数理解析研究所講究録
第2003巻 2016年 66-73

Triply even codes constructed from distance regular graphs

弘前大学・理工学研究科　別宮　耕一
Koichi BETSUMIYA
Graduate School of Science and Technology,
Hirosaki University

2016 年 1 月 6 日

序

ここでは，代表的な距離正則グラフである Johnson グラフ $J(n,2)$ と Hamming グラフ $H(2,n)$ から極大な立方重偶符号を構成法し，それらの性質を述べる．

なお，立方重偶符号の基本的な性質については [1] による．紹介する例は Magma[2] を用いて計算した．

1　立方重偶符号

二元体 $\mathbb{F}_2$ 上の線型符号 C のすべての符合語の Hamming 重みが 8 の倍数であるとき，C を**立方重偶符号**という．立方重偶符号 C が**極大**であるとは，C を含む立方重偶符号が存在しないことをいう．

2　極大性の判定法

本原稿を執筆時点で，立方重偶符号の極大性を判定する一般的な方法は確立できていない．ここでは，ある種の立方重偶符号の極大性を判定するために有用な補題を述べる [1]．

この補題は立方重偶符号が極大であるための十分条件を与える．

補題 1. C を立方重偶符号とする．このとき，$C \subset (C*C)^{\perp}$ となる．

証明. $u_1, u_2, u_3 \in C$ について，$\mathrm{wt}(u_1+u_2) = \mathrm{wt}(u_1)+\mathrm{wt}(u_2)-2\,\mathrm{wt}(u_1*u_2) \equiv 0 \pmod 8$ となるので，$\mathrm{wt}(u_1*u_2) \equiv 0 \pmod 4$ となる．同様にして，$\mathrm{wt}(u_1*u_2*u_3) \equiv 0 \pmod 2$ が得られる．従って，任意の $u_1, u_2, u_3 \in C$ について，$u_1 \perp (u_2*u_3)$ となるので，$C \subset (C*C)^{\perp}$ となる．　□

命題 2. C を長さ n の立方重偶符号とする．

(i) $C = (C*C)^{\perp}$ ならば，C は極大立方重偶符号である．
(ii) $n \not\equiv 0 \pmod 8$ で，$C + \langle \mathbf{1} \rangle = (C*C)^{\perp}$ ならば，C は極大立方重偶符号である．

証明. まず，(i) を示す．$D \supset C$ を立方重偶符号とする．補題 1 と仮定より，

$$C \subset D \subset (D*D)^{\perp} \subset (C*C)^{\perp} = C$$

となる．これは $C = D$ となることを示している．

次に，(ii) を示す．$D \supset C$ を立方重偶符号とする．補題 1 と仮定より，

$$C \subset D \subset (D*D)^{\perp} \subset (C*C)^{\perp} = C + \langle \mathbf{1} \rangle$$

となる．もし，$C \subsetneq D$ とすると，$\mathbf{1} \in D$ となるが，これは，D が立方重偶符号であることに矛盾する． □

3 重偶符号を用いた構成法

距離正則グラフから極大な立方重偶符号を構成する方法を述べる前に，自明な立方重偶符号の構成法について述べ，その立方重偶符号を極大なものに拡張する方法を述べる [1].

まず，$u = (u_1, \ldots, u_{n_1}), v = (v_1, \ldots, v_{n_2})$ に対して，$(u \mid v) = (u_1, \ldots, u_{n_1}, v_1, \ldots, v_{n_2})$ と記号を定義する．長さ n の重偶符号を C に対して，$\mathcal{D}(C) := \{(u \mid u) \in \mathbb{F}_2^{2n} \mid u \in C\}$ とすると，$\mathcal{D}(C)$ は明らかに立方重偶符号となるが，極大ではない．この $\mathcal{D}(C)$ を極大な立方重偶符号に拡張する方法を述べる．

