a \in \widehat{G}$ を具体的に書ける。すなわち、

$$e(x) := \exp(2\pi i x)$$

とおくと、 $G = \mathbb{Z}_n$ の場合は

$$\chi_a(x) := e(ax/n), \tag{3.10}$$

^{†9} G が有限群でない場合は G と \widehat{G} が同型とは限らない。しかし G が局所コンパクトアーベル群ならば、 G と \widehat{G} は同型である（ポントリャーギン双対定理）。

$G = \mathbb{F}_p^n$ の場合は

$$\chi_a(x) := e(ax/p)$$

が同型写像を与える。ただし $a, x \in \mathbb{F}_p^n$ に対して $ax := \sum_{i=1}^n a_i x_i$ とする。読者は $(\chi_a \cdot \chi_b)(x) = \chi_{a+b}(x)$ が成り立つことを確かめられたい。この章の議論には必要ないが、より一般に

$$G = \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k}$$

の場合は、 $a = (a_1, \dots, a_k) \in G$ に対応する指標 χ_a を $x = (x_1, \dots, x_k)$ に対して

$$\chi_a(x) := e\left(\sum_{i=1}^k \frac{a_i x_i}{n_i}\right)$$

と定義すると、 $a \mapsto \chi_a$ が G から \widehat{G} への同型対応を与える。ただし右辺においては、 $a_i x_i \in \mathbb{Z}_{n_i}$ の代表元を \mathbb{Z} から選び、 $a_i x_i / n_i \in \mathbb{Q}$ と考えて和をとる。 $e(\cdot)$ の周期が 1 であるため、この定義は代表元のとり方に依らない。

有限アーベル群 G とその双対群 \widehat{G} は同型であるため、同型写像 $a \mapsto \chi_a$ をひとつ固定してしばしば G と \widehat{G} を同一視する。この対応で χ_a を a と書くこともある。同型写像は一意には定まらない^{†10}が、この章の議論では G または \widehat{G} 上での平均または和のみを扱うため、どの同型写像を固定しているのかは議論に影響しない。

3.3.2 フーリエ変換

関数 $f: G \rightarrow \mathbb{C}$ のフーリエ変換 $\widehat{f}: \widehat{G} \rightarrow \mathbb{C}$ を

$$\widehat{f}(\chi) := \mathbb{E}_x f(x) \overline{\chi(x)} = \langle f, \chi \rangle$$

と定める^{†11}。 $G = \mathbb{Z}_n$ の場合は、 $\omega = e(1/n)$ とおくと

$$\widehat{f}(\chi_a) = \mathbb{E}_x f(x) \omega^{-ax},$$

$G = \mathbb{F}_p^n$ の場合は、 $\omega = e(1/p)$ とおくと

$$\widehat{f}(\chi_a) = \mathbb{E}_x f(x) \omega^{-a \cdot x} \quad (3.11)$$

である。

次に $f \in \mathbb{C}^G$ のノルム $\|f\|$ を

$$\|f\| := \langle f, f \rangle^{1/2}$$

^{†10} これは有限アーベル群の場合で、局所コンパクトアーベル群では自然な同型が定まる。

^{†11} フーリエ変換の定義にはいくつかの流儀があり、その離散版も著者によって様々 [10, 11, 12, 13, 14, 15, 16, 3] である。ここでは [10] にしたがった。どの定義を採用しても得られる結果はもちろん同じであるが、定義の違いから計算の過程では微妙に異なる表示が現れ、混乱の根源とも揶揄される。

と定める。さらに p ノルム $\|f\|_p$ を $\|f\|_p := (\mathbb{E}_x |f(x)|^p)^{1/p}$ と定める。 \mathbb{C}^G に p ノルムを入れた空間を $L_p(G)$ とかく。 G の指標たちは $L_p(G)$ の正規直交基底をなす。

一方、 \widehat{G} 上の複素数値関数 \widehat{f}, \widehat{g} に対しては内積を和によって定める。すなわち

$$\langle \widehat{f}, \widehat{g} \rangle := \sum_{\chi \in \widehat{G}} \widehat{f}(\chi) \overline{\widehat{g}(\chi)}$$

と定義する。同様に p ノルム $\|\widehat{f}\|_p$ を $\|\widehat{f}\|_p := (\sum_x |\widehat{f}(x)|^p)^{1/p}$ と定める。 $\mathbb{C}^{\widehat{G}}$ に p ノルムを入れた空間を $l_p(\widehat{G})$ とかく。二種類の内積およびノルムを同じ記号で表すが、文脈によってそれが $L_p(G)$ のものか $l_p(\widehat{G})$ のものかを区別できるだろう。

補題 3.3. 任意の $a \in G$, $a \neq 0$ に対して、ある指標 $\xi \in \widehat{G}$ が存在して $\xi(a) \neq 1$ をみtas。さらに $\sum_{\chi \in \widehat{G}} \chi(a) = 0$ が成り立つ。

証明. 前半を背理法で示す。 $\widehat{G} = \{\xi_x : x \in G\}$ は \mathbb{C}^G の基底だから、 $f(a) = 0$ かつ $f(0) = 1$ をみtas $f \in \mathbb{C}^G$ をひとつ選ぶと、 $z_x \in \mathbb{C}$ を係数として $f = \sum_x z_x \xi_x$ と表せる。背理法のため、任意の $x \in G$ について $\xi_x(a) = 1$ と仮定する。一方、 ξ_x は指標だから $\xi_x(0) = 1$ もみtas。このとき

$$0 = f(a) = \sum_x z_x \xi_x(a) = \sum_x z_x \xi_x(0) = f(0) = 1$$

で、矛盾が生じた。そこで $\xi(a) \neq 1$ をみtas $\xi \in \widehat{G}$ をとれる。

後半を示そう。 \widehat{G} から \widehat{G} への写像を $\chi \mapsto \xi\chi$ と定めると、これは全単射である。したがって

$$\xi(a) \sum_{\chi} \chi(a) = \sum_{\chi} \xi\chi(a) = \sum_{\chi} \chi(a),$$

つまり $(1 - \xi(a)) \sum_{\chi} \chi(a) = 0$ から $\sum_{\chi} \chi(a) = 0$ を得る。□

補題 3.3 と指標の性質 $\chi(0) = 1$ により、次が成り立つ。

$$\sum_{\chi \in \widehat{G}} \chi(x) = \begin{cases} |\widehat{G}| = |G| & x = 0 \text{ のとき,} \\ 0 & x \neq 0 \text{ のとき.} \end{cases} \quad (3.12)$$

同様に、補題 3.2 と自明な指標 χ_0 が定数関数 1 であることから、次が成り立つ。

$$\mathbb{E}_x \chi(x) = \begin{cases} 1 & \chi = \chi_0 \text{ のとき,} \\ 0 & \chi \neq \chi_0 \text{ のとき.} \end{cases} \quad (3.13)$$

補題 3.4 (Parseval の等式). $f, g \in \mathbb{C}^G$ は $\langle f, g \rangle = \langle \widehat{f}, \widehat{g} \rangle$ をみtas。

証明. 定義にしたがって計算すると、

$$\begin{aligned}\langle \widehat{f}, \widehat{g} \rangle &= \sum_{\chi} \widehat{f}(\chi) \overline{\widehat{g}(\chi)} = \sum_{\chi} \mathbb{E}_x f(x) \overline{\chi(x)} \overline{\mathbb{E}_y g(y) \chi(y)} \\ &= \mathbb{E}_x \mathbb{E}_y f(x) \overline{g(y)} \sum_{\chi} \overline{\chi(x)} \chi(y) = \mathbb{E}_x \mathbb{E}_y f(x) \overline{g(y)} \sum_{\chi} \chi(y-x)\end{aligned}$$

を得る。 $\sum_{\chi} \chi(y-x)$ は 0 または 1 で、1 となるのは $y=x$ のときだから、

$$\langle \widehat{f}, \widehat{g} \rangle = \mathbb{E}_x f(x) \overline{g(x)} = \langle f, g \rangle. \quad \square$$

補題 3.5 (反転公式). $f \in \mathbb{C}^G$ は $f(x) = \sum_{\chi} \widehat{f}(\chi) \chi(x)$ をみたす。

証明. フーリエ変換の定義と (3.12) から、以下のように計算できる。

$$\begin{aligned}\sum_{\chi} \widehat{f}(\chi) \chi(x) &= \sum_{\chi} \mathbb{E}_y f(y) \overline{\chi(y)} \chi(x) = \sum_{\chi} \mathbb{E}_y f(y) \chi(x-y) \\ &= \mathbb{E}_y f(y) \sum_{\chi} \chi(x-y) = f(x).\end{aligned} \quad \square$$

3.4 Meshulam の定理

定理 3.5 (Meshulam). $A \subset \mathbb{F}_3^n$ が $|A| \geq 8 \cdot 3^n/n$ をみたせば、 A は長さ 3 の等差数列を含む。

以下の証明は概ね [11] にしたがった。

証明. $A \subset \mathbb{F}_3^n$ に含まれる等差数列をフーリエ解析を利用して数えたい。そのため、まず A を有限アーベル群 $G := \mathbb{F}_3^n$ 上の関数として表そう。つまり特性関数 $1_A : \mathbb{F}_3^n \rightarrow \{0, 1\}$ を考えるが、記号を濫用して 1_A を A と書く。すなわち $x \in A$ ならば $A(x) = 1$, $x \notin A$ ならば $A(x) = 0$ である。 A が長さ 3 の広義等差数列 (以下、広義 3-AP とかく) $x-d, x, x+d$ を含むことは

$$A(x-d)A(x)A(x+d) = 1$$

と表現できる。そこで $N := 3^n$ とおき、 A に関する広義 3-AP の密度 $T(A)$ を

$$T(A) := \mathbb{E}_x \mathbb{E}_d A(x-d)A(x)A(x+d) = \#(A \text{ 内の広義 3-APs})/N^2 \quad (3.14)$$

と定める。 A に含まれる広義 3-AP の個数は $T(A)N^2$ である。ただしこれは自明な 3-AP ($d=0$ の場合) も数えていることに注意する。自明な 3-AP は高々 N 個だから、 A が非自明な 3-AP を含むには、 $T(A)N^2 > N$ つまり

$$T(A)N > 1 \quad (3.15)$$

であればよい^{†12}。

A の G に占める密度を $\delta := |A|/|G|$, さらに A の非自明な最大フーリエ係数を $M := \max_{\chi \neq \chi_0} |\hat{A}(\chi)|$ とおく。次の補題は一般の有限アーベル群で成り立つ。

補題 3.6. $|T(A) - \delta^3| \leq \delta M$.

証明. 反転公式 (補題 3.5) を用いて $T(A)$ を計算すると

$$\begin{aligned} T(A) &= \mathbb{E}_x \mathbb{E}_d \sum_{\chi} \hat{A}(\chi) \chi(x-d) \sum_{\xi} \hat{A}(\xi) \xi(x) \sum_{\eta} \hat{A}(\eta) \eta(x+d) \\ &= \sum_{\chi} \sum_{\xi} \sum_{\eta} \hat{A}(\chi) \hat{A}(\xi) \hat{A}(\eta) \mathbb{E}_x \mathbb{E}_d \chi(x-d) \xi(x) \eta(x+d) \\ &= \sum_{\chi} \sum_{\xi} \sum_{\eta} \hat{A}(\chi) \hat{A}(\xi) \hat{A}(\eta) \mathbb{E}_x \chi(x) \xi(x) \eta(x) \mathbb{E}_d \chi(-d) \eta(d) \\ &= \sum_{\chi} \sum_{\xi} \sum_{\eta} \hat{A}(\chi) \hat{A}(\xi) \hat{A}(\eta) \mathbb{E}_x \chi \xi \eta(x) \mathbb{E}_d \bar{\chi} \eta(d) \end{aligned}$$

を得る。(3.13) により、 $\mathbb{E}_x \chi \xi \eta(x) \mathbb{E}_d \bar{\chi} \eta(d)$ は 0 または 1 であるが、1 となるのは、 $\chi \xi \eta = \chi_0$ かつ $\bar{\chi} \eta = \chi_0$, すなわち、 $\eta = \chi$, $\xi = \chi^{-2}$ のときである。よって

$$T(A) = \sum_{\chi} \hat{A}(\chi)^2 \hat{A}(\chi^{-2})$$

と表せる。これと

$$\hat{A}(\chi_0) = \mathbb{E}_x A(x) \chi_0(x) = \mathbb{E}_x A(x) = |A|/|G| = \delta$$

とから、

$$T(A) = \delta^3 + \sum_{\chi \neq \chi_0} \hat{A}(\chi)^2 \hat{A}(\chi^{-2})$$

である。また Parseval の等式 (補題 3.4) より $\|A\|^2 = \|\hat{A}\|^2$ に注意すると、

$$\sum_{\chi \neq \chi_0} |\hat{A}(\chi)|^2 \leq \sum_{\chi \in \hat{G}} |\hat{A}(\chi)|^2 = \|\hat{A}\|^2 = \|A\|^2 = \mathbb{E}_x |A(x)|^2 = \mathbb{E}_x |A(x)| = \frac{|A|}{|G|} = \delta$$

であり、

$$|T(A) - \delta^3| = \left| \sum_{\chi \neq \chi_0} \hat{A}(\chi)^2 \hat{A}(\chi^{-2}) \right| \leq \sum_{\chi \neq \chi_0} |\hat{A}(\chi)|^2 M \leq \delta M$$

を得る。 □

^{†12} これは $G = \mathbb{F}_3^n$ だけでなく、奇数 N の $G = \mathbb{Z}_N$ でも正しいが、 N が偶数のとき \mathbb{Z}_N には非自明だが退化した等差数列があることに注意せよ。補題 3.9 の脚注参照。

定理を n に関する帰納法で示す。 $n = 1$ のときは正しい。実際、 \mathbb{F}_3 ($|A| = 3$ の場合) は 9 個の広義 3-AP を含み、そのうち 6 個は非自明な 3-AP である。以下、 $n \geq 2$ とし、 $n - 1$ の場合に定理の主張を仮定する。つまり $A' \subset \mathbb{F}_3^{n-1}$ が $|A'| \geq 8 \cdot 3^{n-1}/(n-1)$ をみたせば、 A' は非自明な等差数列を含むとする。

$M \leq \delta^2/2$ の場合。このとき、定理の仮定 $\delta \geq 8/n$ と補題 3.6 とから

$$T(A) \geq \delta^3 - \delta M \geq \delta^3/2 \geq (8/n)^3/2 = 256/n^3 > 3^{-n} = 1/N$$

である。したがって (3.15) が成り立ち、非自明 3-AP の存在が示せた。

以下、 $M > \delta^2/2$ とする。 $|\widehat{A}(\chi_a)| = M$ をみたす $\chi_a \neq \chi_0$ をとる。 $\omega = e(1/3)$ とおくと、(3.11) より

$$\widehat{A}(\chi_a) = \mathbb{E}_x A(x) \overline{\chi_a(x)} = \mathbb{E}_x A(x) \omega^{-a \cdot x}$$

である。さらに $i \in \mathbb{F}_3$ に対して、 $A_i := \{x \in A : -a \cdot x = i\}$, $\alpha_i := |A_i|/3^{n-1}$ とおく。 α_i は \mathbb{F}_3^n の超平面 $-a \cdot x = i$ における A の相対密度に対応する。この $n-1$ 次元超平面 H は \mathbb{F}_3^{n-1} に同型である。さてこの設定で、 $\alpha_0 + \alpha_1 + \alpha_2 = 3\delta$ および

$$\widehat{A}(\chi_a) = \mathbb{E}_x (|A_0| + |A_1|\omega + |A_2|\omega^2) = (\alpha_0 + \alpha_1\omega + \alpha_2\omega^2)/3$$

が成り立つ。後者と $|\widehat{A}(\chi_a)| = M$ から $|\alpha_0 + \alpha_1\omega + \alpha_2\omega^2| \geq 3M$ を得る。 $\beta_i := \alpha_i - \delta$ とおくと、 $1 + \omega + \omega^2 = 0$ を利用して、

$$\beta_0 + \beta_1 + \beta_2 = 0, \quad |\beta_0| + |\beta_1| + |\beta_2| \geq |\beta_0 + \beta_1\omega + \beta_2\omega^2| \geq 3M,$$

したがって $\sum_{i \in \mathbb{F}_3} (\beta_i + |\beta_i|) \geq 3M$ である。鳩の巣原理からある i について $2\beta_i = \beta_i + |\beta_i| > M$, つまり $\alpha_i \geq \delta + M/2 > \delta + \delta^2/4$ が成り立つ^{†13}。

$A_i \subset H \cong \mathbb{F}_3^{n-1}$ に帰納法の仮定を適用するには、 $|A_i| \geq \frac{8 \cdot 3^{n-1}}{n-1}$, つまり $\alpha_i \geq \frac{8}{n-1}$ であればよい。実際、 $\delta \geq \frac{8}{n}$ より $\alpha_i > \delta + \frac{\delta^2}{4} \geq \frac{8(n+2)}{n^2}$ であり、 $n \geq 2$ なら右辺は $\frac{8}{n-1}$ 以上である。したがって $A_i \subset A$ の中に非自明 3-AP がある。□

定理の仮定 $|A| \geq 8 \cdot 3^n/n$ は $|A| = \Omega(N/\log N)$ と表せる。この評価は多項式の手法 (スライスランク法) を用いて大幅に改善できること (定理 3.7) を後で示す。

補題 3.6 では $T(A)$ と δ^3 の差を評価した。この δ^3 はどこから来たのか? ここで $G = \mathbb{F}_3^n$ の各点を確率 δ で独立ランダムに選んで得られる部分集合 $B \subset G$ を考える。 $|B|$ の期待値は δN である。 B に含まれる自明な 3-AP の個数の期待値は δN , 非自明な 3-AP の個数の期待値は、 $\delta N \cdot \delta(N-1) \cdot \delta = \delta^3(N^2 - N)$ である。したがって $T(B)$ の期待値は $\delta^3 + (\delta - \delta^3)/N$ で、 n が大きい (すなわち N が大きい) ときは、 δ^3 に近い。この意味で、補題 3.6 は A と「密度 δ のランダム部分集合」を比較したものであり、その近さは $M = \max_{\chi \neq \chi_0} |\widehat{A}(\chi)|$ で測られる。

^{†13} $M > \delta^2/2$ の仮定は最後の不等式にのみ使われた。 $\alpha_i \geq \delta + M/2$ は M の大小に依らず成り立つ。

定理の証明の第一の場合は、 M が小さい、すなわち A がランダム部分集合に近い場合を扱った。この場合、 A にはたくさん ($N(256N/n^3 - 1)$ 個以上) の広義 3-AP がある。第二の場合は、 M が大きい、すなわち A に何らかの偏りあるいは構造が見いだせる場合を扱った。この場合、超平面 H が存在して、 A を H に制限すると密度は $\delta^2/4$ 増加した。このような「ランダムに近いもの」対「構造をもつもの」に注目する考え方は組合せ論の基本のひとつである。

定理の証明はアルゴリズムとしても定式化できる。密度 $\delta^{(k)}$ の部分集合 $A^{(k)} \subset \mathbb{F}_3^k$ に 3-AP が存在するか調べる手続き $\text{Find}(A^{(k)}, \delta^{(k)})$ を定義しよう。 $A^{(k)}$ の非自明最大フーリエ係数を $M^{(k)}$ とし、 $M^{(k)}$ が小さい場合は 3-AP の存在を確認して手続きを終了する。 $M^{(k)}$ が大きい場合は、 $A^{(k-1)} \subset \mathbb{F}_3^{k-1}$ で密度 $\delta^{(k-1)}$ が $\delta^{(k)} + (\delta^{(k)})^2/4$ より大きいものを見つけて、 $\text{Find}(A^{(k-1)}, \delta^{(k-1)})$ を再帰的に呼び出す。この手続きを $k = n, \delta^{(n)} \geq 8/n$ からはじめると、有限回の再帰呼び出しの後に手続きは終了する。なぜなら、再帰のたびに密度は少なくとも $(\delta^{(k)})^2/4 \geq (\delta^{(n)})^2/4$ だけ増加するが、密度は 1 を超えないからである。この手法を密度増加法という。正則化補題の証明にもこの手法が用いられる。

3.5 Roth の定理

前節では $G = \mathbb{F}_3^n$ における 3-AP を扱った。その際、密度 δ の部分集合 $A \subset \mathbb{F}_3^n$ の非自明フーリエ係数 M に対して、ある超平面 H が存在して $A' = A \cap H$ とおくと A' の H における密度は $\delta + M/2$ 以上となることを用いた。この事実と $H \cong \mathbb{F}_3^{n-1}$ であることが効いて、容易に密度増加法が適用できた。この節では $[N]$ における 3-AP を扱う。 $[N]$ は群ではないので、補助的に $G = \mathbb{Z}_n$ における 3-AP を扱う。この場合も部分集合 $A \subset \mathbb{Z}_n$ の非自明フーリエ係数が大きければ、ある (長い) 等差数列 $P \subset [n]$ が存在して、 $A' = A \cap P$ とおくと A' の P における密度は A の初期密度より増加する。しかし \mathbb{Z}_n と P の関係は \mathbb{F}_3^n と \mathbb{F}_3^{n-1} ほど単純でないため、密度増加法の適用は技術的にやや込み入った計算を要する。この節の証明は [10] を参考にした。

有限集合 $X \subset \mathbb{C}$ の直径を $\text{diam}(X) := \max\{|x - y| : x, y \in X\}$ と定め、 $\theta \in \mathbb{R}$ のとき $\text{diam}(\{e(\theta x) : x \in X\})$ を $\text{diam}(e(\theta X))$ と略記する。

補題 3.7. 任意の $\epsilon > 0, n \in \mathbb{N}, \theta \in \mathbb{R}$ に対して、 $n \geq 330/\epsilon$ ならば $[n]$ の分割 $P_1 \sqcup \dots \sqcup P_m$ が存在して次の条件をみたす。各 $1 \leq i \leq m$ について P_i は等差数列で、 $|P_i| \geq \sqrt{\epsilon n}/4$ かつ $\text{diam}(e(\theta P_i)) \leq \epsilon$ である。

証明. $t := \lfloor 2\sqrt{\frac{\pi n}{\epsilon}} \rfloor$ とおき、 $t+1$ 個の複素数 $e(0), e(\theta), \dots, e(t\theta)$ を考える。鳩の巣原理により、ある $0 \leq u < v \leq t$ が存在して、 $|e(u\theta) - e(v\theta)| < 2\pi/t$ をみたす。 $d := v - u \leq t$

とくと、 $|1 - e(d\theta)| \leq 2\pi/t$ であり、三角不等式から任意の $s \in \mathbb{N}$ について

$$\begin{aligned} |1 - e(sd\theta)| &\leq |1 - e(d\theta)| + |e(d\theta) - e(2d\theta)| + \cdots + |e((s-1)d\theta) - e(sd\theta)| \\ &= s|1 - e(d\theta)| \leq \frac{2\pi s}{t} \end{aligned}$$

が成り立つ。ここで $s := \lfloor \frac{\epsilon t}{2\pi} \rfloor$ と定めると、公差 d , 長さ s の等差数列 $P = \{d, 2d, \dots, sd\}$ は $\text{diam}(e(\theta P)) \leq \frac{2\pi s}{t} \leq \frac{2\pi}{t} \frac{\epsilon t}{2\pi} = \epsilon$ をみたす。

