# Terwilliger 代数に基づく符号の半正定値計画限界

田中 太初
東北大学大学院情報科学研究科
E-mail: htanaka@ims.is.tohoku.ac.jp

## 1 はじめに

$F := \{0, 1, \ldots, q-1\}$ $(q \geqslant 2)$ とし、$\partial_H(\cdot,\cdot)$ を $F^n$ 上の Hamming 距離とする。すなわち、$x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n) \in F^n$ に対し $\partial_H(x, y) := |\{1 \leqslant i \leqslant n : x_i \neq y_i\}|$ と定める。長さ $n$ の符号 $C \subseteq F^n$ の最小距離を $d(C) := \min\{\partial_H(x, y) : x, y \in C, x \neq y\}$ とする。情報通信に於いて、多くの情報を伝達する上で $C$ の位数はできるだけ大きい方が望ましい。一方で、高い誤り訂正能力を保証するために最小距離 $d(C)$ も大きくすることが要請される。(符号理論に関する基本的文献として [25, 23] を挙げておく。) 以上の動機から次のパラメータを導入する：

$$A_q(n, d) := \max\{|C| : C \subseteq F^n, d(C) \geqslant d\}$$

このパラメータに関しては多くの研究がある (cf. [1]) が、一般に $A_q(n, d)$ をきちんと決定することは極めて難しく、まず良い評価を与えることが問題となる：

**Problem 1.1.** Find a good upper bound on $A_q(n, d)$.

典型的な例として次を挙げる。

**Example 1.2.** 最小距離が $d$ 以上の符号 $C$ の各符号語 $x \in C$ に対し半径 $e := \lfloor d/2 \rfloor$ の球 $B_e(x) := \{y \in F^n : \partial_H(x, y) \leqslant e\}$ を取ると、これらの球は明らかに互いに交わらない (すなわち $C$ は $e$-誤り訂正符号である)。従って $|B_e(x)| = \sum_{i=0}^{e} \binom{n}{i}(q-1)^i$ より次の sphere-packing 限界 を得る：

$$A_q(n, d) \cdot \sum_{i=0}^{e} \binom{n}{i}(q-1)^i \leqslant q^n$$

この限界の等号を満たす符号を完全符号 (perfect code) と呼ぶ。

本稿の目的は最近 Schrijver [34, 18] により提唱された $A_q(n, d)$ の**半正定値計画限界**を紹介することである。Delsarte [10] による**線型計画限界**は $A_q(n, d)$ の上限を与える最も一般的かつ強力な手法として 30 年以上にわたって君臨してきたが[1]、後で見るように Schrijver の半正定値計画限界は少なくとも線型計画限界より良い上限を与えることが保証されている。ただしこれは今後直ちに線型計画限界が半正定値計画限界に席巻される

[1] もちろん Delsarte の手法を拡張する試みは多く行われてきた。§5.2 を参照されたい。

ことを意味するものではない。Delsarte は線型計画限界を単に導入するのみならず、それを駆使して符号 (及びデザイン (§5.1)) に関する驚くべき理論を構築した。特に、上述の最小距離を含む符号のわずか 4 つのパラメータ間の相互関係からその符号の種々の性質を導く彼の議論は圧巻である。半正定値計画限界は現時点では個々の $n$, $q$, $d$ に対し計算機を用いて限界を具体的に計算している段階であり、この限界に基づいて「新たな Delsarte 理論」が生まれるかどうかは今後の進展にかかっている。従って本稿ではその期待も込めて、比較のため線型計画限界に関する解説も加えることにした。Delsarte 理論の多くの部分はアソシエーションスキーム (association scheme) と呼ばれる組合せ構造に於いて一般的に成立する。本稿では基本的に通常の意味での符号の枠組みである Hamming スキームのみを取り扱うが、Delsarte 理論の一般性及び応用範囲の広さを強調するため、アソシエーションスキームの定義、諸性質等から始めることにする[2]。

## 2 Association schemes

以下 $X$ を有限集合とし、$\{\hat{x} : x \in X\}$ を基底とする $\mathbb{C}$ 上ベクトル空間を $\mathbb{C}^X$ と表す。また、$\mathbb{C}^{X\times X}$ を行と列が $X$ で添え字付けられた $\mathbb{C}$ 上の行列全体の成す代数とする。このとき、$\mathbb{C}^{X\times X}$ は $\mathbb{C}^X$ 上に左から自然に作用する。

次に、$R_0, R_1, \ldots, R_n$ を $X \times X$ の空でない部分集合 (relations) とする。各 $0 \leqslant i \leqslant n$ について、$R_i$ の隣接行列 (adjacency matrix) $A_i \in \mathbb{C}^{X\times X}$ を以下の通り定める：

$$(A_i)_{xy} := \begin{cases} 1, & \text{if } (x,y) \in R_i, \\ 0, & \text{if } (x,y) \notin R_i. \end{cases}$$

**Definition 2.1.** We say the pair $(X, \{R_i\}_{i=0}^n)$ is a (symmetric) association scheme with $n$ classes if the following conditions are satisfied:

(AS1) $A_0 = I$ (the identity matrix),

(AS2) $A_0 + A_1 + \cdots + A_n = J$ (the all 1's matrix),

(AS3) $A_i^{\mathsf{T}} = A_i$ $(0 \leqslant i \leqslant n)$,

(AS4) $A_i A_j$ is a linear combination of $A_0, A_1, \ldots, A_n$ $(0 \leqslant i, j \leqslant n)$.

