数理解析研究所講究録 1476 巻 2006 年 88-95

On self-dual codes of length 64 with primitive automorphism groups

室蘭工業大学 工学部　千吉良直紀 (Naoki Chigira)
Muroran Institute of Technology
山形大学 理学部　原田昌晃 (Masaaki Harada)
Yamagata University
千葉大学 理学部　北詰正顕 (Masaaki Kitazume)
Chiba University

1 Introduction

M_{24} を調べる上で extended Golay code が重要な役割を果たしていることはよく知られている。他の単純群（あるいはそれに近い群）が作用する code として $J_2:2$ が作用する長さ 100 の code を構成した（[2], この結果は 2004 年 12 月の数理研の集会で発表している）。どちらの code にも自己同型群が原始的に作用している。100 次以下の原始的な作用をもつ群が不変にする自己同型群の存在を調べてみるとこれまで知られていたもの以外に 64 次のある原始置換群を自己同型にもつ self-dual code があることが分かった。ここではその code の構成、特徴づけや neighbor などの性質について述べる。符号についての計算は基本的に MAGMA によるものである。

2 Preliminaries

ここでは、記号の準備、および我々の議論で重要な役割を果たす定理について述べる。詳しくは [3, 5] を参照されたい。

Gを集合Ω上の置換群とし$\sigma \in G$に対して$\mathrm{Fix}(\sigma) = \{i \in \Omega | \sigma(i) = i\}$とおく。また$I(G) = \{\sigma | \sigma^2 = 1,\ \sigma \neq 1\}$とする。

$$C(G, \Omega) = C(G, |\Omega|) = \langle \mathrm{Fix}(\sigma) | \sigma \in I(G) \rangle^{\perp}$$

とおく。

定理 2.1 ([3]). GはΩ上の置換群としDを長さ$|\Omega|$の self-orthogonal code とする。このとき$D \subseteq C(G, \Omega)$が成り立つ。

古くから知られている散在型単純群に関連した self-orthogonal code は$C(G, \Omega)$と一致していることが多い。これらについては [3, 5] を参照されたい。

self-dual code に注目するとこの定理よりG-不変な self-dual code が存在するならば$C(G, \Omega)$の subcode として得られることになる。さらに$C(G, \Omega)^{\perp}$が self-orthogonal のときに限りGが作用する self-dual code が存在する可能性があることになる。しかしながらすべての位数 2 の元が固定点なしに作用する場合には$C(G, \Omega)$は全空間となってしまい、全空間のG-不変な subcode を探さなくてはならない。そこでここでは、いくつかの位数 2 の元が固定点を持つ場合について考察する。

100 次以下の原始置換群でいくつかの位数 2 の元が固定点を持つものが作用する self-dual code で知られているものは以下の通りである。表のうちJ_2の code 以外は$C(G, \Omega)$自身が self-dual code である。

G	parameters	
M_{22}, $M_{22}{:}2$	$[22, 11, 6]$	shorter Golay code
M_{24}	$[24, 12, 8]$	extended Golay code
$2^3{:}L_3(2)$	$[8, 4, 4]$	$RM(1, 3)$
$2^5{:}L_5(2)$	$[32, 16, 8]$	$RM(2, 5)$
J_2	$[100, 50, 16]$	see [2]
J_2, $J_2{:}2$	$[100, 50, 10]$	see [2]

ここでRMは Reed-Muller code である。一般に$RM(m, 2m{+}1) = C(2^{2m+1}{:}L_{2m+1}(2), 2^{2m+1})$でこれは self-dual code である。

上述の通り self-dual code が存在する可能性があるのは$C(G, \Omega)^{\perp}$が self-orthogonal である場合に限るのであるが、いくつかの位数 2 の元が固定点を持つような 100 次以下の原始置換群で$C(G, \Omega)^{\perp}$が self-orthogonal になるのは表にあげた self-dual code 以外には$C(S_4(3), 40)$, $C(J_2, 100)$と

$|\Omega| = 64$ の場合しかない。$C(S_4(3), 40)$ の場合には実際に self-dual code は存在せず、$C(J_2, 100)$ の場合には表にあげた code 以外には存在しない [3]。そこで残るのは 64 次のところである。

