

有限等質空間上の符号理論における 3-point bound

広島大学 先進理工系科学研究科 伊藤元気*

Genki Ito

Graduate School of Advanced Science and Engineering,
Hiroshima University

概要

誤り訂正符号や多重交差族は、有限等質空間上の符号と捉えることができる。符号理論において、符号のサイズの上限評価は重要な問題である。符号のサイズの上限評価としては Delsarte の線形計画法 [2] が有名であり、これは 2-point bound と呼ばれる事が多い。これに対して、一部の空間では 2-point bound よりも強い評価を与える 3-point bound が知られている。本稿では、有限等質空間に対して表現論的な視点から 3-point bound の一般論を構築する。また、例として誤り訂正符号に対して 3-point bound を適用し、既存の研究と比較する。

1 導入

まずは、等質空間上の符号を定義していく。

以下、群 G が集合 X に推移的に作用しているとする。このとき、 G は X^k に対角に作用する。

$$g \cdot (x_1, \dots, x_k) := (g \cdot x_1, \dots, g \cdot x_k).$$

この作用 $G \curvearrowright X^k$ についての軌道空間 $I_k = G \backslash X^k$ と自然な全射 $R_k : X^k \rightarrow I_k$ を考える。また、 $A \subset I_k$ を一つ固定する。

定義 1.1. 空でない部分集合 $C \subset X$ が (k -relation) A -free code であるとは、任意の $x_1, \dots, x_k \in C$ に対して $R_k(x_1, \dots, x_k) \notin A$ となることをいう。

いくつか例を見ていく。まず有名な例として誤り訂正符号がある。ここでいう誤り訂正符号とは次のものである。

定義 1.2 (誤り訂正符号). $n, e \in \mathbb{Z}_{\geq 0}$ とする。 $C \subset \mathbb{F}_2^n$ が e -誤り訂正符号であるとは、異なる任意の $x, y \in C$ に対して $\partial(x, y) \geq 2e + 1$ となることをいう。ただし、 $\partial : \mathbb{F}_2^n \times \mathbb{F}_2^n \rightarrow \{0, \dots, n\}$ はハミング距離 $\partial(x, y) = \text{wt}(x - y)$ である。

$G = \mathfrak{S}_n \ltimes \mathbb{F}_2^n$, $X = \mathbb{F}_2^n$ とおけば、 $k = 2, 3$ のときの軌道分解は次と同一視できる。

$$R_2 : \mathbb{F}_2^n \times \mathbb{F}_2^n \rightarrow \{0, \dots, n\}; (x, y) \mapsto \partial(x, y),$$

$$R_3 : \mathbb{F}_2^n \times \mathbb{F}_2^n \times \mathbb{F}_2^n \rightarrow \{0, \dots, n\}^3; (x, y, z) \mapsto (\partial(x, y), \partial(y, z), \partial(z, x)).$$

* Email: genki-ito@hiroshima-u.ac.jp

本研究は、JST 次世代研究者挑戦的研究プログラム JPMJSP2132 の支援を受けたものです。

よって

$$A_2 := \{1, \dots, 2e\} \subset I_2,$$

$$A_3 := \{(i, j, k) \in I_3 \mid \{i, j, k\} \cap \{1, \dots, 2e\} \neq \emptyset\} \subset I_3$$

とおけば, e -誤り訂正符号は 2-relation A_2 -free code と 3-relation A_3 -free code の両方と同値である.

次に, 別の例として多重交差族がある.

定義 1.3 (多重交差族). $n, d, k \in \mathbb{Z}_{\geq 0}$ とする. n 点集合 $[n] := \{1, \dots, n\}$ の d 点部分集合全体を $J(n, d)$ と表す. $C \subset J(n, d)$ が k 重交差族であるとは, 任意の $x_1, \dots, x_k \in C$ に対して $\bigcap_{i=1}^k x_i \neq \emptyset$ となることをいう.

$G = \mathfrak{S}_n, X = J(n, d)$ とおけば, $k = 2, 3$ のときの軌道分解は次と同一視できる.

$$R_2 : J(n, d) \times J(n, d) \rightarrow \{0, \dots, d\}; (x, y) \mapsto |x \cap y|,$$

$$R_3 : J(n, d) \times J(n, d) \times J(n, d) \rightarrow \{0, \dots, d\}^4; (x, y, z) \mapsto (|x \cap y|, |y \cap z|, |z \cap x|, |x \cap y \cap z|).$$

よって

$$A_2 := \{0\} \subset I_2,$$

$$A_3 := \{(i, j, s, t) \in I_3 \mid t = 0\} \subset I_3$$

とすれば, 二重交差族は 2-relation A_2 -free code と, 三重交差族は 3-relation A_3 -free code と同値である.