そこで $[n]$ をまず d 個の公差 d の等差数列 $Q_j = \{j, j+d, j+2d, \dots\}$ ($1 \leq j \leq d$) に分割する。次に各 Q_j を公差 d を保ったまま長さ s に切り分けたいが、端数を処理する場合に、最低でも長さ $\frac{s}{2}$ を確保したい。これは残りの長さが $[s+1, 2s-1]$ の範囲になったら、ほぼ等分に切り分けることで実現できる^{†14}。ただし $|Q_j| \geq \frac{s}{2}$ が必要であるが、これは次のように確かめられる。すなわち、定義により $st \leq \frac{\epsilon t^2}{2\pi} \leq \frac{\epsilon}{2\pi} \frac{4\pi n}{\epsilon} = 2n$ であり、また $|Q_j| \geq \frac{n}{d} \geq \frac{n}{t}$ であるから $\frac{n}{t} \geq \frac{s}{2}$ がしたがう。このようにして $[n]$ の等差数列 P_1, \dots, P_m への分割が得られる。このとき $\epsilon n \geq 330$ ならば $|P_i| \geq \frac{s}{2} \geq \sqrt{\epsilon n}/4$ が成り立つ^{†15}。また $P_i \subset P$ だから $\text{diam}(e(\theta P_i)) \leq \text{diam}(e(\theta P)) \leq \epsilon$ である。□

補題 3.8. 任意の $0 < \mu < 1$ と正整数 $N \geq (16/\mu)^3$ をとり、 $G := \mathbb{Z}_N$ とおく。密度 δ の部分集合 $A \subset G$ において $M := \max_{\chi \neq \chi_0} \hat{A}(\chi)$ とする。このとき $M \geq \mu$ ならば、等差数列 $P \subset [N]$ が存在して、 $|P| \geq N^{1/3}$ かつ $|A \cap P| \geq (\delta + \mu/4)|P|$ をみたす。

証明. 各 $x \in G$ について $f(x) = A(x) - \delta$ とおく。フーリエ変換の定義と (3.13) から、 $\hat{f}(\chi_0) = 0$, $\chi \neq \chi_0$ ならば $\hat{f}(\chi) = \hat{A}(\chi)$ を確認できる。 $M = \hat{A}(\chi) = \hat{f}(\chi)$ をみたす指標を χ_r ($r \in G \setminus \{0\}$) とする。 $\omega = e(1/N)$ とおくと、(3.10) により $\overline{\chi_r(x)} = \omega^{-rx}$ である。また補題 3.7 を $\epsilon = \mu/2$, $\theta = 1/N$ として適用する^{†16}と、 $[N]$ の等差数列 P_1, \dots, P_m による分割がとれて、各 $1 \leq i \leq m$ について $|P_i| \geq \sqrt{\mu N}/4 \geq N^{1/3}$ (ここに $N \geq (16/\mu)^3$ を用いた) かつ $\text{diam}(e(P_i/N)) = \text{diam}(\omega^{rP_i}) \leq \mu/2$ をみたす。このとき

$$\mu N = |\hat{f}(\chi_r)|N = N \left| \sum_{x \in G} f(x) \omega^{-rx} \right| \leq \sum_{i=1}^m \left| \sum_{x \in P_i} f(x) \omega^{-rx} \right|$$

である。各 i について $x_i \in P_i$ を固定する。直径に関する仮定から $x \in P_i$ ならば $|\omega^{-rx} - \omega^{-rx_i}| \leq \mu/2$ であり、また $A(x)$ は特性関数だから $|f(x)| \leq 1$ である。つまり $|f(x)(\omega^{-rx} - \omega^{-rx_i})| \leq \mu/2$ である。そこで先の続きを $\omega^{-rx} = \omega^{-rx_i} + (\omega^{-rx} - \omega^{-rx_i})$

^{†14} $|Q_j| = sq + r$ ($0 < r < s$) なら、 $q-1$ 個は長さ s , 残り 2 個の長さは $\lfloor \frac{s+r}{2} \rfloor$, $\lceil \frac{s+r}{2} \rceil$ に分ける。

^{†15} $\frac{s}{2} = \frac{1}{2} \lfloor \frac{\epsilon}{2\pi} \lfloor 2\sqrt{\frac{\pi n}{\epsilon}} \rfloor \rfloor > \frac{1}{2} (\frac{\epsilon}{2\pi} (2\sqrt{\frac{\pi n}{\epsilon}} - 1) - 1) \geq \frac{1}{2} \sqrt{\frac{\epsilon n}{\pi}} - \frac{1}{4\pi} - \frac{1}{2} \geq \sqrt{\epsilon n}/4$.

^{†16} $N \geq 330/\epsilon$ は $N \geq (16/\mu)^3 = (8/\epsilon)^3 \geq 330/\epsilon$ からしたがう。

と分けて評価すると、

$$\begin{aligned}\mu N &\leq \sum_{i=1}^m \left| \sum_{x \in P_i} f(x) \omega^{-rx_i} \right| + \sum_{i=1}^m \left| \sum_{x \in P_i} f(x) (\omega^{-rx} - \omega^{-rx_i}) \right| \\ &\leq \sum_{i=1}^m \left| \sum_{x \in P_i} f(x) \right| + \frac{\mu N}{2}\end{aligned}$$

を得る。ここで $F_i := \sum_{x \in P_i} f(x)$ とおくと、

$$\sum_{i=1}^m |F_i| \geq \frac{\mu N}{2} = \frac{\mu}{2} \sum_{i=1}^m |P_i|$$

と表せる。両辺に $\sum_{i=1}^m F_i = \sum_{x \in G} (A(x) - \delta) = |A| - \delta|G| = 0$ を加えると、

$$\sum_{i=1}^m (|F_i| + F_i) \geq \frac{\mu}{2} \sum_{i=1}^m |P_i|$$

である。したがって鳩の巣原理から、ある i について $|F_i| + F_i \geq \frac{\mu}{2} |P_i|$ が成り立つ。このとき $F_i > 0$ でなければならないから、 $F_i \geq \frac{\mu}{4} |P_i|$ である。これと

$$F_i = \sum_{x \in P_i} f(x) = \sum_{x \in P_i} (A(x) - \delta) = |A \cap P_i| - \delta |P_i|$$

とから $|A \cap P_i| \geq (\delta + \frac{\mu}{4}) |P_i|$ がしたがう。 \square

補題 3.9. N を奇数とし、 $A \subset \mathbb{Z}_N$ は長さ 3 の等差数列を含まないとする^{†17}。このとき $|A| = O(N/\log \log N)$ が成り立つ。

証明. $A \subset \mathbb{Z}_N$ の密度を $\delta := |A|/N$ とおく。 $\delta = \Omega(1/\log \log N)$ を仮定して、 A は 3-AP を含むことを示す。このため、密度 δ の部分集合 $A \subset \mathbb{Z}_N$ に 3-AP が存在するか調べる手続き $\text{Find}(N, A, \delta)$ を以下で定義しよう。 A に関する広義 3-AP の密度を (3.14) で定めると、補題 3.6 が成り立つ。 A の非自明な最大フーリエ係数を $M := \max_{\chi \neq \chi_0} \hat{A}(\chi)$ と定める。

$M \leq \delta^2/2$ の場合。このとき、補題 3.6 から

$$T(A) \geq \delta^3 - \delta M \geq \delta^3/2 = \Omega(1/\log \log N)^3$$

である。右辺は $\gg 1/N$ だから (3.15) がみたされ、 A は非自明 3-AP を含む^{†18}。この場合、 $\text{Find}(N, A, \delta)$ は 3-AP の存在を報告して終了する。

^{†17} $N = 2m$ の場合には、公差 m 、長さ 3 の広義等差数列は $(x, x+m, x+2m) = (x, x+m, x)$ のように退化してしまう。この状況を避けるため、 N を奇数としている。

^{†18} N が奇数であるため、非自明 3-AP は退化しない。

$M > \delta^2/2$ の場合。このとき、 $\mu := \delta^2/2$ として補題 3.8 を適用すると、等差数列 $P \subset [N]$ が存在して、 $|P| \geq N^{1/3}$ かつ $|A \cap P| \geq (\delta + \delta^2/8)|P|$ をみ出す。ただし補題 3.8 の適用には $N \geq (16/\mu)^3 = 32^3\delta^{-6}$ が必要である。次に P を $\{1, \dots, |P|\}$ にうつす線形写像を ϕ とし、 $\text{Find}(|P|, \phi(A), |A \cap P|/|P|)$ を呼び出す。

この手続きを解析するため、 N は十分大きいとし、その評価は後でおこなう。 $N_0 := N$, $A_0 := A$, $\delta_0 := \delta$ とおき、さらに $N_1 := |P|$, $A_1 := \phi(A \cap P)$, $\delta_1 := |A \cap P|/|P|$ とおく。このとき、

$$N_1 \geq N_0^{1/3}, \quad \delta_1 \geq \delta_0 + \delta_0^2/8$$

が成り立つ。一般に、 $k = 0, 1, \dots$ に対して、 $\text{Find}(N_k, A_k, \delta_k)$ は A_k に 3-AP の存在を確認して手続きを終了するか、そうでなければ $\text{Find}(N_{k+1}, A_{k+1}, \delta_{k+1})$ を呼び出す。この再帰呼び出しが有限回で終了することを示そう。ここで

$$N_{k+1} \geq N_k^{1/3} \geq N_0^{(1/3)^{k+1}}, \quad \delta_{k+1} \geq \delta_k + \delta_k^2/8 \geq \delta_0 + \delta_0^2/8$$

に注意する。

したがって Find を $8/\delta_0$ 回繰り返すと^{†19}、注目している部分集合の密度は $2\delta_0$ 以上になる。そこからさらに Find を $8/(2\delta_0) = 4/\delta_0$ 回繰り返すと、密度は $4\delta_0$ 以上になる。結局、この繰り返しの総計は $(8/\delta_0)(1 + 1/2 + 1/4 + \dots) = 16/\delta_0$ 回を超えられない。つまり密度の上限が 1 であることから、 Find の再帰呼び出しは高々有限回しか実行されず、途中で必ず 3-AP の存在が確認されて手続きは終了する。

さてここまでの議論では Find が必要なだけ再帰呼び出しできる、すなわち補題 3.8 が適用できると仮定した。このためには、 $K := 16/\delta$ とおいて $k \leq K$ まで $N_k \geq 32^3\delta_k^{-6}$ であればよいが、より強く $N_k \geq 32^3\delta^{-6}$ とできる条件を考える。これを保証する N を気前よく評価しよう。そこで $N_K \geq N^{(1/3)^{16/\delta}}$ であることから、 $N^{(1/3)^{16/\delta}} \geq 32^3\delta^{-6}$ であれば十分である。 \log を 2 回とると

$$\log \log N \geq \frac{16 \log 3}{\delta} + \log 3 + \log \log 32 + \log 6 + \log \log \frac{1}{\delta},$$

すなわち $\log \log N = \Omega(1/\delta)$, 言い換えれば $\delta = \Omega(1/\log \log N)$ であればよい。これは定理の仮定 $|A| = O(N/\log \log N)$ であった。□

\mathbb{Z}_N の等差数列は $[N]$ の等差数列とは限らないことに注意しよう。 \mathbb{Z}_N の要素の代表元を $[N]$ にとると、例えば、 \mathbb{Z}_5 において $(2, 5, 3)$ は公差 3 の等差数列であるが、これは $[5]$ の等差数列ではない。

定理 3.6 (Roth). 長さ 3 の等差数列を含まない $A \subset [N]$ は、 $|A| = O(N/\log \log N)$ をみ出す。

^{†19} 正確には $\lceil 8/\delta_0 \rceil$ 回とすべきだが、煩雑になるだけで議論の本質には関わらないから、整数への丸めをいちいち表記しない。

証明. $A \subset [N]$ が長さ 3 の等差数列を含まないとする。 $M := 2N - 1$ において、 $A \subset \mathbb{Z}_M$ とみなしたとき、 A が \mathbb{Z}_M においても 3-AP を含まなければ、補題 3.9 により $|A| = O(M/\log \log M) = O(N/\log \log N)$ である。そこで $(x, y, z) \in A^3$ が $x + z - 2y \equiv 0 \pmod{M}$ をみたしたとする。このとき $\{x, y, z\} \subset [N]$ により、

$$-M < 1 + 1 - 2N \leq x + z - 2y \leq N + N - 2 < M,$$

すなわち $x + z - 2y = 0$ であるが、これは $A \subset [N]$ が 3-AP を含まないことに矛盾する。 \square

3.6 スライスランク法

この節では多項式の手法であるスライスランク法を導入し、その応用として二つの結果を紹介する。一つ目は長さ 3 の等差数列を含まない \mathbb{F}_3^n の部分集合のサイズは $(2.76)^n$ を超えないこと、二つ目は「ひまわり」とよばれる構造を含まない $[n]$ の部分集合族のサイズは $(1.9)^n$ を超えないことを主張する。

3.6.1 スライスランクと Tao の補題

対称行列は対角成分に零がなければフルランクである。この事実を「高次元化」するために関数のスライスランクを導入しよう。

有限集合 X と体 \mathbb{F} および k 変数関数 $f : X^k \rightarrow \mathbb{F}$ が与えられたとき、 f が**スライス関数**とは、 f が一変数関数 a と $k-1$ 変数関数 b の積で表されることをいう。例えば $f(x_1, x_2, x_3) = a(x_1)b(x_2, x_3)$ はスライス関数である。どんな関数 f も高々 $|X|$ 個のスライス関数の和の形に表示できる。実際、 $a_z(x) = \delta_{z,x}$, $b_z(x_2, \dots, x_k) = f(z, x_2, \dots, x_k)$ とおけば^{†20}

$$f(x_1, \dots, x_k) = \sum_{z \in X} a_z(x_1)b_z(x_2, \dots, x_k)$$

である。そこで f をスライス関数の和の形に表示するために必要なスライス関数の個数の最小値を f のスライスランクと定義し、 $\text{sr}(f)$ と書く。つまり、

$$\text{sr}(f) = \min \left\{ r : f = \sum_{i=1}^r g_i, g_1, \dots, g_r \text{ はスライス関数} \right\}$$

である。このとき $\text{sr}(f) \leq |X|$ が成り立つ。

^{†20} $\delta_{z,x}$ は $z = 1$ のとき 1, そうでないとき 0 と定める。

補題 3.10 (Tao の補題 [19]). 有限集合 X , 体 \mathbb{F} および整数 $k \geq 2$ を固定する。関数 $f: X^k \rightarrow \mathbb{F}$ が「対角条件」

$$f(x_1, \dots, x_k) \neq 0 \iff x_1 = \dots = x_k$$

をみたすならば、 $\text{sr}(f) = |X|$ である。

証明. $k = 2, 3$ の場合を示す。(後で用いるのは $k = 3$ の場合。一般の場合は k に関する帰納法で示せるが、実質的に $k = 3$ の場合の証明と同様である。)

$k = 2$ の場合。 $\text{sr}(f) \geq |X|$ を示せばよい。 $r := \text{sr}(f)$ とおくと、ある一変数関数 a_i, b_i たちによって

$$f(x, y) = \sum_{i=1}^r a_i(x) b_i(y)$$

と書ける。ここで F (または F_i) を $|X| \times |X|$ 行列で (x, y) 成分が $f(x, y)$ (または $a_i(x) b_i(y)$) であるものとする

$$F = \sum_{i=1}^r F_i$$

である。 F_i は列ベクトル $(a_i(x))_{x \in X}$ と行ベクトル $(b_i(y))_{y \in X}$ の行列としての積だから、 F_i の行列のランクは 1 で、

$$\text{rank } F \leq \sum_{i=1}^r \text{rank}(F_i) = r$$

である。一方 f は対角条件をみたすから F は対角行列で対角成分は非零であり、 $|X| = \text{rank } F \leq r = \text{sr}(f)$ がしたがう。

$k = 3$ の場合。 $f: X^3 \rightarrow \mathbb{F}$ が対角条件をみたすとし、 $r := \text{sr}(f)$ とおく。このとき、ある非零関数 a_i, b_i を用いて

$$f(x, y, z) = \sum_{i \in I} a_i(x) b_i(y, z) + \sum_{j \in J} a_j(y) b_j(x, z) + \sum_{k \in K} a_k(z) b_k(x, y) \quad (3.16)$$

と書ける。ただし $I \sqcup J \sqcup K = [r]$ であり、一般性を失わず $I \neq \emptyset$ としてよい。

すべての $i \in I$ について $\sum_{x \in X} v(x) a_i(x) = 0$ をみたす関数 $v: X \rightarrow \mathbb{F}$ 全体がなすベクトル空間を V とする。この空間は $|I|$ 本の $|X|$ 変数連立一次方程式で定義されるから、

$$\dim V \geq |X| - |I| \geq r - |I| \quad (3.17)$$

である。ここで $v \in V$ を、その台 $S = \{x \in X : v(x) \neq 0\}$ が最大になるようにとる。このとき

$$|S| \geq \dim V \quad (3.18)$$

である。というのも、もし $|S| < \dim V$ であれば、すべての $x \in S$ で $w(x) = 0$ となるような非零 $w \in V$ がある^{†21}。しかしこのとき $v + w$ は S より真に大きい台を持ち、 S の選び方に反する。

関数 $g : S^2 \rightarrow \mathbb{F}$ を $g(y, z) = \sum_{x \in X} v(x)f(x, y, z)$ と定義する。この関数のスライ斯拉ンクを二通りの方法で評価しよう。まず第一の方法として、 g を (3.16) の右辺から計算すると、第一項は $v(x)$ の性質により

$$\sum_{i \in I} \left(\sum_{x \in X} v(x)a_i(x) \right) b_i(y, z) = 0$$

である。第二項と第三項は

$$\sum_{j \in J} a_j(y)c_j(z) + \sum_{k \in K} a_k(z)c_k(y) \quad (3.19)$$

と書き換えられる。ただし

$$\begin{aligned} c_j(z) &= \sum_{x \in X} v(x)b_j(x, z) \quad j \in J \text{ のとき,} \\ c_k(y) &= \sum_{x \in X} v(x)b_k(x, y) \quad k \in K \text{ のとき} \end{aligned}$$

とした。したがって $g(y, z)$ は (3.19) の表示をもつ。つまり g は $|J| + |K|$ 個のスライス関数の和で書けるから、

$$\text{sr}(g) \leq |J| + |K| = r - |I| \quad (3.20)$$

を得る。

次に第二の方法として、 g が対角条件 $g(y, z) \neq 0 \iff y = z$ を満たすことを示そう。実際、 $y \neq z$ ならば、 f の対角条件から $f(x, y, z) = 0$ であり、 $g(y, z) = \sum_x v(x)f(x, y, z) = 0$ がしたがう。逆にもし $y = z$ ならば、 $g(y, y) = \sum_x v(x)f(x, y, y) = v(y)f(y, y, y)$ であるが、 $y \in S$ から $v(y) \neq 0$ 、 f の仮定から $f(y, y, y) \neq 0$ なので、結局 $g(y, y) \neq 0$ である。そこで $k = 2$ の場合の結果を g に適用して、 $\text{sr}(g) = |S|$ 、これと (3.20)、(3.18) から $r - |I| \geq |S| \geq \dim V$ を得る。この最後の不等式と (3.17) から、(3.17) の不等号はすべて等号でなければならず、 $|X| = r = \text{sr}(f)$ がしたがう。□

3.6.2 長さ 3 の等差数列ふたたび

定理 3.7 (Ellenberg–Gijswijt[20]). ある正定数 $c < 3$ が存在して、 $A \subset \mathbb{F}_3^n$ が長さ 3 の等差数列を含まなければ、 $|A| < c^n$ である。特に $c = 2.76$ ととれる。

^{†21} $\dim V = d$ とし、 V の基底を v_1, \dots, v_d とすると $w \in V$ は $w = \sum_{i=1}^d \alpha_i v_i$ と表せる。任意の $x \in S$ で $w(x) = 0$ と仮定し、 $|S|$ 本の d 変数連立一次方程式 $\sum_{i=1}^d \alpha_i v_i(x) = 0$ ($x \in S$) に注目しよう。もし $|S| < d$ ならばこの方程式は非自明な解 (つまり $\alpha_1 = \dots = \alpha_d = 0$ ではない解) をもち、非零 w が得られる。

証明. 正定数 c が $c < 3$ をみたす (c の値は後で決める) とし、部分集合 $A \subset \mathbb{F}_3^n$ が (非自明な) 3-AP を含まないと仮定する。 $|A| < c^n$ を示すには、次の二つの条件を満たす関数 $f: A^3 \rightarrow \mathbb{F}$ を見つければよい。

(C1) f は対角条件をみたす。

(C2) $\text{sr}(f) < c^n$ 。

このとき、これらの条件と補題 3.10 から $|A| = \text{sr}(f) < c^n$ がしたがう。 \mathbb{F}_3^n の元を $x = (x_1, \dots, x_n)$ のように表記し、 $f: A^3 \rightarrow \mathbb{F}_3$ を

$$f(x, y, z) = \prod_{i=1}^n ((x_i + y_i + z_i)^2 - 1). \quad (3.21)$$

と定める。この f が (C1) と (C2) をみたすことを確かめる。

まず (C1) を示す。 $x, y, z \in A$ のとき、 $x + y + z = 0$ と $x = y = z$ は同値である^{†22}。実際、 $x + y + z = 0$ は $x + z = 2y$ と書き換えられるが、これは (x, y, z) が広義 3-AP をなすことであり、 A の仮定から $x = y = z$ である。これをふまえると

$$\begin{aligned} f(x, y, z) \neq 0 &\iff \text{すべての } i \text{ について } (x_i + y_i + z_i)^2 \neq 1 \\ &\iff \text{すべての } i \text{ について } x_i + y_i + z_i = 0 \\ &\iff x + y + z = 0 \iff x = y = z, \end{aligned}$$

つまり f は対角条件をみたす。

次に (C2) を確かめる。 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 (3.21) 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 $i_1 + \cdots + k_n \leq 2n$ 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

$$\text{sr}(f) \leq \text{sr}(f_x) + \text{sr}(f_y) + \text{sr}(f_z) \leq 3 \text{sr}(f_x)$$

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 $f_x = \sum a(x)b(y, z)$ 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, \dots, i_n) は $(j = 1 - i$

^{†22} この条件をみたす A を cap または cap set という。

とおくことで) 次の集合

$$\begin{aligned} I &:= \{(i_1, \dots, i_n) \in \{0, 1, 2\}^n : i_1 + \dots + i_n \leq 2n/3\} \\ &= \{(j_1, \dots, j_n) \in \{-1, 0, 1\}^n : j_1 + \dots + j_n \geq n/3\} \end{aligned}$$

の要素だから、 $\text{sr}(f_x) \leq |I|$ である。そこで $|I|$ を上から評価しよう。

独立な確率変数 X_1, \dots, X_n は、各 $1 \leq i \leq n$ について $X_i \in \{-1, 0, 1\}$ を等確率でとるとする。このとき $\mathbb{E}[X_i] = 0$ であり、系 5.4 から $X := \sum_{i=1}^n X_i$ とおくと $\mathbb{P}[X > \frac{n}{3}] < e^{-n/18}$ が成り立つ。一方、 $|I| = 3^n \mathbb{P}[X \geq n/3]$ だから、 $\text{sr}(f) \leq 3|I| < 3(3e^{-\frac{1}{18}})^n < c^n$ となるような $c < 3$ がとれる。

上記の c をもっと詳しく見積もることもできる。このため $\mathbb{E}[X_i]$ のかわりに $\mathbb{E}[z^{X_i}]$ を利用する。すなわち、任意の $z \geq 1$ に対して、マルコフの不等式から

$$|I| = 3^n \mathbb{P}[X \geq n/3] = 3^n \mathbb{P}[z^X \geq z^{n/3}] \leq 3^n \mathbb{E}[z^X] z^{-\frac{n}{3}}$$

が成り立つ。ここで $\mathbb{E}[z^{X_i}] = (z^{-1} + 1 + z)/3$ より $3^n \mathbb{E}[z^X] = (z^{-1} + 1 + z)^n$ に注意すると $|I|^{\frac{1}{n}} \leq (z^{-1} + 1 + z) z^{-\frac{1}{3}}$ を得る。この右辺は、微分して調べると、 $z = (1 + \sqrt{33})/4$ のとき最小値 $\theta := \frac{3}{8}(207 + 33\sqrt{33})^{\frac{1}{3}} \approx 2.755$ をとる。したがって $A \subset \mathbb{F}_3^n$ が 3-AP を含まなければ、 $|A| \leq 3\theta^n$ である。このとき $A^2 = \{(x, x) : x \in A\} \subset \mathbb{F}_3^{2n}$ も 3-AP を含まないから、 $|A|^2 = |A^2| \leq 3\theta^{2n}$ である。同様に任意の正整数 l に対して $|A|^l \leq 3\theta^{ln}$ 、つまり $|A| \leq 3^{\frac{1}{l}} \theta^n$ である。 $l \rightarrow \infty$ として $|A| \leq \theta^n < 2.76^n$ を得る^{†23}。□