上の (AS4) は $|\{z \in X : (x,y) \in R_i, (y,z) \in R_j\}|$ が $(x,y) \in R_k$ の取り方に依らず、$i$, $j$, $k$ により定まることを意味している。一方代数的には、$A_0, A_1, \ldots, A_n$ が $\mathbb{C}^{X\times X}$ の $n+1$ 次元部分代数を生成することを意味する。この代数を $\mathcal{M}$ $(:= \langle A_0, A_1, \ldots, A_n\rangle)$ と表記し、$(X, \{R_i\}_{i=0}^n)$ の Bose-Mesner 代数と呼ぶ。Bose-Mesner 代数は可換であり、また転置及び複素共役の作用に対し閉じていることから半単純である。従って $\mathcal{M}$ は原始冪等元 $E_0, E_1, \ldots, E_n$ から成る基底を持つ。ただし $E_0 := |X|^{-1}J$ とおく[3]。これら二種類の基底間の変換行列を $P$, $Q$ と表す：

$$(A_0, A_1, \ldots, A_n) = (E_0, E_1, \ldots, E_n)P$$
$$(E_0, E_1, \ldots, E_n) = |X|^{-1} \cdot (A_0, A_1, \ldots, A_n)Q$$

以後 $P$, $Q$ をそれぞれ第一固有行列 (first eigenmatrix), 第二固有行列 (second eigenmatrix) と呼ぶ。

[2] より詳しく知りたい方は [10, 7, 8] 等をご覧いただきたい。

[3] 明らかに $|X|^{-1}J$ は冪等であり、しかも $\mathrm{rank}(J) = 1$ より原始的である。

**Example 2.2.** $F := \{0, 1, \ldots, q-1\}$ $(q \geqslant 2)$ とし、$X := F^n$ とおく。$X$ 上の $n+1$ 個の関係 $R_0, R_1, \ldots, R_n$ を Hamming 距離により定める。すなわち

$$(x, y) \in R_i \Longleftrightarrow \partial_H(x, y) = i \quad (0 \leqslant i \leqslant n)$$

このとき $H(n, q) := (X, \{R_i\}_{i=0}^n)$ を Hamming スキームと呼ぶ。

実際 $H(n, q)$ が (AS4) を満たすことは、$R_0, R_1, \ldots, R_n$ が対称群 $\mathfrak{S}_q$ と $\mathfrak{S}_n$ の wreath 積 $G := \mathfrak{S}_q \wr \mathfrak{S}_n$ の $X \times X$ 上の軌道になっていることからも確認できる。さらにこの場合 $\mathcal{M} = \mathrm{End}_{\mathbb{C}[G]}(\mathbb{C}^X)$ (中心化環) となることが直ちに検証される。また、Delsarte は Hamming スキームの固有行列 $P, Q$ が Krawtchouk 多項式

$$K_j(z) = K_j(z; n, q) := \sum_{k=0}^{j} (-1)^k \binom{z}{k} \binom{n-z}{j-k} (q-1)^{j-k}$$

を用いて $P_{ij} = Q_{ij} = K_j(i)$ と表示されることを見出した。定義から既に明らかであるが、Hamming スキームは (通常の意味での) 符号の枠組みとして用いられる。

なお、$x = (x_1, \ldots, x_n) \in X$ の Hamming 重みを $\mathrm{wt}_H(x) := |\{1 \leqslant i \leqslant n : x_i \neq 0\}| = \partial_H(x, \mathbf{0})$ (ここで $\mathbf{0} := (0, \ldots, 0)$) により定めると、$q = 2$ の場合、各 $0 \leqslant k \leqslant n$ について部分集合 $\{x \in X : \mathrm{wt}_H(x) = k\}$ はまたアソシエーションスキームの構造を持つ。これを通常 $J(n, k)$ と表し、Johnson スキームと呼ぶ。Johnson スキームは等重み符号 (constant-weight code) や組合せ $t$-デザイン の枠組みである (§5.1)。

# 3 線型計画限界 (Delsarte, 1973)

前節の記号をそのまま用い、$H(n, q)$ を Hamming スキームとする $(q \geqslant 2)$。符号 $C \subseteq X(:= F^n)$ の内分布 (inner distribution) $\boldsymbol{a} = (a_0, a_1, \ldots, a_n)$ を

$$a_i := |C|^{-1} \cdot |\{(x, y) \in C \times C : \partial_H(x, y) = i\}| \quad (0 \leqslant i \leqslant n)$$

により定義する。$C$ の特性ベクトル (characteristic vector) $\chi_C := \sum_{x \in C} \hat{x} \left(\in \mathbb{C}^X\right)$ を用いると、$a_i = |C|^{-1} \cdot \chi^{\mathsf{T}} A_i \chi$ と表される。また、明らかに $a_i$ 達は非負であり、$a_0 = 1$, $|C| = a_0 + \cdots + a_d$ が成り立つ。内分布に関して決定的に重要なのが次の事実である[4]。

**Lemma 3.1.** *We have* $(\boldsymbol{a}Q)_j \geqslant 0$ *for* $0 \leqslant j \leqslant n$.

*Proof.* Note $(\boldsymbol{a}Q)_j = |C|^{-1} \cdot \sum_{i=0}^n \chi^{\mathsf{T}} A_i \chi \cdot Q_{ij} = |X||C|^{-1} \cdot \chi^{\mathsf{T}} E_j \chi$. □

内分布の成分 $a_0, a_1, \ldots, a_n$ を変数とみなすことにより、Delsarte は次の**線型計画限界**(**linear programming bound**) を得た：

**Theorem 3.2** (Delsarte [10])**.** *Consider the following linear programming problem:*

$$\ell_{\mathrm{LP}} = \ell_{\mathrm{LP}}(n, q, d) := \max \sum_{i=0}^{n} a_i$$

*subject to* $a_0 = 1$, $a_1 = \cdots = a_{d-1} = 0$, $a_i \geqslant 0$ $(d \leqslant i \leqslant n)$, $(\boldsymbol{a}Q)_j \geqslant 0$ $(1 \leqslant j \leqslant n)$. *Then* $A_q(n, d) \leqslant \ell_{\mathrm{LP}}$.