もう一つ, 有限等質空間ではないが, コンパクト等質空間上の符号の例として Spherical code がある.

定義 1.4 (spherical code). 有限集合 $C \subset S^{n-1}$ が, 任意の $x, y \in C (x \neq y)$ に対して $\langle x, y \rangle \leq \cos \theta$ を満たすとき, C を minimal angular distance θ の spherical code という.

これは直交群 $O(n)$ による作用 $O(n) \curvearrowright S^{n-1}$ のもとでの free code として理解できる. この spherical code は, 組合せ論における古典的な問題である「接吻数問題」と関連する. 接吻数問題とは n 次元球の表面に (同じ半径の) 球をいくつ置けるかの最大値を求める問題である. この問題は minimal angular distance が $\frac{\pi}{3}$ である spherical code の最大サイズを求める問題と同値である. 接吻数の上限評価については, Delsarte–Goethals–Seidel による 2-point bound [3] よりも Bachoc–Vallentin による 3-point bound [1] のほうが多くの次元でよい評価を与えている.

2 2-point bound

まず, 2-point bound について復習する.

設定は以下のとおりである.

- $G \curvearrowright X$: 有限等質空間,
- $I_2 := G \backslash X^2$,
- $R_2 : X^2 \twoheadrightarrow I_2$: 自然な全射,
- $i_2^0 := R_2(x, x) \in I_2$,
- $A \subset I_2$.
- $C \subset X$: 2-relation A -free code.

定義 2.1 (2-inner distribution). $a_2^C : I_2 \rightarrow \mathbb{R}$ を次で定義する.

$$a_2^C(i_2) := \frac{|\{(c_1, c_2) \in C \times C \mid R_2(c_1, c_2) = i_2\}|}{|C|}.$$

これを C の 2-inner distribution という.

すぐに次がわかる.

命題 2.2. $\sum_{i_2 \in I_2} a_2^C(i_2) = |C|$.

よって, これを目的関数にすることで, C のサイズを評価することができる. 以下, 制約条件を導出していく.

命題 2.3. (1) 任意の $i_2 \in I_2$ に対して, $a_2^C(i_2) \geq 0$.

(2) $a_2^C(i_2^0) = 1$.

(3) I_2 には $\mathfrak{S}_2$ が自然に作用し, a_2^C は $\mathfrak{S}_2$ 不変である.

(4) $i_2 \in A$ ならば, $a_2^C(i_2) = 0$.

以下, $(W, \langle \cdot, \cdot \rangle)$ を $\mathbb{R}$ 上の有限次元内積空間とする. さらに, $\delta : X \rightarrow W; x \mapsto \delta_x$ に対して, $\langle \delta, \delta \rangle : X \times X \rightarrow \mathbb{R}$ は G 不変であるとする. すなわち, 次の図式を可換にするような $Q^2 : I_2 \rightarrow \mathbb{R}$ が取れる.

$$\begin{array}{ccc} X^2 & \xrightarrow{R} & I_2 \\ \delta^2 \downarrow & \circlearrowleft & \downarrow Q^2 \\ W^2 & \xrightarrow{\langle \cdot, \cdot \rangle} & \mathbb{R} \end{array}$$

このとき, 次が成り立つ.

命題 2.4. $\sum_{i_2 \in I_2} Q^2(i_2) a_2^C(i_2) \geq 0$.

Delsarte の 2-point bound [2] の制約条件はこの枠組みで導出できる.

$(Q_\xi^2)_{\xi \in \Xi}$ を上の方法で得られる $Q_\xi^2 : I_2 \rightarrow \mathbb{R}$ の族とする.

定理 2.5. 2-relation A -free code のサイズは, 次の線型計画問題の最適解以下である.

$$\begin{array}{ll} \text{Maximize} & \sum_{i_2 \in I_2} a(i_2) \\ \text{Subject to} & \bullet a : I_2 \rightarrow \mathbb{R}_{\geq 0} : \mathfrak{S}_2 \text{ 不変,} \\ & \bullet a(i_2^0) = 1, \\ & \bullet a(i_2) = 0 \text{ if } i_2 \in A, \\ & \bullet \forall \xi \in \Xi, \sum_{i_2 \in I_2} Q_\xi^2(i_2) a(i_2) \geq 0. \end{array}$$

3 3-point bound

3.1 抽象論

設定は以下のとおりである.