$D_1 \subset \mathbb{F}_2^{n_1}$, $D_2 \subset \mathbb{F}_2^{n_2}$ に対して，$D_1 \oplus D_2 := \{(u \mid v) \in \mathbb{F}_2^{n_1+n_2} \mid u \in D_1, v \in D_2\}$ と表記し，D_1 と D_2 の**直和**と呼ぶ．非自明な符号の直和と置換同値な符号を**可約**といい，可約でないものを **既約** という．D を既約な重偶自己双対符号とする．$\mathbf{0}, \mathbf{1} \in D$ に対して，$\tilde{\mathcal{D}}(D) = \mathcal{D}(D) + \langle (\mathbf{0} \mid \mathbf{1}) \rangle$ と定義すると次が成立する．

本節では以下 D を既約な重偶双対符号とする．

定理 3. $\tilde{\mathcal{D}}(D)$ は極大な立方重偶符号となる．

証明の前に，必要な補題を示す．

補題 4. $(D*D)^{\perp} = \langle \mathbf{1} \rangle$.

証明. $v \in (D*D)^{\perp}$, $x, y \in D$ について，$(v*x) \cdot y = v \cdot (x*y) = 0$ となるので，$(v*x) \in D^{\perp} = D$ となる．今，$\{1, \ldots, n\}$ のベキ集合と $\mathbb{F}_2^n$ を同一視して，$v = \{i_1, i_2, \ldots, i_t\}$, $\mathbf{1} + v = \{j_1, j_2, \ldots, j_s\}$ としたとき，$D_1 := \{(u_{i_1}, \ldots, u_{i_t}) \in \mathbb{F}_2^t \mid (u_1, \ldots, u_n) \in D\}$, $D_2 := \{(u_{j_1}, \ldots, u_{j_s}) \in \mathbb{F}_2^s \mid (u_1, \ldots, u_n) \in D\}$ と定義すると，$D \cong D_1 \oplus D_2$ となる．よって，もし，$v \notin \langle \mathbf{1} \rangle$ とすると，D が既約であることに矛盾する． □

補題 5. $(\tilde{\mathcal{D}}(D) * \tilde{\mathcal{D}}(D))^{\perp} = \tilde{\mathcal{D}}(D)$.

証明. $\dim D = k$ とする．補題 4 より，$\tilde{\mathcal{D}}(D) * \tilde{\mathcal{D}}(D) = D \oplus \langle \mathbf{0} \rangle + \mathcal{D}(D) * \mathcal{D}(D) = D \oplus \langle \mathbf{0} \rangle + \mathcal{D}(D * D) = D \oplus \langle \mathbf{0} \rangle + \mathcal{D}(\langle \mathbf{1} \rangle^{\perp})$ となるので，$\dim(\tilde{\mathcal{D}}(D) * \tilde{\mathcal{D}}(D)) = k + 2k - 1 = 3k - 1 = 4k - \dim \tilde{\mathcal{D}}(D)$ となる．補題 1 より，$(\tilde{\mathcal{D}}(D) * \tilde{\mathcal{D}}(D))^{\perp} \supset \tilde{\mathcal{D}}(D)$ となるので，$(\tilde{\mathcal{D}}(D) * \tilde{\mathcal{D}}(D))^{\perp} = \tilde{\mathcal{D}}(D)$ となる． □

定理 3 の証明. 補題 5，命題 2(i) より，$\tilde{\mathcal{D}}(D)$ は極大立方重偶符号となる． □

命題 6. $i \in \{1, \ldots, k\}$ について，C_i を立方重偶自己同型符号とし，$(C_i * C_i)^{\perp} = C_i$ とする．このとき，$C_1 \oplus \cdots \oplus C_k$ は極大立方重偶符号となる．

証明. $C := C_1 \oplus \cdots \oplus C_k$ とすると，$C * C = \bigoplus_{i=1}^{k} C_i * C_i = \bigoplus_{i=1}^{k} C_i^{\perp} = C^{\perp}$ となる． □

系 7. $D_1, \ldots, D_k$ を既約な重偶自己同型符号とする．このとき，$\tilde{\mathcal{D}}(D_1) \oplus \cdots \oplus \tilde{\mathcal{D}}(D_k)$ は極大立方重偶符号となる．

