数理解析研究所講究録 1440 巻 2005 年 5-12

Some self-dual codes invariant under the Hall-Janko group

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

散在型単純群 J_2 は 100 点からなる rank 3 のグラフの自己同型群の指数 2 の部分群として得られる。このグラフの性質をいろいろ調べてみると面白い性質を持つものをいくつか作り出すことが出来る。そのうちの 1 つがタイトルにある self-dual code である。ここではまず、グラフの構成の復習から初めて self-dual code の構成、ある 2-design の構成をする。また、単純群の作用する self-dual code の存在や self-orthogonal code の存在についても触れる。

2 Hall-Janko graph

鈴木通夫先生による散在型単純群 Suz の構成の論文 [4] にある方法に従って J_2 が作用するグラフについて復習をする。

まず Γ_1 を 4 点からなる edge のないグラフとする。

Γ_1 : ○ ○ ○ ○

$\mathrm{Aut}(\Gamma) \simeq S_4$ である。次に $i = 2,3,4$ に対して

$$\Gamma_i = \{\infty_{i-1}\} \cup \Delta_{i-1} \cup \Sigma_{i-1}$$

を次のように定義する。

(1) $\Delta_{i-1} = \Gamma_{i-1}$ とする。
(2) G_{i-1} を $\mathrm{Aut}(\Gamma_{i-1})$ のある部分群とするとき $\Sigma_{i-1} = I(G_{i-1})$ とする。
(3) ∞ は Δ_{i-1} のすべての点と辺で結ばれる。
(4) $a \in \Delta_{i-1}$ と $x \in \Delta_{i-1}$ は $a^x = a$ であるとき辺で結ばれる。
(5) $x, y \in \Sigma_{i-1}$ は $[x,y] \neq 1$ かつ $[x,z] = 1 = [y,z]$ となる $z \in \Sigma_{i-1}$ が存在するとき辺で結ばれる。

ここで、$(\mathrm{Aut}(\Gamma_1), G_1) = (S_4, S_4)$, $(\mathrm{Aut}(\Gamma_2), G_2) = (L_2(7) : 2, L_2(7))$, $(\mathrm{Aut}(\Gamma_3), G_3) = (U_3(3) : 2, U_3(3))$ である。このとき $\mathrm{Aut}(\Gamma_4) \simeq J_2 : 2$ となる。$\Gamma = \Gamma_4$ とおく。Γ の頂点集合を $V(\Gamma)$ と書くことにする。

以下、次のような特徴を持った $V(\Gamma)$ の部分集合に着目する。

- a coclique set: $X \subseteq V(\Gamma)$ が任意の $x, y \in X$ に対して $d(x,y) = 2$ であるとき coclique set であるという。
- an edge set: $d(x,y) = 1$ なる $x, y \in V(\Gamma)$ に対して $E_{\{x,y\}} = \{z \in V(\Gamma) | d(x,z) = 1 = d(y,z)\}$ を edge set という。
- a neighbor set: $N(x) = \{y \in V(\Gamma) | d(x,y) = 1\}$ を $x \in V(\Gamma)$ の neighbor set という。
- $B(x,y) = N(x) \setminus E_{\{x,y\}} = \{y\} \cup \{z \in V(\Gamma) | d(x,z) = 1, d(y,z) = 2\}$

まずは、∞_3 を含む coclique set X を考える。X のその他の点は $I(U_3(3))$ の元である。$I(U_3(3))$ は次のように記述される。

V をエルミート内積 $(\ ,\ )$ をもつ $\mathbb{F}_9 = \{0, \pm 1, \pm i, \pm 1 \pm i\}$ 上の 3 次元のユニタリ空間とする。$\mathcal{P} = \{[u] | 0 \neq u \in V\}$ とする。ここで $[u] = \{\lambda u | \lambda \in \mathbb{F}_9\}$ とおく。non-isotropic な元 u に対して

$$\sigma_u(w) = w - \frac{2(w,u)}{(u,u)}u$$

とするときこれから得られる $\sigma_{[u]} : \mathcal{P} \longrightarrow \mathcal{P}$ $(\sigma_{[u]}([w]) = [\sigma_u(w)])$ を考えると

$$I(U_3(3)) = \{\sigma_{[u]} | (u,u) \neq 0\}$$

である。non-isotropic な $u_1, u_2 \in V$ に対して

$$(u_1, u_2) = 0 \Longleftrightarrow [\sigma_{[u_1]}, \sigma_{[u_2]}] = 1$$

となる。

命題 2.1. (1) $X \subseteq V(\Gamma)$ が maximal coclique set ならば $|X| = 4, 6, 7, 10$ である。

