符号の重み多項式に関する話題 *

大浦　学
金沢大学理工研究域

本講演の最終目標は、長岡昇勇先生（近畿大学名誉教授）との共同研究の結果 [4] を紹介することです。目標はそうなのですが、所々脱線しながら話しを進めたいと思います。ここで紹介する研究には、長岡先生と竹森翔さん [5] の先行研究（格子、テータ関数）があり、それに忠実に従った形で本研究は行われました。講演ではその先行研究については触れずに、符号理論に関する部分についてのみ述べました。この報告集でもそれに倣います。

1　符号の一般論

まず、$\mathbf{F}_2 = \{0, 1\}$ を 2 元体とします。2 元体以外での議論も可能ですが、この講演では 2 元体のみ扱います。この体の n 次元ベクトル空間 $\mathbf{F}_2^n$ の元 $u = (u_1, \ldots, u_n)$ に対して、0 でない座標の数を u の重さと言い、$wt(u)$ と表します。ベクトル空間 $\mathbf{F}_2^n$ の元 $u = (u_1, \ldots, u_n), v = (v_1, \ldots, v_n)$ に対して、内積を

$$u \cdot u = u_1 v_1 + \cdots + u_n v_n$$

で定義します。さて、$\mathbf{F}_2$ 上の符号を取り扱う訳ですが、講演では線形符号のみ扱います。そこで、部分空間 $\mathcal{C}$ を、長さ n の符号（線形符号とは呼ばないこと）と呼ぶことにします。単にベクトル空間というだけでは色々な結果も得られづらく、我々は符号にいくつかの条件を課します。長さ n の符号 $\mathcal{C}$ に対して、その双対符号 $\mathcal{C}^\perp$ を

$$\mathcal{C}^\perp = \{u \in \mathbf{F}_2^n : \ u \cdot v = 0, \ \forall v \in \mathcal{C}\}$$

で定義します。この $\mathcal{C}$ は、次元 $n - \dim \mathcal{C}$ を持ちます。符号 $\mathcal{C}$ が自己双対符号とは、$\mathcal{C} = \mathcal{C}^\perp$ が成り立つときに言います。もし、$\mathcal{C}$ が自己双対であれば、一般に成り立つ関係式

$$\dim \mathcal{C} + \dim \mathcal{C}^\perp = n$$

から、n は偶数で、さらに $\dim \mathcal{C} = n/2$ であることがわかります。自己双対に加えて、別のクラス、重偶符号は、任意の $u \in \mathcal{C}$ に対して

$$wt(u) \equiv 0 \pmod 4$$

が成り立つときに言います。我々が興味があるのは

$$\text{自己双対} + \text{重偶}$$

の 2 つの性質を持つクラスです。このクラスを Type II 符号と呼びます。すなわち

$$\text{Type II} \ = \text{自己双対} + \text{重偶}$$

* 第３９回代数的組合せ論シンポジウムにおける講演をかなり忠実に再現したものです。

です。

一般的な符号の定義は終わりまして、次に符号から得られる多項式に話しを移します。今、$\mathcal{C}$ を長さ n の符号とします。それに付随する重み多項式を

$$\begin{aligned} W_{\mathcal{C}}(x,y) &= \sum_{u\in\mathcal{C}} x^{n-wt(u)}y^{wt(u)} \\ &= \sum_{i=0}^{n} A_i x^{n-i}y^i, \end{aligned}$$

ただし $A_i = \sharp\{u\in\mathcal{C}:\ wt(u)=i\}$、で定義します。これは、次数 n の斉次多項式となっています。ここで、この重み多項式の一般化を念頭においた、テクニカルな話題を入れておきます。重さを復習しておくと、u の重さとは、$0\in\mathbf{F}_2$ とは異なる u の座標の数でした。ところで、u は 0 か 1 がならんでいるので、0 と異なるとは、つまり 1 ということです。なぜ最初から 0 とは異なる、ではなく、1 である、という言い方をしないのかと言うと、2 元体以外を取り扱う場合を考えて、なのです。しかし、$\mathbf{F}_2$ のみ扱います、と最初に宣言しているので、まあ最初から重さを 1 が現れる個数と言っても良さそうですが。戻ります。次でした。

$$\begin{aligned} wt(u) &= \sharp\{i:\ u_i\neq 0\} \\ &= \sharp\{i:\ u_i = 1\}. \end{aligned}$$