3 $n = 64$

64 次の原始置換群は全部で 74 個あることが知られている。そのうちいくつかの位数 2 の元が固定点持ち、かつ $C(G, \Omega)^{\perp}$ が self-orthogonal になるのは 16 個である。その中で、まず次の群を考える。

$$G = 2^6{:}(3^3{:}S_4), \quad 2^6{:}A_7, \quad 2^6{:}U_3(3), \quad 2^6{:}A_8, \quad 2^6{:}S_4(3)$$

のいずれかであるとする。いずれの場合にも $C = C(G, 64)$ は $[64, 43, 8]$ code で自己同型群は $2^6 : S_6(2)$ であり、$C^{\perp}$ は self-orthogonal $[64, 21, 6]$ code である。C には G-不変な self-dual code が含まれている可能性があるので、C の subcode を調べればよい。方法はいろいろ考えられるが、ここでは次のことを用いて調べる。

定理 3.1 (Mallows-Sloane [8]). 長さ n の doubly even self-dual code の minimum weight を d とするとき $d \leq 4\left[\frac{n}{24}\right] + 4$ が成り立つ。

定理 3.2 (Rains [9]). 長さ n の singly even self-dual code の minimum weight を d とするとき $d \leq \begin{cases} 4\left[\frac{n}{24}\right] + 4 & n \not\equiv 22 \pmod{24} \\ 4\left[\frac{n}{24}\right] + 6 & n \equiv 22 \pmod{24} \end{cases}$ が成り立つ。

$n = 64$ のときには $d \leq 12$ となる。すなわち weight 12 以下の codeword が必ず存在する。そこで C の weight 12 以下の codewords を G-orbit に分解しそれらから生成される code を構成し、さらにそれをもとにして self-dual code が存在するかどうかを調べればよい。

定理 3.3 ([4]). $2^6{:}A_8$-不変な self-dual code は

(i) 2 つの同値な extremal singly even $[64, 32, 12]$ code,

(ii) 4 つ（うち 2 つずつは同値）の doubly even self-dual $[64, 32, 8]$ code,

に限る。またこれらの code の自己同型群は $2^6{:}A_8$ である。

同様の方法で探してみると $2^6{:}(3^3{:}S_4)$, $2^6{:}U_3(3)$, $2^6{:}S_4(3)$ -不変な長さ 64 の self-dual code は存在しないことも分かる。

注意 3.4. $2^6:A_7 \subset 2^6:A_8$ なので定理3.3で得られた6個のself-dual codeは$2^6:A_7$-不変であるが、$2^6:A_7$-不変な長さ64のself-dual codeは他には存在しない。

16個のうち残りの11個も同じ$C(G,64)$をもつ次の4つのクラスに分けることが出来る。

$C(G,64)$	$C(G,64)^\perp$	♯ of such G
$[64,45,4]$	$[64,19,16]$	1
$[64,48,6]$	$[64,16,16]$	3
$[64,49,6]$	$[64,15,16]$	6
$[64,51,4]$	$[64,13,16]$	1

これらのいずれの場合にもG-不変なself-dual codeは存在しないことが分かる[1]。

以上により、いくつかの位数2の元が固定点を持つ場合、原始置換群が作用するself-dual codeは64次では$2^6:A_8$が自己同型群として作用するもの6個しかないという結果が得られた。

定理3.3で得られたcodeのうち非同値なもので minimum weightが12のものをD_1, minimum weightが8のものをD_2, D_3とする。weight enumerator W_{D_i} $(i=1,2,3)$は

$$W_{D_1} = 1 + 2456y^{12} + 11264y^{14} + 223020y^{16} + \cdots$$
$$W_{D_2} = 1 + 120y^8 + 5376y^{12} + 455196y^{16} + \cdots$$
$$W_{D_3} = 1 + 64y^8 + 4256y^{12} + 455084y^{16} + \cdots$$

となる。$n=64$の場合のextremal（すなわちminimum weight 12）のcodeのweight enumeratorは一般に次のような形で知られている。