例 8. H_8 を $[8, 4, 4]$ 拡張 Hamming 符号とする．H_8 は既約な重偶自己双対符号である．$\tilde{\mathcal{D}}(H_8)$ は $[16, 5, 8]$ Reed-Muller 符号 RM$(4, 1)$ と同値であり，極大立方重偶符号となる．

4 距離正則グラフを用いた構成法

4.1 千吉良-原田-北詰符号

G を $\Omega_n := \{1, \ldots, n\}$ 上の置換群とする．$I(G) := \{g \in G \setminus \{1_G\} \mid g^2 = 1_G\}$ とし，$\mathrm{Fix}_{\Omega_n}(g) := \{x \in \Omega_n \mid x^g = x\}$ と表記することとする．本節では Ω_n のベキ集合と $\mathbb{F}_2^n$ を自然に同一視する．この同一視のもとで，$\mathrm{CHK}(G, \Omega) := \langle \mathrm{Fix}_{\Omega_n}(g) \in \mathbb{F}_2^n \mid g \in I(G) \rangle^{\perp}$ と定義する．この符号を**千吉良-原田-北詰符号**と呼ぶ [5].

4.2 Johnson グラフ $J(n, 2)$ を用いた構成法

$X := \binom{\Omega_n}{k}$, $E := \{\{\alpha, \beta\} \in \binom{X}{2} \mid |\alpha \cap \beta| = k - 1\}$ とする．このとき隣接構造 $J(n, k) = (X, E)$ を Johnson グラフと呼ぶ．

Johnson グラフ $J(n, 2)$ の自己同型群は n 次対称群と同型である．つまり，$\mathrm{Aut}(J(n, 2)) \cong S_n$ であることはよく知られている [6]. この S_n と $J(n, 2)$ について，千吉良-原田-北詰符号 $\mathrm{CHK}(S_n, \binom{\Omega_n}{2})$ を構成する．$i \in \{0, 1\}$ について，

$$W_i := \left\{ \binom{A}{2} \cup \binom{\Omega_n \setminus A}{2} \;\middle|\; A \subset \Omega_n, \quad |A| \equiv i \pmod 2 \right\}$$

とし，$\overline{W_i} := \{\Omega_n \setminus A \mid A \in W_i\}$ とすると次が成立する．

定理 9. $n \equiv 2 \pmod 4$ のとき，$\mathrm{CHK}(S_n, \binom{\Omega_n}{2}) = \overline{W}_0 \cup W_1$ となる．

証明の前に，必要な補題を示す．

補題 10. $Y \subset \binom{\Omega_n}{2}$ が次の条件をみたすものとする．

(i) ある $\{u,v,w\} \in \binom{\Omega_n}{3}$ について，$\binom{\{u,v,w\}}{2} \subset Y$，
(ii) $\left|\{(Y, \mathrm{Fix}_{\binom{\Omega_n}{2}}(\sigma)) \mid \sigma \in I(S_n)\}\right| = 1$．
ただし，$\mathrm{Fix}_{\binom{\Omega_n}{2}}(\sigma) = \{\{i,j\} \in \binom{\Omega_n}{2} \mid \{i^\sigma, j^\sigma\} = \{i,j\}\}$ とする．

このとき，ある $A \subset \Omega_n$ について，$Y = \binom{A}{2} \cup \binom{\Omega_n \setminus A}{2}$ となる．

証明. $Y = \Omega_n$ の場合は補題が成立するので，以下，$Y \subsetneq \Omega_n$ とする．A をグラフ $\Gamma_Y = (\Omega_n, Y)$ の最大クリークとすると，(i) より，$|A| \geq 3$ となる．$\overline{A} := \Omega_n \setminus A$ とする．