変数 x のべきも同様に考えると

$$n - wt(u) = \sharp\{i:\ u_i = 0\}$$

となります。そう理解すると、

$$n_a(u) = \sharp\{i:\ u_i = a\},\ a\in\mathbf{F}_2$$

を導入することで

$$\begin{aligned} W_{\mathcal{C}}(x_0,x_1) &= \sum_{u\in\mathcal{C}} x_0^{n_0(u)}x_1^{n_1(u)} \\ &= W_{\mathcal{C}}(x_a : a\in\mathbf{F}_2) \end{aligned}$$

という表示ができます。この表示が、重み多項式の一般化（多変数化）には都合がいいようです。

上で、我々は Type II 符号に興味がある、と述べましたが

我々は Type II 符号の重み多項式に興味がある

というのが、より適切かもしれません。では、その重み多項式について、我々は何が言えるのでしょうか。

2　重み多項式の性質

長さ n の符号 $\mathcal{C}$ に対して

$$W_{\mathcal{C}^\perp}(x,y) = \frac{1}{|\mathcal{C}|}W_{\mathcal{C}}(x+y,x-y)$$

が知られています（MacWilliams）。変数 x,y の代わりに x_0,x_1 を導入するんじゃなかったの、と言われそうですが、ここでは x,y の方が簡単だから、ということです。使い分けていきます。さて、MacWilliams 恒等式は、双対符号の重み多項式は、もとの符号の重み多項式から代数的な操作で得ることができると述べてい

ます。例えば、双対符号の構造が複雑で、双対符号の重み多項式が直接には求めづらい場合で、もとの符号の符号の重み多項式が比較的容易に得られる場合などに有効です。我々は、MacWilliams 恒等式を長さ n の自己双対符号 $\mathcal{C} = \mathcal{C}^{\perp}$ に適用します。この場合、n は偶数で $\dim \mathcal{C} = n/2$、言い換えると $|C| = 2^{n/2}$ でした。これらを MacWilliams 恒等式にあてはめると

$$\begin{aligned} W_{\mathcal{C}}(x,y) &= \left(\frac{1}{\sqrt{2}}\right)^{n} W_{\mathcal{C}}(x+y, x-y) \\ &= W_{\mathcal{C}}\left(\frac{x+y}{\sqrt{2}}, \frac{x-y}{\sqrt{2}}\right) \end{aligned}$$

となります。つぎに $\mathcal{C}$ が重偶の場合に考えます。今、$\mathcal{C}$ を重偶符号とすると

$$\begin{aligned} W_{\mathcal{C}}\left(x, \sqrt{-1}y\right) &= \sum_{u \in \mathcal{C}} x^{n-wt(u)} \left(\sqrt{-1}y\right)^{wt(u)} \\ &= \sum_{u \in \mathcal{C}} x^{n-wt(u)} y^{wt(u)} \\ &= W_{\mathcal{C}}(x,y) \end{aligned}$$

となります。

今までの話しを Type II 符号についてまとめますと、Type II 符号 $\mathcal{C}$ の重み多項式は

$$\begin{aligned} W_{\mathcal{C}}\left(\frac{x+y}{\sqrt{2}}, \frac{x-y}{\sqrt{2}}\right) &= W_{\mathcal{C}}(x,y), \\ W_{\mathcal{C}}\left(x, \sqrt{-1}y\right) &= W_{\mathcal{C}}(x,y) \end{aligned}$$

を満たすことになります。

ここで、個人的な思い出話しを挿入します。吉田知行先生の数学セミナー（１９８７年４月号、数学との出会い）の記事です。実際には、それらがまとめられた増刊号だったかもしれません。吉田先生は「２４との出会いと再会」と題する文章で、次で締めくくられています。「最後に計算問題をひとつ。

$$f(x,y) = x^{24} + 759x^{16}y^{8} + 2576x^{12}y^{12} + 759x^{8}y^{16} + y^{24}$$

とおけば

$$\begin{aligned} f\left(\frac{x+y}{\sqrt{2}}, \frac{x-y}{\sqrt{2}}\right) &= f(x,y), \\ f\left(x, \sqrt{-1}y\right) &= f(x,y) \end{aligned}$$

であることを示せ。」この $f(x,y)$ はあとで出てくる、長さ 24 の Type II 符号、いわゆる Golay 符号の重み多項式です。今までの議論から、この $f(x,y)$ が上記 2 つの等式を満たすことは分かります。