- $G \curvearrowright X$: 有限等質空間,
- $I_2 := G \backslash X^2$, $I_3 := G \backslash X^3$,
- $R_2 : X^2 \twoheadrightarrow I_2$, $R_3 : X^3 \twoheadrightarrow I_3$: 自然な全射,
- $i_3^0 := R_3(x, x, x) \in I_3$.
- $A \subset I_3$.
- $C \subset X$: 3-relation A -free code.

定義 3.1 (3-inner distribution). $a_3^C : I_3 \rightarrow \mathbb{R}$ を次で定義する.

$$a_3^C(i_3) := \frac{|\{(c_1, c_2, c_3) \in C \times C \times C \mid R_3(c_1, c_2, c_3) = i_3\}|}{|C|}.$$

これを C の 3-inner distribution という.

3-inner distribution の性質として, 直ぐに次がわかる.

命題 3.2. (1) 任意の $i_3 \in I_3$ に対して, $a_3^C(i_3) \geq 0$.

(2) $a_3^C(i_3^0) = 1$.

(3) I_3 には $\mathfrak{S}_3$ が自然に作用し, a_3^C は $\mathfrak{S}_3$ 不変である.

(4) $i_3 \in A$ ならば, $a_3^C(i_3) = 0$.

定義 3.3 (generalized 3-inner product space). W を $\mathbb{R}$ 上の有限次元線形空間とし, $\Omega \subset W$ を convex cone とする. W 上の $\mathfrak{S}_3$ 不変三重線型写像 $\theta : W \times W \times W \rightarrow \mathbb{R}$ が, 任意の $\omega \in \Omega$ に対して $\theta(\omega, \omega, \omega) \geq 0$ を満たすとき, (W, Ω, θ) を generalized 3-inner product space という.

以下, (W, Ω, θ) を generalized 3-inner product space とする. ここで, 写像 $\eta : X \rightarrow \Omega$ であって $\theta \circ \eta^3 : X^3 \rightarrow \mathbb{R}$ が G 不変となるものを考える. すなわち, 次の図式を可換にするような $Q^3 : I_3 \rightarrow \mathbb{R}$ が取れる.

$$\begin{array}{ccc} X^3 & \xrightarrow{R} & I_3 \\ \eta^3 \downarrow & \circlearrowleft & \downarrow Q^3 \\ W^3 & \xrightarrow{\theta} & \mathbb{R} \end{array}$$

この Q^3 を用いて, 次のような条件を手に入れる.

命題 3.4. $\sum_{i_3 \in I_3} Q^3(i_3) a_3^C(i_3) \geq 0$.

ここで, 3-point bound の条件に 2-point bound の条件を含めるために, 次の写像を定義する.

命題 3.5. $\gamma : I_2 \rightarrow I_3$ を

$$\gamma([x, y]) := [x, y, y]$$

とすれば, γ は well-defined である.

この γ を通すと, 次がわかる.

命題 3.6. (1) $a_2^C = a_3^C \circ \gamma$.

(2) $\gamma(i_2^0) = i_3^0$.

(3) C が 3-relation A -free code ならば, C は 2-relation $\gamma^{-1}(A)$ -free code である.

特に, 3-inner distribution を用いても C のサイズを表すことができる.

系 3.7. $\sum_{i_2 \in I_2} a_3^C(\gamma(i_2)) = |C|.$

よって、これを最適化問題の目的関数にできる。また、命題 3.6 により、2-inner distribution の性質を 3-point bound に持ち込むことができる。

さらに、もう一つ条件を追加する。

命題 3.8. $\left(\sum_{i_2 \in I_2} a_3^C(\gamma(i_2)) \right)^2 \leq \sum_{i_3 \in I_3} a_3^C(i_3).$

系 3.9. $\begin{pmatrix} 1 & \sum_{i_2 \in I_2} a_3^C(\gamma(i_2)) \\ \sum_{i_2 \in I_2} a_3^C(\gamma(i_2)) & \sum_{i_3 \in I_3} a_3^C(i_3) \end{pmatrix} \succeq 0.$