まず，$|A| \equiv 0 \pmod 2$ の場合を考える．$A = \{u_1, \ldots, u_k\} \cup \{v_1, \ldots, v_k\}$ を A の分割とし，$\overline{A} = \{x_1, \ldots, x_l\} \cup \{x_1, \ldots, v_l\}$ を $\overline{A}$ の分割とする．

$$\sigma := (u_1\, v_1)(u_2\, v_2) \cdots (u_k\, v_k)(x_1\, y_1) \cdots (x_l\, y_l),$$
$$\sigma' := (u_1\, x_1)(v_1\, y_1)(x_1\, y_1)(u_1\, v_1)\sigma.$$

とする．A が Γ_Y の最大クリークであることより，$\{u, x_1\} \notin Y$ となる $u \in A$ が存在する．$\sigma'' = (u\, u_1)\sigma'(u\, u_1)$ とする．

(ii) より，$(Y, \mathrm{Fix}_{\binom{\Omega_n}{2}}(\sigma')) = (Y, \mathrm{Fix}_{\binom{\Omega_n}{2}}(\sigma''))$ となるため，$(Y, \{\{u_1, x_1\}\}) = (Y, \{\{u, x_1\}\}) = 0$ となる．よって，$\{u_1, x_1\} \notin Y$ が得られる．$u_1 \in A$, $x_1 \in \overline{A}$ は任意の元であるため，$Y \subset \binom{A}{2} \cup \binom{\overline{A}}{2}$ となる．

逆に，(ii) より，$(Y, \mathrm{Fix}_{\binom{\Omega_n}{2}}(\sigma)) = (Y, \mathrm{Fix}_{\binom{\Omega_n}{2}}(\sigma'))$ となるため，$(Y, \{\{u_1, v_1\}, \{x_1, y_1\}\}) = (Y, \{\{u_1, x_1\}, \{v_1, y_1\}\}) = 0$ となる．よって，$\{x_1, y_1\} \in Y$ が得られるが，$x_1, y_1 \in \overline{A}$ は任意の元なので，$Y \supset \binom{\overline{A}}{2}$ となる．従って，$Y = \binom{A}{2} \cup \binom{\overline{A}}{2}$ が得られる．

次に，$|A| \equiv 1 \pmod 2$ の場合を考える．$A = \{u_0, u_1, \ldots, u_k\} \cup \{v_1, \ldots, v_k\}$, $\overline{A} = \{x_0, x_1, \ldots, x_l\} \cup \{y_1, \ldots, y_l\}$ をそれぞれ A, $\overline{A}$ の分割とする．ここで，$\tau \in I(S_n)$ を次のように定義する．

$$\tau = (u_0\, x_0)(u_1\, v_1)(u_2\, v_2) \cdots (u_k\, v_k)(x_1\, y_1) \cdots (x_l\, y_l)$$

A が (Ω_n, Y) の最大クリークであることより，$\{u, x_0\} \notin Y$ となる $u \in A$ が存在する．今，$\tau'' := (u\, u_0)\tau(u\, u_0)$ とすると，(ii) より，$(Y, \mathrm{Fix}_{\binom{\Omega_n}{2}}(\tau)) = (Y, \mathrm{Fix}_{\binom{\Omega_n}{2}}(\tau''))$ となるので，

$$(Y, \{\{u_0, x_0\}\}) = (Y, \{\{u, x_0\}\}) = 0$$

が得られる．従って，$\{u_0, x_0\} \notin Y$ となる．$u_0 \in A$, $x_0 \in \overline{A}$ は任意の元なので，$Y \subset \binom{A}{2} \cup \binom{\overline{A}}{2}$ となる．

逆に，$\tau' := (u_1\, x_1)(v_1\, y_1)(x_1\, y_1)(u_1\, v_1)\tau$ とすると，(ii) より，$(Y, \mathrm{Fix}_{\binom{\Omega_n}{2}}(\tau)) = (Y, , \mathrm{Fix}_{\binom{\Omega_n}{2}}(\tau'))$ となるので，

$$(Y, \{\{u_1, v_1\}, \{x_1, y_1\}\}) = (Y, \{\{u_1, x_1\}, \{v_1, y_1\}\}) = 0.$$