重み多項式と有限群の不変式論を結びつける Gleason の定理に移っていきます。Gleason の定理への入門的な論文を引用します。N. J. A. Sloane [11] は符号理論を不変式論の観点から解説しました。その論文では、Type II 符号の重み多項式が 2 つの等式

$$W\left(\frac{x+y}{\sqrt{2}}, \frac{x-y}{\sqrt{2}}\right) = W(x,y), \tag{1}$$

$$W\left(x, \sqrt{-1}y\right) = W(x,y) \tag{2}$$

を満たすことを注意したあと、つぎのように述べます。“The problem we want to solve is to find all polynomials $W(x,y)$ satisfying (1) and (2).” 求めたいのは

$$\{W(x,y) \in \mathbf{C}[x,y] :\ W(x,y) \text{ satisfies } (1)+(2)\}$$

で、この集合は環をなすことが分かります。今、

$$G = \left\langle \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},\ \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{-1} \end{pmatrix} \right\rangle$$

とおくと、我々がターゲットとしている環は、群 G の不変式環

$$R^G = \left\{ W(x,y) \in \mathbf{C}[x,y] :\ W(ax+by, cx+dy) = W(x,y),\ \forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G \right\}$$

です。ここで、G は位数 192 の複素鏡映群で、Shephard-Todd [10] のリストにおいて、No. 9 です。今までの議論から

$$\begin{array}{c} R^G \\ \cup \\ \text{Type II 符号の重み多項式で生成される } \mathbf{C}[x,y] \text{ の部分環} \\ \cup \\ \mathbf{C}[W_{e_8}, W_{g_{24}}] \end{array}$$

の包含関係が成り立ちます。ここで、e_8 は長さ 8 の Type II 符号で Hamming 符号、g_{24} は長さ 24 の Type II 符号で Golay 符号、とそれぞれ呼ばれるものです。Gleason は、1970 年の国際数学者会議で、不変式環 R^G が 2 つの Type II 符号の重み多項式 W_{e_8}, $W_{g_{24}}$ で生成されることを発表します [3]、すなわち、3 つの環

$$\boxed{R^G}, \boxed{\text{Type II 符号の重み多項式で生成される } \mathbf{C}[x,y] \text{ の部分環}}, \boxed{\mathbf{C}[W_{e_8}, W_{g_{24}}]}$$

は一致します。

3 Type II 符号の分類

ここで、Type II 符号がどれほどあるのか、述べておきます。長さ n の 2 つの符号がある程度同じ性質を持つ場合を除くため、同値の概念を導入します。長さ n の符号 $\mathcal{C}$, $\mathcal{C}'$ が同値であるとは、$\mathcal{C}$ の座標の置換をした後、$\mathcal{C}'$ と一致するときに言います。つまり、

$$\mathcal{C} \text{ と } \mathcal{C}' \text{ が同値} \Leftrightarrow \exists \sigma \in S_n,\ \mathcal{C}^\sigma = \mathcal{C}'$$

です。この同値関係のもと、Type II 符号の分類を述べる訳ですが、その前に次の命題を述べておきます。

命題 1. 長さ n の *Type II* 符号が存在するための必要十分条件は $n \equiv 0 \pmod 8$ である。

Type II 符号の同値類を除いた個数はつぎの表 1 になります ([8, 9, 2, 1])。

長さを固定した場合の重み多項式のなす空間について述べます。まず同値な符号の重み多項式は一致します。しかし、非同値な符号であっても、同じ重み多項式を持つ場合があります。長さ 16 の Type II 符号は 2

表 1　長さ 24 の Type II 符号の分類

符号の長さ n	8	16	24	32	40	≥ 48
Type II 符号の個数	1	2	9	85	94343	unknown

つ（e_8^2, d_{16}^+ と表される）ありますが、それの重み多項式は一致します。この点は、種数の概念を取り入れることで、ある意味、解決します。符号 $\mathcal{C}$ の種数 g の重み多項式は

$$W_{\mathcal{C}}^{(g)}(x_a:\ a\in\mathbf{F}_2^g)=\sum_{u_1,\dots,u_g\in\mathcal{C}}\prod_{a\in\mathbf{F}_2^g}x_a^{n_a(u_1,\dots,u_g)}$$

ここで

$$n_a(u_1,\dots,u_g)=\sharp\{i:\ a=(u_{1i},\dots,u_{gi})\}$$

です。すると長さ 16 の Type II 符号の種数 g の重み多項式ですが

$$W_{e_8^2}^{(g)}\neq W_{d_{16}^+}^{(g)}\Leftrightarrow g\geq 3$$

が知られています。同様の問題を長さ 24 の場合に考えますと

$$\dim\langle W_{\mathcal{C}_1}^{(g)},\dots,W_{\mathcal{C}_9}^{(g)}\rangle=9\Leftrightarrow g\geq 6$$