3.6.3 ひまわり

相異なる部分集合 $A, B, C \subset [n]$ が $A \cap B = B \cap C = C \cap A$ をみたすとき、これを (花びら 3 枚の) ひまわりという。

定理 3.8. ある $c < 2$ が存在して、ひまわりを含まない $\mathcal{F} \subset 2^{[n]}$ は $|\mathcal{F}| < c^n$ をみたす。さらに、ある n_0 が存在して $n \geq n_0$ ならば、 $c = 1.9$ ととれる。

証明. 以下の証明は Naslund と Sawin[21] による。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 $\mathcal{F} \subset 2^{[n]}$ がひまわりを含まないとし、 $X \subset \{0, 1\}^n$ を \mathcal{F} の特性ベクトルの集合とする。各 $0 \leq k \leq n$ について $\mathcal{F}_k = \mathcal{F} \cap \binom{[n]}{k}$ 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^{†24}：どんな 3 個のベ

^{†23} この $|A| \leq 3\theta^n$ から $|A| \leq \theta^n$ に評価を改善する手順を (tensor) power trick という。

^{†24} この条件は X_k で正しいが、 X では一般には成立しない。ひまわりのない集合族において二つの相異なる部分集合 $A \subsetneq B$ があれば、対応する特性ベクトルを x, y とするとき、 $w := x + x + y$ はすべての i で $w_i \neq 2$ である。

54 第3章 加法的組合せ論の話題から

ベクトル $x, y, z \in X_k$ もそれら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。そこで関数 $f_k : X_k^3 \rightarrow \mathbb{R}$ を

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

と定める。このとき f_k は対角条件をみたし、補題 3.10 から $\text{sr}(f_k) = |X_k|$ である。

定理 3.7 の証明と同様に $f_k = f_x + f_y + f_z$ とし、 f_x から定まる指数の集合を

$$I := \{(i_1, \dots, i_n) \in \{0, 1\}^n : i_1 + \dots + i_n \leq n/3\}$$

とおく。このとき $\text{sr}(f_k) \leq 3|I|$ である。独立な確率変数 X_1, \dots, X_n は、各 $1 \leq i \leq n$ について $X_i \in \{0, 1\}$ を等確率でとるとし、 $X := \sum_{i=1}^n X_i$ とおく。このとき任意の $0 < z \leq 1$ に対して、マルコフの不等式から

$$|I| = 2^n \mathbb{P}[X \leq n/3] = 2^n \mathbb{P}[z^X \geq z^{n/3}] \leq 2^n \mathbb{E}[z^X] z^{-n/3} = ((1+z)z^{-1/3})^n$$

である。右辺は $z = \frac{1}{2}$ で最小値 $\theta := 3/2^{2/3} \approx 1.889$ をとる。ここから $\text{sr}(f_k) \leq 3\theta^n$ 、さらに power trick から $\text{sr}(f_k) \leq \theta^n$ を得る。したがって

$$|\mathcal{F}| = |X| = \sum_{k=0}^n |X_k| = (n+1) \text{sr}(f_k) < (n+1)\theta^n$$

がしたがう。このとき、ある $c < 2$ が存在して $|\mathcal{F}| < c^n$ が成り立ち、特に $n > n_0$ ならば、 $c = 1.9$ ととれる。 \square

3.7 長さ 3 の等差数列を含まない部分集合の構成

ユークリッド空間における球面は、どんな直線とも高々 2 点でしか交わらない。まずこの性質を利用して、長さ 3 の等差数列を含まない \mathbb{F}_3^n の部分集合を構成しよう。 \mathbb{R}^n の半径 r (ただし $r^2 \in \{0, 1, \dots, 4n\}$ とする) の球面上の格子点で各座標が 0 または 1 であるものを

$$S_r(n) = \left\{ (x_1, \dots, x_n) \in \{0, 1\}^n : \sum_{i=1}^n x_i = r^2 \right\} \subset \mathbb{R}^n$$

とおく。 $x, y, z \in S_r(n)$ が $x + z = 2y$ をみたすならば、球面の凸性から $x = y = z$ である。つまり \mathbb{R}^n の部分集合としての $S_r(n)$ は、非自明な 3-AP を含まない。 $S_r(n)$ を \mathbb{F}_3^n の部分集合と考えた場合はどうか？ \mathbb{F}_3 の加法は、 \mathbb{R} の加法とは異なって $1 + 2 = 0$ 、 $2 + 2 = 1$ であるが、 $S_r(n)$ の各座標は 2 を含まないため、 $S_r(n)$ の二元の加法でこのようなことは生じない。したがって $S_r(n) \subset \mathbb{F}_3^n$ においても $x + z = 2y$ ならば $x = y = z$ であり、 $S_r(n)$ は \mathbb{F}_3^n の部分集合としても非自明な 3-AP を含まない。 $\bigcup_r S_r(n)$ に含まれ

る格子点の総数は 2^n であり、半径は $4n+1$ 通りあるから、鳩の巣原理により、ある r において $|S_r(n)| \geq \frac{2^n}{4n+1}$ が成り立つ。

事実 3.1. 長さ 3 の等差数列を含まない $A \subset \mathbb{F}_3^n$ で $|A| \geq \frac{2^n}{4n+1}$ のものがある^{†25}。

球面の凸性を利用するアイデアは Behrend によるもので、彼は $[N]$ において 3-AP を含まない大きな部分集合を構成した。

定理 3.9 (Behrend[23]). 長さ 3 の等差数列を含まない部分集合 $A \subset [N]$ で $|A| = N \cdot 2^{-(2\sqrt{2}+o(1))\sqrt{\log_2 N}}$ をみたすものがある。

証明. d, m, N を (後で指定する) 十分大きい整数とし、 $(2m-1)^d \leq N < (2m+1)^d$ とする。非負整数 r は $r^2 \leq d(m-1)^2$ をみたすとする。このとき $x \in [N]$ を $(2m-1)$ 進法で表示し、次の部分集合

$$S_r(d, m) := \left\{ x = \sum_{i=1}^d x_i (2m-1)^{i-1} : 0 \leq x_i < m, \sum_{i=1}^d x_i^2 = r^2 \right\} \subset [N]$$

を考える。 $S_r(d, m)$ は $(2m-1)$ 進 d 桁、かつどの桁も m 未満で、さらに「ノルム」が r の整数の集合である。 m, d, r をうまく選ぶと、この集合が定理の A の条件をみたすことを示す。

まず $S_r(d, m)$ は非自明な 3-AP を含まないことを確かめよう。 $x, y \in S_r(d, m)$ のとき、 $x+y$ を $(2m-1)$ 進で計算すると、桁の繰上りが生じない、つまりどの i についても $x_i + y_i < 2m-1$ である。この性質から、 $x \in S_r(d, m)$ を $(x_1, \dots, x_d) \in \mathbb{R}^d$ に対応させる単射を f とすると、 $f(x+y) = f(x) + f(y)$ が成り立つ。ここで $S' := f(S_r(d, m))$ は \mathbb{R}^d の半径 r の球面上にある。球面の凸性から、球面上の異なる 3 点は同一直線上にはない。特に、 $x', y', z' \in S'$ が $x' + z' = 2y'$ を満たすならば、 $x' = y' = z'$ である。さて、 $S_r(d, m)$ に広義 3-AP (x, y, z) があれば、 $x+z = 2y$ を満たす。このとき $f(x) + f(z) = f(x+z) = f(2y) = 2f(y)$ だから、 $f(x) = f(y) = f(z)$ であり、 f は単射だから $x = y = z$ である。したがって $S_r(d, m)$ に非自明な 3-AP はない。

あとは $S_r(d, m)$ のサイズが大きくなるようにパラメタを調整する。はじめに r を選ぶ。半径 r は $0 \leq r^2 \leq d(m-1)^2$ を満たすから、半径の種類は高々 $d(m-1)^2 + 1$ である。また $(2m-1)$ 進 d 桁で各桁 m 未満の整数の総数は、 m^d である。したがって鳩の巣原理からある r に対して $|S_r(d, m)| \geq m^d / (d(m-1)^2 + 1) > m^{d-2} / d$ が成り立つ。さらに

^{†25} Edel[22] の有限射影空間における cap の研究から、 $A \subset \mathbb{F}_3^n$ で 3-AP を含まず $|A| > 2.21^n$ のものが存在することが知られている。

$d := \sqrt{2 \log_2 N}$ とおいて $2m + 1 > N^{\frac{1}{d}}$ を用いると、 N が大きいとき

$$\begin{aligned} |S_r(d, m)| &> \frac{m^{d-2}}{d} > \frac{(N^{\frac{1}{d}} - 1)^{d-2}}{d 2^{d-2}} = \frac{N^{1-\frac{2}{d}}}{d 2^{d-2}} \left(1 - N^{-\frac{1}{d}}\right)^{d-2} > \frac{N^{1-\frac{2}{d}}}{d 2^{d-1}} \\ &= N^{1-\frac{2}{d} - \frac{\log d + (d-1) \log 2}{\log N}} = N \cdot 2^{-(2\sqrt{2} + o(1))\sqrt{\log_2 N}} \end{aligned}$$

を得る。

□

最近、Elsholtz ら [18] は、3-AP を含まない $[N]$ の部分集合でサイズが

$$N \cdot 2^{-(2\sqrt{\log_2(24/7)} + o(1))\sqrt{\log_2 N}}$$

のものを構成した。また彼らは、ある定数 $c > 1/2$ が存在して、任意の奇素数 p と十分大きな n に対して、3-AP を含まない \mathbb{F}_p^n の部分集合でサイズが $(cp)^n$ 以上の部分集合の存在を示した。

参考文献

- [1] T. Kövári, V. T. Sós and P. Turán, On a problem of K. Zarankiewicz, *Colloq. Math.* **3** (1954), 50–57; MR0065617
- [2] E. Szemerédi and W. T. Trotter Jr., Extremal problems in discrete geometry, *Combinatorica* **3** (1983), no. 3-4, 381–392; MR0729791
- [3] L. A. Székely, Crossing numbers and hard Erdős problems in discrete geometry, *Combin. Probab. Comput.* **6** (1997), no. 3, 353–358; MR1464571
- [4] M. Ajtai, V. Chvátal, M. M. Newborn, E. Szemerédi, Crossing-free subgraphs, in *Theory and practice of combinatorics*, 9–12, North-Holland Math. Stud. Ann. Discrete Math., 60 12, North-Holland, Amsterdam, ; MR0806962
- [5] F. T. Leighton. Complexity issues in VLSI: optimal layouts for the shuffle-exchange graph and other networks. MIT Press Cambridge, MA, USA 1983.
- [6] P. Erdős, E. Szemerédi. On sums and products of integers. *Studies in Pure Mathematics*, 1983, 213–218.
- [7] G. Elekes. On the number of sums and products. *Acta Arith.* 81 (1997), 365–367.
- [8] L. Guth, *Polynomial methods in combinatorics*, University Lecture Series, 64, Amer. Math. Soc., Providence, RI, 2016; MR3495952
- [9] T. C. Tao and V. H. Vu, *Additive combinatorics*, Cambridge Studies in Advanced Mathematics, 105, Cambridge Univ. Press, Cambridge, 2006; MR2289012
- [10] T. Gowers, Introduction to additive combinatorics, <https://drive.google.com/file/d/1ut0mUqSyPMweoxoDTfhXverEONyFgcU0/view>
- [11] I. Kantor, J. Matoušek and R. Šámal, *Mathematics++*, Student Mathematical Library, 75, Amer. Math. Soc., Providence, RI, 2015; MR3379631
- [12] B. J. Green, Finite field models in additive combinatorics, in *Surveys in combinatorics 2005*, 1–27, London Math. Soc. Lecture Note Ser., 327, Cambridge Univ. Press, Cambridge, ; MR2187732 (ちなみに、<https://arxiv.org/abs/math/0409420> のタイトルは Finite field models in arithmetic combinatorics である。)
- [13] J. Wolf, Finite field models in arithmetic combinatorics—ten years on, *Finite Fields Appl.* **32** (2015), 233–274; MR3293412
- [14] S. Peluse, Recent progress on bounds for sets with no three terms in arithmetic progression [after Bloom and Sisask, Croot, Lev, and Pach, and Ellenberg and

- Gijswijt], Astérisque No. 438 (2022), Exp. No. 1196, 547–581; MR4576028
- [15] S. Peluse, Finite field models in arithmetic combinatorics—twenty years on, in *Surveys in combinatorics 2024*, 159–199, London Math. Soc. Lecture Note Ser., 493, Cambridge Univ. Press, Cambridge, ; MR4749041
 - [16] T. Bloom, Additive combinatorics, <http://thomasbloom.org/teaching/AC2021.pdf>
 - [17] Y. Zhao, *Graph theory and additive combinatorics—exploring structure and randomness*, Cambridge Univ. Press, Cambridge, 2023; MR4603631
 - [18] C. Elsholtz, Z. Hunter, L. Proske, L. Sauermann, Improving Behrend’s construction: Sets without arithmetic progressions in integers and over finite fields <https://doi.org/10.48550/arXiv.2406.12290>
 - [19] 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>
 - [20] 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.
 - [21] E. Naslund, W. Sawin. Upper bounds for sunflower-free sets. *Forum Math. Sigma* 5 (2017), e15, 10 pp.
 - [22] Y. Edel, Extensions of generalized product caps, *Des. Codes Cryptogr.* **31** (2004), no. 1, 5–14; MR2031694
 - [23] F. A. Behrend, On sets of integers which contain no three terms in arithmetical progression, *Proc. Nat. Acad. Sci. U.S.A.* **32** (1946), 331–332; MR0018694

第 4 章

正則化の手法

正則化の手法は組合せ論における最も重要な手法のひとつである。この章ではその出発点である Szemerédi の正則化補題 [1] とその基本的な応用例を紹介する。グラフの正則化は、与えられたグラフをランダムグラフのように見る見方を提供する。その見方の下で、例えば指定された部分構造の個数を評価する数え上げ補題が得られる。この正則化と数え上げは密接に関連し、どのように正則化すべきかは適用したい問題に依存する。taylored regularity lemma という言い方もある。つまり正則化の定義や正則化補題の定式化には一定の自由度がある。この章の記述は Schacht[2] の定式化にしたがう^{†1}。

4.1 正則化補題

4.1.1 正則化補題の定式化と指数の性質

グラフ $G = (V, E)$ において、 V の部分集合 U, W が共通部分をもたないとする。このとき

$$e(U, W) = \#\{u, w\} : u \in U, w \in W\}$$

とおく。つまり $e(U, W)$ は U, W 間の辺の本数である。実数 $\epsilon > 0$ と $d \geq 0$ が与えられたとき、ペア (U, W) が (ϵ, d) 正則とは、任意の $A \subset U$ と $B \subset W$ について

$$|e(A, B) - d|A||B|| \leq \epsilon|U||W|$$

をみたすことである。さらにペア (A, B) の密度を

$$d(A, B) = \frac{e(A, B)}{|A||B|}$$

と定める。ただし $|A||B| = 0$ のときは $d(A, B) = 0$ とする。ペア (U, W) が $(\epsilon, d(U, W))$ 正則の場合には、これを単に ϵ 正則ともいう。

^{†1} この定式化の利点は、(この章では扱わないが) 一般の k グラフ (ハイパーグラフ) への拡張が自然におこなえることである。

定理 4.1 (正則化補題). 任意の実数 $0 < \epsilon < \frac{1}{2}$ と $t_0 \in \mathbb{N}$ に対して、ある $T_0 = T_0(\epsilon, t_0) \in \mathbb{N}$ が存在して、任意の $n \geq T_0$ と n 頂点グラフ $G = (V, E)$ に対して、頂点集合の分割

$$V = V_0 \sqcup V_1 \sqcup \cdots \sqcup V_t \quad (4.1)$$

が存在して、次をみたす。

- (i) $|V_0| \leq \epsilon n$, $|V_1| = \cdots = |V_t|$.
- (ii) $t_0 \leq t \leq T_0$.
- (iii) $\binom{t}{2}$ 個のペア (V_i, V_j) ($1 \leq i < j \leq t$) のうち、 ϵ 正則でないペアの個数は高々 ϵt^2 である。

頂点集合の分割 (4.1) を $\mathcal{P} = (V_0, V_1, \dots, V_t)$ と表記する。定理の証明のために、分割 \mathcal{P} の指数 $\text{ind}(\mathcal{P})$ を導入する。

$$\text{ind}(\mathcal{P}) := \frac{1}{|V|^2} \sum_{1 \leq i < j \leq t} d(V_i, V_j)^2 |V_i| |V_j|.$$

指数には次の性質がある。

- (P1) 指数は $1/2$ を超えない。
- (P2) 指数は分割を細分しても減らない。
- (P3) 指数は ϵ 正則でないペアを細分すると増える。

これらの性質が示されると、 ϵ 正則でないペアの細分を有限回繰り返して、ついにはすべてのペアを ϵ 正則にできる。これが定理の証明の基本アイデアである。

上記の (P1) は簡単で、次の計算からわかる。

$$\text{ind}(\mathcal{P}) \leq \frac{1}{|V|^2} \sum_{1 \leq i < j \leq t} \frac{e(V_i, V_j)^2}{|V_i| |V_j|} \leq \frac{1}{|V|^2} \sum_{1 \leq i < j \leq t} e(V_i, V_j) \leq \frac{|E|}{|V|^2} \leq \frac{1}{2}.$$

次に (P2) を示す。まず、分割 $\mathcal{P}' = (W_1, \dots, W_s)$ が分割 $\mathcal{P} = (U_1, \dots, U_t)$ の細分であるとは、任意の W_j について $W_j \subset U_i$ をみたす U_i が存在することをいう。このとき $\mathcal{P}' \preceq \mathcal{P}$ と表記する。

実数 x_1, \dots, x_k と非零実数 a_1, \dots, a_k に対して

$$\frac{x_1^2}{a_1^2} + \cdots + \frac{x_k^2}{a_k^2} \geq \frac{(x_1 + \cdots + x_k)^2}{a_1^2 + \cdots + a_k^2} \quad (4.2)$$

が成り立つ。これはベクトル $\mathbf{x} = (x_1/a_1, \dots, x_k/a_k)$ と $\mathbf{y} = (a_1, \dots, a_k)$ にコーシー・シュワルツの不等式 $|\mathbf{x}|^2 |\mathbf{y}|^2 \geq (\mathbf{x} \cdot \mathbf{y})^2$ を適用して得られる。

補題 4.1. 二部グラフ $G = (U \sqcup W, E)$ と U の分割 $U = U_1 \sqcup U_2$ に対して、

$$\sum_{i=1}^2 d(U_i, W)^2 |U_i| |W| \geq d(U, W)^2 |U| |W|$$

が成り立つ。

証明. $i = 1, 2$ に対して、 $e_i = e(U_i, W)$, $u_i = |U_i|$, さらに $w = |W|$ とおくと、 $d(U_i, W)^2 |U_i| |W| = e_i^2 / (u_i w)$ である。したがって目標の不等式の左辺は (4.2) より

$$\frac{e_1^2}{u_1 w} + \frac{e_2^2}{u_2 w} \geq \frac{(e_1 + e_2)^2}{u_1 w + u_2 w} = \frac{e(U, W)^2}{|U| |W|} = d(U, W)^2 |U| |W|$$

と評価できる。 \square

この補題を繰り返し適用することで、

$$U = U_1 \sqcup \cdots \sqcup U_s, \quad W = W_1 \sqcup \cdots \sqcup W_t$$

のときに

$$\sum_{i=1}^s \sum_{j=1}^t d(U_i, W_j)^2 |U_i| |W_j| \geq d(U, W)^2 |U| |W|$$

を得る。これは (P2) を意味する。

最後に (P3) を補題 4.2 の形で提示する。分割 $\mathcal{P} = (U, W)$ において、 $U_1 \subset U$ と $W_1 \subset W$ があって、ペア (U_1, W_1) の密度が全体の密度 $d(U, W)$ からずれているとしよう。このずれをパラメタ η によって測る。このとき \mathcal{P} を細分して分割 $\mathcal{Q} = (U_1, U_2, W_1, W_2)$ を作ると、 \mathcal{Q} の指数は \mathcal{P} の指数より η に応じて増加する。これを次の補題のように定式化できる。

補題 4.2. 二部グラフ $G = (U \sqcup W, E)$ と頂点集合の分割 $U = U_1 \sqcup U_2$, $W = W_1 \sqcup W_2$ に対して、実数 η を用いて

$$e(U_1, W_1) = d(U, W) |U_1| |W_1| + \eta |U_1| |W| \quad (4.3)$$

と表したとき、

$$\sum_{i=1}^2 \sum_{j=1}^2 d(U_i, W_j)^2 |U_i| |W_j| \geq (d(U, W)^2 + 4\eta^2) |U| |W|$$

が成り立つ。

証明. $i = 1, 2$ に対して、 $e_{i,j} = e(U_i, W_j)$, $u_i = |U_i|$, $w_j = |W_j|$ とおくと、 $d(U_i, W_j)^2 |U_i| |W_j| = e_{i,j}^2 / (u_i w_j)$ と表せる。さらに $d = d(U, W)$, $u = |U|$, $w = |W|$ とおくと目標の不等式の左辺は次のように評価できる。

$$\frac{e_{1,1}^2}{u_1 w_1} + \left(\frac{e_{1,2}^2}{u_1 w_2} + \frac{e_{2,1}^2}{u_2 w_1} + \frac{e_{2,2}^2}{u_2 w_2} \right) \geq \frac{(du_1 w_1 + \eta u w)^2}{u_1 w_1} + \frac{(e_{1,2} + e_{2,1} + e_{2,2})^2}{u_1 w_2 + u_2 w_1 + u_2 w_2}. \quad (4.4)$$

ここで左辺 1 項には (4.3) を、残り 3 項の和には (4.2) を用いた。次に再び (4.3) を用いて $e_{1,2} + e_{2,1} + e_{2,2} = e(U, V) - e_{1,1} = duw - (du_1w_1 + \eta uw)$ を得る。これと $u_1w_2 + u_2w_1 + u_2w_2 = uw - u_1w_1$ より (4.4) の右辺は

$$\frac{(du_1w_1 + \eta uw)^2}{u_1w_1} + \frac{(duw - du_1w_1 - \eta uw)^2}{uw - u_1w_1} = d^2uw + \eta \frac{u^3w^3}{(uw - u_1w_1)u_1w_1} \quad (4.5)$$

と書き換えられる。最後に $2\sqrt{(uw - u_1w_1)u_1w_1} \leq (uw - u_1w_1) + u_1w_1 = uw$ を (4.5) の右辺第 2 項の分母に用いて、目標の不等式を得る。 \square

4.1.2 正則化補題の証明

$0 < \epsilon < \frac{1}{2}$ と $t_0 \geq 1$ が与えられたとする。数列 t_0, t_1, \dots を再帰的に

$$t_i := \left\lceil \frac{t_{i-1}2^{i+t_{i-1}}}{\epsilon} \right\rceil$$

と定め、 $T_0 := t_{\lfloor 1/\epsilon^3 \rfloor}$ とおく。 $n \geq T_0$ と n 頂点グラフ $G = (V, E)$ が与えられたとする。定理 4.1 の条件 (i)–(iii) をみたす分割 \mathcal{P} が存在することを示す。

$s_0 = t_0$ とし、分割 $\mathcal{P}^0 = (V_0^0, V_1^0, \dots, V_{s_0}^0)$ を $|V_1^0| = \dots = |V_{s_0}^0| = \lfloor n/s_0 \rfloor$ をみたすように (任意に) 作る。つまり V を s_0 個のサイズが等しい部分集合に分け、残り (V_0^0) のサイズを最小にする。このとき $t_1 \geq s_0 2^{1+s_0}/\epsilon > 2s_0/\epsilon$ より

$$|V_0^0| < s_0 \leq \frac{\epsilon}{2} t_1 \leq \frac{\epsilon}{2} T_0 \leq \frac{\epsilon}{2} n$$

である。したがって \mathcal{P}^0 は $t = s_0$ に対して (i), (ii) をみたす。もし (iii) もみたせば \mathcal{P}^0 が定理の条件をみたす分割である。そこで \mathcal{P}^0 は (iii) をみたさないとしよう。

以下、 $i = 1, 2, \dots$ の順に分割 $\mathcal{P}^i = (V_0^i, V_1^i, \dots, V_{s_i}^i)$ を構成したいが、その際、直前の \mathcal{P}^{i-1} は次の (i'), (ii') をみたすことを要請する。(具体的な構成法は後述する。)

(i') $|V_0^{i-1}| \leq (1 - 2^{-i})\epsilon n$, $|V_1^{i-1}| = \dots = |V_{s_{i-1}}^{i-1}|$.