[4] $F$ が有限体かつ $C$ が線型符号のとき、$|C|^{-1} \cdot \boldsymbol{a}Q$ は $C$ の双対符号 $C^\perp$ の内分布に一致する [10, Chapter 6]。

一般に線型計画問題は simplex method により解くことができる。線型計画限界は非常に単純であるが、先に述べたように極めて強力な限界を与える。一例として、$(n,q,d)=(16,2,6)$ に対し $\ell_{\mathrm{LP}}(16,2,6)=256$ であるが、このパラメータを持つ位数 256 の符号は実際存在する (Nordstrom-Robinson 符号)。従って $A_2(16,6)=256$ を得る。

この例程度であれば線型計画問題を手計算で解くこともできるが、一般に $\ell_{\mathrm{LP}}(n,q,d)$ の値を公式の形で述べることは恐らく不可能であるし、たとえ計算機を用いるとしても誰も $n=1,000,000$ に対して実際に $\ell_{\mathrm{LP}}$ を求めようとは思わない。にも拘らず、Delsarte は線型計画法の双対性を導入することにより符号の種々の情報を得る手法を開発した：

**Theorem 3.3** (Delsarte [10])**.** *Set*

$$\ell^*_{\mathrm{LP}}=\ell^*_{\mathrm{LP}}(n,q,d):=\min\sum_{j=0}^{n}\binom{n}{j}(q-1)^j b_j$$

*subject to* $b_0=1$, $b_j\geqslant 0$ $(1\leqslant j\leqslant n)$, $(\boldsymbol{b}Q^{\mathsf{T}})_i\leqslant 0$ $(d\leqslant i\leqslant n)$. *Then* $\ell_{\mathrm{LP}}=\ell^*_{\mathrm{LP}}$.

ちなみに、不等式 $\ell_{\mathrm{LP}}\leqslant\ell^*_{\mathrm{LP}}$ は次の様に簡単に確かめられる。まず、$\boldsymbol{a}=(a_0,a_1,\ldots,a_n)$ 及び $\boldsymbol{b}=(b_0,b_1,\ldots,b_n)$ をそれぞれの問題の実行可能解とする。このとき $Q_{0j}=K_j(0)=\binom{n}{j}(q-1)^j$ に注意すると、

$$\sum_{i=0}^{n}a_i=(\boldsymbol{a}Q)_0\leqslant\sum_{j=0}^{n}(\boldsymbol{a}Q)_j b_j=\sum_{i=0}^{n}a_i\left(\boldsymbol{b}Q^{\mathsf{T}}\right)_i\leqslant\left(\boldsymbol{b}Q^{\mathsf{T}}\right)_0=\sum_{j=0}^{n}\binom{n}{j}(q-1)^j b_j$$

を得る。この証明はまた、$\boldsymbol{a}$, $\boldsymbol{b}$ が最適解であるための必要十分条件が

$$(\boldsymbol{a}Q)_j b_j=a_i\left(\boldsymbol{b}Q^{\mathsf{T}}\right)_i=0\quad(1\leqslant i,j\leqslant n)$$

で与えられることを示している。

Delsarte は sphere-packing 限界, Singleton 限界, Plotkin 限界等の普遍的限界 (universal bound) が双対問題の良い実行可能解 $\boldsymbol{b}$ を構成することによっても証明できることを示した。また、最も強力な漸近的限界 (asymptotic bound) である McEliece-Rodemich-Rumsey-Welch 限界 [27] も線型計画限界を極めて巧妙に用いることにより得られる。

例えば sphere-packing 限界は次の実行可能解 $\boldsymbol{b}=(b_0,b_1,\ldots,b_n)$ により与えられる[5]：

$$b_j:=\left(|B_e(\mathbf{0})|^{-1}\cdot K_e(j-1;n-1,q)\right)^2\quad(0\leqslant j\leqslant n)$$

ただし $e:=\lfloor d/2\rfloor$ である。実際、$b_0=1$, $(\boldsymbol{b}Q^{\mathsf{T}})_i=0$ $(d\leqslant i\leqslant n)$, $\sum_{j=0}^{n}\binom{n}{j}(q-1)^j b_j=q^n\cdot|B_e(\mathbf{0})|^{-1}$ 等が Krawtchouk 多項式の直交性等を用いて確かめられる。もし $e$-誤り訂正完全符号が存在するならば、上で述べたことによりこの解は最適解である。さらに Delsarte はそのような符号の内分布 $\boldsymbol{a}=(a_0,a_1,\ldots,a_n)$ について $|\{j\neq 0:(\boldsymbol{a}Q)_j\neq 0\}|=e$ が成り立つことを示した [10, Theorem 5.14][6]。従ってこれらを組み合わせると、次の Lloyd の定理が得られる。

[5] この実行可能解は球 $B_e(\mathbf{0})$ の内分布にごく簡単な変形を加えることにより構成される。このテクニックについては [10, §3.3], [8, §2.5] を参照されたい。

[6] より正確には、この等式が成り立つことが完全符号であることの必要十分条件である。なお、左辺の数 $s^*:=|\{j\neq 0:(\boldsymbol{a}Q)_j\neq 0\}|$ は $C$ の双対次数 (dual degree) と呼ばれ、冒頭に述べた符号の基本的な 4 つのパラメータの一つである。

**Theorem 3.4** (Lloyd)**.** *If a perfect $e$-error-correcting code exists, then the Lloyd polynomial $\Psi_e(z) := K_e(z-1; n-1, q)$ has $e$ distinct zeros among the integers $1, 2, \ldots, n$.*

ちなみに、Lloyd 多項式 $\{\Psi_e(z)\}_{e=0}^{n-1}$ は $\{1, 2, \ldots, n\}$ 上の直交多項式なので、一般論から各 $\Psi_e(z)$ は実区間 $[1, n]$ 上に $e$ 個の単根を持つことが分かるが、Lloyd の定理の主張はそれらの根が全て整数でなければならないという非常に強烈なものである。

以下代表的な完全符号を挙げる：

| $e$ | $q$ | $n$ | $\lvert C\rvert$ | Description |
|---|---|---|---|---|
| 0 | $q$ | $n$ | $q^n$ | complete code |
| $n$ | $q$ | $n$ | 1 | trivial code |
| $e$ | 2 | $2e+1$ | 2 | repetition code |
| 3 | 2 | 23 | $2^{12}$ | binary Golay code |
| 2 | 3 | 11 | $3^6$ | ternary Golay code |
| 1 | $q$ | $\frac{q^m-1}{q-1}$ | $q^{n-m}$ | Hamming code[1] |

[1] For Hamming codes, $q$ is a prime power.