この条件は、目的関数として $\sum_{I_3} a(i_3)$ ではなく $\sum_{i_2 \in I_2} a(\gamma(i_2))$ を使う理由である。

これによって、 A -free code のサイズの上限評価を得ることができる。 $(Q_\lambda^3)_{\lambda \in \Lambda}$ を上の方法で得られる $Q_\lambda^3 : I_3 \rightarrow \mathbb{R}$ の族とする。

定理 3.10. 3-relation A -free code のサイズは、次の半正定値計画問題の最適解以下である。

$$\begin{aligned} & \text{Maximize} && \sum_{i_2 \in I_2} a(\gamma(i_2)) \\ & \text{Subject to} && \begin{aligned} & \bullet \ a : I_3 \rightarrow \mathbb{R}_{\geq 0} : \mathfrak{S}_3 \text{ 不変}, \\ & \bullet \ a(i_3^0) = 1, \\ & \bullet \ a(i_3) = 0 \text{ if } i_3 \in A, \\ & \bullet \ \forall \xi \in \Xi, \sum_{i_2 \in I_2} Q_\xi^2(i_2) a(\gamma(i_2)) \geq 0, \\ & \bullet \ \forall \lambda \in \Lambda, \sum_{i_3 \in I_3} Q_\lambda^3(i_3) a(i_3) \geq 0, \\ & \bullet \ \begin{pmatrix} 1 & \sum_{i_2 \in I_2} a(\gamma(i_2)) \\ \sum_{i_2 \in I_2} a(\gamma(i_2)) & \sum_{i_3 \in I_3} a(i_3) \end{pmatrix} \succeq 0. \end{aligned} \end{aligned}$$

注意 3.11. 変数の $\mathfrak{S}_3$ 不変性により、この SDP は $I'_3 = I_3 / \mathfrak{S}_3$ 上の SDP と捉えられる。すなわち、変数を $a' : I'_3 \rightarrow \mathbb{R}$ として扱える。 Q^3 も $\mathfrak{S}_3$ 不変であるため、3-point 条件 $\sum_{i_3 \in I_3} Q^3(i_3) a(i_3)$ も I'_3 上の線型結合に書き換えられる。

また、変数の $\mathfrak{S}_3$ 不変性を条件から除くと、上限評価の精度は落ちるようである [4]。

3.2 既約分解を用いた具体的な generalized 3-inner product

ここから、具体的な generalized 3-inner product を用意し、これにより 3-point bound を構築する。ここでは、[1] を参考に表現論的な視点で構築していく。

先程の設定に加えて、以下を付け足す。

- $x_0 \in X$,
- $H := G_{x_0} : G$ の x_0 における安定化群,
- $H \curvearrowright \mathbb{R}^X$ の各既約部分表現は絶対既約を仮定。

generalized 3-inner product として次を用意する.

$$W := \mathbb{R}^X \oplus S^2(\mathbb{R}^X),$$

$$\Omega := \mathbb{R}^X \oplus S^2(\mathbb{R}^X)_{\geq 0},$$

$$\theta : W^3 \rightarrow \mathbb{R}; \quad ((f_1, \alpha_1), (f_2, \alpha_2), (f_3, \alpha_3)) \mapsto \langle f_1 \odot f_2, \alpha_3 \rangle + \langle f_2 \odot f_3, \alpha_1 \rangle + \langle f_3 \odot f_1, \alpha_2 \rangle.$$

ここで, $S^2(\mathbb{R}^X)$ は対称テンソル空間であり, $\odot$ は対称テンソル積である.

ここから, $H \curvearrowright \mathbb{R}^X$ の標準分解を用いていく.

$$\mathbb{R}^X = \bigoplus_{\rho=1}^s \bigoplus_{l=1}^{m_\rho} V_{\rho,l}$$

を H 表現についての標準分解とする. すなわち, 各 $V_{\rho,l}$ は H 既約であり, $V_{\rho,l} \cong V_{\rho',l'}$ ならば $\rho = \rho'$ である. このとき, Schur の補題により次の同型が得られる.

命題 3.12. $S^2(\mathbb{R}^X)^H \cong \bigoplus_{\rho=1}^s \text{Sym}_{m_\rho}(\mathbb{R})$. ただし, $\text{Sym}_{m_\rho}(\mathbb{R})$ は m_ρ 次の対称行列全体の空間である.