(ii') $t_0 \leq s_{i-1} \leq t_{i-1}$.

さらに、 \mathcal{P}^i は \mathcal{P}^{i-1} を細分して作りたいが、 V_0^i は各細分で生じるゴミを回収するため一般には $V_0^{i-1} \subset V_0^i$ となってしまうので、この部分が細分の定義をみたさない。そこで形式的に細分の定義が適用できるように、 \mathcal{P}^i に対応する分割 $\mathcal{P}^{\cdot i}$ を定義する。これは \mathcal{P}^i において V_0^i をさらに一点集合に分割したものである。すなわち $V_0^i = \{v_1, \dots, v_m\}$ のとき $\mathcal{P}^{\cdot i} := (\{v_1\}, \dots, \{v_m\}, V_1^i, \dots, V_{s_i}^i)$ と定める。このとき、 \mathcal{P}^i は $\mathcal{P}^{\cdot i-1} \succ \mathcal{P}^{\cdot i}$ をみたすように構成する。

もし \mathcal{P}^{i-1} が (i'), (ii') に加えて次の条件もみたしたとしよう。

(iii') $\binom{s_{i-1}}{2}$ 個のペア (V_a, V_b) ($1 \leq a < b \leq s_{i-1}$) のうち、 ϵ 正則でないペアの個数は高々 ϵs_{i-1}^2 である。

このとき、 \mathcal{P}^{i-1} は (i)–(iii) をみたし、定理が得られる。そこで \mathcal{P}^{i-1} は (iii') をみたさないとしよう。このとき \mathcal{P}^{i-1} を細分して \mathcal{P}^i をつくると、実は

$$\text{ind}(\mathcal{P}^i) \geq \text{ind}(\mathcal{P}^{i-1}) + \epsilon^3 \quad (4.6)$$

が成り立つ (ことを後で示す)。しかし (P1) より指数は $1/2$ を超えないから、 $i > 1/(2\epsilon^3)$ となることはない。つまり有限回の細分の後に、ある \mathcal{P}^i で必ず (iii') がみたされ、定理が得られる。

したがって証明を完成させるには、 \mathcal{P}^{i-1} が (i'), (ii') をみたし (iii') をみたさないと仮定して、 \mathcal{P}^i を (i'), (ii') (の $i-1$ を i にかえたもの) をみたすように構成し、(4.6) を示せばよい。

さて \mathcal{P}^{i-1} は (iii') をみたさないから、 ϵ 正則でないペアがたくさんある。そこで

$$I = \{\{a, b\} : (V_a^{i-1}, V_b^{i-1}) \text{ は } \epsilon \text{ 正則でない}\}$$

とおくと、

$$|I| > \epsilon s_{i-1}^2 \quad (4.7)$$

である。各 $\{a, b\} \in I$ には対応する $(U_a^b, U_b^a) \in V_a^{i-1} \times V_b^{i-1}$ がある。この (U_a^b, U_b^a) を $(\{a, b\} \in I \text{ であることの})$ witness という。 V_1^{i-1} に注目して、 $\{1, b\} \in I$ となる b が例えば 3 と 7 だったとしよう。このとき $W_1^b = V_1^{i-1} \setminus U_1^b$ とおくと、witnesses によって次の分割が得られる。(図)

$$V_1^{i-1} = (U_1^3 \cap U_1^7) \sqcup (U_1^3 \cap W_1^7) \sqcup (W_1^3 \cap U_1^7) \sqcup (W_1^3 \cap W_1^7).$$

これを V_1^{i-1} のベン図分解とよぼう。一般に V_j^{i-1} に $\{j, b\} \in I$ となる b が k 個あれば、 V_j^{i-1} はベン図分解により高々 $2^k \leq 2^{s_{i-1}-1}$ 個に分割される。この分割をすべての $1 \leq j \leq s_{i-1}$ におこなうと、 $V \setminus V_0^{i-1}$ は高々

$$s_{i-1} 2^{s_{i-1}-1} \leq \frac{1}{2} t_{i-1} 2^{t_{i-1}} \quad (4.8)$$

個に分割される。 $s_{i-1} 2^{s_{i-1}-1} \leq \frac{1}{2} t_{i-1} 2^{t_{i-1}}$ 個に分割される。これらの分割に V_0^{i-1} を加えた V の分割を \mathcal{Q} とおく。このとき V_0^{i-1} をさらに一点ずつに分割して得られる分割 \mathcal{Q}^i は \mathcal{P}^{i-1} の細分だから、補題 4.2 を用いると

$$\text{ind}(\mathcal{Q}^i) \geq \text{ind}(\mathcal{P}^{i-1}) + \frac{1}{n^2} \sum_{\{a,b\} \in I} 4\eta_{a,b}^2 |V_a^{i-1}| |V_b^{i-1}|$$

を得る。ただし $|\eta_{a,b}| > \epsilon$ である。そこで上式右辺の二項目は

$$\geq \frac{1}{n^2} |I| 4\epsilon^2 \left(\frac{n - |V_0^{i-1}|}{s_{i-1}} \right)^2$$

と評価できる。さらに (4.7) と $|V_0^{i-1}| \leq (1 - 2^i)\epsilon n \leq \epsilon n \leq \frac{n}{2}$ を用いると

$$\text{ind}(\mathcal{Q}_{..}) \geq \text{ind}(\mathcal{P}_{..}^{i-1}) + \epsilon^3 \quad (4.9)$$

がしたがう。分割 \mathcal{Q} の V_0^{i-1} 以外の部分をサイズが $\lceil \frac{n}{t_i} \rceil$ の部分集合に細分し、このサイズに足りなかった部分をすべて V_0^{i-1} に加えたものを V_0^i として、分割 $\mathcal{P}^i = (V_0^i, V_1^i, \dots, V_{s_i}^i)$ をつくる。このとき (4.8) と (4.7) から

$$|V_0^i \setminus V_0^{i-1}| \leq \frac{1}{2} t_{i-1} 2^{t_{i-1}} \left(\left\lceil \frac{n}{t_i} \right\rceil - 1 \right) \leq \frac{t_{i-1} 2^{t_{i-1}} n}{2t_i} \leq 2^{-(i+1)} \epsilon$$

である。これと (i') から

$$|V_0^i| = |V_0^{i-1}| + |V_0^{i-1} \setminus V_0^i| \leq (1 - 2^{-i})\epsilon n + 2^{-(i+1)}\epsilon n = (1 - 2^{-(i+1)})\epsilon n$$

を得る。また $|V_1^i| = \dots = |V_{s_i}^i|$ だから、 \mathcal{P}^i は (i') と (ii') (の $i-1$ を i にかえたもの) をみたす。また $\mathcal{P}_{..}^i$ は $\mathcal{Q}_{..}$ の細分だから補題 4.1 より $\text{ind}(\mathcal{P}_{..}^i) \geq \text{ind}(\mathcal{Q}_{..})$ であり、これと (4.9) から (4.6) が成り立つ。これで定理 4.1 の証明が完了した。 \square

正整数 t_0 と $N := \lceil 1/\epsilon \rceil$ が与えられたとき、数列 a_i を $a_0 := 2^{t_0}$, $a_i := 2^{a_{i-1}}$ ($i \geq 1$) と定め、数列 s_i を $s_i = a_{N_i}$ と定める。このとき $t_i \leq s_i$ が成り立ち、

$$s_i = 2^{2^{2^{\cdot^{\cdot^{\cdot^{2^{t_0}}}}}}} \quad (4.10)$$

のタワーの高さは $Ni + 1$ である。 $T_0 = t_{\lfloor 1/\epsilon^3 \rfloor}$ であるから、 T_0 は (4.10) の形のタワーで高さが $1/\epsilon$ の多項式のもので上から押さえられる。一方、Gowers は T_0 の下界も 2 べきのタワーで高さが $1/\epsilon$ の関数であることを示した。現在では Fox と Lovász により T_0 の上界も下界も 2 べきのタワーで高さが $1/\epsilon^2$ のオーダーであることがわかっている。

4.2 数え上げ補題と除去補題

4.2.1 数え上げ補題

グラフ F, G に対して、 $\phi: V(F) \rightarrow V(G)$ が準同型写像であるとは、任意の $i, j \in V(F)$ に対して $ij \in E(F)$ ならば $\phi(i)\phi(j) \in E(G)$ が成り立つことである。 G における F のラベル付きコピーとは、 F の単射準同型 (injective homomorphism) による像のことをいう。例えば、 $F = K_2$, $G = K_3$ のとき、 G には F のラベル付きコピーが 6 個あり、 $F = G = K_3$ のときも 6 個である。

条件を追加して $V(F) = [l]$, $V(G) = V_1 \sqcup \dots \sqcup V_l$ であるとき、 F から G への単射準同型 ϕ で各 $i \in [l]$ について $\phi(i) \in V_i$ をみたすものの全体を $\text{Hom}_l(F, G)$ とかく。 $\phi \in \text{Hom}_l(F, G)$ を表すとき、記号を濫用して $\phi: F \rightarrow G$ ともかく。

図

$\text{Hom}_l(F, G)$ の元は G における F のラベル付きコピーであるが、さらに頂点の並び順が制限されていることに注意する。 $h_l(F, G) = |\text{Hom}_l(F, G)|$ とおく。

定理 4.2. l 頂点グラフ $F = ([l], E_F)$ と l 部グラフ $G = (V_1 \sqcup \cdots \sqcup V_l, E_G)$, ただし $|V_1| = \cdots = |V_l| = m$, および実数 $\epsilon > 0$ が与えられ、ペア (V_i, V_j) は $ij \in E_F$ ならば (ϵ, d_{ij}) 正則であるとする。このとき

$$\left| h_l(F, G) - m^l \prod_{uw \in E_F} d_{uw} \right| \leq \epsilon |E_F| m^l \quad (4.11)$$

が成り立つ。

証明. $|E_F|$ に関する帰納法で (4.11) を証明する。 $|E_F| = 1$ のとき、 $E_F = \{12\}$ としてよい。 $h_l(F, G) = e(V_1, V_2)m^{l-2}$ だから、(4.11) は

$$|e(V_1, V_2)m^{l-2} - d_{12}|V_1||V_2|m^{l-2}| \leq \epsilon |V_1||V_2|m^{l-2}$$

と書け、これは (V_1, V_2) が (ϵ, d_{12}) 正則であることと同値である。

$|E_F| > 1$ とし、辺数が $|E_F|$ より小さい l 頂点グラフから G への単射準同型については定理が成り立つと仮定する。 F の辺 ab を固定し、 F からこの辺を除去した全域部分グラフを F' とおく。 $x, y \in V(G)$ に対して、 $\mathbf{1}_G(x, y)$ は $xy \in E(G)$ ならば 1, そうであれば 0 と定める。 $\phi \in \text{Hom}_l(F, G)$ であることと、 $\phi \in \text{Hom}_l(F', G)$ かつ $\phi(a)\phi(b) \in E(G)$ は等価だから、

$$h_l(F, G) = \sum_{\phi \in \text{Hom}_l(F', G)} \mathbf{1}_G(\phi(a), \phi(b))$$

と表せる。 $d = d_{a,b}$, $H' = \text{Hom}_l(F', G)$ において、上式右辺を

$$\sum_{\phi \in H'} (\mathbf{1}_G(\phi(a), \phi(b)) - d + d) = \sum_{\phi \in H'} (\mathbf{1}_G(\phi(a), \phi(b)) - d) + d \cdot h_l(F', G) \quad (4.12)$$

と書き直す。右辺の二項目を評価するため、 $h_l(F', G)$ に帰納法の仮定を適用して

$$\begin{aligned} \left| d \cdot h_l(F', G) - m^l \prod_{uw \in E_F} d_{uw} \right| &= d \left| h_l(F', G) - m^l \prod_{uw \in E_{F'}} d_{uw} \right| \\ &\leq d\epsilon |F'| m^l \leq \epsilon |F'| m^l \end{aligned}$$

を得る。つまり (4.12) の第 2 項は

$$\begin{aligned} d \cdot h_l(F', G) &\leq dm^l \prod_{uw \in E_{F'}} d_{uw} + \epsilon |E_{F'}| m^l \\ &= m^l \prod_{uw \in E_F} d_{uw} + \epsilon (|E_F| - 1) m^l \end{aligned}$$

と評価できる。したがって (4.11) を示すには

$$\left| \sum_{\phi \in H'} (\mathbf{1}_G(\phi(a), \phi(b)) - d) \right| \leq \epsilon m^l$$

を確かめればよい。 F から 2 頂点 a, b を除去した部分グラフを F^* とし、 $H^* = \text{Hom}_l(F^*, G)$ とおく。 $\psi^* \in H^*$ に対して、 $H'(\psi^*) \subset H'$ を次の条件をみたす $\phi \in H'$ の集合と定める：すなわち、 ϕ の定義域を $[l] \setminus \{a, b\}$ に制限したものが ψ^* に一致する。 H' の準同型を H^* の準同型で同値類に分けて数えると

$$\begin{aligned} \left| \sum_{\phi \in H'} (\mathbf{1}_G(\phi(a), \phi(b)) - d) \right| &= \left| \sum_{\psi^* \in H^*} \sum_{\phi \in H'(\psi^*)} (\mathbf{1}_G(\phi(a), \phi(b)) - d) \right| \\ &\leq \sum_{\psi^* \in H^*} \left| \sum_{\phi \in H'(\psi^*)} (\mathbf{1}_G(\phi(a), \phi(b)) - d) \right| \end{aligned} \quad (4.13)$$

である。ここで固定された $\psi^* \in H^*$ を拡張して得られる $\phi \in H'(\psi^*)$ においては、 $\phi(a)$ に次の制限が生じる。すなわち、 $u \in N_{F'}(a)$ をみたす各 u について $\phi(a) \in N_G(\psi^*(u))$ でなければならない。つまり

$$W_a := V_a \cap \bigcap_{u \in N_{F'}(a)} N_G(\psi^*(u))$$

とおくと $\phi(a) \in W_a$ である。同様に W_b も定めると $\phi(b) \in W_b$ である。よって

$$\begin{aligned} \left| \sum_{\phi \in H'(\psi^*)} (\mathbf{1}_G(\phi(a), \phi(b)) - d) \right| &= \left| \sum_{x \in W_a, y \in W_b} (\mathbf{1}_G(x, y) - d) \right| \\ &= |e_G(W_a, W_b) - d|W_a||W_b|| \\ &\leq \epsilon m^2 \end{aligned}$$

がしたがう。最後の不等式に (V_a, V_b) が (ϵ, d) 正則であることを用いた。これと (4.13) および $|H^*| = |\text{Hom}_l(F^*, G)| \leq m^{l-2}$ から

$$\left| \sum_{\phi \in H'(\psi^*)} (\mathbf{1}_G(\phi(a), \phi(b)) - d) \right| \leq |H^*| \epsilon m^2 \leq \epsilon m^l$$

を得る。これが確かめたいことであった。 \square

4.2.2 除去補題

定理 4.3. l 頂点 e 辺グラフ F と実数 $0 < \rho < \frac{1}{2}$ が与えられたとき、ある実数 $\eta > 0$ と正整数 n_0 が存在して次が成り立つ。グラフ $G = (V, E)$ が $|V| = n \geq n_0$ をみたし、 G

に含まれる F のラベル付きコピーの個数が高々 ηn^l ならば、ある $E_* \subset E$ が存在して、 $|E_*| \leq \rho n^2$ であるが $G' = (V, E \setminus E_*)$ は F を部分グラフに含まない。

証明. 正則化補題を利用するため、定数 ϵ, t_0 を以下のように設定する。

$$\epsilon = \frac{\rho^e}{4e} \leq \frac{\rho}{8}, \quad t_0 = \left\lceil \frac{2}{\rho} \right\rceil. \quad (4.14)$$

定理 4.1 より $T_0 = T_0(\epsilon, t_0)$ を得る。これを用いて定数 η, n_0 を以下のように設定する。

$$\eta = \frac{3\rho^e}{4(2T_0)^l}, \quad n_0 = T_0. \quad (4.15)$$

グラフ $G = (V, E)$ は $|V| = n \geq n_0$ をみたすとする。定理 4.1 と (4.14) の第 2 式から、分割 $V = V_0 \sqcup V_1 \sqcup \cdots \sqcup V_t$ が存在して

$$\frac{2}{\rho} \leq t_0 \leq t \leq T_0, \quad (4.16)$$

および $|V_0| \leq \epsilon n$, $|V_1| = \cdots = |V_t|$ をみたし、 ϵ 正則でないペア (V_i, V_j) の個数は高々 ϵt^2 である。

次に除去する辺の集合 E_* を定める。これは数え上げに不都合な辺たちで、ゴミ箱およびその周辺の辺、 V_i の内部の辺、 ϵ 正則でないペア間の辺、密度が低いペア間の辺である。正確に述べると、以下に当てはまる x または y があれば、辺 xy を E_* に入れる。

- $x \in V_0$ または $y \in V_0$. このような辺の個数は高々 $|V_0|n \leq \epsilon n^2$
- ある $i \in [t]$ において、 $x \in V_i$ かつ $y \in V_i$. このような辺の個数は高々 $t \binom{n/t}{2} < \frac{n^2}{2t} \leq \frac{n^2}{2t_0} \leq \frac{\rho}{4} n^2$, ただし (4.16) と (4.14) を用いた。
- ある $\{i, j\} \in \binom{[t]}{2}$ において、 (V_i, V_j) が ϵ 正則でないとき、 V_i, V_j 間の辺 xy . このような辺の個数は高々 $\epsilon t^2 (n/t)^2 = \epsilon n^2$.
- ある $\{i, j\} \in \binom{[t]}{2}$ において、 $d(V_i, V_j) < \rho$ のとき、 V_i, V_j 間の辺 xy . このような辺の個数は高々 $\binom{t}{2} \rho (n/t)^2 < \frac{\rho n^2}{2}$.

したがって $|E_*| < (\epsilon + \frac{\rho}{4} + \epsilon + \frac{\rho}{2}) n^2 = (2\epsilon + \frac{3}{4}\rho) n^2$ であるが、(4.14) より $2\epsilon \leq \frac{1}{4}\rho$ であるから、結局 $|E_*| < \rho n^2$ が得られた。

最後に G' が F を部分グラフに持たないことを背理法で確かめる。 G' に F のコピーがあるとする。番号をつけかえて、そのコピーは $V' := V_1 \sqcup \cdots \sqcup V_t$ 上にあるとしてよい。 $F = ([l], E_F)$ とし、 l 部グラフ $H = (V', E_H)$ を V' による G' の誘導部分グラフとする。ただし V' の番号は $\text{Hom}_l(F, H) \neq \emptyset$ となるようにつけてあり、したがって $ij \in E_F$ ならば (V_i, V_j) は (ϵ, d_{ij}) 正則で、 $d_{ij} \geq \rho$ である。 $m := |V_1| = \cdots = |V_t|$ とおくと、

$$m = \frac{(1-\epsilon)n}{t} \geq \frac{(1-\epsilon)n}{T_0} > \frac{n}{2T_0}$$

である。このとき定理 4.2 と (4.14), (4.15) から

$$h_l(F, H) \geq m^l \prod_{uw \in E_F} d_{uw} - \epsilon |E_F| m^l > (\rho^e - \epsilon e) \left(\frac{n}{2T_0} \right)^l = \eta n^l$$

を得る。これは H に含まれる F のコピーの個数が ηn^l より多いことを意味しており、 G に含まれる F のコピーの個数に関する仮定に反する。 \square

系 4.1. 任意の $\delta > 0$ に対して、ある正整数 n_1 が存在し、次が成り立つ。任意の $n \geq n_1$ と n 頂点グラフ $G = (V, E)$ に対して、もし G の各辺がちょうどひとつの三角形に含まれるならば、 $|E| \leq \delta n^2$ である。

証明. 定理 4.3 に $F = K_3$ と $\rho := \delta/3$ を入力し、出力として η と n_0 を得る。さらに $n_1 := \max\{n_0, 1/\eta\}$ とおく。 $n \geq n_1$ とし、 n 頂点グラフ $G = (V, E)$ の各辺はちょうどひとつの K_3 に含まれるとする。このとき G に含まれるラベルなし K_3 の個数は $|E|/3$ だから、 $h = |\text{Hom}(K_3, G)|$ においてラベル付きで数えると

$$h = 6(|E|/3) = 2|E| \leq 2 \binom{n}{2} < n^2 \leq \eta n^3$$

である。ただし最後の不等式で、 $1 \leq \eta n_0 \leq \eta n$ を用いた。

再び定理 4.3 により、ある $E_* \subset E$ が存在して、 $|E_*| \leq \rho n^2 = \delta n^2/3$ かつ $G' = (V, E \setminus E_*)$ には三角形がない。 G から辺をひとつ除去するごとに破壊されるラベル付き K_3 は高々 6 個だから、 $h \leq 6|E_*| \leq 2\delta n^2$ である。ここから $|E| = h/2 \leq \delta n^2$ がしたがう。 \square

この系を簡略に「 n 頂点グラフ $G = (V, E)$ の各辺がちょうどひとつの三角形に含まれるならば、 $|E| = o(n^2)$ である」と述べることもある。同様に次の定理は「 $A \subset [n]$ が長さ 3 の等差数列を含まなければ、 $|A| = o(n)$ である」と述べることもできる。

定理 4.4. 任意の $\epsilon > 0$ に対して、ある n_1 が存在し、次が成り立つ。任意の $n \geq n_1$ と $A \subset [n]$ に対して、もし A が長さ 3 の等差数列を含まなければ、 $|A| \leq \epsilon n$ である。

証明. 与えられた ϵ に対して $\delta := \epsilon/12$ において系 4.1 を適用して n_1 を得る。 $n \geq n_1$ とし、 $A \subset [n]$ は長さ 3 の等差数列を含まないとする。 $6n$ 頂点 3 部グラフ $G = (V, E)$ を $V = [n] \sqcup [n+1, 3n] \sqcup [3n+1, 6n]$ 上に構成する。 $i \in [n]$ と $a \in A$ に対して、三角形 $T(i, a) := \{i, i+a+n, i+2a+3n\}$ を定め、

$$E := \bigcup \left\{ \binom{T(i, a)}{2} : i \in [n], a \in A \right\}$$

とおく。

G の各辺にはそれを含む三角形として $T(i, a)$ と表せるものがただひとつ定まるが、それ以外の三角形はないことを背理法で示そう。このため、三つの三角形 $T(i, a), T(i', a'), T(i'', a'')$ から一辺ずつ取り出してできる三角形が G 内にあるとしよう。例えばその 3 辺が

$$\{i, i+a+n\}, \{i'+a'+n, i'+2a'+3n\}, \{i'', i''+2a''+3n\}$$

であるとする。このとき

$$i = i'', i + a + n = i' + a' + n, i' + 2a' + 3n = i'' + 2a'' + 3n$$

図

で、ここから $a + a' = 2a''$ つまり A 内に長さ 3 の等差数列が見つかる。これは矛盾だから、 G の各辺はちょうどひとつの三角形 $T(i, a)$ に含まれることがわかった。このような三角形は $n|A|$ 個あるから、 $|E| = 3n|A|$ である。系 4.1 により $|E| \leq \delta|V|^2 = (\epsilon/12)(6n)^2 = 3\epsilon n^2$, すなわち $|A| \leq \epsilon n$ である。 \square

