数理解析研究所講究録
第1593巻 2008年 178-184

An Extremal Doubly Even Self-Dual Code of Length 112[1]

山形大学・理学部 原田 昌晃 (Masaaki Harada)
Faculty of Science,
Yamagata University

1 はじめに

長さ n の doubly even self-dual code が存在するのであれば, n は 8 の倍数であり, その minimum weight d は $d \leq 4[n/24]+4$ を満たすことが知られている [5]. $d = 4[n/24]+4$ の場合は extremal とよばれる. どの長さで extremal doubly even self-dual code が存在するのかを決定することは基本的な問題である. 例えば, 長さ 72 の場合に存在性を決めることは, 既に 1973 年には Sloane [8] によって問題提起されている有名な未解決問題である.

本講演の目的は, extremal doubly even self-dual code の存在について知られている結果を紹介し, 今までに存在の分かっていなかった長さ 112 において最初の例を与えることであった. 講演と同様に, この原稿では, まず第 2 節で extremal doubly even self-dual code の存在について知られている結果を述べて, 第 3 節で長さ 112 の extremal doubly even self-dual code の構成を与えることにする.

2 Extremal doubly even self-dual code

2.1 準備

本原稿では, 一般的によく使われている用語を用いているが, 紹介していない用語については [7] などを見ていただきたい. code は特に注意をしない限り (Theorem 1 以外は) 全て binary code を考えることにする. $C = C^{\perp}$ が成り立つとき C を self-dual とよぶ, ただし $C^{\perp}$ は通常の直交補空間 (dual code) を表す. C が self-dual であるとき, 全ての codeword

[1]本原稿は講演内容を簡潔にまとめたものである. なお, 講演は英語で行なったが, 既に講演内容の preprint [3] も出来上がっていることから, 本原稿は敢えて日本語で書くことにしました.

$x \in C$ の weight $\mathrm{wt}(x)$ は偶数になる. 全ての codeword の weight が 4 の倍数になる self-dual code を *doubly even* とよぶ. $A_i = |\{c \in C \mid \mathrm{wt}(c) = i\}|$ とするとき, 多項式 $W_C(x,y) = \sum_{i=0}^{n} A_i x^{n-i} y^i$ を code C の weight enumerator とよぶ.

Theorem 1 (Gleason–Pierce ([7] を参照)). q を素数または素数べきとし, 位数 q の有限体を $\mathbb{F}_q$ で表す. C を $\mathbb{F}_q$ 上の formally self-dual code とする, つまり C は $W_C(x,y) = W_{C^\perp}(x,y)$ を満たす. C の全ての codeword の weight は $\alpha > 1$ で割り切れるとき, 次のいずれかが成り立つ :

(1) $q = 2, \alpha = 2$

(2) $q = 2, \alpha = 4$

(3) $q = 3, \alpha = 3$

(4) $q = 4, \alpha = 2$

(5) q は任意, $\alpha = 2$ で $W_C(x,y) = (x^2 + (q-1)y^2)^{n/2}$.

ここで (5) を除いて[2], (2) と (3) の場合のみ自動的に self-dual になり, (2) の場合が doubly even self-dual code であり, これらが古くから広く研究されている理由の 1 つである.

doubly even self-dual code の weight enumerator に対しては次の有名な結果が知られている.

Theorem 2 (Gleason [1]). doubly even self-dual code の weight enumerator は

$$\mathbb{C}[x^8 + 14x^4y^4 + y^8, x^4y^4(x^4 - y^4)^4]$$

に属する.

ただちに, 長さ n の doubly even self-dual code が存在するのであれば n は 8 の倍数であることが分かる. さらに, この Gleason の定理を用いて minimum weight に関する上限が与えられた.

[2] この場合の code は例えば $(1,1)$ を generator matrix とする長さ 2 の code の直和を考えれば得られるので, 通常, この場合は自明な場合として除外して考える.

Theorem 3 (Mallows–Sloane [5]). 長さ n で minimum weight d の doubly even self-dual code に対して

$$d \leq 4\left[\frac{n}{24}\right] + 4 \tag{1}$$

が成り立つ.

上の不等式 (1) において等号が成り立つ doubly even self-dual code を *extremal* とよぶ. 長さ 112 の場合は minimum weight 20 の doubly even self-dual code を extremal とよぶわけである.