定理 3.5 (Conway-Sloane [6]). $n=64$のextremal singly even self-dual codeのweight enumeratorは

$$W_{64,1} = 1 + (1312+16\beta)y^{12} + (22016-64\beta)y^{14} + \cdots \quad (14 \le \beta \le 104),$$
$$W_{64,2} = 1 + (1312+16\beta)y^{12} + (23040-64\beta)y^{14} + \cdots \quad (0 \le \beta \le 277)$$

のいずれかである。

[1]最後の2クラスについては講演後に存在しないことを示すことが出来た。宗政昭弘氏（東北大学）には有益な助言をいただいた。

Conway-Sloane[6] では「各 β に対して code の存在、非存在を示せ」という問題が出されている。この問題に関して最近の Huffman による論説 [7] によれば次の β については存在が知られている。

	β
$W_{64,1}$	14, 18, 44
$W_{64,2}$	2, 8, 9, 10, 16, 23, 30, 32, 37, 40, 44, 64

我々の W_{D_1} の weight enumerator をみると $\beta = 184$ の $W_{64,2}$ の weight enumerator であることが分かり、D_1 はこれまで存在が知られていなかった weight enumerator をもつ code であることが分かる。

系 3.6. $\beta = 184$ である $W_{64,2}$ の weight enumerator をもつ singly even self-dual $[64, 32, 12]$ code が存在する。

4 Characterization of D_1, D_2, D_3

ここでは、得られた長さ 64 の code のグラフからの特徴づけを行う。

V を $\mathbb{F}_q$ 上 $2m$ 次元のベクトル空間としタイプ ε の 2 次形式 Q を持つとする。V の q^{2m} 個のベクトルを頂点とし 2 点 u, v が $Q(u-v) = 0$ であるときに辺で結ぶことにより出来るグラフを affine polar graph といい $VO^{\varepsilon}_{2m}(q)$ で表す。

$m = 3$, $q = 2$, Q が $+$ タイプの場合を考える。$\mathrm{Aut}(VO^{+}_{6}(2)) \cong 2^6 : (O^{+}_{6}(2) : 2)$ であることが知られている。ここで、$O^{+}_{6}(2) \cong A_8$ であり、$O^{+}_{6}(2) : 2 \cong S_8$ であることに注意する。

ベクトル 0 を含む $VO^{+}_{6}(2)$ の maximum clique set（完全連結集合で最大のもの）は V の極大全特異部分空間 (maximal totally isotropic subspace) に含まれるベクトルの集合に他ならない。1 つ fix してそれを X とおく。$|X| = 8$ である。このとき

$$\mathcal{O} = \{X^{\sigma} | \sigma \in 2^6 : O^{+}_{6}(2)\}$$

とおくと $|\mathcal{O}| = 120$ である（X の $2^6 : (O^{+}_{6}(2) : 2)$-orbit の長さは 240 である。$2^6 : O^{+}_{6}(2)$ では 2 つに分かれる。）

$$D = \langle \mathcal{O} \rangle$$

を対称差で $\mathbb{F}_2$ 上の code とする。

定理 4.1 ([4]). D は doubly even self-dual $[64,32,8]$ code で $\mathrm{Aut}(D) \cong 2^6{:}O_6^+(2)$ である。

$|\mathcal{O}| = 120$ であることから D は D_2 と同値であることがわかる。

$X_1, X_2 \in \mathcal{O}$ に対して $|X_1 \cap X_2| = 0, 2, 8$ のいずれかとなる。$|X_1 \cap X_2| = 2$ のとき $|X_1 + X_2| = 12$ である。

$$W = \langle X_1 + X_2 | X_1, X_2 \in \mathcal{O}, |X_1 \cap X_2| = 2 \rangle$$

とおくと W は $[64,31,12]$ code となる。

定理 4.2. $W^\perp$ は D のほかに D_1 と同値な self-dual code と D_3 と同値な self-dual code を含む。

このように我々の code はグラフ $VO_6^+(2)$ を用いて構成することが出来る。

注意 4.3. $C(2^6{:}A_8, 64)$ には 6 個の self-dual code があったが、残りの 3 つは $\mathcal{O}$ の代わりにもう一方の $2^6{:}O_6^+(2)$-orbit をとることにより得られる。