定理 4.4 の証明は Ruzsa と Szemerédi[3] による。除去補題の歴史的経緯は [2] を見よ。

4.3 To be written

参考文献

- [1] E. Szemerédi, Regular partitions of graphs, in *Problèmes combinatoires et théorie des graphes (Colloq. Internat. CNRS, Univ. Orsay, Orsay, 1976)*, pp. 399–401, Colloq. Internat. CNRS, 260, CNRS, Paris, ; MR0540024
- [2] M. Schacht, Regularity lemma and applications,
<https://www.math.uni-hamburg.de/home/schacht/lnotes/GT/SzRL.pdf>
- [3] I. Z. Ruzsa and E. Szemerédi, Triple systems with no six points carrying three triangles, in *Combinatorics (Proc. Fifth Hungarian Colloq., Keszthely, 1976)*, Vol. II, pp. 939–945, Colloq. Math. Soc. János Bolyai, 18, North-Holland, Amsterdam-New York, ; MR0519318

第 5 章

確率手法

組合せ論の古の教えに「神はサイコロを振る」あるいは「わからなければサイコロに聞け」という。この章では確率手法の基本とその典型的な応用例を紹介する^{†1}。

5.1 確率手法の基本アイデア

5.1.1 独立数の下界

グラフ G の独立集合 I を次の貪欲法で得ることができる。すなわち G の最大次数をもつ頂点 v をとり、 $I = \{v\}$ とおいて、 G から v とその近傍を除去し、残ったグラフを G' とする。次に G' の最大次数をもつ頂点 v' をとり、 I に v' を加え、 G' から v' とその近傍を除去し、残ったグラフに同じ操作を続ける。最終的に得られる独立集合 I は $|I| \geq n/(1 + \Delta)$ をみたす。ただし Δ は G の最大次数である。この評価は次のように改善できる。この結果は Caro と Wei が独立に得たものだが、ここでは [2] の証明を紹介する。

定理 5.1. グラフ $G = (V, E)$ において頂点 v の次数を d_v とかくとき、

$$\alpha(G) \geq \sum_{v \in V} \frac{1}{1 + d_v}$$

が成り立つ。

証明. V 上の全順序 $<$ を固定して

$$I := \{v \in V : \{v, w\} \in E \implies v < w\}$$

とおく。 V の要素を $<$ にしたがって左から右に並べると、 I は左向きの辺をもたない頂点の集合だから G の独立集合である。

$v \in I$ のとき $X_v = 1$, $v \notin I$ のとき $X_v = 0$ とし、 $X := \sum_{v \in V} X_v$ とおくと $X = |I|$ である。全順序を $(|V|!)$ 個の中から一様ランダムに選び、上記の X_v, X を確率変数と

^{†1} Erdős と Spencer による [1] は組合せ論の確率手法の古典であり、Alon と Spencer による [2] はその現代版である。Zhao[3] の講義ノートも参考にするとよい。

考える。 $v \in I$ となるのは、 v およびその近傍にある合計 $1 + d_v$ 個の頂点の中で v が最小 (左端) であるときで、その確率は $\frac{1}{1+d_v}$ である。よって

$$\mathbb{E}[X_v] = \mathbb{P}[v \in I] = \frac{1}{1+d_v}, \quad \mathbb{E}[X] = \sum_{v \in V} \frac{1}{1+d_v}$$

を得る。したがってある全順序 $<$ が存在して、 $|I| \geq \sum_{v \in V} \frac{1}{1+d_v}$ である。 \square

系 5.1. $\alpha(G) \geq \frac{n^2}{n+2e}$.

証明. $f(x) = \frac{1}{1+x}$ に Jensen の不等式 $\frac{1}{n} \sum f(d_v) \geq f(\frac{1}{n} \sum d_v)$ を適用すると

$$\frac{1}{n} \sum \frac{1}{1+d_v} \geq \frac{1}{1+\frac{1}{n} \sum d_v} = \frac{n}{n+2e}$$

である。これと定理 5.1 から目標の不等式を得る。 \square

ハイパーグラフの独立数の下界を与えるため、正整数 d に対して

$$f(d) = \prod_{i=1}^d \left(1 - \frac{1}{(r-1)i+1}\right)$$

とおく。 $r \geq 2$ とし、 r グラフ H において頂点 v の次数を d_v とかく。このとき、Caro と Tuza は

$$\alpha(H) \geq \sum_{v \in V} f(d_v)$$

が成り立つことを示した。 $r = 2$ ならば $f(d) = (1 - \frac{1}{2})(1 - \frac{1}{3}) \cdots (1 - \frac{1}{d+1}) = \frac{1}{d+1}$ であるから、この結果は定理 5.1 の拡張になっている。Csaba らは $f(d)$ を評価することで、例えば H が n 頂点 3 グラフならば

$$\alpha(H) > \frac{\sqrt{\pi}}{2} \sum_{i=1}^n \frac{1}{\sqrt{1+d_v}}$$

であることを示した。

5.1.2 内周と染色数が大きいグラフ

内周と染色数の両方が大きいグラフを構成するのは容易ではない (がいくつかの方法が知られている)。Erdős は確率手法を用いた短い議論で、そのようなグラフが存在することを鮮やかに示した。

定理 5.2 (Erdős). 任意の正整数 l, r に対して、内周が l より大きく、染色数が r より大きいグラフがある。

証明. n が十分大きいとき、ランダムグラフ $G = G_{n,p}$ (を少し変更したグラフ) が条件をみたす確率が正であることを示したい。そこで $G = G_{n,p}$ において、確率変数 X を G 内の長さ l 以下の閉路の個数、確率変数 Y を独立数 $\alpha(G)$ とする。さらにある定数 $0 < \epsilon < 1$ と数列 $a_n = o(n)$ が存在して、次の 2 条件

$$\mathbb{P}[X \geq \epsilon n] = o(1), \quad (5.1)$$

$$\mathbb{P}[Y \geq a_n] = o(1) \quad (5.2)$$

が成り立つと仮定しよう。このとき n が十分大きければ

$$\mathbb{P}[X < \epsilon n \text{ かつ } Y > a_n] > 0$$

だから、 n 頂点グラフで、長さ l 以下の閉路の個数が ϵn 未満、かつ独立数が a_n より大のグラフがある。このグラフから高々 ϵn 頂点を除去して (つまり短い閉路から 1 点ずつ選んで除去して) 残ったグラフ G' の内周を l より大きくできる。ここで一般に $\chi(G') \alpha(G') \geq n$ であることに注意すると、

$$\chi(G') \geq \frac{(1-\epsilon)n}{\alpha(G')} \geq \frac{(1-\epsilon)n}{a_n}$$

を得る。 $a_n = o(n)$ なので上式右辺は n を十分大きくとると r より大きい。つまり G' が条件をみたすグラフである。

そこで (5.1) および (5.2) が成り立つことを確かめる。このため $0 < \theta < \frac{1}{l}$ をみたす θ を固定し、 $p = (1/n)^{1-\theta}$ とおく。 $G = G_{n,p}$ における長さ j の閉路の個数の期待値は $\binom{n}{j} \frac{(j-1)!}{2} p^j \leq (np)^j = n^{\theta j}$ であり、

$$\mathbb{E}[X] \leq \sum_{j=3}^n n^{\theta j} = n^{l\theta} + n^{(l-1)\theta} + \cdots + n^{3\theta} \leq \frac{n^{l\theta}}{1 - n^{-\theta}}$$

を得る。 $\theta > 0$ と $l\theta < 1$ から上式右辺は $o(1)$ であり、マルコフの不等式から (5.1) がしたがう。次に $a_n = \lceil 3n^{1-\theta} \log n \rceil = o(n)$ において、 $1-p \leq e^{-p}$, $pa_n > 3 \log n$ を用いると

$$\mathbb{P}[Y \geq a_n] \leq \binom{n}{a_n} (1-p)^{\binom{a_n}{2}} \leq n^{a_n} e^{-pa_n \frac{a_n-1}{2}} \leq n^{a_n - \frac{3}{2}(a_n-1)} = \left(\frac{1}{\sqrt{n}}\right)^{a_n-3}$$

を得る。この右辺は $o(1)$ だから (5.2) がしたがう。 \square

5.1.3 2 着色可能性

ハイパーグラフ $H = (V, E)$ の 2 着色とは $\chi: V \rightarrow [2]$ のことである。辺 $e \in E$ が χ において単色とは、 e の各点が同色、つまり χ の e への制限が定数関数であることである。

H の辺に単色のものがないとき、 χ を適切な 2 着色という。 H が適切な 2 着色をもつとき、 H は 2 着色可能^{†2}であるという。

定理 5.3. $H = (V, E)$ が n グラフで $|E| < 2^{n-1}$ ならば、2 着色可能である。

証明. n グラフ $H = (V, E)$ は $|E| < 2^{n-1}$ をみたすとする。 H の各頂点を独立ランダムに等確率で 2 色に塗り分ける。辺 e が単色である事象を A_e とおくと $\mathbb{P}[A_e] = (1/2)^n \times 2 = 2^{1-n}$ である。よって union bound から

$$\mathbb{P}\left[\bigcup_{e \in E} A_e\right] \leq \sum_{e \in E} \mathbb{P}[A_e] = |E|2^{1-n} < 1$$

を得る。つまり単色の辺がある確率は 1 より小さいから、2 着色可能である。□

2 着色可能でない n グラフの辺数の最小値を $m(n)$ とかく。このとき $m(n) > m'$ ならば辺数 m' の n グラフは必ず 2 着色可能である。定理 5.3 は $m(n) \geq 2^{n-1}$ と言い換えることができる。Beck はランダム着色したあと都合の悪い頂点の色をうまく塗りかえることで $m(n) = \Omega(2^n n^{1/3})$ を示した。同様の手法を洗練させて Radhakrishnan と Srinivasan は $m(n) = \Omega(2^n \sqrt{n/\log n})$ を示した。さらに Cherkashin と Kozik はこのバウンドを達成するランダム貪欲着色アルゴリズムを見出した^{†3}。以下にその方法を紹介する。

定理 5.4. $m(n) = \Omega(2^n \sqrt{n/\log n})$.

証明. はじめに n グラフ $H = (V, E)$ のランダム 2 着色アルゴリズムを述べる。各頂点 $v \in V$ に独立一様ランダムに実数 $t(v) \in [0, 1]$ を割り当てる。 $t(v)$ を v の生成時刻という。 V の頂点を生成時刻順にならべて v_1, v_2, \dots とおく。 $i = 1, 2, \dots$ の順に以下の着色をおこなう。もし v_i を青で塗っても単色辺（すべての頂点が青の辺）が生じない場合は v_i を青で、そうでなければ赤で塗る。

頂点を全部塗り終わったとき、着色規則から青い単色辺はない。頂点 v が赤で塗られるのは、 v を含む辺 e があり、かつ e の頂点で v が最後に塗られる場合に限られる。赤の単色辺 f が生じたとき、 f の最初に塗られた頂点 v に対して、 v を赤で塗らせた辺 e がある。この (e, f) を危険対とよぶ。このとき $e \cap f = \{v\}$ であり、 e の v 以外の頂点は青である。 v をこの危険対の共有点という。

以下、 H の辺数を $k2^{n-1}$ とし、 k が適切な条件をみたせば危険対が生じる確率が 1 より小さいことを示す。したがって危険対がない着色、すなわち H の適切な 2 着色がある。このときその条件のもとで H の辺数を評価すると定理が得られる。

^{†2} H は property B をもつともいう。[\[1\]](#) によると、これは Edwin W. Miller の命名で B は Felix Bernstein のことらしい。

^{†3} 彼らは独立に同じ主結果を得て、それぞれの論文を統合した共著論文を出版した。

単位区間 $[0, 1]$ を 3 分割して、 $B = [0, \frac{1-p}{2}]$, $P = [\frac{1-p}{2}, \frac{1+p}{2}]$, $R = [\frac{1+p}{2}, 1]$ とおく。パラメタ $p \in (0, 1)$ は後で最適化する。 B に共有点の生成時刻をもつ危険対がある事象を \mathbf{B} とし、同様に事象 \mathbf{P}, \mathbf{R} を定める。辺 e の頂点の生成時刻がすべて B に含まれるとき、記号を濫用して $e \subset B$ とかく。このとき

$$\mathbb{P}[\mathbf{B}] \leq \mathbb{P}[e \subset B \text{ なる辺 } e \text{ がある}] \leq \sum_{e \in E} \mathbb{P}[e \subset B] = |E| \left(\frac{1-p}{2} \right)^n$$

より、

$$\mathbb{P}[\mathbf{B} \cup \mathbf{R}] \leq \mathbb{P}[\mathbf{B}] + \mathbb{P}[\mathbf{R}] = 2\mathbb{P}[\mathbf{B}] \leq 2|E| \left(\frac{1-p}{2} \right)^n = k(1-p)^n$$

を得る。

次に $\mathbb{P}[\mathbf{P}]$ を評価するため、危険対 (e, f) の共有点 v について $t(v) \in P$ とすると、 e の頂点の生成時刻は $t(v)$ 以下、 f の頂点の生成時刻は $t(v)$ 以上である。ここで $e \setminus \{v\}$ の頂点の生成時刻が $t(v)$ 以下で、かつ $f \setminus \{v\}$ の頂点の生成時刻が $t(v)$ 以上である確率は $t(v)^{n-1}(1-t(v))^{n-1} \leq (1/4)^{n-1}$ である。また v の生成時刻が P にある確率は p である。したがって (e, f) が危険対で、かつ共有点の生成時刻が P にある確率は高々 $p(1/4)^{n-1}$ である。このようなペアの総数は高々 $\binom{|E|}{2} < k^2 4^{n-1}$ だから

$$\mathbb{P}[\mathbf{P}] \leq k^2 4^{n-1} p(1/4)^{n-1} = k^2 p$$

を得る。

まとめると

$$\mathbb{P}[\mathbf{B} \cup \mathbf{P} \cup \mathbf{R}] \leq \mathbb{P}[\mathbf{B}] + \mathbb{P}[\mathbf{P}] + \mathbb{P}[\mathbf{R}] \leq k(1-p)^n + k^2 p < k e^{-pn} + k^2 p \quad (5.3)$$

である。この右辺が 1 より小さければ、 H に危険対が存在しない、すなわち適切な 2 着色をもつ確率が正となる。(5.3) の右辺は $p = \frac{1}{n} \log \frac{n}{k}$ のとき最小となる。この p を代入すると、 H が適切な 2 着色をもつには

$$\frac{k^2}{n} \left(1 + \log \frac{n}{k} \right) < 1 \quad (5.4)$$

であればよい。この条件のもとで $|E| = k2^{n-1}$ を最大にしよう。 $c < \sqrt{2}$ に対して $k = c\sqrt{n/\log n}$ とおくと、 n が十分大きいとき (5.4) が成り立つ。つまり $m(n) = \Omega(2^n \sqrt{n/\log n})$ である。□

5.2 Lovász の局所補題

5.2.1 局所補題とその証明

複数の条件をみたすものを探しているとしよう。つまり、どれかの条件が破れるような状況をさけたい。そこで確率空間 $(\Omega, \mathcal{F}, \mathbb{P})$ において、 n 個の「悪い」事象 $B_1, \dots, B_n \in$

\mathcal{F} が指定され、すべて $\mathbb{P}[B_i] < 1$ であるとする。もしこれらの事象が独立ならば、 $\mathbb{P}[\bigcap_{i=1}^n \bar{B}_i] = \prod_{i=1}^n (1 - \mathbb{P}[B_i]) > 0$ 、つまり悪い事象がまったく生じないことがある^{†4}。Lovász の局所補題は、 n 個の事象が「かなり」独立で、各 $\mathbb{P}[B_i]$ が大きすぎなければ、同様に $\mathbb{P}[\bigcap_{i=1}^n \bar{B}_i] > 0$ を保証する。

ここで事象の独立性の定義を思い出そう。確率空間 $(\Omega, \mathcal{F}, \mathbb{P})$ において、事象 $F_1, \dots, F_n \in \mathcal{F}$ が独立、あるいは事象の集合 $\{F_1, \dots, F_n\}$ が独立とは、任意の $\emptyset \neq I \subset [n]$ について $\mathbb{P}[\bigcap_{i \in I} F_i] = \prod_{i \in I} \mathbb{P}[F_i]$ が成り立つことである。また事象 F が事象の集合 $\{F_1, \dots, F_n\}$ と独立であるとは、任意の $\emptyset \neq I \subset [n]$ について $\mathbb{P}[F] = \mathbb{P}[F | \bigcap_{i \in I} F_i]$ が成り立つことと定める。ただし条件付き確率は $\mathbb{P}[A|B] := \mathbb{P}[A \cap B] / \mathbb{P}[B]$ と定義され、したがって

$$\mathbb{P}[A|B \cap C] = \frac{\mathbb{P}[A \cap B|C]}{\mathbb{P}[B|C]} \quad (5.5)$$

をみtas。

確率空間 $(\Omega, \mathcal{F}, \mathbb{P})$ および事象の集合 $\mathcal{B} = \{B_1, \dots, B_n\} \subset \mathcal{F}$ に対して、頂点集合 $[n]$ 上のグラフ G が依存グラフであるとは、各 $i \in [n]$ について事象 B_i と事象の集合 $\{B_j : j \in [n] \setminus (N(i) \cup \{i\})\}$ が独立であることをいう^{†5}。このとき $i \neq j$ で $i \not\sim j$ ならば B_i と B_j は独立であるが、逆は必ずしも成り立たない。依存グラフ G は \mathcal{B} から一意的に定まるとは限らないが、必ず存在する。例えば完全グラフ K_n は自明な依存グラフである(が、もちろん役には立たない)。

例えば $\Omega = [4]$, $\mathbb{P}[\{i\}] = \frac{1}{4}$ ($i \in \Omega$)、つまり各 i が等確率に選ばれるとき、3 個の事象を $B_1 = \{1, 4\}$, $B_2 = \{2, 4\}$, $B_3 = \{3, 4\}$ と定める。このとき $\mathbb{P}[B_1] = \mathbb{P}[B_1|B_2] = \mathbb{P}[B_1|B_3] = \frac{1}{2}$, $\mathbb{P}[B_1|B_2 \cap B_3] = 1$ より B_1 は B_2 と B_3 とともに独立であるが、 $B_2 \cap B_3$ とは独立でない。つまり B_1 は $\{B_2, B_3\}$ とは独立でない。これらを考慮すると $\{B_1, B_2, B_3\}$ に対応する依存グラフは次の 4 通りである。



定理 5.5 (Lovász). $(\Omega, \mathcal{F}, \mathbb{P})$ を確率空間、 $\mathcal{B} \subset \mathcal{F}$ を有限集合とする。各事象 $B \in \mathcal{B}$ に対して $N(B) \subset \mathcal{B}$ が与えられ、 B と $\mathcal{B} \setminus (N(B) \cup \{B\})$ は独立であると仮定する。このとき実数値関数 $x : \mathcal{B} \rightarrow (0, 1)$ が存在して、各 $A \in \mathcal{B}$ が

$$\mathbb{P}[A] \leq x(A) \prod_{B \in N(A)} (1 - x(B))$$

^{†4} \bar{B}_i は B_i の余事象、すなわち $\bar{B}_i := \Omega \setminus B_i$ である。

^{†5} $N(i)$ は i の近傍、すなわち $N(i) := \{j \in [n] : ij \in E(G)\}$ である。なお B_i と B_i は独立でないが、定義により各頂点にループはつけない。

をみたせば (0 個の積は 1 とみなす)、

$$\mathbb{P}[\bigcap_{B \in \mathcal{B}} \bar{B}] \geq \prod_{B \in \mathcal{B}} (1 - x(B)) > 0$$

が成り立つ。

証明. $\mathcal{B} = \{B_1, \dots, B_n\}$ とし、 $x_i := x(B_i)$ とおく。頂点集合 $[n]$ 上の \mathcal{B} についての依存グラフを用いると、関数 x に関する仮定は、 $\mathbb{P}[B_i] \leq x_i \prod_{j \in N(i)} x_j$ が各 $i \in [n]$ について成り立つことである。特に $\mathbb{P}[B_i] \leq x_i$ である。はじめに $i \notin J \subset [n]$ をみたす任意の i, J について

$$\mathbb{P}[B_i | \bigcap_{j \in J} \bar{B}_j] \leq x_i \quad (5.6)$$

が成り立つとしよう。このとき、各 $i \in [n]$ について

$$\frac{\mathbb{P}[\bar{B}_1 \cap \dots \cap \bar{B}_j]}{\mathbb{P}[\bar{B}_1 \cap \dots \cap \bar{B}_{j-1}]} = \mathbb{P}[\bar{B}_j | \bigcap_{i \in [j-1]} \bar{B}_i] \geq 1 - x_i$$

だから、これらを $i = 1, 2, \dots, n$ についてかけ合わせて

$$\begin{aligned} \mathbb{P}[\bigcap_{i \in [n]} \bar{B}_i] &= \mathbb{P}[\bar{B}_1] \cdot \frac{\mathbb{P}[\bar{B}_1 \cap \bar{B}_2]}{\mathbb{P}[\bar{B}_1]} \cdot \frac{\mathbb{P}[\bar{B}_1 \cap \bar{B}_2 \cap \bar{B}_3]}{\mathbb{P}[\bar{B}_1 \cap \bar{B}_2]} \cdots \frac{\mathbb{P}[\bar{B}_1 \cap \dots \cap \bar{B}_n]}{\mathbb{P}[\bar{B}_1 \cap \dots \cap \bar{B}_{n-1}]} \\ &\geq (1 - x_1)(1 - x_2)(1 - x_3) \cdots (1 - x_n) > 0 \end{aligned}$$

を得る。これは定理の結論にほかならない。

そこで (5.6) を $|J|$ に関する帰納法で示す。まず $J = \emptyset$ のときは定理の仮定から $\mathbb{P}[B_i] \leq x_i$ である。以下 $J \neq \emptyset$ とし、 i, J を固定する。さらに $J_1 = N(i)$, $J_2 = J \setminus J_1$ として、 J を $J_1 \sqcup J_2$ に分割する。 $J_1 = \emptyset$ ならば再び定理の仮定より (5.6) がしたがうから、 $J_1 \neq \emptyset$ とする。(5.6) の左辺は、(5.5) により

$$\mathbb{P}[B_i | \bigcap_{j \in J} \bar{B}_j] = \frac{\mathbb{P}[B_i \cap (\bigcap_{j \in J_1} \bar{B}_j) | \bigcap_{j \in J_2} \bar{B}_j]}{\mathbb{P}[\bigcap_{j \in J_1} \bar{B}_j | \bigcap_{j \in J_2} \bar{B}_j]} \quad (5.7)$$

と書ける。ここで B_i が $\{B_j : j \in J_2\}$ と独立であることと、定理の仮定から

$$(5.7) \text{ の右辺の分子 } \leq \mathbb{P}[B_i | \bigcap_{j \in J_2} \bar{B}_j] = \mathbb{P}[B_i] \leq x_i \prod_{j \in N(i)} (1 - x_j)$$