2.2 Extremal doubly even self-dual code の存在について

長さ $n = 8, 16, \ldots, 64, 80, 88, 104$ の場合は, 既に MacWilliams–Sloane [4] の Fig. 19.2 (626 ページ) にその存在について書かれてある. $n = 8, 16$ の場合は extended Hamming $[8, 4, 4]$ code とその直和で構成される. $n = 24$ の場合は extended Golay $[24, 12, 8]$ code, $n = 32, 48, 80, 104$ の場合は extended quadratic residue code がその例となり, $n = 40, 56, 64, 88$ の場合は double circulant code で構成出来ると書かれている. そこには, 最後の double circulant code については Fig. 16.7 を参照するように書かれており, 実際に $n = 40, 88$ の場合にはその構成方法が書かれてある. 1981 年の Pasquier [6] によれば MacWilliams–Sloane [4] の古い版に書かれてある $n = 64$ の double circulant code の構成には間違いがあり, [6] で長さ 64 の最初の例を与えたと書かれてある.

また $n = 136$ においては Rains–Sloane [7] によると Moore の 1976 年の学位論文の中で構成されている. これらの長さが, 現在のところ extremal doubly even self-dual code の存在が分かっている長さになり, 既に存在の分かっている長さにおいては, 少なくとも２５年前には最初の例が分かっていたことになる.

表 1 に, 今回のテーマとは少々離れるが, 著者が把握している現在までに知られている長さ n の非同値の extremal doubly even self-dual code の個数 $N(n)$ を参考までに載せておく. 表中, d は extremal となる minimum weight の値を表す. なお, 長さ 32 までは doubly even self-dual code の分類が完成している ([7] を参照).

表 1: Extremal doubly even self-dual code について

長さ n	d	$N(n)$	長さ n	d	$N(n)$	長さ n	d	$N(n)$
8	4	1	64	12	≥ 3270	120	24	?
16	4	2	72	16	?	128	24	?
24	8	1	80	16	≥ 15	136	24	≥ 1
32	8	5	88	16	≥ 470	144	28	?
40	8	≥ 12579	96	20	?	152	28	?
48	12	1	104	20	≥ 1	160	28	?
56	12	≥ 1151	112	20	≥ 1	$\vdots$		

3 構成方法

C_{112} を次の行列を generator matrix としてもつ code とする:

$$G = \begin{pmatrix} & & A & B \\ & I_{56} & & \\ & & B^T & A^T \end{pmatrix}$$

ここで I_{56} は位数 56 の単位行列, A, B は第 1 行目が

$$r_A = (1,0,0,1,0,1,0,0,0,0,0,0,0,0,1,0,1,0,0,1,1,1,1,0,0,1,1,1),$$
$$r_B = (1,0,1,1,1,0,0,1,1,1,1,1,0,0,0,0,1,1,1,1,0,1,1,1,1,0,1,1),$$

である 28×28 circulant 型の行列とし, A^T, B^T は A, B の転置行列を表す.

Lemma 4. C_{112} は長さ 112 の doubly even self-dual code.

Proof. まず $AA^T + BB^T = I_{28}$ が成り立つ. また A, B は circulant matrix なので $AB = BA$ であることに注意. この 2 つの事実から

$$M = \begin{pmatrix} A & B \\ B^T & A^T \end{pmatrix}$$

とすると $MM^T = I_{56}$ となるので C_{112} は self-dual code になる.

さらに $\mathrm{wt}(r_A) + \mathrm{wt}(r_B) = 31$ であることから C_{112} は doubly even self-dual code になる. □

Lemma 5. c を weight が 16 以下の C_{112} の codeword とすると c は G の高々 8 行の和または $H = (\ M^T\ ,\ I_{56}\ )$ の高々7 行の和として表せる.

Proof. $c = (c_1, c_2)$ $(c_i \in \mathbb{F}_2^{56})$ を $\mathrm{wt}(c) = 16$ の codeword とすると

$$(\mathrm{wt}(c_1), \mathrm{wt}(c_2)) = (0,16), (1,15), (2,14), \ldots, (15,1), (16,0)$$

となる. G の型から直ちに $\mathrm{wt}(c_1) = i$ の場合には c は G の i 行の和と表せることが分かる.

ここで C_{112} は self-dual code なので dual code の generator matrix H も C_{112} の generator matrix になる. したがって $(\mathrm{wt}(c_1), \mathrm{wt}(c_2)) = (i, 16-i)$ のときは G を考えれば i 行の和として表せるが H を考えれば $16-i$ 行の和として表せることになる. つまり, $\mathrm{wt}(c_1) = 9, \ldots, 16$ のときは H の高々 7 行の和で表せることが分かる. $\mathrm{wt}(c) \leq 12$ の場合も同様に示せる. □

これによって minimum weight を決めるための計算量は単純に計算するよりもかなり減らせる.