これらの完全符号はどれも有名（或いは自明）なものであるが、Lloyd の定理を強力な道具として、van Lint, Tietäväinen, Bannai, Best 等により次の結果が得られた：

**Theorem 3.5.** *For $e \geqslant 3$ (and for $e = 2$, $q$ a prime power), no other perfect $e$-error-correcting codes exist.*

Lloyd の定理の証明は他にもいくつか知られているが、ここで紹介した Delsarte による証明は非常に応用性が高く、Johnson スキームを含む多くのアソシエーションスキーム上 (より正確には $P$-多項式スキーム [10, 7, 8] 上) に於いてそのまま成立する。

線型計画限界に基づく Delsarte の手法は他のいろいろな問題に対しても有効に用いられる。一例として、極値集合論に於いて非常に有名な Erdős-Ko-Rado の定理 [15, 45] は Johnson スキームに於ける結果と解釈できるが、Delsarte の手法を組み合わせることにより Hamming スキーム, Johnson スキーム及びそれらの $q$-類似上で同様の定理を統一的に証明することができる [38]。

# 4 半正定値計画限界 (Schrijver, 2005)

引き続き同じ記号を用いるが、この節では簡単のため 2 進符号のみを考察する。従って、$F = \{0, 1\}$ であり $B$ 型 Weyl 群 $G := \mathfrak{S}_2 \wr \mathfrak{S}_n$ が $X(:= F^n)$ 上に作用している。線型計画限界は Bose-Mesner 代数 $\mathcal{M} = \langle A_0, A_1, \ldots, A_n \rangle = \mathrm{End}_{\mathbb{C}[G]}(\mathbb{C}^X)$ 上で定式化されたが、Schrijver [34] は新たな半正定値計画限界を定式化する上で、ゼロベクトル $\mathbf{0} := (0, 0, \ldots, 0) \in X$ の安定部分群 $H := \mathrm{Stab}_G(\mathbf{0}) = \mathfrak{S}_n$ の中心化環 $\mathrm{End}_{\mathbb{C}[H]}(\mathbb{C}^X)$ を考察した。本稿の目的は Schrijver の半正定値計画限界を紹介することであるが、冒頭に述べたようにこの限界はまだ提唱されたばかりであり、Delsarte 理論の様に符号の解析に応用する手法はまだ確立されていない。一方、後述するように中心化環 $\mathrm{End}_{\mathbb{C}[H]}(\mathbb{C}^X)$ は Hamming スキーム $H(n, 2)$ の Terwilliger 代数に一致する。Terwilliger 代数[7] [40, 41, 42] はアソシエーションスキームの構造の研究に於いて極めて重要な役割を果たす代数であ

[7] Terwilliger 自身はこの代数を subconstituent algebra と呼んでいる。

るが、本稿では Schrijver の結果を可能な限り Terwilliger 代数の用語・理論を用いて解説することを試みる。

Terwilliger [40] にならって双対冪等元 (dual idempotents) $E_0^*, E_1^*, \ldots, E_n^* \in \mathbb{C}^{X\times X}$ を次の様に定める：

$$(E_i^*)_{xy} := \begin{cases} 1, & \text{if } x = y,\ \mathrm{wt}_H(x) = i, \\ 0, & \text{otherwise.} \end{cases}$$

従って各 $E_i^*$ は $\{x \in X : \mathrm{wt}_H(x) = i\}$ で張られる $\mathbb{C}^X$ の部分空間上への直交射影である。このとき、$\mathrm{End}_{\mathbb{C}[H]}(\mathbb{C}^X)$ が隣接行列 $A_0, A_1, \ldots, A_n$ 及び双対冪等元 $E_0^*, E_1^*, \ldots, E_n^*$ で生成されることが容易に確かめられる。より正確には

$$\mathrm{End}_{\mathbb{C}[H]}(\mathbb{C}^X) = \langle A_0, \ldots, A_n, E_0^*, \ldots, E_n^* \rangle = \langle E_i^* A_j E_k^* : 0 \leqslant i, j, k \leqslant n \rangle .$$

なお $E_i^* A_j E_k^*$ も 0-1 行列であり、$(E_i^* A_j E_k^*)_{xy} = 1$ となることと $x, y$ が $\mathrm{wt}_H(x) = i$, $\partial_H(x, y) = j$, $\mathrm{wt}_H(y) = k$ を満たすことが同値である。

ちなみに、任意のアソシエーションスキームについても (各基点 (basepoint) に対し) 双対冪等元を同様に定義できるが、一般に隣接行列及び双対冪等元で生成される $\mathbb{C}^{X\times X}$ の部分代数 $\mathcal{T} := \langle A_0, \ldots, A_n, E_0^*, \ldots, E_n^* \rangle$ を Terwilliger 代数と呼ぶ。Hamming スキーム $H(n, q)$ や Johnson スキーム $J(v, n)$ については Terwilliger 代数と一点の安定部分群の中心化環が一致することが確かめられる (cf. [18]) が、Terwilliger 代数が真に小さくなるような (群の軌道として得られる) アソシエーションスキームの例は多く存在する。

さて、$C \subseteq X(:= F^n)$ を符号とし、$G$ の部分集合 $\Pi^{(1)}, \Pi^{(2)}$ を $\Pi^{(1)} := \{g \in G : \mathbf{0} \in g(C)\}$, $\Pi^{(2)} := G \backslash \Pi^{(1)}$ と定める。さらに $s = 1, 2$ に対し

$$R^{(s)} := (|C|n!)^{-1} \cdot \sum_{g \in \Pi^{(s)}} \chi_{g(C)} \left(\chi_{g(C)}\right)^{\mathsf{T}} (\in \mathbb{C}^{X\times X})$$

と定義する。まず、$\Pi^{(1)}, \Pi^{(2)}$ は $G$ の $H$ による剰余類の和集合であることから $R^{(1)}, R^{(2)}$ が $\mathrm{End}_{\mathbb{C}[H]}(\mathbb{C}^X)$ に含まれることが分かる。さらに各 $\chi_{g(C)} \left(\chi_{g(C)}\right)^{\mathsf{T}}$ が非負 ($\geqslant 0$) かつ半正定値 ($\succcurlyeq 0$) なので、それらの和である $R^{(1)}, R^{(2)}$ も明らかに非負かつ半正定値である。これらの行列の定義は不自然に思われるかもしれないが、以下に述べるように非常にきれいな表示を持つ。