(2) $|X| = 10$ で $\infty_3 \in X$ ならば $(v, v) = 0$ なる $v \in V$ があって、$X = \{\infty_3\} \cup \{\sigma_{[u]} | (u, v) = 0\}$ となる。

注意 2.2. isotropic points は $(3^3 - (-1)^3)(3^2 - (-1)^2)/(3^2 - 1) = 28$ 個あるので ∞_3 を含む size 10 の coclique set は 28 個あることがわかる。

isotropic な $v \in V$ に対して

$$\tau_v(w) = w + i(w, v)v$$

とおくとき $\mathcal{P}$ 上の置換 $\tau_{[v]}$ を $\tau_{[v]}([w]) = [\tau_v(w)]$ と定義すると $\tau_{[v]}$ は位数 3 の元になる。non-isotropic な $u \in V$ と isotropic な $v \in V$ に対して

$$(u, v) = 0 \Longleftrightarrow [\sigma_{[u]}, \tau_{[v]}] = 1$$

となるので coclique な 10 点集合 X は

$$X = \{\infty_3\} \cup \{\sigma_{[u]} | [\sigma_{[u]}, \tau_{[v]}] = 1\}$$

となる。ここで $\tau_{[v]}$ を J_2 の元と思うと $\tau_{[v]}$ は 10 点を固定することになる。$\tau_{[v]}$ は J_2 においては 3A-class に入る。置換表現を計算してみると J_2 の 3A での値は 10 なのでこの 10 点が $\tau_{[v]}$ の fixed points の集合となる。 □

$Q \in Syl_3(U_3(3))$, $Z(Q) = \langle \tau_{[v]} \rangle$ とすると

$$\{\sigma_{[u]} | [\sigma_{[u]}, \tau_{[v]}] = 1\} = I(N_{U_3(3)}(Q))$$

である。$G = \mathrm{Aut}(\Gamma)' \simeq J_2$ とする。

$$\mathfrak{D} = \{\{a\} \cup I(N_{G_a}(Q)) | Q \in Syl_3(G_a)\}$$

とおく。これが Γ の maximum coclique set の集合である。$|\mathfrak{D}| = 280$ である。

対称差を和として $\mathbb{F}_2$ 上の code を自然に考えることが出来る。$C_{10} = \langle \mathfrak{D} \rangle$ とおく。

命題 2.3. $\emptyset \neq X \in C_{10}$ とする。

(1) $|X| \geq 10$ である。
(2) $|X| = 10$ ならば $X \in \mathfrak{D}$ である。すなわち、C_{10} の weight 10 の codewords は $\mathfrak{D}$ である。

定理 2.4. C_{10} は self-dual $[100, 50, 10]$ code で $\mathrm{Aut}(C_{10}) \simeq J_2 : 2$ である。

C_{10} の weight enumerator は

$$1 + 280y^{10} + 1800y^{14} + 33075y^{16} + 156800y^{18} + 1236375y^{20} + 14752200y^{22} + 148974000y^{24} + \cdots + y^{100}$$

となる。

さて、ほかにあげた集合について次のこともわかる。

命題 2.5. $x, y \in V(\Gamma)$, $d(x, y) = 1$ とする。

(1) $N(x) \in C_{10}$.
(2) $E_{\{x,y\}} \in C_{10}$.
(3) $B(x, y) \in C_{10}$.

注意 2.6. Key-Moori により J_2 の原始的置換表現の suborbit を生成集合とする binary code が調べられている。100 次の置換表現の場合には $\langle N(x) | x \in V(\Gamma) \rangle$ である。これを C_A とおくと、C_A は doubly-even $[100, 36, 16]$ self-orthogonal code である。上の命題より $C_A \subset C_{10}$ であることがわかる。

Tits [5] は J_2 の outer automorphism の involution を構成しているが、そのことから次のことがわかる。

命題 2.7 (Tits[5]). $\sigma \in \mathrm{Aut}(J_2) \setminus J_2$, $o(\sigma) = 2$ とする。このときある $x, y \in V(\Gamma)$, $d(x, y) = 1$ が存在して $\mathrm{Fix}(\sigma) = E_{\{x,y\}}$ となる。

系 2.8. C_{10} の weight 14 の codewords は $E_{\{x,y\}}$ である。さらに、$C_{10} = \langle E_{\{x,y\}} | d(x, y) = 1 \rangle$ となる。