計算機によって G の 8 行までの和と H の 7 行までの和の weight が全て 20 以上であることを確認した. したがって C_{112} は extremal doubly even self-dual code であることが分かった.

Theorem 6. 長さ 112 の extremal doubly even self-dual code が存在する.

Remark 7. C_{112} は self-dual code としてだけでなく linear $[112, 56]$ code 全体としても今まで知られていた最大の minimum weight を超える code であった ([2] を参照[3]).

この節の最後に C_{112} の幾つかの性質を挙げる. extremal doubly even self-dual code の weight enumerator は Gleason の定理より一意的に決まり, 長さ 112 の場合は

$$\begin{aligned} W_{C_{112}}(1, y) = 1 &+ 355740y^{20} + 95307030y^{24} + 10847290300y^{28} \\ &+ 582017237802y^{32} + 15627131952432y^{36} + 219380334493320y^{40} \\ &+ 1662576783018480y^{44} + 6958460336232405y^{48} \\ &+ 16331108474136456y^{52} + 21682101997880004y^{56} + \cdots + y^{112} \end{aligned}$$

[3]linear code の minimum weight についてのデータベースは [2] がメンテナンスもされており便利である.

となる. Assmus–Mattson の定理 ([4] を参照) によって minimum weight の codeword は 1-(112, 20, 63525) design になることが分かる. この 1-design の 2-rank は 56 になることを確認した. つまり C_{112} は minimum weight の codeword によって生成されることが分かる. また MAGMA を用いて位数 112 の自己同型群を持つことを確認した.

4 おわりに

今回, 約 25 年ぶりに新たな長さでの extremal doubly even self-dual code の存在が分かったことになる. 長さ $n = 24k$ の場合の知られている extremal doubly even self-dual code は $k = 1, 2$ のときのみであり, 長さ 72 の場合は有名な未解決問題であることから, 存在性を決めることはなかなか難しいと思われる. まずは, 長さ $n \not\equiv 0 \pmod{24}$ の extremal doubly even self-dual code の存在性を考えたいと思っており, 分かっていなかった最小の場合が今回構成をした 112 であった.

今回は長さ 112 での構成をすることが最終的な目的だったので, とにかく Lemma 4 で考えた条件 ($AA^T + BB^T = I_{28}$, $\mathrm{wt}(r_A) + \mathrm{wt}(r_B) \equiv 3 \pmod 4$) を満たす circulant 型行列 A, B を探し, これらから得られる code の minimum weight が 20 になるかどうかを Lemma 5 を使って求めた. この構成方法に何か意味があるのかどうかはまだ分かっていない. 小さなところから推測すると多くの extremal doubly even self-dual code が存在してその一つを見付けたに過ぎないのかもしれない. 長さ $n \not\equiv 0 \pmod{24}$ の extremal doubly even self-dual code で存在の分かっていない最小の長さは 128 となった.

参考文献

[1] A.M. Gleason, Weight polynomials of self-dual codes and the MacWilliams identities, Actes Congrés Intern. Math. (Nice, 1970), pp. 211–215. Gauthier-Villars, Paris, 1971.

[2] M. Grassl, Code tables: Bounds on the parameters of various types of codes, Available online at "`http://www.codetables.de/`".

[3] M. Harada, An extremal doubly even self-dual code of length 112, (submitted).

[4] F.J. MacWilliams and N.J.A. Sloane, "The Theory of Error-Correcting Codes," North-Holland, Amsterdam, 1977.

[5] C.L. Mallows and N.J.A. Sloane, An upper bound for self-dual codes, *Inform. Control* **22** (1973), 188–200.

[6] G. Pasquier, A binary extremal doubly even self-dual code (64, 32, 12) obtained from an extended Reed–Solomon code over F_{16}, *IEEE Trans. Inform. Theory* **27** (1981), 807–808.

[7] E. Rains and N.J.A. Sloane, "Self-dual codes," Handbook of Coding Theory, V.S. Pless and W.C. Huffman (Editors), Elsevier, Amsterdam 1998, pp. 177–294.

[8] N.J.A. Sloane, Is there a $(72, 36)$ $d = 16$ self-dual code? *IEEE Trans. Inform. Theory* **19** (1973), 251.