が得られる．従って，$\{x_1, y_1\} \in Y$ となる．$x_1, y_1 \in \overline{A}$ は任意の元なので，$Y \supset \binom{\overline{A}}{2}$ が得られる．よって，$Y = \binom{A}{2} \cup \binom{\overline{A}}{2}$ となり，補題が示された． □

定理 9 の証明．$n \equiv 2 \pmod 4$ より，任意の $\sigma \in I(S_n)$ について，$\left|\mathrm{Fix}_{\binom{\Omega_n}{2}}(\sigma)\right| \equiv 1 \pmod 2$ となるので，もし，$(Y, \mathrm{Fix}_{\binom{\Omega_n}{2}}(\sigma)) \equiv k \pmod 2$ とすると，$(\Omega_n \setminus Y, \mathrm{Fix}_{\binom{\Omega_n}{2}}(\sigma)) \equiv 1 + k \pmod 2$ となる．$|Y| \equiv 1 \pmod 2$ のとき，Ramsay の定理 [8, Chapter 9] より，$R_2(3,3) = 6$ となるので，グラフ (Ω_n, Y) の中に頂点数が 3 以上のクリークは存在しないとすると，その補グラフ $(\Omega_n, \overline{Y})$ が頂点数が 3 以上のクリークを含む．従って，補題 10 より，

$$\left\{ Y \subset \binom{\Omega_n}{2} \;\middle|\; \left|\left\{ (Y, \mathrm{Fix}_{\binom{\Omega_n}{2}}(\sigma)) \;\middle|\; \sigma \in I(S_n) \right\}\right| = 1 \right\} = W_0 \cup W_1 \cup \overline{W}_0 \cup \overline{W}_1$$

実際，

$$\left\{ (Y, \mathrm{Fix}_{\binom{\Omega_n}{2}}(\sigma)) \;\middle|\; \sigma \in I(S_n) \right\} = \begin{cases} \{1\} & \text{if } Y \in W_0 \cup \overline{W}_1 \\ \{0\} & \text{if } Y \in \overline{W}_0 \cup W_1 \end{cases}$$

となるので，

$$\mathrm{CHK}(S_n, \binom{\Omega_n}{2}) = \left\langle \left\{ \mathrm{Fix}_{\binom{\Omega_n}{2}}(\sigma) \;\middle|\; \sigma \in I(S_n) \right\} \right\rangle^{\perp} = \overline{W}_0 \cup W_1$$

が得られる． □

$\Omega_n = A_1 \cup A_2 \cup A_3 \cup A_4$ を $|A_1 \cup A_2| \equiv |A_1 \cup A_3| \equiv 0 \pmod 2$ をみたす分割とする．$\overline{\binom{A_1 \cup A_2}{2} \cup \binom{A_3 \cup A_4}{2}} + \overline{\binom{A_1 \cup A_3}{2} \cup \binom{A_2 \cup A_4}{2}} = \overline{\binom{A_1 \cup A_4}{2} \cup \binom{A_2 \cup A_3}{2}}$ となるので，$\overline{W}_0$ は線形部分空間となっている．

ここで，$J(n,2)$ の隣接行列を生成行列とする線形二元符号を T_n とする．このとき，ここまでの議論を踏まえると，$\overline{W}_0 = T_n$ となることが分かり，以下の先行の結果を直ちに導出することができる．

定理 11 (Haemers, Peeters and van Rijckevorsel [7, Subsection 4.1])．$n \equiv 2 \pmod 4$ とする．このとき，T_n の重み枚挙多項式は

$$W_{T_n}(x, y) = \sum_{l=0}^{\lfloor (n-1)/4 \rfloor} \binom{n}{2l} x^{2l(n-2l)} y^{\binom{n}{2} - 2l(n-2l)}$$