注意 2.9. outer involution は 2C-class なので

$$C_{10} = \langle \mathrm{Fix}(\sigma) | \sigma\text{: 2C-class} \rangle$$

と書くこともできる。 □

$\mathfrak{B} = \{B(x, y) | x, y \in V(\Gamma),\ d(x, y) = 1\}$ とおく。

命題 2.10. $\mathfrak{X} = (V(\Gamma), \mathfrak{B})$ は 2-$(100, 22, 168)$ design で $\mathrm{Aut}(\mathfrak{X}) \simeq J_2 : 2$ である。

3 neighbors of C_{10}

C_{10} は singly-even self-dual code であるから、doubly-even subcode を共通に含む C_{10} の neighbor を作ることが出来る。

定義．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。

次のことが知られている。

補題 3.1 (Brualdi-Pless[1]). C を長さ n の singly-even self-dual code とする。C_0 を weight$\equiv 0 \pmod 4$ の subcode として、

$$C_0^{\perp} = C_0 \cup (\alpha_1 + C_0) \cup (\alpha_2 + C_0) \cup (\alpha_3 + C_0).$$

を $C_0^{\perp}$ の C_0 による coset 分解とする。ここで $C = C_0 \cup (\alpha_2 + C_0)$ とする。$n \equiv 0 \pmod 4$ ならば、$C_0 \cup (\alpha_1 + C_0)$ および $C_0 \cup (\alpha_3 + C_0)$ も self-dual code になる。

上の補題を $C = C_{10}$ に適用すれば新しく 2 つの self-dual code が出来ることになる。補題の記号をそのまま使うことにして $S = (\alpha_1 + C_0) \cup (\alpha_3 + C_0)$（これは shadow と呼ばれている）の weight enumerator を計算してみると

$$20198400y^{22} + 2486937600y^{26} + \cdots + 20198400y^{78}$$

となるので、新しく出来た 2 つの self-dual codes は $[100, 50, 16]$ code であることがわかる。そこでそれぞれ C_{16}, C'_{16} と書くことにする。

定理 3.2. C_{16}, C'_{16} は同値な $[100, 50, 16]$ self-dual code で $\mathrm{Aut}(C_{16}) = \mathrm{Aut}(C'_{16}) \simeq J_2$ となる。ある $\sigma \in J_2 : 2 \setminus J_2$ があって $C_{16}^{\sigma} = C'_{16}$ となる。

$[100, 50]$ self-dual code のうち minimum weight が最大である code の可能性は $[100, 50, 18]$ であるが具体的に構成はされていない。

命題 3.3. $[100, 50, 18]$ self-dual code は C_{10}, C_{16}, C'_{16} の neighbor としては現われない。

4 fixed points set と self-orthogonal code

$J_2:2$ を自己同型群にもつ self-dual code と J_2 を自己同型群にもつ self-dual code が作られた。ほかの群についてもそのような self-dual code が存在するであろうか。

よく知られている例として M_{24} を自己同型群にもつ extended binary Golay $[24,12,8]$ code G_{24} がある。また、$M_{22}:2$ を自己同型群にもつ $[22,11,6]$ code もある。今まで binary で散在型単純群あるいはその自己同型群を自己同型群として持つ code は知られていなかった。

M_{24} を 24 点上の置換群とみたとき 2A-class (2^8 type) の fixed points set の集合は Steiner system $S(5,8,24)$ をなし、また 2B-class は 2^{12}-type で固定点を持たないので

$$G_{24}=\langle \mathrm{Fix}(u)|u\text{: 2A-class}\rangle=\langle \mathrm{Fix}(u)|u\in I(M_{24})\rangle$$

となる。

C_{10} は 3A-class あるいは 2C-class(outer) の fixed points set で生成された code であった。involution に注目してみると

class D	$\lvert\mathrm{Fix}(u)\rvert$	$\langle \mathrm{Fix}(u)\rvert u\in D\rangle$	dual
2A	20	$[100,37,16]$	$[100,63,8]$
2B	f.p.f	$[100,0]$	$[100,100]$
2C	14	C_{10}	C_{10}

なので、

$$C_{10}=\langle \mathrm{Fix}(u)|u\text{: 2C-class}\rangle=\langle \mathrm{Fix}(u)|u\in I(J_2:2)\rangle$$

となる。2A-class の $[100,37,16]$ code は $\langle C_A,\mathbf{1}_{100}\rangle$ と等しい。

注目すべきは実は involution の固定点の集合の作る code の dual である。

定義．G を $\Omega=\{1,2,\cdots,n\}$ の置換群とする。

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

とする。

例 4.1. 上に挙げた例をまとめておく。

- $C(J_2,100)$ は $[100,63,8]$ code である。

- $C(J_2:2,100)=C_{10}$ である。
- $C(M_{24},24)=G_{24}$ である。
- $C(M_{22},22)=C(M_{22}:2,22)$ は $[22,11,6]$ code である。