注意 4.4. 同様にして他の $V_{2m}^\varepsilon(2)$ で code を構成してみると

graph	code
$VO_6^-(2)$	$[64,56,4]$
$VO_8^+(2)$	$[256,127]$
$VO_8^-(2)$	$[256,211,8]$
$VO_{10}^+(2)$	$[1024,501]$
$VO_{10}^-(2)$	$[1024,803]$

となり、$VO_6^+(2)$ のときのようにはならない。

5 Neighbors of $[64,32,8]$ codes

ここでは D_2, D_3 の neighbor について考える。長さ n の self-dual code C, C' が neighbor であるとは $\dim(C \cap C') = n/2 - 1$ であるときをいう。D_1, D_2, D_3 は互いに neighbor の関係にある。

C を self-dual $[n, n/2, d]$ code とする。M を C の weight d の codeword を行にもつ行列とする。$\mathbf{j}$ をすべての成分が 1 の codeword とする。

$$x\,{}^tM = \mathbf{j}$$

の解となる x が存在するとき、$C_0 = \langle x \rangle^{\perp} \cap C$ とおくと $\dim(C_0) = n/2-1$ であり、$\langle C_0, x \rangle$ と $\langle C_0, x+y \rangle$ $(y \in C \setminus C_0)$ はどちらも C の neighbor でかつ C の weight d の codeword を含まないものになっている。$\operatorname{rank} M = t$ ならばそのような code は $2 \times 2^{n/2-t}$ 個ある。

$C = D_2$, または D_3 の場合を考えたい。これらの neighbor に extremal なものがあるならば上述の方法ですべて得られることに注意する。

$C = D_2$ の場合 $\operatorname{rank} M = 32$ となるので D_1, D_3 以外にはない。

$C = D_3$ の場合 $\operatorname{rank} M = 28$ なので $2 \times 2^4 = 32$ 個の code が得られるが実際 16 個の extremal singly even（うち 1 つは D_1）と 16 個の doubly even（うち 1 つは D_2）が得られる。15 個ずつは互いに同値となるので、extremal singly even の 1 つを E_1, doubly even の 1 つを E_2 とする。$\mathrm{Aut}(E_1) \cong 2^3.2^3.2^3.L_3(2)$, $\mathrm{Aut}(E_2) \cong 2^3.2^3.2.2^3.L_3(2)$ となる。weight enumerator は

$$W_{E_1} = 1 + 2464y^{12} + 18432y^{14} + 226604y^{16} + \cdots$$
$$W_{E_2} = 1 + 8y^8 + 3136y^{12} + 454972y^{16} + \cdots$$

となる。E_1 は $\beta = 72$ の $W_{64,2}$ の weight enumerator になっている。

同様の方法でさらに E_2 の neighbor を調べると $\beta = 24$ の code も存在することが分かる。

定理 5.1. $\beta = 24, 72$ である $W_{64,2}$ の weight enumerator をもつ singly even $[64, 32, 12]$ self-dual code が存在する。

参考文献

[1] W. Bosma and J. Cannon, Handbook of Magma Functions, Department of Mathematics, University of Sydney, Available online at `http://magma.maths.usyd.edu.au/magma/`.

[2] N. Chigira, M. Harada and M. Kitazume, Some self-dual codes invariant under the Hall–Janko group, submitted.

[3] N. Chigira, M. Harada and M. Kitazume, Finite permutation groups and self-orthogonal codes, submitted.

[4] N. Chigira, M. Harada and M. Kitazume, On self-dual codes of length 64 with primitive automorphism groups , in preparation.

[5] 千吉良直紀, 原田昌晃, 北詰正顕, 有限置換群と自己直交符号, 第 22 回代数的組合せ論シンポジウム報告集 (掲載予定)

[6] J.H. Conway and N.J.A. Sloane, A new upper bound on the minimal distance of self-dual codes, *IEEE Trans. Inform. Theory* **36** (1990), 1319–1333.

[7] W.C. Huffman, On the classification and enumeration of self-dual codes, *Finite Fields Appl.* **11** (2005), 451–490.

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

[9] E. M. Rains, Shadow bounds for self-dual codes, *IEEE Trans. Inform. Theory* **44** (1998), 134–139.