となる．特に，T_n は次元 $n-2$ の立方重偶符号となる．

更に，$T_n * T_n$ の次元を計算し，命題 2(ii) を適用することで，次が確認できる．

定理 12 ([1])．T_n は極大立方重偶符号である．

4.3 Hamming グラフ $H(2,n)$ を用いた構成法

$X := \Omega_n^d$, $E := \{\{(a_1,\dots,a_d),(b_1,\dots,b_d)\} \in \binom{X}{2} \mid d_H((a_1\dots,a_d),(b_1,\dots,b_d)) = d-1\}$ とする．ただし，d_H は Hamming 距離とする．つまり，$d_H((a_1\dots,a_d),(b_1,\dots,b_d)) := \#\{i \in \{1,\dots,d\} \mid a_i \neq b_i\}$ と定義される．このとき隣接構造 $H(d,n) = (X,E)$ を Hamming グラフと呼ぶ．

$H(2,n)$ の隣接行列を生成行列とする線形二元符号を $\tilde{H}_n$ とし，$H(2,n)$ の隣接行列の偶数個の行ベクトルの和全体がなす $\tilde{H}_n$ の部分符号を H_n とする．

Hamming グラフ $H(2,n)$ の自己同型群について，$\mathrm{Aut}(H(2,n)) \cong S_n \wr 2$ となることはよく知られている [6]．この $S_n \wr 2$ と $H(2,n)$ に関する千吉良-原田-北詰符号 $|(S_n \wr 2, H(2,n))$ について，次が成立する．

定理 13. m を正整数, $n = 4m$ とする．このとき千吉良-原田-北詰符号は $\mathrm{CHK}(S_n \wr 2, \Omega_n^2) = \tilde{H}_n$ となり，次元は $2n-2$ である．加えて，H_n は極大立方重偶符号となり，次元は $2n-3$ となる．更に，重み枚挙多項式は

$$W_{H_n}(x,y) = \sum_{u=0}^{2m^2} x^{8u} y^{16m^2-8u} \sum_{\substack{-m\le t,s\le m \\ st=m^2-u}} \binom{4m}{2(m-t)}\binom{4m}{2(m-s)}.$$

となる．

証明の前に，必要となる記号の導入と補題を示す．

$\sigma \in I(S_n \wr 2)$ に対して，$\mathrm{Fix}_{\Omega_n^2}(\sigma)$ を support とする $n \times n$ 行列を E_σ と表すこととする．つまり，$E_\sigma = (f_{ij})$ を $(i,j) \in \mathrm{Fix}_{\Omega_n^2}(\sigma)$ のとき $f_{ij} = 1$，$(i,j) \notin \mathrm{Fix}_{\Omega_n^2}(\sigma)$ のとき $f_{ij} = 0$ で定める．$\boldsymbol{x} = (x_1,\dots,x_n) \in \mathbb{F}_2^n$ に対して，$n \times n$ 行列を $R_{\boldsymbol{x}} = {}^t(x_1 \cdots x_n)(1 \cdots 1)$ と定める．

補題 14. A を $\mathbb{F}_2$ を成分とする $n \times n$ 行列とする．もし，任意の $\sigma \in I(S_n \wr 2)$ に対して，$(A, E_\sigma) = 0$ とすると，$\mathrm{wt}(\boldsymbol{x}) + \mathrm{wt}(\boldsymbol{y}) \equiv 0 \pmod 2$ をみたす，ある $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{F}_2^n$ について，$A = R_{\boldsymbol{x}} + {}^t R_{\boldsymbol{y}}$ となる．

証明. $A = (a_{ij})$ と定め，$\{x,y\},\{z,w\} \in \binom{\Omega_n}{2}$ とする．適当な番号付けの下で $\Omega_n \setminus \{x,y\} =$

$\{u_1,\dots,u_{n-2}\}$ と定め，同様に $\Omega_n\setminus\{z,w\}=\{v_1,\dots,v_{n-2}\}$ と定める．更に，置換を次のように定める．

$$\sigma:=((u_1,u_2)\cdots(u_{n-3},u_{n-2}),(v_1,v_2)\cdots(v_{n-3},v_{n-2}))\in S_n\times S_n\subset S_n\wr 2.$$