定理 4.2. C を長さ n の self-orthogonal code とし $G=\mathrm{Aut}(C)$ とする。このとき $C\subseteq C(G,n)$ となる。

Proof. $X\in C$ とし $\sigma\in I(G)$ をとる。$X\cap X^\sigma$ を考えるとこの集合に σ は作用する。C は self-orthogonal であるから $|X\cap X^\sigma|$ は偶数になる。$\mathrm{Fix}(\sigma)\cap X\subseteq X\cap X^\sigma$ である。$(X\cap X^\sigma)\setminus(\mathrm{Fix}(\sigma)\cap X)$ を考えると σ により 2 点ずつの組に分けることが出来るので $|(X\cap X^\sigma)\setminus(\mathrm{Fix}(\sigma)\cap X)|$ は偶数になる。したがって $|\mathrm{Fix}(\sigma)\cap X|$ も偶数となり、$X\in\langle\mathrm{Fix}(\sigma)|\sigma\in I(G)\rangle^\perp$ となる。 □

この定理により $C(G,n)$ が G-不変な self-orthogonal code の上限を与えていることがわかる。

注意 4.3. $C(G,n)$ が self-orthogonal なわけではない。また、$C(G,n)$ の自己同型群に G は含まれるが、勿論等しいとは限らない。 □

系 4.4. C_{10} は $J_2:2$ を自己同型群にもつ長さ 100 の唯一の self-dual code である。

$C(J_2,100)$ は $[100,63,8]$ code であるから J_2-不変な長さ 100 の self-dual code は必ず $C(J_2,100)$ に含まれる。実際に $C(J_2,100)$ を調べると次のことがわかる。

系 4.5. J_2-不変な長さ 100 の self-dual code は C_{10}, C_{16}, C'_{16} しかない。

他の群について考えてみる。まず、M_{22} の 176 点上の置換を考える。

命題 4.6. $G=M_{22}$ の 176 点 Ω 上の置換を考える。このとき

(1) $\mathfrak{X}=(\Omega,\{\mathrm{Fix}(\sigma)|\sigma\in I(G)\})$ は 2-(176,16,9) design (with 1155 blocks) となる。$\mathrm{Aut}(\mathfrak{X})=M_{22}$ となる。
(2) $C(M_{22},176)$ は $[176,22,50]$ code で $\mathrm{Aut}(C(M_{22},176))\simeq HS$ となる。

例 4.7. $C(HS,176)$ は $[176,22,50]$ code である。つまり $C(HS,176)=C(M_{22},176)$ であることがわかる。この code は Higman's geometry の incidence matrix が生成する code と一致している。また、HS が作用する長さ 176 の self-dual code は存在しないこともわかる。

例 4.8. $C(HS:2,100)$ は [100, 22, 22] self-orthogonal code になる。これは $HS:2$ の 100 次の rank 3 のグラフ (Higman-Sims graph) の近傍によって生成された code と一致する。Higman-Sims が作ったグラフは $HS:2$ を自己同型群にもつ最大の self-orthogonal code を与えていることになる。

例 4.9. $C(McL,275) = C(McL:2,275)$ は [275, 22, 100] code になる。これは McL-graph の近傍によって生成された code に一致する。

例 4.10. $C(Co_3,276)$ は [276, 23, 100] code になる。これも上の McL graph から作られる code を 1 次元拡大したものと一致している。

このようにある幾何に関係して得られていた code が involution の Fixed points の生成する code の dual としてとらえられることがある。

self-dual code に注目すると他にもいくつかの結果が得られている。

命題 4.11.

(1) M_{11} を自己同型群にもつ [132, 66, 6], [132, 66, 12] self-dual code が存在する。
(2) $M_{12}:2$ を自己同型群にもつ [132, 66, 12] self-dual code が存在する。
(3) $L_3(4):2^2$ を自己同型群にもつ [112, 56, 16] self-dual code が存在する。

参考文献

[1] R. Brualdi and V. Pless, Weight enumerators of self-dual codes, *IEEE Trans. Inform. Theory* **37** (1991), 1222–1225.

[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, Permutation groups and self-orthogonal codes, in preparation.

[4] M. Suzuki, A finite simple group of order 448,345,497,600, in "Theory of Finite Groups (R. Brauer and C. Sah, eds.)", 113–119, Benjamin, New York-Amsterdam, 1969.

[5] J. Tits, Le groupe de Janko d'ordere 604,800, in "Theory of Finite Groups (R. Brauer and C. Sah, eds.)", 91–95, Benjamin, New York-Amsterdam, 1969.