となります（[6]. *cf.* [7]）。

4　結果（長岡昇勇先生との共同研究）

長さ 24 の Type II 符号を述べるため、具体的な符号を生成行列の形で表しておきます。添え字が符号の長さを表し、行ベクトルがその符号の基底となります。

$$d_n:\ \begin{pmatrix}111100 & \dots & 0000\\ 001111 & \dots & 0000\\ & \ddots & \\ 000000 & \dots & 1111\end{pmatrix},\quad n\equiv 0\pmod 2,$$

$$e_7:\ \begin{pmatrix}0111100\\ 0110011\\ 1101010\end{pmatrix},$$

$$e_8:\ \begin{pmatrix}11110000\\ 00111100\\ 00001111\\ 10101010\end{pmatrix}.$$

すでに何度かでてきましたが、長さ 24 の 2 元体上の Golay 符号を g_{24} で表します。この符号 g_{24} は重さ 4 の元を持たず、最小重みが 8 です。

一つ、記号を導入しましょう。長さ n, n' の符号 $\mathcal{C}$, $\mathcal{C}'$ をとります。このとき、長さ $n+n'$ の符号となる、$\mathcal{C}$ と $\mathcal{C}'$ の直和を積の形で表します：

$$\mathcal{C}\mathcal{C}'=\{(u\ u'):\ u\in\mathcal{C},\ u'\in\mathcal{C}'\}.$$

後の計算で必要となる h_i $(i = 1, 2, \ldots, 9)$ について述べておきます。例で説明します。2 番目の符号 $\mathcal{C}_2$ を考えます。この符号の成分は $d_{10}e_7^2$ です。d_{10} の重さ 4 の元の個数は 10 で、e_7 の重さ 4 の元の個数は 7 です。重さ 4 の元の個数をその符号の長さで割ると

$$\frac{10}{10} = \frac{7}{7} = 1$$

となります。この数字を h_2 とします。このように計算しますと、長さ 24 の Type II 符号の成分と h_i は次のようになります。

表 2　長さ 24 の Type II 符号

i	1	2	3	4	5	6	7	8	9
Components	d_{12}^2	$d_{10}e_7^2$	d_8^3	d_6^4	d_{24}	d_4^6	g_{24}	$d_{16}e_8$	e_8^3
h_i	$\frac{5}{4}$	1	$\frac{3}{4}$	$\frac{1}{2}$	$\frac{11}{4}$	$\frac{1}{4}$	0	$\frac{7}{4}$	$\frac{7}{4}$

ここで

$$\begin{aligned}\Delta &= \frac{1}{42}\left(W_{\mathcal{C}_9}^{(1)} - W_{\mathcal{C}_7}^{(1)}\right)\\ &= x^4y^4(x^4 - y^4)^4\end{aligned}$$

とおきましょう。種数 1 の場合の結果を述べます。

定理 2.　(1) $i = 1, 2, \ldots, 9$ のとき、

$$W_{C_i}^{(1)} = W_{C_9}^{(1)} + 6(4h_i - 7)\Delta$$

が成り立つ。

(2) i, j は $1, 2, \ldots, 8$ の整数で、異なるとする。このときある整数 m について $4h_i \equiv 4h_j \pmod{m}$ が成り立つならば

$$W_{C_i}^{(1)} \equiv W_{C_j}^{(1)} \pmod{6m}$$

である。

(3) C_α, C_β を長さ 24 の *Type II* で $h_\alpha < h_\beta$ とする。このとき、$i = 1, 2, \ldots, 9$ について

$$W_{C_i}^{(1)} = \frac{h_i - h_\beta}{h_\alpha - h_\beta}W_{C_\alpha}^{(1)} + \frac{h_i - h_\alpha}{h_\beta - h_\alpha}W_{C_\beta}^{(1)}$$

が成り立つ。

種数 2 について結果を述べるため、つぎの整数係数の多項式を準備します。

$$\begin{aligned}X &= \frac{1}{42}\left(W_{C_9}^{(2)} - W_{C_7}^{(2)}\right),\\ Y &= -\frac{11}{7}W_{C_9}^{(2)} + \frac{4}{7}W_{C_7}^{(2)} + W_{C_5}^{(2)}\end{aligned}$$