その設定の下で $(A,E_\sigma)=\#\{(i,j)\in\{x,y\}\times\{z,w\}\mid a_{ij}=1\}$ となることが分かる．もし $(A,E_\sigma)=0$ ならば，$(a_{xw},a_{yw})\in\{(a_{xz},a_{yz}),(1+a_{xz},1+a_{yz})\}$ となる．従って，任意に対して，$(a_{i1},\dots,a_{in})+(a_{11},\dots,a_{1n}),(a_{1i},\dots,a_{ni})+(a_{11},\dots,a_{n1})\in\{\mathbf{0},\mathbf{1}\}$ なることが分かる．これは，ある $\boldsymbol{x},\boldsymbol{y}\in\mathbb{F}_2^n$ について，$A=R_{\boldsymbol{x}}+{}^tR_{\boldsymbol{y}}$ となることを意味する．

逆に $\tau\in S_n\wr 2$ を $(x,y)\in\Omega_n^2$ について $(x,y)^\tau=(y,x)$ と定める．このとき $\boldsymbol{x},\boldsymbol{y}\in\mathbb{F}_2^n$ について，$(R_{\boldsymbol{x}}+{}^tR_{\boldsymbol{y}},E_\tau)=\#\{i\in\Omega_n\mid a_{ii}=1\}\equiv\mathrm{wt}(\boldsymbol{x}+\boldsymbol{y})\pmod 2$ が得られる．次に，$(\sigma_1,\sigma_2)\in S_n\times S_n$ とし，$\tau\in S_n\wr 2$ を先に定めたものとする．もし，$((\sigma_1,\sigma_2)\tau)^2=1$ とすると，$\sigma_1=\sigma_2^{-1}$ となる．従って，$\sigma\in S_n$ に対して $\alpha:=(\sigma,\sigma^{-1})\tau$ と定めると，$\boldsymbol{x},\boldsymbol{y}\in\mathbb{F}_2^n$ について，$(R_{\boldsymbol{x}}+{}^tR_{\boldsymbol{y}},E_\alpha)\equiv\mathrm{wt}(\boldsymbol{x}+\boldsymbol{y})\pmod 2$ となることが分かる．

よって，補題は証明された． □

定理 *13* の証明．まず，$\boldsymbol{x},\boldsymbol{y}\in\mathbb{F}_2^n$ を $\mathrm{wt}(\boldsymbol{x})\equiv 0\pmod 2$，$\mathrm{wt}(\boldsymbol{y})\equiv 0\pmod 2$ となるように選び，$2a:=\mathrm{wt}(\boldsymbol{x})$ and $2b:=\mathrm{wt}(\boldsymbol{y})$ と定める．更に $A:=R_{\boldsymbol{x}}+{}^tR_{\boldsymbol{y}}$ とすると

$$\begin{aligned}\mathrm{wt}(A)&=2b(4m-2a)+2a(4m-2b)\\&=-8(m-a)(m-b)+8m^2.\end{aligned}$$

となる．従って，$n\equiv 0\pmod 4$ に関して，H_n が立方重偶符号となることが分かる．

更に，$A=R_{\boldsymbol{x}}+{}^tR_{\boldsymbol{y}}$ について，$\#\{(\boldsymbol{u},\boldsymbol{v})\in\mathbb{F}_2^n\mid A=R_{\boldsymbol{u}}+{}^tR_{\boldsymbol{v}}\}=\#\{(\boldsymbol{x},\boldsymbol{y}),(\mathbf{1}+\boldsymbol{x},\mathbf{1}+\boldsymbol{y})\}=2$ となることと，補題 14 より，