を得る。次に、必要なら番号を付け替えて $J_1 = [t]$ とし、 $C := \bigcap_{j \in J_2} \bar{B}_j$ とおく。(5.5) から $i \in [t]$ について

$$\begin{aligned} &\mathbb{P}[\bar{B}_1 \cap \dots \cap \bar{B}_i | \bar{B}_{i+1} \cap \dots \cap \bar{B}_t \cap C] \\ &= \mathbb{P}[\bar{B}_1 \cap \dots \cap \bar{B}_{i-1} | \bar{B}_i \cap \dots \cap \bar{B}_t \cap C] \mathbb{P}[\bar{B}_j | \bar{B}_{i+1} \cap \dots \cap \bar{B}_t \cap C] \end{aligned}$$

が成り立つ。これを用いると (5.7) の分母は

$$\begin{aligned} \mathbb{P}\left[\bigcap_{j \in J_1} \bar{B}|C\right] &= \mathbb{P}[\bar{B}_1|\bar{B}_2 \cap \cdots \cap \bar{B}_t \cap C] \mathbb{P}[\bar{B}_2|\bar{B}_3 \cap \cdots \cap \bar{B}_t \cap C] \cdots \\ &\quad \cdots \mathbb{P}[\bar{B}_{t-2}|\bar{B}_{t-1} \cap \bar{B}_t \cap C] \mathbb{P}[\bar{B}_{t-1}|\bar{B}_t \cap C] \mathbb{P}[\bar{B}_t|C] \end{aligned}$$

と書ける。この右辺に帰納法の仮定 (5.6) を適用すると

$$\mathbb{P}\left[\bigcap_{j \in J_1} \bar{B}|C\right] \geq (1-x_1)(1-x_2) \cdots (1-x_t)$$

を得る。結局、(5.7) について $\mathbb{P}[B_i|\bigcap_{j \in J} \bar{B}_j] \leq x_i$ が示された。 \square

系 5.2 (対称的な場合). $(\Omega, \mathcal{F}, \mathbb{P})$ を確率空間、 $\mathcal{B} \subset \mathcal{F}$ を有限集合とする。定数 p, d が $ep(d+1) \leq 1$ をみたし、各事象 $B \in \mathcal{B}$ について $\mathbb{P}[B] \leq p$ 、また \mathcal{B} を頂点集合とする依存グラフの最大次数は d 以下とする。このとき $\mathbb{P}[\bigcap_{B \in \mathcal{B}} \bar{B}] > 0$ である。

証明. 依存グラフの最大次数に関する仮定は、定理 5.5 において $|N(B)| \leq d$ を意味する。このとき定数関数 $x(B) = \frac{1}{d+1}$ が定理の仮定をみたすことを確かめよう。実際、 $(d/d+1)^d > 1/e$ に注意すると、 $A \in \mathcal{B}$ について

$$\begin{aligned} x(A) \prod_{B \in N(A)} (1-x(B)) &= \frac{1}{d+1} \prod_{B \in N(A)} \frac{d}{d+1} \geq \frac{1}{d+1} \left(\frac{d}{d+1}\right)^d \\ &> \frac{1}{(d+1)e} \geq p \geq x(A) \end{aligned}$$

が成り立つ。したがって定理 5.5 から $\mathbb{P}[\bigcap_{B \in \mathcal{B}} \bar{B}] > 0$ である。 \square

5.2.2 局所補題の応用

(1) ラムゼー数

ランダムグラフ $G(n, p)$ は、ラベル付き n 頂点グラフで、各頂点ペア $\{i, j\}$ に対して独立に確率 p で辺をつける確率モデルである。形式的には、これは確率空間 $(\Omega, \mathcal{F}, \mathbb{P})$ で以下のように定義される。頂点集合 $[n]$ のグラフは $\omega : \binom{[n]}{2} \rightarrow \{0, 1\}$ で指定できる。つまり $\omega(\{i, j\}) = 1$ ならば i, j は隣接し、0 ならば非隣接である。 Ω をこのような ω 全体とし、 $\mathcal{F} = 2^\Omega$ とする。このとき $|\Omega| = 2^{\binom{n}{2}}$ であり、 $\omega^{-1}(1)$ は辺集合に対応する。さらに辺数を $m = |\omega^{-1}(1)|$ として

$$\mathbb{P}[\omega] := p^m (1-p)^{\binom{n}{2}-m}$$

と定める。 ω を対応するグラフ G と同一視して、 $\mathbb{P}[\omega]$ を $\mathbb{P}[G]$ ともかく。

$\omega \in \Omega$ は完全グラフ K_n の辺の 2 着色ともみなせる。この場合には $\omega^{-1}(0)$ を赤で塗られた辺の集合、 $\omega^{-1}(1)$ を青で塗られた辺の集合のように考える。正整数 k, l に対して

n を十分大きくとると、 K_n の辺のどんな 2 着色に対しても赤の K_k (すべての辺が赤の K_k) または青の K_l が存在することが知られている。このような n の最小値をラムゼー数 $R(k, l)$ とよぶ。例えば $R(3, 3) = 6$ である。つまり K_5 の辺の 2 着色で赤の K_3 も青の K_3 もない (略して、これを単色 K_3 がないという) ものがあるが、 K_6 の辺のどんな 2 着色にも単色 K_3 がある。

Erdős にしたがって

$$R(k, k) > k(\sqrt{2})^k \left(\frac{1}{e\sqrt{2}} + o(1) \right)$$

を確かめよう。ランダムグラフ $G(n, p)$ に対応する確率空間 $(\Omega, \mathcal{F}, \mathbb{P})$ を考える。頂点の k 点部分集合 $A \in \binom{[n]}{k}$ に対して、 A 上の K_k が単色であるようなグラフの集合を $\mathcal{G}_A \in \mathcal{F}$ とおくと、

$$\mathbb{P}[\mathcal{G}_A] = p^{\binom{k}{2}} + (1-p)^{\binom{k}{2}}$$

である。ここでさらに $p = 1/2$ とすると、 $\mathbb{P}[\mathcal{G}_A] = 2(1/2)^{\binom{k}{2}}$ である。また $G(n, p)$ に単色 K_k が存在する事象は $\bigcup_{A \in \binom{[n]}{k}} \mathcal{G}_A$ である。よって union bound から

$$\mathbb{P}\left[\bigcup_{A \in \binom{[n]}{k}} \mathcal{G}_A\right] \leq \sum_{A \in \binom{[n]}{k}} \mathbb{P}[\mathcal{G}_A] \leq \binom{n}{k} 2(1/2)^{\binom{k}{2}}$$

を得る。右辺が < 1 であれば、 $G(n, p)$ に単色 K_k が存在しない確率が正、つまり単色 K_k をもたない K_n の辺の 2 着色が存在する。したがって $\binom{n}{k} 2(1/2)^{\binom{k}{2}} < 1$ をみたす n に対して、 $R(k, k) > n$ が成り立つ。局所補題によってこの評価を以下のように改善できる。

定理 5.6 (Spencer).

$$R(k, k) \geq k(\sqrt{2})^k \left(\frac{\sqrt{2}}{e} + o(1) \right).$$

証明. $G(n, 1/2)$ に対応する確率空間を $(\Omega, \mathcal{F}, \mathbb{P})$ とする。 $A \in \binom{[n]}{k}$ とし、 A 上の K_k が単色である事象を $\mathcal{G}_A \in \mathcal{F}$ とかく。頂点集合 $\{\mathcal{G}_A : A \in \binom{[n]}{k}\}$ の依存グラフ H を構成する。各 $A \in \binom{[n]}{k}$ に対して、 $\mathcal{B}_A = \{B \in \binom{[n]}{k} : |A \cap B| \leq 1\}$ とおく。このとき、 \mathcal{G}_A は $\{\mathcal{G}_B : B \in \mathcal{B}_A\}$ と独立である。そこで H において 2 頂点 \mathcal{G}_A と \mathcal{G}_B を $|A \cap B| \geq 2$ のときに隣接させる。定義から H は正則グラフで次数 Δ は

$$\Delta = |\mathcal{B}_A| < \binom{k}{2} \binom{n}{k-2}$$

をみたす。この右辺を d とし、 $p = \mathbb{P}[\mathcal{G}_A] = 2(1/2)^{\binom{k}{2}}$ とし系 5.2 を適用する。すなわち、もし $ep(d+1) \leq 1$ であれば、 $\mathbb{P}[\bigcap_{A \in \binom{[n]}{k}} \bar{\mathcal{G}}_A] > 0$ が成り立つ。これは n 頂点グラフの辺の 2 着色で、単色 K_k を含まないものがあること、つまり $R(k, k) > n$ を意味する。

$k \geq 3$ とすると

$$ep(d+1) < 4pd \leq 4 \cdot 2(1/2)^{\binom{k}{2}} \binom{k}{2} \binom{n}{k-2}$$

である。右辺が ≤ 1 となる n の条件を $n, k \rightarrow \infty$ のもとで求める。両辺の \log をとると

$$\log \binom{n}{k-2} \leq \binom{k}{2} \log 2 - \log \binom{k}{2} + O(1)$$

である。 $\log \binom{n}{k-2} = (k-2) \log n - k \log k + k + O(\log k)$ に注意して整理すると

$$(k-2) \log n \leq k \log k - k + \frac{1}{2} k(k-1) \log 2 + O(\log k)$$

を得る。両辺を $k-2$ で割り、 $\frac{k(k-1)}{2(k-2)} = \frac{k}{2} + \frac{1}{2} + o(1)$ を用いると

$$\log n \leq \log k - 1 + \left(\frac{k}{2} + \frac{1}{2} \right) \log 2 + o(1) = \log \left(k 2^{\frac{k}{2} + \frac{1}{2}} e^{-1+o(1)} \right),$$

つまり

$$n \leq k (\sqrt{2})^k \left(\frac{\sqrt{2}}{e} + o(1) \right)$$

を得る。この条件のもとで $ep(d+1) \leq 1$ が成り立ち、証明が完了した。 \square

(2) 2 着色可能性 (property B)

ハイパーグラフ $H = (V, E)$ の頂点のランダム 2 着色を考えよう。すなわち確率空間 $(\Omega, \mathcal{F}, \mathbb{P})$ を次のように定める。頂点の 2 着色は $\omega : V \rightarrow \{0, 1\}$ で指定される。このような ω 全体を Ω とし、 $\mathcal{F} = 2^\Omega$ とする。このとき $|\Omega| = 2^n$ である。さらに $\mathbb{P}[\omega] = (1/2)^{|V|}$ と定める。つまり各頂点は、独立かつ等確率に（例えば、赤または青に）2 着色される。2 着色 ω において辺 $e \in E$ が単色とは、 e に含まれる頂点が同色であること、つまり ω が e 上で定数関数であることをいう。 H の 2 着色で単色辺を含まないものがあるとき、 H は 2 着色可能（あるいは property B をもつ）というのであった。

定理 5.7. ハイパーグラフ $H = (V, E)$ は各辺が k 点以上を含み、高々 d 個の他の辺と交わるとする。このとき $e(d+1) \leq 2^{k-1}$ ならば、 H は 2 着色可能である。特に、 H が k 正則 k グラフで $k \geq 9$ ならば、 H は 2 着色可能である。

証明. H の各頂点を独立かつ等確率に 2 着色する。辺 $f \in E$ が単色である事象を B_f とすると、 $\mathbb{P}[B_f] = 2(1/2)^{|f|} \leq (1/2)^{k-1}$ である。 $\{B_f : e \in E\}$ を頂点集合とする依存グラフ G を $B_f \sim B_{f'} \iff f \cap f' \neq \emptyset$ と定義できる。 G の最大次数は d 以下である。したがって系 5.5 より H は 2 着色可能である。

H が k 正則 k グラフのとき、辺 f の各頂点は f 以外の $k-1$ 辺に含まれるから、 f と交わる (f 以外の) 辺の総数は $\Delta := k(k-1)$ であり、依存グラフは Δ 正則である。 H が 2 着色可能であるには、 $e(\Delta+1) \leq 2^{k-1}$ であればよく、これは $k \geq 9$ でみたされる。□

閉路グラフは 2 正則 2 グラフで、頂点数が奇数のときは property B をもたない。Fano 平面グラフは 3 正則 3 グラフで、property B をもたない。一方、 $k \geq 4$ ならば k 正則 k グラフは 2 着色可能であることが知られている。

5.2.3 Moser–Tardos アルゴリズム

定理 5.7 によれば、任意の 9 正則 9 グラフ H は 2 着色可能である。これは H のランダム 2 着色に局所補題を適用すると、単色辺が現れない確率が正であるからだ。しかしその確率が小さければ^{†6}、 H に実際にランダム 2 着色を施してもそれが適切な 2 着色であることは期待できない。そこで局所補題に「構成的な」証明を与えることが望まれる。例えば上記 H の適切な 2 着色を見つけるうまいアルゴリズムがあるだろうか？そのような研究は Beck にはじまり、特に Moser によって推し進められた。以下に紹介する Moser と Tardos の結果は、ごく弱い仮定 (確率変数モデル) を付加することで局所補題の証明を構成的にできることを主張する。

確率空間 $(\Omega, \mathcal{F}, \mathbb{P})$ において、独立な確率変数の集合 \mathcal{P} と事象の集合 $\mathcal{B} \subset \mathcal{F}$ が与えられているとする。さらに

$$\text{各 } B \in \mathcal{B} \text{ に対して } S \subset \mathcal{P} \text{ が定まり、} B \text{ は } S \text{ の確率変数の値で決まる} \quad (5.8)$$

と仮定する。このような S のうち (包含関係で) 極小のものが一意に定まるから、これを $\text{vbl}(B)$ とかく^{†7}。このとき頂点集合 \mathcal{B} のグラフを $B, B' \in \mathcal{B}$ について

$$B \neq B' \text{ かつ } B \sim B' \iff \text{vbl}(B) \cap \text{vbl}(B') \neq \emptyset$$

と定めると、これは依存グラフになる。なお B は「悪い事象」を想定していて、どの $B \in \mathcal{B}$ も生じないように \mathcal{P} に属する確率変数の値を割り当てることが目標となる。

例えば、前項で扱ったハイパーグラフ $H = (V_H, E_H)$ のランダム 2 着色の場合は、 p_i を頂点 i の色に対応する確率変数とし、つまり $\omega \in \Omega$ に対して $p_i(\omega) = \omega(i)$ と定めて、 $\mathcal{P} = \{p_i : i \in V_H\}$ とおく。次に、各 $f \in E_H$ に対して、事象 B_f を辺 f が単色である事象とし、 $\mathcal{B} = \{B_f : f \in E_H\}$ とおく。このとき事象 B_f は $\{p_i : i \in f\}$ から定まり、 $\text{vbl}(B_f) = \{p_i : i \in f\}$ とおいて依存グラフを作ると、前項で構成したグラフと同型なものが得られる。もし各 p_i の値をうまく設定して、どの B_f も生じないようにできれば、それは H の適切な 2 着色を与える。

^{†6} 局所補題を適用する問題では「悪い事象が起きない確率」は非常に小さいことが多い。

^{†7} B に対応する random variables の意味。

局所補題の仮定に (5.8) を付け加えたものを確率変数モデルという。これは形式的には、局所補題が適用できる状況のうち、特別なものを扱っていることになるが、局所補題が適用される具体的な問題では（ほとんどいつでも）(5.8) がみたされるため、実質的な制限にはならないと考えられている。

それでは Moser–Tardos アルゴリズムを述べよう。 $(\Omega, \mathcal{F}, \mathbb{P})$ を確率空間とし、独立な確率変数の有限集合 \mathcal{P} と事象の有限集合 $\mathcal{B} \subset \mathcal{F}$ からなる確率変数モデルが与えられたとする。

1. 各 $p \in \mathcal{P}$ に任意の値を設定する。
2. もし現在の \mathcal{P} の各変数の値によって生じる \mathcal{B} の事象があれば、そのひとつ B を任意に選び、 $\text{vbl}(B)$ に属する p の値をランダムに変更（リサンプル）する。
3. 前項を該当する B の事象がなくなるまで繰り返す。

定理 5.8 (Moser–Tardos). $(\Omega, \mathcal{F}, \mathbb{P})$ を確率空間とし、独立な確率変数の有限集合 \mathcal{P} と事象の有限集合 $\mathcal{B} \subset \mathcal{F}$ からなる確率変数モデルを考える。このとき実数値関数 $x : \mathcal{B} \rightarrow (0, 1)$ が存在して、各 $A \in \mathcal{B}$ が

$$\mathbb{P}[A] \leq x(A) \prod_{B \in N(A)} (1 - x(B))$$

をみたせば、上で述べたアルゴリズムで \mathcal{P} の変数の値を設定して、どの $B \in \mathcal{B}$ も生じないようにできる。さらにひとつの $B \in \mathcal{B}$ が生じないようになるまでに必要なリサンプルの回数の期待値は高々 $\frac{x(B)}{1-x(B)}$ であり、したがってアルゴリズムが終了するまでのリサンプルの総数の期待値は高々 $\sum_{B \in \mathcal{B}} \frac{x(B)}{1-x(B)}$ である。

この驚くほど単純なアルゴリズムがうまく動く理由はまったく自明でないが、原著論文 [4] ではわずか 3 ページ半で証明されている。さらにアルゴリズムを並列化したり脱乱択化する方法も述べられている。Moser と Tardos はこの業績で 2020 年のゲーデル賞を受賞した。

5.3 測度の集中

距離と確率測度が与えられた空間で、全空間の半分の測度をもつ任意の部分集合を考える。このとき、この集合から遠くにある点の集合の測度は必ず小さいと主張できることがある。例えば \mathbb{R}^n の $n-1$ 次元単位球面 S^{n-1} に、全球面の測度が 1 となるような一様な測度を与えたとき、球面の部分集合 A の測度が $\frac{1}{2}$ ならば、 A からのユークリッド距離が t 以内でない球面上の点の集合の測度は、高々 $2e^{-t^2 n/2}$ であることが知られている。

この節では、Matoušek の [6] の 14 章（とその前後の章）の一部およびその離散構造への応用を中心に紹介する。Ball の [5] と Matoušek らの [7] の 2 章も参考にした。興味をもたれた読者はぜひこれらの文献を読みたい。

5.3.1 裾評価の不等式

x が ± 1 の値をそれぞれ確率 $\frac{1}{2}$ でとるとき、これをベルヌーイ確率変数という。

定理 5.9 (Bernstein の不等式). x_1, \dots, x_n が独立なベルヌーイ確率変数で、実数 a_1, \dots, a_n が $\sum_{i=1}^n a_i^2 = 1$ をみたすとする。このとき任意の $t > 0$ に対して

$$\mathbb{P}\left[\left|\sum_{i=1}^n a_i x_i\right| > t\right] \leq 2e^{-\frac{t^2}{2}} \quad (5.9)$$

が成り立つ。

証明. 次の不等式を利用する。すなわち、任意の実数 x に対して

$$\frac{1}{2}(e^x + e^{-x}) \leq e^{x^2/2} \quad (5.10)$$

が成り立つ。これをみるには、両辺をテーラー展開して項ごとに比較すればよい。

パラメタ $\lambda > 0$ を導入する。(5.10) により、

$$\mathbb{E}[e^{\lambda a_i x_i}] = \frac{1}{2}(e^{\lambda a_i} + e^{-\lambda a_i}) \leq e^{\lambda^2 a_i^2 / 2}$$

である。したがって

$$\mathbb{E}[e^{\lambda \sum a_i x_i}] = \mathbb{E}[\prod e^{\lambda a_i x_i}] = \prod \mathbb{E}[e^{\lambda a_i x_i}] \leq \prod e^{\lambda^2 a_i^2 / 2} = e^{\lambda^2 / 2}, \quad (5.11)$$

さらにマルコフの不等式から

$$\mathbb{P}[\sum a_i x_i \geq t] = \mathbb{P}[e^{\lambda \sum a_i x_i} \geq e^{\lambda t}] \leq \mathbb{E}[e^{\lambda \sum a_i x_i}] / e^{\lambda t} \leq e^{\lambda^2 / 2 - \lambda t}$$

である。右辺を最小化するため $\lambda = t$ とおくと、

$$\mathbb{P}[\sum a_i x_i \geq t] \leq e^{-t^2/2} \quad (5.12)$$

を得る。同様に $\mathbb{P}[\sum a_i x_i \leq -t] \leq e^{-t^2/2}$ も示せるので (5.9) が成り立つ。 \square

組合せ論や理論計算機分野では定理 5.9 を Chernoff の不等式とよぶことも多いようだが、Ball は [5] で「函数解析の習慣にしたがって私は定理 5.9 を Bernstein の不等式とよぶが、確率論界限には Hoeffding の不等式として知られているおり、より強力で一般的な結果に Azuma–Hoeffding の不等式という名前がついている」と述べている。定理 5.9 にはいろいろな拡張、一般化があり、例えば [2] の付録 A を見るとよい。

系 5.3. 独立な確率変数 y_1, \dots, y_n が、各 i について $\mathbb{P}[y_i = 0] = \mathbb{P}[y_i = 1] = \frac{1}{2}$ をみたすならば、 $y := \sum_{i=1}^n y_i$ は $\mathbb{P}[|y - \frac{n}{2}| > t] \leq 2e^{-2t^2/n}$ をみたす。

証明. 定理 5.9 の確率変数 x_i を用いて $y_i = \frac{1}{2}(x_i + 1)$ とかける。(5.12) より

$$\mathbb{P}[y - \frac{n}{2} > t] = \mathbb{P}[\frac{1}{2} \sum x_i > t] = \mathbb{P}[\sum \frac{1}{\sqrt{n}} x_i > \frac{2t}{\sqrt{n}}] \leq e^{-(2t/\sqrt{n})^2/2} = e^{-2t^2/n}$$

を得る。同様に $\mathbb{P}[y - \frac{n}{2} < -t]$ も評価できる。 \square

系 5.4. 独立な確率変数 x_1, \dots, x_n が、各 i について $x_i \in [-1, 1]$ かつ $\mathbb{E}[x_i] = 0$ をみたすならば、 $\mathbb{P}[\sum_{i=1}^n x_i > s] \leq e^{-s^2/(2n)}$ が成り立つ。

証明. 実数 λ に対して $f(x) = e^{\lambda x}$ とおくと、曲線 $y = f(x)$ は下に凸で二点 $(-1, e^{-\lambda})$, $(1, e^{\lambda})$ を通る。この二点を通る直線を $y = g(x)$ とすると

$$\mathbb{E}[f(x_i)] \leq \mathbb{E}[g(x_i)] = g(\mathbb{E}[x_i]) = g(0) = \frac{e^{\lambda} + e^{-\lambda}}{2}$$

である。これと (5.10) から $a_i = 1/\sqrt{n}$ として (5.11) が成り立ち、(5.12) がしたがう。ここで $t = s/\sqrt{n}$ とおくと目標の不等式を得る。 \square

5.3.2 立方体の測度集中

頂点集合 $[n]$ 上のハイパーグラフは、以下のように n 次元立方体 $\{0, 1\}^n$ と関連づけられる。 $a \in \{0, 1\}^n$ の第 i 成分を a_i とかく。つまり $a = (a_1, \dots, a_n)$ である。このとき $\tilde{a} = \{i : a_i = 1\} \in 2^{[n]}$ が一意に定まり、 a は \tilde{a} の特性ベクトルであるという。この対応で $\{0, 1\}^n$ と $2^{[n]}$ をしばしば同一視する。

n 次元立方体 $C_n := \{0, 1\}^n$ にハミング距離と一様確率測度を入れる。すなわち、 $a, b \in C_n$ に対してその距離を $d(a, b) := \#\{i : a_i \neq b_i\} = |\tilde{a} \triangle \tilde{b}|$ とし、 $A \subset C_n$ の測度を $P(A) := 2^{-n}|A|$ と定める。さらに $t > 0$ に対して、 A の t 近傍を

$$A_t := \{b \in C_n : \text{ある } a \in A \text{ が存在して } d(a, b) \leq t\}$$

と定める。 C_n における中心 a , 半径 r の球 $B(a, r)$ とは、 $\{a\}_r$ のこと (つまり $A = \{a\}$ の r 近傍) のことである。中心を指定しないときは、 $B(r)$ ともかく。部分集合 $A \subset C_n$ が擬球であるとは、ある r について $B(r) \subset A \subset B(r+1)$ をみたすことをいう。