**Lemma 4.1.** *We have*

$$R^{(1)} = \sum_{i,j,k} \lambda_{ijk} E_i^* A_j E_k^* \quad (\geqslant 0, \succcurlyeq 0),$$
$$R^{(2)} = \sum_{i,j,k} (\lambda_{0jj} - \lambda_{ijk}) E_i^* A_j E_k^* \quad (\geqslant 0, \succcurlyeq 0),$$

*with*

$$\lambda_{ijk} := \frac{|X|}{|C|} \cdot \frac{|\{(x, y, z) \in C^3 : (x, y, z) \text{ satisfies } (*)\}|}{|\{(x, y, z) \in X^3 : (x, y, z) \text{ satisfies } (*)\}|},$$

*where the condition* (*) *is defined by*

$$\partial_H(x, y) = i,\ \partial_H(y, z) = j,\ \partial_H(x, z) = k. \qquad (*)$$

既に $R^{(1)}, R^{(2)}$ が $\mathrm{End}_{\mathbb{C}[H]}(\mathbb{C}^X)$ の元であることは分かっているので、係数 $\lambda_{ijk}$ 等は各 0-1 行列 $E_i^* A_j E_k^*$ との内積を計算することで容易に求められる。特に $\lambda_{000} = 1$ 及び $|C| = \sum_{i=0}^n \binom{n}{i} \lambda_{0ii}$ に注意されたい。線型計画限界のときと同様に係数 $\lambda_{ijk}$ の満たす性質を制約条件として課すことにより次の**半正定値計画限界**(**semidefinite programming bound**) を得る：

**Theorem 4.2** (Schrijver [34])**.** *Set*

$$\ell_{\mathrm{SDP}} = \ell_{\mathrm{SDP}}(n, 2, d) := \max \sum_{i=0}^{n} \binom{n}{i} \lambda_{0ii}$$

*subject to (i)* $\lambda_{000} = 1$*, (ii)* $0 \leqslant \lambda_{ijk} \leqslant \lambda_{0jj}$*, (iii)* $\lambda_{ijk} = \lambda_{i'j'k'}$ *if* $(i', j', k')$ *is a permutation of* $(i, j, k)$*, (iv)* $\sum_{i,j,k} \lambda_{ijk} E_i^* A_j E_k^* \succcurlyeq 0$*, (v)* $\sum_{i,j,k} (\lambda_{0jj} - \lambda_{ijk}) E_i^* A_j E_k^* \succcurlyeq 0$*, (vi)* $\lambda_{ijk} = 0$ *if* $\{i, j, k\} \cap \{1, 2, \ldots, d-1\} \neq \emptyset$*. Then* $A_2(n, d) \leqslant \ell_{\mathrm{SDP}}$*.*

一般に半正定値計画問題は interior-point method により解くことができる[8] [44]。上の制約条件の中で最も重要なのは (iii) である。実際 Gijswijt [17, Chapter 6] は多くのパラメータに於いて (iii) を省いても計算を行い、ほとんどの場合線型計画限界と一致することを確認した。次の表は Schrijver [34] による。

Bounds on $A_2(n, d)$

| $n$ | $d$ | best lower bound known | $\ell_{\mathrm{SDP}}$ | best upper bound previously known | $\ell_{\mathrm{LP}}$ |
|---|---|---|---|---|---|
| 19 | 6 | 1024 | 1280 | 1288 | 1289 |
| 23 | 6 | 8192 | 13766 | 13774 | 13775 |
| 25 | 6 | 16384 | 47998 | 48148 | 48148 |
| 19 | 8 | 128 | 142 | 144 | 145 |
| 20 | 8 | 256 | 274 | 279 | 290 |
| 25 | 8 | 4096 | 5477 | 5557 | 6474 |
| 27 | 8 | 8192 | 17768 | 17804 | 18189 |
| 28 | 8 | 16384 | 32151 | 32204 | 32206 |
| 22 | 10 | 64 | 87 | 88 | 95 |
| 25 | 10 | 192 | 503 | 549 | 551 |
| 26 | 10 | 384 | 886 | 989 | 1040 |

例えば $(n, d) = (25, 8)$ 等では大きく限界を改善していると言える[9]。実際、半正定値計画限界は線型計画限界より優れた限界であることが次の様に確かめられる。まずベクトル $\boldsymbol{a} = (a_0, a_1, \ldots, a_n)$ に対し行列 $R := \sum_{j=0}^n \lambda_{0jj} A_j$ (ただし $\lambda_{0jj} := a_j \binom{n}{j}^{-1}$) を対応させる。このとき Krawtchouk 多項式の性質 $\binom{n}{j} K_i(j) = \binom{n}{i} K_j(i)$ を用いると

$$R = \sum_{j=0}^{n} \lambda_{0jj} \sum_{i=0}^{n} K_j(i) E_i = \sum_{i=0}^{n} (\boldsymbol{a}Q)_i \binom{n}{i}^{-1} E_i$$

[8] ただし interior-point method は近似計算なので、計算機により得られた結果が実際に有効な限界を与えるかどうかは検証の必要がある。これについては [17, Chapter 7] を参照されたい。

[9] De Klerk と Pasechnik [21] はグラフ $(X, R_{n/2})$ (orthogonality graph) の独立数を求める問題に Schrijver の半正定値計画限界を適用したが、彼らの計算結果によると $n = 16$ の場合線型計画限界が 4096 を与えるのに対し半正定値計画限界は 2304 となり、しかもこの値は実際の独立数に一致する。

を得る。よって線型計画限界中の制約条件 $a_i \geqslant 0$, $(\boldsymbol{a}Q)_i \geqslant 0$ $(0 \leqslant i \leqslant n)$ は $R$ が非負かつ半正定値であることと同値である。一方半正定値計画限界は二つの行列 $R^{(1)}, R^{(2)}$ が非負かつ半正定値であることに基づいていたが、双対冪等元 $E_0^*, E_1^*, \ldots, E_n^*$ が直交冪等元であることから実際 $R^{(1)} + R^{(2)} = R$ となり、これは半正定値計画限界の制約条件が線型計画限界のそれよりも強い条件であることを意味している。従っていずれの限界も同じ目的関数を最大化していることから $A_2(n,d) \leqslant \ell_{\mathrm{SDP}} \leqslant \ell_{\mathrm{LP}}$ が結論される。