$$\begin{aligned}\left|\mathrm{CHK}(S_n\wr 2,\Omega_n^2)\right|&=\#\{R_{\boldsymbol{x}}+{}^tR_{\boldsymbol{y}}\mid\boldsymbol{x},\boldsymbol{y}\in\mathbb{F}_2^n,\ \mathrm{wt}(\boldsymbol{x}+\boldsymbol{y})\equiv 0\pmod 2\}\\&=\frac{1}{2}\sum_{k=0}^{n}\sum_{l=0}^{n-1}\binom{n}{k}\binom{n-1}{l}\\&=2^{2n-2},\\|H_n|&=\#\{R_{\boldsymbol{x}}+{}^tR_{\boldsymbol{y}}\mid\boldsymbol{x},\boldsymbol{y}\in\mathbb{F}_2^n,\ \mathrm{wt}(\boldsymbol{x})\equiv 0\pmod 2,\ \mathrm{wt}(\boldsymbol{y})\equiv 0\pmod 2\}\\&=\frac{1}{2}\sum_{k=0}^{n-1}\sum_{l=0}^{n-1}\binom{n-1}{k}\binom{n-1}{l}\\&=2^{2n-3}.\end{aligned}$$

となることが分かる．つまり $\dim\mathrm{CHK}(S_n\wr 2,\Omega_n^2)=2n-2$，$\dim H_n=2n-3$ となる．加えて，$u:=-(m-a)(m-b)+m^2$ とすると，H_n の重み枚挙多項式が得られる．

ここで，$\dim(H_n * H_n) \geq (n-1)^2 + 2$ となることを示す．
そのために，まず

$$\mathcal{E} := \{A \in \mathbb{F}_2^{n\times n} \mid A\,{}^t(1\cdots 1) = {}^t(0\cdots 0),\ (1\cdots 1)A = (0\cdots 0)\}$$

とすると，$\mathcal{E} \subset H_n * H_n$ が得られる．なぜなら，任意の $\mathcal{E}$ の元は

$$\{R_{\{i,n\}} \circ {}^tR_{\{j,n\}} \mid i,j \in \{1,\ldots,n-1\}\}$$

の一次結合で得られる．ただし，$\circ$ は Hadamard 積を表す．次に $E_1,\ldots,E_{(n-1)^2}$ を $\mathcal{E}$ の基底とする．そのとき，

$$E_1,\ldots E_{(n-1)^2}, R_{\{n\}} = R_{\{1,n\}} \circ R_{\{2,n\}}, {}^tR_{\{n\}} = {}^tR_{\{1,n\}} \circ {}^tR_{\{2,n\}}$$

は $H_n * H_n$ において一次独立となる．よって $\dim(H_n * H_n) \geq (n-1)^2 + 2$ が言えた．

補題 1 より，$H_n \subset (H_n * H_n)^\perp$ となるので，$\dim(H_n * H_n)^\perp \leq n^2 - (n-1)^2 - 2 = 2n-3$ となることが分かる．従って $H_n = (H_n * H_n)^\perp$ となり，命題 2 となるので，H_n は極大立方重偶符号となる． □

参考文献

[1] K. Betsumiya and A. Munemasa, On triply even binary codes, J. London Math. Soc. (2) 86 (2012), 1–16, doi: 10.1112/jlms/jdr054.

[2] W. Bosma, J. Cannon and C. Playoust, The Magma algebra system. I. The user language, J. Symbolic Comput., **24** (1997), 235–265.

[3] K. Betsumiya, DATABASE: Triply even codes of length 48, `http://www.st.hirosaki-u.ac.jp/~betsumi/triply-even/`

[4] A. E. Brouwer, A. M. Cohen and A. Neumaier, Distance-regular graphs, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) 18, Springer-Verlag, Berlin, 1989.

[5] C. Naoki, H. Masaaki and K. Masaaki, Permutation groups and binary self-orthogonal codes, J. Algebra, **309** (2007), no. 2, 610–621.

[6] I. A. Faradžev, A. A. Ivanov, M. H. Klin and A. J. Woldar, Investigations in algebraic theory of combinatorial objects, Mathematics and its Applications (Soviet Series), **84**, Kluwer Academic Publishers Group, Dordrecht, 1994, xii+510.

[7] W.H. Haemers, R. Peeters and J.M. van Rijckevorsel, Binary codes of strongly regular graphs, Des. Codes Cryptogr. **17** (1999), no. 1-3, 187–209.

[8] R. Diestel, Graph Theory, 3rd edition, GTM 173, Springer-Verlag, 2005