定理 5.10 (Harper). 任意の正整数 t と $A \subset C_n$ が与えられたとき、ある擬球 $B \subset C_n$ が存在して $|A| = |B|$ かつ $|A_t| \geq |B_t|$ をみたす。

この定理は立方体の等周定理と考えられる。特に $|A| = 2^{n-1}$ の場合は、 n が奇数ならば $B = B(\frac{n-1}{2})$, n が偶数ならば $B = B(0, \frac{n}{2} - 1) \cup \{b \in B(0, \frac{n}{2}) : b_n = 0\}$ が定理をみたす。後者に対応する $2^{[n]}$ の部分集合族は $\bigcup_{k=0}^{\frac{n}{2}-1} \binom{[n]}{k} \cup \binom{[n-1]}{n/2}$ である。

定理 5.11 (立方体の測度集中). $A \subset C_n$ が $P[A] \geq \frac{1}{2}$ をみたせば、

$$1 - P[A_t] \leq \exp(-2t^2/n)$$

が成り立つ。

証明. C_n を $2^{[n]}$ と同一視して、 $A \subset 2^{[n]}$ と考える。

$n = 2k + 1$ の場合。球 $B = \binom{[n]}{0} \cup \cdots \cup \binom{[n]}{k}$ は $P[B] = \frac{1}{2}$ で、その t 近傍は

$$B_t = \binom{[n]}{0} \cup \cdots \cup \binom{[n]}{k+t}$$

より、

$$\begin{aligned} 1 - P[B_t] &= 1 - 2^{-n} \left(\binom{n}{0} + \cdots + \binom{n}{k+t} \right) \\ &= 2^{-n} \left(\binom{n}{k+t+1} + \cdots + \binom{n}{n} \right) \\ &= 2^{-n} \left(\binom{n}{0} + \cdots + \binom{n}{k-t} \right) \end{aligned}$$

である。

$P[A] \geq P[B]$ と定理 5.10 から $P[A_t] \geq P[B_t]$ である。したがって

$$1 - P[A_t] \leq 1 - P[B_t] = 2^{-n} \left(\binom{n}{0} + \cdots + \binom{n}{k-t} \right) =: x$$

を得る。そこで $x < \exp(-2t^2/n)$ を示したい。

独立な確率変数 y_1, \dots, y_n が $\mathbb{P}[y_i = 0] = \mathbb{P}[y_i = 1] = \frac{1}{2}$ をみたすとする。 $y = y_1 + \cdots + y_n$ とおく。補題 5.3 (の証明) から、 $a > 0$ に対して

$$\mathbb{P}[y \leq \frac{n}{2} - a] \leq \exp(-2a^2/n)$$

が成り立つ。 $\mathbb{P}[y = i] = 2^{-n} \binom{n}{i}$ だから

$$\begin{aligned} x &= \mathbb{P}[y \leq k - t] = \mathbb{P}[y \leq \frac{n}{2} - (\frac{1}{2} + t)] \\ &\leq \exp(-2(\frac{1}{2} + t)^2/n) \leq \exp(-2t^2/n) \end{aligned}$$

を得る。つまり $1 - P[A_t] \leq \exp(-2t^2/n)$ である。

$n = 2k$ の場合。擬球 $B = \binom{[n]}{0} \cup \cdots \cup \binom{[n]}{k-1} \cup \binom{[n-1]}{k}$ は $P[B] = \frac{1}{2}$ で $B_t = \binom{[n]}{0} \cup \cdots \cup \binom{[n]}{k+t}$ より、 $1 - P[B_t] = 2^{-n} \left(\binom{n}{0} + \cdots + \binom{n}{k-t-1} \right)$ である。したがって

$$1 - P[A_t] \leq 1 - P[B_t] = 2^{-n} \left(\binom{n}{0} + \cdots + \binom{n}{k-t-1} \right) =: z$$

が成り立つ。先と同様に

$$\begin{aligned} z &= \mathbb{P}[Y \leq k - t - 1] = \mathbb{P}[y \leq \frac{n}{2} - (1 + t)] \\ &\leq \exp(-2(1 + t)^2/n) \leq \exp(-2t^2/n) \end{aligned}$$

を得る。つまりこの場合も $1 - P[A_t] \leq \exp(-2t^2/n)$ である。 □

5.3.3 エクспанダグラフの測度集中

グラフ $G = (V, E)$ と $A, B \subset V$ に対して、 A, B 間の辺数を $e(A, B)$ とかく。つまり $e(A, B) = \#\{ab \in E : a \in A, b \in B\}$ である。 G の辺拡大率 $\Phi(G)$ を

$$\Phi(G) := \min \left\{ \frac{e(A, V \setminus A)}{|A|} : A \subset V, 1 \leq |A| \leq |V|/2 \right\}$$

と定める。 G の最大次数を $\Delta(G)$ とかく。 n 頂点グラフ G_n の列 $\{G_n\}$ が定数次数エクспанダであるとは、定数 n_0, Φ, Δ が存在して、 $n \geq n_0$ ならば $\Phi(G_n) \geq \Phi$ かつ $\Delta(G_n) \leq \Delta$ をみたすことをいう。

n 頂点グラフ G に距離 d と一様確率測度 P を入れる。すなわち、 $a, b \in V$ の対して $d(a, b)$ は a と b を結ぶ最短パスの辺数、 $A \subset V$ に対して $P(A) = |A|/n$ である。さらに A の t 近傍 A_t を $\{v \in V : \text{ある } a \in A \text{ が存在して } d(v, a) \leq t\}$ と定める。

定理 5.12. 定数 $0 < \Phi \leq \Delta$ が与えられ、 n 頂点グラフ $G = (V, E)$ が $\Phi(G) \geq \Phi$ かつ $\Delta(G) \leq \Delta$ をみたすとする。このとき $A \subset V$ が $P(A) \geq \frac{1}{2}$ をみたせば、任意の $t > 0$ に対して

$$1 - P(A_t) \leq \frac{1}{2} \exp(-2t\Phi/\Delta)$$

が成り立つ。

証明. V の分割 $V = B^0 \sqcup B^1 \sqcup \dots$ を $B^0 := A, i \geq 1$ に対して $B^i := A_i \setminus A_{i-1}$ と定める。さらに $e_i := e(B^i, B^{i+1}), C^i := V \setminus A_i$ とおく。 t に関する帰納法で

$$1 - P(A_t) \leq \frac{1}{2} \left(\frac{\Delta - \Phi}{\Delta + \Phi} \right)^t \quad (5.13)$$

を示す。これがいえると

$$\frac{1}{2} \left(\frac{\Delta - \Phi}{\Delta + \Phi} \right)^t = \frac{1}{2} \left(1 - \frac{2\Phi}{\Delta + \Phi} \right)^t < \frac{1}{2} \left(1 - \frac{2\Phi}{\Delta} \right)^t < \frac{1}{2} \exp(-2t\Phi/\Delta)$$

から目標の評価が得られる。 $b_i := |B^i|, c_i := |C_i|$ とおく。

$t = 1$ のとき、

$$\Delta b_1 \geq e_0 + e_1, \quad e_0 \geq \Phi(b_1 + c_1), \quad e_1 \geq \Phi c_1$$

より、 $\Delta b_1 \geq \Phi(b_1 + 2c_1)$ 、すなわち $(\Delta - \Phi)b_1 \geq 2\Phi c_1$ である。これと $b_1 + c_1 \leq n/2$ から $(\Delta - \Phi)(n/2 - c_1) \geq (\Delta - \Phi)b_1 \geq 2\Phi c_1$ である。これを整理すると

$$1 - P(A_1) = P(C_1) = \frac{c_1}{n} \leq \frac{1}{2} \left(\frac{\Delta - \Phi}{\Delta + \Phi} \right)$$

を得る。

次に $t-1$ まで (5.13) が成り立つと仮定する。つまり

$$\frac{c_{t-1}}{n} = \frac{b_t + c_t}{n} \leq \frac{1}{2} \left(\frac{\Delta - \Phi}{\Delta + \Phi} \right)^{t-1}$$

である。 $t=1$ の場合と同様に

$$\Delta b_t \geq e_{t-1} + e_t, \quad e_{t-1} \geq \Phi(b_t + c_t), \quad e_t \geq \Phi c_t$$

から $\Delta b_t \geq \Phi(2b_t + c_t)$ を得る。これと帰納法の仮定から

$$1 - P(A_t) = \frac{c_t}{n} \leq \frac{1}{2} \left(\frac{\Delta - \Phi}{\Delta + \Phi} \right)^t$$

がしたがう。 \square

5.3.4 球面の測度集中

部分集合 $A, B \subset \mathbb{R}^n$ に対して $A + B := \{a + b : a \in A, b \in B\}$ と定める。 A または B が空集合のときは、 $A + B$ も空集合と定める。

補題 5.1. 非空な可測集合 $A, B \subset \mathbb{R}$ に対して $\mu^*(A + B) \geq \mu(A) + \mu(B)$ が成り立つ^{†8}。ただし μ はルベーグ測度、 μ^* は外測度をあらわす。

証明. A, B がコンパクトのときは、 $A + B$ もコンパクトで可積分である。この場合は平行移動して $\max A = 0 = \min B$ とすると、 $A \cap B = \{0\}$,

$$A + B \supset (A + \{0\}) + (\{0\} + B) = A \cup B$$

である。したがって $\mu(A + B) \geq \mu(A \cup B) = \mu(A) + \mu(B)$ を得る。

一般に可測集合は内側からコンパクト集合で近似できる。つまり A が可測で $\mu(A) = a$ のとき、任意の $\epsilon > 0$ に対して測度が $a - \epsilon$ 以上の A のコンパクトな部分集合が存在する。そこで A, B のかわりにこのようなコンパクト部分集合を考えることで目標の不等式が得られる。 \square

定理 5.13 (Prékopa–Leindler の不等式). \mathbb{R}^n 上の非負可測実数値関数 m, f, g と実数 $t \in (0, 1)$ が与えられ、任意の $x, y \in \mathbb{R}^n$ について

$$m((1-t)x + ty) \geq f(x)^{1-t} g(y)^t \quad (5.14)$$

を仮定する。このとき

$$\int m \geq \left(\int f \right)^{1-t} \left(\int g \right)^t \quad (5.15)$$

が成り立つ。ただし積分は全空間 \mathbb{R}^n でおこなう。

^{†8} A, B が可測でも $A + B$ は可測とはかぎらない。

証明. m, f, g が有界で、積分値が有限の場合が本質的なので、このことを仮定する。また f, g をそれぞれ $f/\sup f, g/\sup g$ で置きかえる^{†9} ことで、はじめから $\sup f = \sup g = 1$ と仮定してよい。

定理を次元 n に関する帰納法で証明する。はじめに $n = 1$ の場合を示す。 f のレベル集合を $F_z := \{x \in \mathbb{R} : f(x) \geq z\}$ と定め、 $|F_z|$ でその長さ（測度）をあらわす。このときルベグ積分の定義（あるいはフビニの定理）から

$$\int_{\mathbb{R}} f(x) dx = \int_0^1 |F_z| dz$$

であり、同様のことが m, g についても成り立つ。(5.14) により、 $f(x) \geq z$ かつ $g(x) \geq z$ ならば $m((1-t)x + ty) \geq z$ だから

$$M_z \supset (1-t)F_z + tG_z$$

である。この右辺の F_z, G_z は $0 \leq z < 1$ のとき空でない^{†10} から、補題 5.1 により

$$|M_z| \geq (1-t)|F_z| + t|G_z|$$

がしたがう。これを 0 から 1 まで積分すると

$$\int_{\mathbb{R}} m(x) dx = (1-t) \int_{\mathbb{R}} f(x) dx + t \int_{\mathbb{R}} g(x) dx$$

であり、右辺に AM/GM 不等式^{†11} を適用して (5.15) の $n = 1$ の場合を得る。

次に定理が $n - 1$ まで正しいと仮定して、 m, f, g が \mathbb{R}^n 上の関数の場合を扱う。 f から $n - 1$ 変数関数 f_z を $f_z(x_1, \dots, x_{n-1}) := f(x_1, \dots, x_{n-1}, z)$ と定め、同様に g_z, m_z も定める。 (x_1, \dots, x_{n-1}, z) を (x, z) と略記し、 $c := (1-t)a + tb$ とおくと、(5.14) より $m((1-t)(x, a) + t(y, b)) \geq f(x, a)^{1-t} g(y, b)^t$ 、つまり

$$m_c((1-t)(x) + ty) \geq f_a(x)^{1-t} g_b(y)^t$$

である。したがって帰納法の仮定から

$$\int_{\mathbb{R}^{n-1}} m_c \geq \left(\int_{\mathbb{R}^{n-1}} f_a \right)^{1-t} \left(\int_{\mathbb{R}^{n-1}} g_b \right)^t \quad (5.16)$$

を得る。ここで 1 変数関数 F を $F(a) := \int_{\mathbb{R}^{n-1}} f_a$ と定め、同様に G_b, M_c も定めると、(5.16) は $M(c) = M((1-t)a + tb) \geq F(a)^{1-t} G(b)^t$ とかける。これに既に示した帰納法

^{†9} この置き換えで (5.14) および結論の不等式の右辺の値は変化しない。

^{†10} このために $\sup f = \sup g = 1$ とした。

^{†11} $p, q > 0, t \in (0, 1)$ のとき $(1-t)p + tq \geq p^{1-t} q^t$ 。

の $n = 1$ の場合を適用すると $\int_{\mathbb{R}} M \geq \left(\int_{\mathbb{R}} F\right)^{1-t} \left(\int_{\mathbb{R}} G\right)^t$ である。ここでフビニの定理から $\int_{\mathbb{R}} F = \int_{\mathbb{R}} \left(\int_{\mathbb{R}^{n-1}} f_a\right) = \int_{\mathbb{R}^n} f$ 等に注意すると

$$\int_{\mathbb{R}^n} m \geq \left(\int_{\mathbb{R}^n} f\right)^{1-t} \left(\int_{\mathbb{R}^n} g\right)^t$$

を得る。 \square

補題 5.2. 任意のコンパクト集合 $A, B \subset \mathbb{R}^n$ と任意の実数 $s \in (0, 1)$ に対して

$$\mu((1-s)A + sB) \geq \mu(A)^{1-s} \mu(B)^s \quad (5.17)$$

が成り立つ^{†12}。ただし μ はルベグ測度をあらわす。

証明. A の特性関数を $f : \mathbb{R}^n \rightarrow \mathbb{R}$ とすると $\mu(A) = \int_{\mathbb{R}^n} f$ である。同様に B の特性関数を g とし、 $C := (1-s)A + sB$ とおいてその特性関数を m とする。 $f(x) = 1$ かつ $g(y) = 1$ ならば $m((1-s)x + sy) = 1$ だから、任意の $x, y \in \mathbb{R}^n$ について $m((1-s)x + sy) \geq f(x)^{1-s} g(y)^s$ が成り立つ。したがって定理 5.13 から (5.17) を得る。 \square

$n-1$ 次元単位球面 S^{n-1} 上の一様確率測度を \mathbb{P} とする。 $t > 0$ と $A \subset S^{n-1}$ に対して、 A_t で A からのユークリッド距離が t 以下の S^{n-1} 上の点全体をあらわす。 A_t を A の t 近傍という。

定理 5.14 (球面の測度集中). 任意の $t > 0$ と任意の $A \subset S^{n-1}$ に対して、もし $\mathbb{P}[A] \geq \frac{1}{2}$ ならば、 $1 - \mathbb{P}[A_t] \leq 2 \exp(-t^2 n/4)$ が成り立つ^{†13}。

証明. S^{n-1} に対応する球体 B^n の中心を原点とし、 $C := S^{n-1} \setminus A_t$ とおく。このとき任意の $a \in A$ と $c \in C$ について $|a - c| \geq t$ である。 \tilde{A} で A の点と原点を結ぶ線分上の点全体をあらわすと、 $\mathbb{P}[A] = \mu(\tilde{A})/\mu(B^n)$ である。

まずミンコフスキー和 $\frac{1}{2}(\tilde{A} + \tilde{C})$ が、原点中心で半径 $1 - t^2/8$ の n 次元球体に含まれることを示そう。つまり任意の $\tilde{x} \in \tilde{A}$ と $\tilde{y} \in \tilde{C}$ について

$$\left| \frac{\tilde{x} + \tilde{y}}{2} \right| \leq 1 - \frac{t^2}{8} \quad (5.18)$$

を示す。 $x, y \in A$ を用いて $\tilde{x} = \alpha x$, $\tilde{y} = \beta y$ とあらわす。ただし、 $0 < \alpha \leq \beta < 1$ としてよい。原点、 x , $z := \frac{x+y}{2}$ を頂点とする直角三角形において、 $|x| = 1$ と $|z - x| \geq \frac{t}{2}$ より

$$|z| \leq \sqrt{1 - (t/2)^2} \leq 1 - (t^2/8)$$

^{†12} A または B は空集合でもよい。

^{†13} 実は右辺は $\sqrt{\frac{\pi}{8}} \exp(-t^2 n/2)$ に改善できる [11]。

が成り立つ。三角不等式から

$$\begin{aligned} \left| \frac{\tilde{x} + \tilde{y}}{2} \right| &= \left| \frac{\alpha x + \beta y}{2} \right| = \left| \alpha \frac{x+y}{2} + (\beta - \alpha) \frac{y}{2} \right| \leq \alpha \left| \frac{x+y}{2} \right| + (\beta - \alpha) \left| \frac{y}{2} \right| \\ &\leq \alpha |z| + \frac{1-\alpha}{2} \leq \alpha \left(1 - \frac{t^2}{8} \right) + \frac{1-\alpha}{2} = \alpha \left(\frac{1}{2} - \frac{t^2}{8} \right) + \frac{1}{2} \leq 1 - \frac{t^2}{8}, \end{aligned}$$

すなわち (5.18) が示された。

次に \tilde{A}, \tilde{C} に補題 5.2 を ($s = \frac{1}{2}$ として) 適用すると

$$\begin{aligned} \left(1 - \frac{t^2}{8} \right)^n \mu(B^n) &\geq \mu \left(\frac{1}{2} (\tilde{A} + \tilde{C}) \right) \geq \sqrt{\mu(\tilde{A})\mu(\tilde{C})} \\ &= \mu(B^n) \sqrt{\mathbb{P}[A]\mathbb{P}[C]} \geq \mu(B^n) \sqrt{\frac{1}{2} \mathbb{P}[C]}, \end{aligned}$$

つまり

$$1 - \mathbb{P}[A_t] = \mathbb{P}[C] \leq 2 \left(1 - \frac{t^2}{8} \right)^{2n} \leq 2 \exp(-t^2 n/4)$$

を得る。 □

定理 5.15 (Brunn–Minkowski). 任意の非空コンパクト集合 $A, B \subset \mathbb{R}^n$ に対して

$$\mu(A+B)^{1/n} \geq \mu(A)^{1/n} + \mu(B)^{1/n}$$

が成り立つ。

証明. $\mu(A) = 0$ または $\mu(B) = 0$ ならば目標の不等式は自明なので、 $\mu(A) > 0$ かつ $\mu(B) > 0$ とする。 $\alpha = \mu(A)^{1/n}$, $\beta = \mu(B)^{1/n}$, $s = \beta/(\alpha + \beta)$, $A' = (1/\alpha)A$, $B' = (1/\beta)B$ とおく。 A', B' に補題 5.2 を適用する。まず

$$(1-s)A' + sB' = \frac{\alpha}{\alpha + \beta} A' + \frac{\beta}{\alpha + \beta} B' = \frac{1}{\alpha + \beta} (A + B)$$

より、(5.17) の左辺は $\mu((1-s)A' + sB') = (\alpha + \beta)^{-n} \mu(A+B)$ である。次に $\mu(A') = \alpha^{-n} \mu(A) = 1$, 同様に $\mu(B') = 1$ より、(5.17) の右辺は 1 である。したがって $\mu(A+B) \geq (\alpha + \beta)^n$, つまり $\mu(A+B)^{1/n} \geq \alpha + \beta = \mu(A)^{1/n} + \mu(B)^{1/n}$ を得る。 □

B を \mathbb{R}^n の単位球体とし、その体積を $v(B)$ とかく。 $t > 0$ に対して、 B の t 近傍 B_t を B からの距離が t 以内の点全体と定める。このとき、コンパクト集合 $A \subset \mathbb{R}^n$ が B と等積、つまり $v(A) = v(B)$ ならば、 $v(A_t) \geq v(B_t)$ が成り立つ。これを確かめるため、 $B_t = B + tB$ より、 $v(B_t) = (1+t)^n v(B)$ であることに注意すると、定理 5.15 より、

$$\begin{aligned} v(A_t) &= v(A + tB) \geq (v(A)^{1/n} + v(tB)^{1/n})^n = (v(B)^{1/n} + v(tB)^{1/n})^n \\ &= ((1+t)v(B)^{1/n})^n = v(B_t) \end{aligned}$$

を得る。これは等周定理とよばれる結果の典型であって、定理 5.10 はこれの離散版のひとつである。

5.3.5 Johnson–Lindenstrauss の平坦化補題

単位球面 S^{n-1} は \mathbb{R}^n のユークリッド距離によって距離空間とみなせる。 S^{n-1} 上の実数値関数 f がリプシッツ連続であるとは、任意の $x, y \in S^{n-1}$ について

$$|f(x) - f(y)| \leq |x - y|$$

をみたすことをいう。確率論の習慣にしたがって $\mathbb{P}[\{x \in S^{n-1} : f(x) \geq m\}]$ を $\mathbb{P}[f \geq m]$ 等と略記し、 $\{x \in S^{n-1} : f(x) \geq m\}$ を $(f \geq m)$ ともかく。

定理 5.16 (Lévy の補題). 関数 $f : S^{n-1} \rightarrow \mathbb{R}$ がリプシッツ連続ならば、ある $m \in \mathbb{R}$ が存在して任意の $t \in (0, 1]$ について

$$\mathbb{P}(|f - m| > t) \leq 4 \exp(-t^2 n/4)$$

が成り立つ。

証明. ある m が存在して、 $L := (f \leq m)$ および $H := (f \geq m)$ の両者の測度が $1/2$ 以上になる。実際、中央値 $m := \sup\{\mathbb{P}[f \leq z] \leq \frac{1}{2}\}$ をとればよい。

L の t 近傍を L_t とかくとき、任意の $x \in L_t$ について

$$f(x) \leq m + t \tag{5.19}$$

が成り立つとしよう。このとき $L_t \subset (f \leq m + t)$ より

$$\mathbb{P}[f > m + t] = 1 - \mathbb{P}[f \leq m + t] \leq 1 - \mathbb{P}[L_t]$$

であり、右辺は定理 5.14 から $\leq 2 \exp(-t^2 n/4)$ と評価できる。

そこで (5.19) を示そう。 $x \in L_t$ とすると、ある $y \in L$ が存在して $|x - y| \leq t$ および $f(y) \leq m$ をみたす。さらに f がリプシッツ連続であることも用いると

$$f(x) - m \leq f(x) - f(y) \leq |f(x) - f(y)| \leq |x - y| \leq t$$

を得る。同様に H を用いて $\mathbb{P}[f < m + t] \leq 2 \exp(-t^2 n/4)$ もしたがう。 \square

単位球面 S^{n-1} 上の点 $x = (x_1, \dots, x_n)$ から、先頭 k 個の座標が張る k 次元空間 L_0 への正射影を $\phi(x) = (x_1, \dots, x_k)$ とし、その長さを

$$f(x) = |\phi(x)| = \sqrt{x_1^2 + \dots + x_k^2}$$

とおく。 $f : S^{n-1} \rightarrow \mathbb{R}$ はリプシッツ連続である。次の補題は Maoušek による？

補題 5.3. 任意の $n > k$ に対して、ある m が存在して、任意の $t > 0$ に対して

$$\mathbb{P}[|f - m| > t] \leq 4 \exp(-t^2 n/4)$$

が成り立つ。さらに任意の $c_1 > 4$, $0 < c_2 < 1 - 2/\sqrt{c_1}$ に対して、ある n_0 が存在して、任意の $n \geq n_0$ に対して、 $k \geq c_1 \log n$ ならば $m \geq c_2 \sqrt{k/n}$ が成り立つ。