Schrijver [33] はグラフの独立数の評価を与える Lovász の $\vartheta$-限界を強めた彼の $\vartheta'$-限界がアソシエーションスキームの場合には Delsarte の線型計画限界 $\ell_{\mathrm{LP}}$ に一致することを示したが、Schrijver の半正定値計画限界 $\ell_{\mathrm{SDP}}$ はさらに Lovász-Schrijver [24] によるグラフの独立数の評価を改良する一般的手法 (matrix cuts) を応用したものである。最近 Laurent [22] は半正定値計画問題の階層

$$\ell_+^{(1)} \geqslant \ell_+^{(2)} \geqslant \cdots \geqslant \ell_+^{(k)} \geqslant \ldots (\geqslant A_2(n,d))$$

を定式化した。この列に於いて実際 $\ell_{\mathrm{LP}} = \ell_+^{(1)} \geqslant \ell_{\mathrm{SDP}} \geqslant \ell_+^{(2)}$ となっている。しかしながら、$\ell_{\mathrm{LP}}, \ell_{\mathrm{SDP}}$ がそれぞれ $O(n)$ 及び $O(n^3)$ 変数であったのに対し、次の段階である $\ell_+^{(2)}$ は $O(n^7)$ 変数であり、$n$ が小さい場合ですら計算は現実的に困難だと思われる。

さて、半正定値計画限界中の二つの行列 $R^{(1)}, R^{(2)}$ は $2^n \times 2^n$ 行列なので、半単純代数である $\mathrm{End}_{\mathbb{C}[H]}(\mathbb{C}^X)$ の Wedderburn 分解を求め、考察する行列のサイズを小さくすることが限界の計算を実行する上で不可欠である。$\mathrm{End}_{\mathbb{C}[H]}(\mathbb{C}^X)$ の分解は Krawtchouk 多項式の加法公式に関連して Dunkl [12] によって既に研究されている[10]が、ここでは限界の計算上都合の良い分解について (Terwilliger 代数の用語等を用いて) 解説する。まず、$\mathrm{End}_{\mathbb{C}[H]}(\mathbb{C}^X)$ は Terwilliger 代数と一致したことを思い出そう：

$$\mathcal{T} = \mathrm{End}_{\mathbb{C}[H]}(\mathbb{C}^X) = \langle E_i^* A_j E_k^* : 0 \leqslant i,j,k \leqslant n \rangle$$

既約 $\mathcal{T}$-加群 $W \subseteq \mathbb{C}^X$ の終点 (endpoint) を $r(W) := \min\{0 \leqslant i \leqslant n : E_i^* W \neq 0\}$ により定める[11]。このとき次が成り立つ [42, 19]：

**Theorem 4.3.** *Let $W \subseteq \mathbb{C}^X$ denote an irreducible $\mathcal{T}$-module and set $r = r(W)$. Then we have*

$$W = E_r^* W \perp E_{r+1}^* W \perp \cdots \perp E_{n-r}^* W \quad (\textit{orthogonal direct sum}).$$

*More precisely,*

$$\dim E_i^* W = \begin{cases} 1, & \text{if } r \leqslant i \leqslant n-r, \\ 0, & \text{otherwise.} \end{cases}$$

*The isomorphism class of $W$ is determined by the endpoint $r$.*

各部分空間 $E_i^* W$ の次元が高々 1 であることは、$\{x \in X : \mathrm{wt}_H(x) = i\}$ がまたアソシエーションスキーム (すなわち Johnson スキーム $J(n,i)$) の構造を持っていることから Terwilliger 代数の一般論より従う [42, Theorem 5.1]。定理中の直交分解 $W = E_r^* W \perp$

[10]他の直交多項式については [13] (Hahn 多項式), [14] ($q$-Hahn 多項式), [35] ($q$-Krawtchouk 多項式) 等を参照されたい。

[11]Terwilliger は初めこのパラメータを dual endpoint と呼んでいた。

$E^*_{r+1}W \perp \cdots \perp E^*_{n-r}W$ に関して、各 $E^*_i$ の作用は $(\delta_{i\alpha}\delta_{i\beta})_{r\leqslant\alpha,\beta\leqslant n-r}$ と表せる。従って、$\mathcal{T}$ の 0-1 基底の各元 $E^*_iA_jE^*_k$ は $(a_{ijk}\delta_{i\alpha}\delta_{k\beta})_{r\leqslant\alpha,\beta\leqslant n-r}$ の形で作用することが分かる。このような疎行列 (sparse matrix) で $E^*_iA_jE^*_k$ を表示することにより、計算の効率を大幅に高めることができるのである。Schrijver はここに現れた $a_{ijk}$ を具体的に決定したが、これらはまた Terwilliger の結果から求めることも可能である [42, 19]。

なお、$q > 2$ についても半正定値計画限界 $\ell_{\mathrm{SDP}}(n, q, d)$ は定式化されている [18]。$H(n, 2)$ と比べ Terwilliger 代数の既約加群の記述がかなり複雑になるが、やはり多くのパラメータで線型計画限界を改善することが分かった。3 進符号に関する結果をここに載せる：

Bounds on $A_3(n, d)$

| $n$ | $d$ | best lower bound known | $\ell_{\mathrm{SDP}}$ | best upper bound previously known | $\ell_{\mathrm{LP}}$ |
|---|---|---|---|---|---|
| 12 | 4 | 4374 | 6839 | 7029 | 7029 |
| 13 | 4 | 8019 | 19270 | 19682 | 19683 |
| 14 | 4 | 24057 | 54774 | 59046 | 59049 |
| 15 | 4 | 72171 | 149585 | 153527 | 153527 |
| 16 | 4 | 216513 | 424001 | 434815 | 434815 |
| 12 | 5 | 729 | 1557 | 1562 | 1562 |
| 13 | 5 | 2187 | 4078 | 4163 | 4163 |
| 14 | 5 | 6561 | 10624 | 10736 | 10736 |
| 15 | 5 | 6561 | 29213 | 29524 | 29524 |
| 13 | 6 | 729 | 1449 | 1562 | 1562 |
| 14 | 6 | 2187 | 3660 | 3885 | 4163 |
| 15 | 6 | 2187 | 9904 | 10736 | 10736 |
| 16 | 6 | 6561 | 27356 | 29524 | 29524 |
| 14 | 7 | 243 | 805 | 836 | 836 |
| 15 | 7 | 729 | 2204 | 2268 | 2268 |
| 16 | 7 | 729 | 6235 | 6643 | 6643 |
| 13 | 8 | 42 | 95 | 103 | 103 |
| 15 | 8 | 243 | 685 | 711 | 712 |
| 16 | 8 | 297 | 1923 | 2079 | 2079 |
| 14 | 9 | 31 | 62 | 66 | 81 |
| 15 | 9 | 81 | 165 | 166 | 166 |
| 16 | 10 | 54 | 114 | 117 | 127 |