各 $\rho \in \{1, \dots, s\}$ と $w \in \mathbb{R}^{m_\rho}$ に対して, $w \otimes w \in \text{Sym}_{m_\rho}(\mathbb{R}) \subset \bigoplus_{\rho} \text{Sym}_{m_\rho}(\mathbb{R})$ を上の同型で移したものを $\alpha_w \in S^2(\mathbb{R}^X)^H$ とする. ここで, $\eta_w : X \rightarrow \Omega$ を

$$\eta_w(x) := (\delta_x, g_x \cdot \alpha_w)$$

とおく. ただし, $g_x \in G$ は $g_x \cdot x_0 = x$ を満たすものであり, $g_x \cdot \alpha_w$ は g_x の取り方によらないため, これは well-defined である.

命題 3.13. $\theta \circ \eta_w^3 : X^3 \rightarrow \mathbb{R}$ は G 不変である.

よって, $Q_{\rho,w}^3 : I_3 \rightarrow \mathbb{R}$ が誘導される.

$$\begin{array}{ccc} X^3 & \xrightarrow{R} & I_3 \\ \eta_w^3 \downarrow & \circlearrowleft & \downarrow Q_{\rho,w}^3 \\ W^3 & \xrightarrow{\theta} & \mathbb{R} \end{array}$$

ところで, $\theta \circ \eta_w^3$ を具体的に計算すると

$$\theta \circ \eta_w^3(x, y, z) = {}^t w B_\rho(x, y, z) w$$

のような二次形式の形になる (B_ρ は w に依存しない). よって, I_3 上に誘導されるものは

$$Q_{\rho,w}^3(i_3) = {}^t w \tilde{Q}_\rho^3(i_3) w$$

と書ける. よって, これらの無限個の線型条件は一つの半正定値条件にまとめることができる.

系 3.14. $\sum_{i_3 \in I_3} \tilde{Q}_\rho^3(i_3) a_3^C(i_3) \succeq 0$.

4 計算結果

ここでは, 上で構成した具体的な generalized 3-inner product を用いた 3-point bound を誤り訂正符号に対して計算した. 既約分解の方法は [5] を参考にした. 以下, 最小ハミング距離 d 以上の誤り訂正符号 $C \subset \mathbb{F}_2^n$ のサイズの上限評価を, Schrijver [5] による 3-point bound と比較した結果を示す. 計算には

SDPA (Version 7.3.16) を使用した.

n	d	Schrijver [5]	今回の結果
19	6	1280	1280
23	6	13766	13766
25	6	47998	48008
19	8	142	142
20	8	274	274
25	8	5477	5477
27	8	17768	17768
28	8	32151	32151
22	10	87	87
25	10	503	503
26	10	886	886

表 1 誤り訂正符号のサイズの上限評価

多くの次元で Schrijver の評価と同じ結果が得られたが, 一部のパラメータでは Schrijver よりも弱い評価となっている. そのため, Schrijver の結果を今回の 3-point bound の枠組みで再現するためには, 別の generalized 3-inner product を追加で構築する必要があると考えられる.

また, 今回 2-point bound の条件としては従来の Delsarte bound の条件を使用した, この条件を除いても数値は変わらなかった.

謝辞

本稿は, 2026 年 6 月に開催された RIMS 共同研究「表現論とその周辺分野の交流」における著者の講演内容に基づいて作成した講究録である. このような貴重な発表の機会を賜りました神奈川大学の小林雅人先生に, 心より感謝申し上げます.

参考文献

- [1] C. Bachoc and F. Vallentin. *New upper bounds for kissing numbers from semidefinite programming*. J. Amer. Math. Soc. 21.3 (2008).
- [2] P. Delsarte. *An algebraic approach to the association schemes of coding theory*. Philips Res. Rep. Suppl. 10 (1973).
- [3] P. Delsarte, J. M. Goethals, and J. J. Seidel. *Spherical codes and designs*. Geometriae Dedicata 6.3 (1977).
- [4] D. C. Gijswijt. *Matrix Algebras and Semidefinite Programming Techniques for Codes*. PhD thesis. University of Amsterdam, 2005. arXiv: 1007.0906.
- [5] A. Schrijver. *New code upper bounds from the Terwilliger algebra and semidefinite programming*. IEEE Trans. Inform. Theory 51.8 (2005).