に対して、

$$X_{24} = X - \frac{1}{44}Y,$$
$$Y_{24} = \frac{1}{2^4 3 \cdot 11}Y.$$

とおきます。種数 2 の多項式は、Φ 作用素

$$\Phi : \mathbf{C}[x_a \in \mathbf{F}_2^g] \to \mathbf{C}[x_{a'} : a' \in \mathbf{F}_2^{g-1}]$$
$$x_a \mapsto \begin{cases} x_{a'} & \text{if } a = \begin{pmatrix} a' \\ 0 \end{pmatrix}, \\ 0 & \text{if } a = \begin{pmatrix} a' \\ 1 \end{pmatrix} \end{cases}$$

で、種数 1 の多項式と結びつきます。

命題 3. $\Phi(X_{24}) = \Delta$ および $\Phi(Y_{24}) = 0$.

種数 2 の場合の結果を述べます。

定理 4. (1) $i = 1, 2, \ldots, 9$ に対して

$$W_{C_i}^{(2)} = W_{C_9}^{(2)} + 6(4h_i - 7)X_{24} + 24(2h_i + 3)(4h_i - 7)Y_{24}$$

が成り立つ。

(2) i, j は $1, 2, \ldots, 8$ の整数で、異なるとする。このときある整数 m について $4h_i \equiv 4h_j \pmod{m}$ が成り立つならば

$$W_{C_i}^{(2)} \equiv W_{C_j}^{(2)} \pmod{6m}.$$

である。

(3) $C_\alpha, C_\beta, C_\gamma$ を長さ 24 の *Type II* 符号とし $h_\alpha < h_\beta < h_\gamma$ が成り立っている。このとき、$i = 1, 2, \ldots, 9$ に対して

$$W_{C_i}^{(2)} = \ell_\alpha(h_i)W_{C_\alpha}^{(2)} + \ell_\beta(h_i)W_{C_\beta}^{(2)} + \ell_\gamma(h_i)W_{C_\gamma}^{(2)}.$$

が成り立つ。ここで $\epsilon \in \{\alpha, \beta, \gamma\}$ に対して

$$\ell_\epsilon(x) = \prod_{\substack{\mu \in \{\alpha,\beta,\gamma\} \\ \mu \neq \epsilon}} \frac{x - x_\mu}{x_\epsilon - x_\mu}$$

である。

すでに出てきた事実 $W_{e_8}^{(3)} \neq W_{d_{16}^+}^{(3)}$ と $h_8 = h_9$ から、定理 2 と定理 4 それぞれにおける (1) の等式の種数 3 への拡張はないことを注意して終わりたいと思います。

参考文献

[1] Betsumiya, K., Harada, M., Munemasa, A.: A complete classification of doubly even self-dual codes of length 40. Electron. J. Combin. **19** (2012), no.3, Paper 18, 12 pp.

[2] Conway, J. H., Pless, V., Sloane, N. J. A.: The binary self-dual codes of length up to 32: a revised enumeration. J. Combin. Theory Ser. A **60** (1992), no.2, 183-195.

[3] Gleason, A. M.: Weight polynomials of self-dual codes and the MacWilliams identities. Actes du Congrès International des Mathématiciens (Nice, 1970), Tome 3, pp. 211-215. Gauthier-Villars, Paris, 1971.

[4] Nagaoka, S., Oura, M.: Note on the Type II codes of length 24. Preprint.

[5] Nagaoka, S., Takemori, S.: Notes on theta series for Niemeier lattices Ramanujan J. **42** (2017), no. 2, 385-400.

[6] Nebe, G.: Kneser-Hecke-operators in coding theory. Abh. Math. Sem. Univ. Hamburg **76** (2006), 79-90.

[7] Oura, M., Poor, C.,; Yuen, D.: Towards the Siegel ring in genus four. Int. J. Number Theory **4** (2008), no. 4, 563-586.

[8] Pless, V.: A classification of self-orthogonal codes over GF(2). Discrete Math. **3** (1972), 209-246.

[9] Pless, V., Sloane, N. J. A.: On the classification and enumeration of self-dual codes. J. Combinatorial Theory Ser. A **18** (1975), 313-335.

[10] Shephard, G. C., Todd, J. A.: Finite unitary reflection groups. Canad. J. Math. **6** (1954), 274–304.

[11] Sloane, N. J. A.: Error-correcting codes and invariant theory: new applications of a nineteenth-century technique. Amer. Math. Monthly **84** (1977), no.2, 82-107.