# 5 関連した話題

## 5.1 Designs

Hamming スキーム $H(n, q)$ や Johnson スキーム $J(v, n)$ (より一般に $Q$-多項式スキーム [7]) の部分集合 $C$ の内分布 $\boldsymbol{a} = (a_0, a_1, \ldots, a_n)$ が $(\boldsymbol{a}Q)_1 = \cdots = (\boldsymbol{a}Q)_t = 0$ を満たすとき、$C$ を (Delsarte) $t$-デザインという [10]。Johnson スキームについては $t$-デザインの概念は通常の $t$-$(v, k, \lambda)$ デザインと一致し、Hamming スキームについては直交配列 (orthogonal array) と一致する。他の多くの良いアソシエーションスキームに関しても $t$-デザインの概念の自然な幾何的解釈が可能である [11, 29, 36]。Delsarte はデザインに対しても線型計画限界を定式化し、符号と対をなす理論を展開した。従ってこの場合

についても半正定値計画限界を考察することは自然かつ重要な問題だと思われる。ただ、Bose-Mesner 代数 (= 中心化環) では原始冪等元の基底が隣接行列の基底と完全に双対的な役割を果たすのに対し、一点の安定化群の中心化環は非可換であり、そのような基底は一般に取れない (と思われる) のが難点である[12]。

## 5.2 Spherical codes, spherical designs

線型計画限界を含む Delsarte の理論は球面等のランク 1 コンパクト対称空間に於いても展開される。これについては [9, 6, 16, 32, 4, 5] 等をご覧いただきたい。ここではキッシング数 (kissing number) に関する最近の進展について手短に紹介する。キッシング数 $k(n)$ は「$n$ 次元 Euclid 空間 $\mathbb{R}^n$ に於いて与えられた一つの球の周りにそれと同じサイズの球をそれに接するようにかつ互いに重なり合わないように置く最大の数」として定義される。明らかに $k(2) = 6$ であるが、数年前の時点では 3 次元以上で値が判明していたのは $k(3) = 12$, $k(8) = 240$ 及び $k(24) = 196560$ のみであった[13]。特に $k(8)$ 及び $k(24)$ は線型計画限界を有効に活用して証明される (Odlyzko-Sloane, Levenshtein, cf. [9])。一方 $k(4)$ の決定は非常に難しい問題であると考えられていたが、最近 Musin [31, 30] は Delsarte の手法を幾何的考察を用いて非常に巧妙に拡張し、$k(3) = 12$ の明快な別証明を与え、さらに $k(4) = 24$ を示すことに成功した。なお、2 進符号についてはある意味で類似した手法が提唱されている [28][14]。球面上の符号についても Bachoc-Vallentin [3] によりごく最近半正定値計画限界が定式化された。彼らの計算によると半正定値計画限界により $k(4) = 24$ が得られるとのことである。

## 5.3 Terwilliger 代数に基づいた符号理論

本稿で解説した半正定値計画限界は Terwilliger 代数上に定式化されたが、それを用いた符号の性質等の研究はまだ進んでいない。しかしながら、一方で Terwilliger 代数の理論を本格的に符号理論に応用する動きも始まっている。Assmus-Mattson の定理 [2] は良い (線型) 符号を用いた $t$-$(v, k, \lambda)$ デザインの構成法を与える非常に有名な結果であるが、Terwilliger による最新の結果 [43] 等を用いることにより別証明を与え、拡張することが可能である [39]。同様の手法は他のいろいろな符号理論の問題に適用できる[15]。また、W. J. Martin は Terwilliger 代数を用いた 2 進符号の研究を行っているとのことである[16]。

本稿では Terwilliger 代数の側面を意図的に強く強調したが、それによって (特にアソシエーションスキームに既に馴染んでいる方にとっては) 元論文 [34] と比べ解説が多少明

[12] Johnson スキーム $J(v, k)$ 上のデザインに対し最も安直な方法で半正定値計画限界を設定して計算を行ってみたところ、確かに線型計画限界を多くのパラメータに於いて改善するものの、その改善幅はデザインの位数の満たす強烈な整数条件に比べて小さく、現時点では実際に知られている最善の限界を改善する例は見つかっていない。

[13] $k(3)$ に関して 1694 年頃に Newton と Gregory の間で論争があったと言われている。

[14] この情報は金沢大学の田上真氏に教えていただいた。なお、田上氏はこの Musin の研究に大きな貢献を行った。

[15] 例えば最小距離に関する Martin [26] の結果も Terwilliger 代数の観点から捉えることができる。

[16] ここで述べたことと多少方向性は異なるが、Suzuki [37] は (基 '点' ではなく) 各 '部分集合' に対して Terwilliger 代数を定義し、その部分集合の組合せ的性質と Terwilliger 代数の性質との関係を詳細に論じた。[20] も合わせて参照されたい。

快になったのではないかと期待する。半正定値計画限界、及びここで述べた Terwilliger 代数の理論の符号理論への応用の双方をさらに推し進め、(何らかの意味で) 融合を図ることが、冒頭に述べた「新たな Delsarte 理論」への重要なステップだと思われる。

# 参考文献


[1] E. Agrell, A. Vardy and K. Zeger, A table of upper bounds for binary codes, IEEE Trans. Inform. Theory 47 (2001) 3004-3006.

[2] E. F. Assmus, Jr. and H. F. Mattson, Jr., New 5-designs, J. Combinatorial Theory 6 (1969) 122-151.

[3] C. Bachoc and F. Vallentin, New upper bounds for kissing numbers from semidefinite programming, arXiv:math.MG/0608426.