証明. 前半の主張は定理 5.16 からただちに仕がう。

後半の主張を示すため、 $\mathbb{E}[f^2]$ を評価して m の下界を得よう。 $x \in S^{n-1}$ を一様ランダムに選ぶとき、 $1 = \mathbb{E}[|x|^2] = \sum_{i=1}^n \mathbb{E}[x_i^2]$ と対称性から $\mathbb{E}[x_i^2] = 1/n$ 、したがって $\mathbb{E}[f^2] = k/n$ である。ここで任意の $t > 0$ に対して、 $\mathbb{P}[f \leq m+t] \leq 1$, $\mathbb{P}[f > m+t] \leq 2 \exp(-t^2 n/4)$ および $\max_x f(x)^2 \leq 1$ から、

$$\begin{aligned} \frac{k}{n} &= \mathbb{E}[f^2] \\ &\leq \mathbb{P}[f \leq m+t](m+t)^2 + \mathbb{P}[f > m+t] \max_x f(x)^2 \\ &\leq (m+t)^2 + 2 \exp(-t^2 n/4) \end{aligned}$$

を得る。 $t = \sqrt{4k/(c_1 n)}$ とおくと $t^2 n/4 = k/c_1 \geq \log n$ より $\exp(-t^2 n/4) \leq 1/n$ だから、

$$\frac{k}{n} \leq (m+t)^2 + \frac{2}{n},$$

すなわち

$$m \geq \sqrt{\frac{k-2}{n}} - t = \sqrt{\frac{k}{n}} \left(1 - \frac{2}{\sqrt{c_1}} - o(1)\right) > c_2 \sqrt{\frac{k}{n}}$$

が仕がう。 □

補題 5.3 では S^{n-1} から L_0 への正射影を考えたが、 L_0 を任意の k 次元部分空間 $L \subset \mathbb{R}^n$ に取りかえても同じ結論が得られる。ここでは L が固定され、 $x \in S^{n-1}$ が一様ランダムに選ばれた。逆に $x \in S^{n-1}$ を固定して、 L を一様ランダムに選ぶことも考えられる。つまり L として、一様ランダムに選んだ回転 ρ を L_0 に施したものをとる。これは回転全体 $\text{SO}(n)$ に適切な確率測度（ハール測度）を入れることで実現できる。この測度を P_H とかき、 $\rho \in \text{SO}(n)$ に対して ϕ_ρ で S^{n-1} から $L = \rho(L_0)$ への正射影をあらわすと、補題 5.3 の結果は固定した $x \in S^{n-1}$ について

$$P_H[\{\rho \in \text{SO}(n) : |\phi_\rho(x) - m| > t\}] \leq 4 \exp(-t^2 n/4) \quad (5.20)$$

と書き換えられる。

次の定理は Johnson–Lindenstrauss の平坦化補題とよばれる。これは \mathbb{R}^n 上に与えられた n 点について、2 点間の距離を「ほとんど」保ったまま、ずっと低い次元 k に埋め込めることを主張する。つまり 2 点間の距離の $1 \pm \epsilon$ 倍程度の歪みを許容するなら、

$k \sim \epsilon^{-2} \log n$ の次元の空間に n 点配置を実現できる。証明のアイデアは単純で、 \mathbb{R}^n の k 次元部分空間 L を「ランダムに」選び、与えられた n 点を L に正射影するだけである。

定理 5.17 (Johnson–Lindenstrauss). 任意の $\epsilon \in (0, 1)$ と $\{p_1, \dots, p_n\} \subset \mathbb{R}^n$ に対して、ある $k = \Omega(\epsilon^{-2} \log n)$ と $\{q_1, \dots, q_n\} \subset \mathbb{R}^k$ が存在して、

$$(1 - \epsilon) |p_i - p_j| \leq |q_i - q_j| \leq (1 + \epsilon) |p_i - p_j|$$

が任意の $1 \leq i < j \leq n$ について成り立つ。

証明. k 次元部分空間 $L = \rho(L_0) \subset \mathbb{R}^n$ を一様ランダムに選び、 S^{n-1} から L への正射影を ϕ_ρ とする。(5.20) で定まる m をとり、 $1 \leq i < j \leq n$ について

$$A_{i,j} := \{\rho : (1 - \epsilon)m |p_i - p_j| \leq |\phi_\rho(p_i) - \phi_\rho(p_j)| \leq (1 + \epsilon)m |p_i - p_j|\}$$

とおく。 ϕ_ρ は線形なので、 $\phi_\rho(p_i) - \phi_\rho(p_j) = \phi_\rho(p_i - p_j)$ であり、 $u = p_i - p_j$ とおくと

$$A_{i,j} = \{\rho : (1 - \epsilon)m |u| \leq |\phi_\rho(u)| \leq (1 + \epsilon)m |u|\}$$

とかける。さらに $|u| = 1$ としてよいから、 $u \in S^{n-1}$ を固定して $A_{i,j}$ のかわりに

$$A = \{\rho : (1 - \epsilon)m \leq |\phi_\rho(u)| \leq (1 + \epsilon)m\} = \{\rho : ||\phi_\rho(u)| - m| \leq \epsilon m\}$$

とおく。このとき

$$P_H[\rho \notin A] < 1/n^2 \tag{5.21}$$

を示そう。これがいえると、ペア i, j の総数が $\binom{n}{2}$ であることと union bound から、 $P_H[\bigcap_{1 \leq i < j \leq n} A_{i,j}] > 0$ である。この条件をみたす ρ を選び、各 i について $q_i := \phi_\rho(p_i)/m$ とおくと定理の不等式がしたがう。

さて (5.21) であるが、(5.20) で $t = \epsilon m$ とおくと

$$P_H[\rho \notin A] \leq 4 \exp(-\epsilon^2 m^2 n/4)$$

である。さらに補題 5.3 において $k \geq 36\epsilon^{-2} \log n$ とし n を十分大きくとると $m \geq \frac{1}{2}\sqrt{k/n}$ とできる。このとき $\epsilon^2 m^2 n/4 \geq \epsilon^2 k/16 \geq (9/4) \log n$ だから、

$$4 \exp(-\epsilon^2 m^2 n/4) \leq 4n^{-9/4}$$

を得る。右辺は $n > 256$ ならば $1/n^2$ より小さい。つまり (5.21) が成り立つ。 \square

5.3.6 マルチンゲールと置換の測度集中

Ω を有限集合、 $(\Omega, \mathcal{F}, \mathbb{P})$ を確率空間、 f を確率変数とする。 σ 代数の列

$$\mathcal{F}_0 \subset \mathcal{F}_1 \subset \cdots \subset \mathcal{F}_n = \mathcal{F} \quad (5.22)$$

が与えられ、 $\mathcal{F}_0 = \{\emptyset, \Omega\}$, $\mathcal{F}_n = 2^\Omega$ とする。このとき、確率変数の列 f_0, f_1, \dots, f_n が各 i について $f_i = \mathbb{E}[f_{i+1} | \mathcal{F}_i]$ をみたせば、列 f_i を $\{\mathcal{F}_i\}$ によるマルチンゲールという。特に確率変数 f に対して $f_i := \mathbb{E}[f | \mathcal{F}_i]$ と定めると、列 f_0, f_1, \dots, f_n ($f_0 = \mathbb{E}[f]$, $f_n = f$) は $\{\mathcal{F}_i\}$ によるマルチンゲールである^{†14}。

以下ではさらに

$$\Omega \text{ の分割 } \Omega_0, \Omega_1, \dots, \Omega_n \text{ があり、} \Omega_{i+1} \text{ は } \Omega_i \text{ の細分で、} \mathcal{F}_i = 2^{\Omega_i} \quad (5.23)$$

を仮定する。例えば $\Omega = \{1, 2, 3\}$ で、

$$\begin{aligned} \Omega_0 &= \{\{1, 2, 3\}\}, & \mathcal{F}_0 &= \{\emptyset, \Omega\}, \\ \Omega_1 &= \{\{1\}, \{2, 3\}\}, & \mathcal{F}_1 &= \{\emptyset, \{1\}, \{2, 3\}, \Omega\}, \\ \Omega_2 &= \Omega, & \mathcal{F}_2 &= 2^\Omega \end{aligned}$$

などである^{†15}。 Ω_i の要素をアトムとよぶ。上の例では $\Omega_0, \Omega_1, \Omega_2$ のアトムの個数はそれぞれ 1, 2, 3 である。一般に $\omega \in A \in \mathcal{F}_i$ ならば、任意の確率変数 g に対して

$$\mathbb{E}[g | \mathcal{F}_i](\omega) = \frac{1}{|A|} \sum_{a \in A} g(a)$$

が成り立つ。(これを条件付き期待値の定義として、以下を読んでもよい。) さらに

$$\begin{aligned} \mathbb{E}[\mathbb{E}[g | \mathcal{F}_i]] &= \mathbb{E}[g], \\ \mathbb{E}[hg | \mathcal{F}_i] &= h\mathbb{E}[g | \mathcal{F}_i] \end{aligned}$$

などが成り立つ。ただし h は \mathcal{F}_i 可測、すなわち任意の区間 $I \subset \mathbb{R}$ に対して $h^{-1}(I) \in \mathcal{F}_i$ とする。次の補題は吾妻一興 (あづまかずおき) による結果 [8] の特別な場合である。この不等式から、列 $\mathbb{E}[f] = f_0, f_1, \dots, f_n = f$ において、隣り合う確率変数の差が小さければ、 f はその平均から大きく離れないことがわかる。

^{†14} これを Doob のマルチンゲールという。なお、この定義や以下に述べる補題 5.4 は、 Ω が有限集合でない場合も適切な設定と解釈のもとで正当化できて、むしろ確率論ではその場合が本質的である。 Ω が有限の場合には、期待値の計算に有限個の足し算しか現れず、積分に関するあらゆる面倒を避けられる。また定理 5.18 の証明にはそれで十分である。しかしマルチンゲールは組合せ論においても強力な手法なので、興味をもたれた読者はぜひ標準的な確率論の教科書 (例えば [10]) を参照されたい。

^{†15} 厳密には $\Omega_n = \{\{i\} : i \in [n]\}$ とすべきだが、これを Ω と同一視する。

補題 5.4. Ω を有限集合、 $(\Omega, \mathcal{F}, \mathbb{P})$ を確率空間、 f を確率変数とする。(5.22), (5.23) によるマルチンゲール f_0, \dots, f_n において、 $d_i := f_i - f_{i-1}$, $c_i := \max_{\omega \in \Omega} |d_i(\omega)|$ とおく。このとき任意の $t > 0$ について

$$\max \{ \mathbb{P}[f - \mathbb{E}[f] \geq t], \mathbb{P}[f - \mathbb{E}[f] \leq -t] \} \leq \exp \left(-\frac{t^2}{2 \sum_{i=1}^n c_i^2} \right)$$

が成り立つ^{†16}。

証明. $m_i := f_i - f_0$ とおくと、 $m_0 = 0$, $m_n = f - \mathbb{E}[f]$, $m_i - m_{i-1} = d_i$ である。 c_i の定義と (5.10) を用いると、 $\lambda > 0$ と任意の $\omega \in \Omega$ に対して

$$e^{\lambda d_i(\omega)} \leq (e^{\lambda c_i} + e^{-\lambda c_i})/2 \leq e^{\lambda^2 c_i^2/2},$$

よって $\mathbb{E}[e^{\lambda d_i} | \mathcal{F}_{i-1}] \leq e^{\lambda^2 c_i^2/2}$ である。ここから

$$\mathbb{E}[e^{\lambda m_n} | \mathcal{F}_{n-1}] = \mathbb{E}[e^{\lambda d_n} e^{\lambda m_{n-1}} | \mathcal{F}_{n-1}] = e^{\lambda m_{n-1}} \mathbb{E}[e^{\lambda d_n} | \mathcal{F}_{n-1}] \leq e^{\lambda m_{n-1}} e^{\lambda^2 c_n^2/2}$$

を得る。したがって

$$\mathbb{E}[e^{\lambda m_n}] = \mathbb{E}[\mathbb{E}[e^{\lambda m_n} | \mathcal{F}_{n-1}]] \leq \mathbb{E}[e^{\lambda m_{n-1}} e^{\lambda^2 c_n^2/2}] = e^{\lambda^2 c_n^2/2} \mathbb{E}[e^{\lambda m_{n-1}}]$$

が成り立つ。これを繰り返して

$$\begin{aligned} \mathbb{E}[e^{\lambda m_n}] &\leq e^{\lambda^2 c_n^2/2} \mathbb{E}[e^{\lambda m_{n-1}}] \leq e^{\lambda^2 c_n^2/2} e^{\lambda^2 c_{n-1}^2/2} \mathbb{E}[e^{\lambda m_{n-2}}] \\ &\leq \dots \leq e^{\lambda^2 (c_n^2 + c_{n-1}^2 + \dots + c_1^2)/2} \mathbb{E}[e^{\lambda m_0}] = e^{\lambda^2 \sum_{i=1}^n c_i^2/2} \end{aligned}$$

がしたがう。これとマルコフの不等式から

$$\mathbb{P}[m_n \geq t] = \mathbb{P}[e^{\lambda m_n} \geq e^{\lambda t}] \leq e^{-\lambda t} \mathbb{E}[e^{\lambda m_n}] \leq e^{-\lambda t + \lambda^2 \sum_{i=1}^n c_i^2/2}$$

であるが、ここで $\lambda := t / \sum_{i=1}^n c_i^2$ とおくと

$$\mathbb{P}[m_n \geq t] \leq \exp \left(-\frac{t^2}{2 \sum_{i=1}^n c_i^2} \right)$$

である。 $\mathbb{P}[-m_n \geq t]$ についても同じ評価が成り立つ。 \square

正整数 n を固定する。全単射 $\sigma : [n] \rightarrow [n]$ を n 文字の置換とよび、その全体を S_n とかく。 $|S_n| = n!$ である。ここでは S_n を n 文字の順列の集合と捉え、群構造は考慮しない。 S_n に一様な測度を入れる。つまり $A \subset S_n$ に対して

$$\mathbb{P}[A] := |A|/n!$$

^{†16} したがって union bound から $\mathbb{P}[|f - \mathbb{E}[f]| \geq t] \leq 2 \exp \left(-\frac{t^2}{2 \sum_{i=1}^n c_i^2} \right)$ がしたがう。

とおく。また正規化されたハミング距離 d を $\sigma, \rho \in S_n$ に対して

$$d(\sigma, \rho) := \#\{i : \sigma(i) \neq \rho(i)\}/n$$

と定める。さらに $U \subset S_n$, $t > 0$ に対して

$$\begin{aligned} d(\sigma, U) &:= \min\{d(\sigma, \rho) : \rho \in U\}, \\ U_t &:= \{\sigma \in S_n : d(\sigma, U) \leq t\} \end{aligned}$$

とおく。

定理 5.18 (Maurey [9]). 任意の $U \subset S_n$ と $t > 0$ に対して、

$$\mathbb{P}[U] (1 - \mathbb{P}[U_t]) \leq \exp\left(-\frac{t^2 n}{32}\right)$$

が成り立つ。特に $\mathbb{P}[U] \geq \frac{1}{2}$ ならば $1 - \mathbb{P}[U_t] \leq 2 \exp(-t^2 n/32)$ である。

証明. S_n にマルチンゲールを構成する。 $\Omega = [n]$ とし、 $1 \leq j < n$ に対して Ω の分割 Ω_j をアトム A_{i_1, \dots, i_j} の集合とする。ここで i_1, \dots, i_j は相異なる添字で、

$$A_{i_1, \dots, i_j} := \{\sigma \in S_n : \sigma(1) = i_1, \dots, \sigma(j) = i_j\}$$

とする。つまり A_{i_1, \dots, i_j} は先頭 j 文字を指定した文字列集合で、 $|\Omega_j| = \binom{n}{j} j!$ である。 $\Omega_0 := \{\Omega\}$, $\Omega_n := \Omega$ とし、 $0 \leq j \leq n$ に対して $\mathcal{F}_j := 2^{\Omega_j}$ とおく。このとき列 (5.22) と確率空間 $(\Omega, \mathcal{F}_n, \mathbb{P})$ 上の任意の確率変数 f から $f_j := \mathbb{E}[f | \mathcal{F}_j]$ はマルチンゲールを定める。

ここで $U \subset S_n$ を固定し、あらためて f を $f(\sigma) := d(\sigma, U)$ と定義する。このとき $d_j := f_j - f_{j-1}$ とおくと任意の $\sigma \in \Omega$ について

$$|d_j(\sigma)| \leq \frac{2}{n} \quad (5.24)$$

が成り立つ。まずこれを仮定して、ここから定理がしたがうことを確認しよう。 $c_j := \frac{2}{n}$, $\mu := \mathbb{E}[f]$ において補題 5.4 を適用すると、任意の $t > 0$ について

$$\max\{\mathbb{P}[f - \mu \geq t], \mathbb{P}[f - \mu \leq -t]\} \leq \exp\left(-\frac{t^2 n}{8}\right) \quad (5.25)$$

である。 $U = \{\sigma \in \Omega : f(\sigma) = 0\} \subset \{\sigma \in \Omega : f(\sigma) - \mu \leq -\mu\}$ に注意して、(5.25) で $t := \mu$ とおくと、 $\mathbb{P}[U] \leq \mathbb{P}[f - \mu \leq -\mu] \leq \exp(-\mu^2 n/8)$ を得る。よって $\rho := \mathbb{P}[U]$ とおくと、 $\mu \leq \sqrt{\frac{8}{n} \log \frac{1}{\rho}}$ である。この右辺を t_0 と定め、再び (5.25) から $\mathbb{P}[f - t_0 \geq t] \leq \mathbb{P}[f - \mu \geq t] \leq \exp(-t^2 n/8)$, さらに $t \geq t_0$ ならば t を $t - t_0$ で置き換えて $\mathbb{P}[f \geq t] \leq \exp(-(t - t_0)^2 n/8)$ を得る。そこで、 $t \geq 2t_0$ の場合には、 $(t - t_0)^2 \geq t^2/4$ を用いて

$$1 - \mathbb{P}[U_t] = \mathbb{P}[f \geq t] \leq \exp(-t^2 n/32)$$

がしたがう。次に $0 < t \leq 2t_0$ の場合には、 t_0 の定義により

$$\mathbb{P}[U] = \rho = \exp(-t_0^2 n/8) \leq \exp(-t^2 n/32)$$

である。まとめると、 $\mathbb{P}[U]$ と $1 - \mathbb{P}[U_t]$ はどちらも 1 以下であり、どんな $t > 0$ に対しても、少なくとも片方は $\exp(-t^2 n/32)$ 以下である。つまり (5.24) を仮定すると、定理の不等式が得られた。

最後に (5.24) を示す。 $\sigma \in A = A_{i_1, \dots, i_{j-1}} \in \Omega_{j-1}$ とする。 A は Ω_j のアトム $B = A_{i_1, \dots, i_{j-1}, r}$, $C = A_{i_1, \dots, i_{j-1}, s}$ 等によって、 $A = B \sqcup C \sqcup \dots$ のように分割される。このとき全単射 $\phi: B \rightarrow C$ で、任意の $b \in B$ について $d(b, \phi(b)) = \frac{2}{n}$ となるものがある。実際、 b における r, s の位置を交換したものを $\phi(b)$ とすればよい。つまり、 $b(k) = s$ として、 $c := \phi(b) \in C$ を $c(j) := s$, $c(k) := r$, $i \notin \{j, k\}$ ならば $c(i) := b(i)$ と定める。さらに $|f(b) - f(c)| \leq \frac{2}{n}$ が成り立つ。これをみるために、 $f(b) = d(b, x)$, $f(c) = d(c, y)$, $x, y \in T$ としよう。一般性を失わず $f(b) \geq f(c)$ としてよい。このとき三角不等式により、

$$f(b) - f(c) = d(b, x) - d(c, y) \leq d(b, y) - d(c, y) \leq d(b, c) = \frac{2}{n}$$

である。つまり各 $b \in B$ について

$$|f(b) - f(\phi(b))| \leq \frac{2}{n} \quad (5.26)$$

が成り立つことが確かめられた。さて $\sigma \in B$ とすると、定義から

$$f_j(\sigma) = \frac{1}{|B|} \sum_{b \in B} f(b), \quad f_j(\phi(\sigma)) = \frac{1}{|C|} \sum_{c \in C} f(c)$$

である。これと (5.26) から

$$|f_j(b) - f_j(\phi(b))| \leq \frac{2}{n}$$

を得る。したがって A が $|A|/|B|$ 個の Ω_j のアトムに分割されることに注意すると

$$\begin{aligned} f_{j-1}(\sigma) &= \frac{1}{|A|} \sum_{a \in A} f(a) = \frac{1}{|A|} \left(\sum_{b \in B} f(b) + \sum_{c \in C} f(c) + \dots \right) \\ &= \frac{|B|}{|A|} (f_j(\sigma) + f_j(\phi(\sigma)) + \dots) \\ &\leq \frac{|B|}{|A|} \left(f_j(\sigma) + \left(f_j(\sigma) + \frac{2}{n} \right) + \dots \right) \leq f_j(\sigma) + \frac{2}{n}, \end{aligned}$$

つまり $f_{j-1}(\sigma) - f_j(\sigma) \leq \frac{2}{n}$, 同様に $f_{j-1}(\sigma) - f_j(\sigma) \geq -\frac{2}{n}$ も得られる。□

定理 5.18 の証明は Milman–Schechtman の [11] および McDiarmid の [12] を参考にした。

参考文献

- [1] P. Erdős and J. H. Spencer, *Probabilistic methods in combinatorics*, Probability and Mathematical Statistics, Vol. 17, Academic Press, New York-London, 1974; MR0382007
- [2] N. Alon and J. H. Spencer, *The probabilistic method*, fourth edition, Wiley Series in Discrete Mathematics and Optimization, Wiley, Hoboken, NJ, 2016; MR3524748
- [3] Y. Zhao, Lecture notes (MIT 18.226 Fall 2022) Probabilistic Methods in Combinatorics, Massachusetts Institute of Technology, https://yufeizhao.com/pm/probmethod_notes.pdf
- [4] R. A. Moser and G. Tardos, A constructive proof of the general Lovász local lemma, *J. ACM* **57** (2010), no. 2, Art. 11, 15 pp.; MR2606086
- [5] K. M. Ball, An elementary introduction to modern convex geometry, in *Flavors of geometry*, 1–58, Math. Sci. Res. Inst. Publ., 31, Cambridge Univ. Press, Cambridge, ; MR1491097
- [6] J. Matoušek, *Lectures on discrete geometry*, Graduate Texts in Mathematics, 212, Springer, New York, 2002; MR1899299
- [7] I. Kantor, J. Matoušek and R. Šámal, *Mathematics++*, Student Mathematical Library, 75, Amer. Math. Soc., Providence, RI, 2015; MR3379631
- [8] K. Azuma, Weighted sums of certain dependent random variables, *Tohoku Math. J. (2)* **19** (1967), 357–367; MR0221571
- [9] B. Maurey, Construction de suites symétriques, *C. R. Acad. Sci. Paris Sér. A-B* **288** (1979), no. 14, A679–A681; MR0533901
- [10] 舟木 直久, 確率論, 講座 数学の考え方 20, 276 pp. 朝倉書店 2004 年
- [11] V. D. Milman and G. Schechtman, *Asymptotic theory of finite-dimensional normed spaces*, Lecture Notes in Mathematics, 1200, Springer, Berlin, 1986; MR0856576
- [12] C. J. H. McDiarmid, Concentration, in *Probabilistic methods for algorithmic discrete mathematics*, 195–248, Algorithms Combin., 16, Springer, Berlin, ; MR1678578