[4] E. Bannai (Ed.), The proceedings of COE workshop on sphere packings (Nov. 1-5, 2004), Kyushu University, 2005. (Available at http://www.math.kyushu-u.ac.jp/coe/report/mhf2.cgi)

[5] E. Bannai (Ed.), The proceedings of second COE workshop on sphere packings (May. 30-Jun. 3, 2005), Kyushu University, 2005. (Available at http://www.math.kyushu-u.ac.jp/coe/report/mhf2.cgi)

[6] 坂内英一, 坂内悦子, 球面上の代数的組合せ理論, Springer-Verlag, Tokyo, 1999.

[7] E. Bannai and T. Ito, Algebraic combinatorics I, Benjamin/Cummings, Menlo Park, 1984.

[8] A. E. Brouwer, A. M. Cohen and A. Neumaier, Distance-regular graphs, Springer-Verlag, Berlin, 1989.

[9] J. H. Conway and N. J. A. Sloane, Sphere packings, lattices and groups, Third edition, Springer-Verlag, New York, 1999.

[10] P. Delsarte, An algebraic approach to the association schemes of coding theory, Philips Res. Rep. Suppl. No. 10 (1973).

[11] P. Delsarte, Association schemes and $t$-designs in regular semilattices, J. Combinatorial Theory Ser. A 20 (1976) 230-243.

[12] C. F. Dunkl, A Krawtchouk polynomial addition theorem and wreath products of symmetric groups, Indiana Univ. Math. J. 25 (1976) 335-358.

[13] C. F. Dunkl, An addition theorem for Hahn polynomials: the spherical functions, SIAM J. Math. Anal. 9 (1978) 627-637.

[14] C. F. Dunkl, An addition theorem for some $q$-Hahn polynomials, Monatsh. Math. 85 (1978) 5-37.

[15] P. Erdős, C. Ko and R. Rado, Intersection theorems for systems of finite sets, Quart. J. Math. Oxford Ser. (2) 12 (1961) 313-320.

[16] T. Ericson and V. Zinoviev, Codes on Euclidean spheres, North-Holland, Amsterdam, 2001.

[17] D. Gijswijt, Matrix algebras and semidefinite programming techniques for codes, Ph.D. thesis, The Universiteit van Amsterdam, Amsterdam, The Netherlands, 2005.

[18] D. Gijswijt, A. Schrijver and H. Tanaka, New upper bounds for nonbinary codes based on the Terwilliger algebra and semidefinite programming, J. Combin. Theory Ser. A 113 (2006) 1719-1731.

[19] J. T. Go, The Terwilliger algebra of the hypercube, European J. Combin. 23 (2002) 399-429.

[20] R. Hosoya and H. Suzuki, Tight distance-regular graphs with respect to subsets, European J. Combin. 28 (2007) 61-74.

[21] E. de Klerk and D.V. Pasechnik, A note on the stability number of an orthogonality graph, European J. Combin., to appear.

[22] M. Laurent, Strengthened semidefinite programming bounds for codes, Math. Program., to appear.

[23] J. H. van Lint, Introduction to coding theory, Third edition, Springer-Verlag, Berlin, 1999.

[24] L. Lovász and A. Schrijver, Cones of matrices and set-functions and 0-1 optimization, SIAM J. Optim. 1 (1991) 166-190.

[25] F. J. MacWilliams and N. J. A. Sloane, The theory of error-correcting codes, North-Holland, Amsterdam, 1977.

[26] W. J. Martin, Minimum distance bounds for $s$-regular codes, Des. Codes Cryptogr. 21 (2000) 181-187.

[27] R. J. McEliece, E. R. Rodemich, H. Rumsey, Jr. and L. R. Welch, New upper bounds on the rate of a code via the Delsarte-MacWilliams inequalities, IEEE Trans. Information Theory IT-23 (1977) 157-166.

[28] B. Mounits, T. Etzion and S. Litsyn, Improved upper bounds on sizes of codes, IEEE Trans. Inform. Theory 48 (2002) 880-886.

[29] A. Munemasa, An analogue of $t$-designs in the association schemes of alternating bilinear forms, Graphs Combin. 2 (1986) 259-267.

[30] O. R. Musin, The kissing problem in three dimensions, Discrete Comput. Geom. 35 (2006) 375-384.

[31] O. R. Musin, The kissing number in four dimensions, arXiv:math.MG/0309430.

[32] F. Pfender and G. M. Ziegler, Kissing numbers, sphere packings, and some unexpected proofs, Notices Amer. Math. Soc. 51 (2004) 873-883.

[33] A. Schrijver, A comparison of the Delsarte and Lovász bounds, IEEE Trans. Inform. Theory 25 (1979) 425-429.

[34] A. Schrijver, New code upper bounds from the Terwilliger algebra and semidefinite programming, IEEE Trans. Inform. Theory 51 (2005) 2859-2866.

[35] D. Stanton, Three addition theorems for some $q$-Krawtchouk polynomials, Geom. Dedicata 10 (1981) 403-425.

[36] D. Stanton, $t$-designs in classical association schemes, Graphs Combin. 2 (1986) 283-286.

[37] H. Suzuki, The Terwilliger algebra associated with a set of vertices in a distance-regular graph, J. Algebraic Combin. 22 (2005) 5-38.

[38] 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) 903-910.

[39] H. Tanaka, New proofs of the Assmus-Mattson theorem based on the Terwilliger algebra, in preparation.

[40] P. Terwilliger, The subconstituent algebra of an association scheme I, J. Algebraic Combin. 1 (1992) 363-388.

[41] P. Terwilliger, The subconstituent algebra of an association scheme II, J. Algebraic Combin. 2 (1993) 73-103.

[42] P. Terwilliger, The subconstituent algebra of an association scheme III, J. Algebraic Combin. 2 (1993) 177-210.

[43] P. Terwilliger, The displacement and split decompositions for a $Q$-polynomial distance-regular graph, Graphs Combin. 21 (2005) 263-276.

[44] M. J. Todd, Semidefinite optimization, Acta Numer. 10 (2001) 515-560.

[45] R. M. Wilson, The exact bound in the Erdős-Ko-Rado theorem, Combinatorica 4 (1984) 247-257.