自己双対符号とその周辺

山形大学理学部／ＪＳＴさきがけ
原田 昌晃

2010 年 8 月 12 日

1 はじめに

この原稿は, 北海道大学で行なわれた「第５５回代数学シンポジウム」での講演内容をまとめたものである．講演では, self-dual code (自己双対符号) について, 著者自身の結果を交えながら, どのような研究が行われてきたのかを非専門家向けに紹介した．この原稿も, 非専門家向けの self-dual code についての概説となることを心掛けたい.

まず, q を素数べきとし, 位数 q の有限体を $\mathbb{F}_q$ で表すことにする．次に, k を 2 以上の自然数とし, $\mathbb{Z}_k$ で有限環 $\mathbb{Z}/k\mathbb{Z}$ を表すことにする．講演と同じように, この原稿では $\mathbb{F}_q$-code だけでなく $\mathbb{Z}_k$-code も扱うので, R で $\mathbb{F}_q$ か $\mathbb{Z}_k$ を意味することにして必要な定義を与える．長さ n の R-code とは R^n の R-部分加群のことである．C の dual code $C^\perp$ を $\{x \in R^n \mid \ x \cdot y = 0\ (\forall y \in C)\}$ で定義する, ただし $x \cdot y$ は標準的な内積を表す. $C = C^\perp$ であるとき C を *self-dual* とよぶ. $x = (x_1, x_2, \ldots, x_n) \in R^n$ の weight $\mathrm{wt}(x)$ を $|\{i \mid x_i \neq 0\}|$ とする．C の minimum weight を $\min\{\mathrm{wt}(x) \mid \mathbf{0} \neq x \in C\}$ で定義して $d(C)$ で表す, ただし $\mathbf{0}$ はゼロベクトルを表す.

次に同値と自己同型群の定義を述べよう．C, C' を長さ n の self-dual R-code とする．$C' = CP\ (= \{xP \mid x \in C\})$ となる n 次正方行列 P が存在するときに C と C' は同値であると定義し, また $C = CP$ となる行列 P の集合を C の自己同型群 $\mathrm{Aut}(C)$ とよぶ, ただし $R = \mathbb{F}_2$ のときは P は置換行列, $R = \mathbb{F}_4$ のときは P は $\mathbb{F}_4$-monomial 行列, それ以外の R では P は $(\pm 1, 0)$-monomial 行列とする.

C の weight enumerator とは $\mathbb{C}$ 上の 2 変数の多項式で $W_C(x, y) = \sum_{c \in C} x^{n-\mathrm{wt}(c)} y^{\mathrm{wt}(c)}$ である. $W_C(x, y) = W_{C^\perp}(x, y)$ となる場合 C を formally self-dual とよぶ. 明らかに self-dual code は formally self-dual になる．C の全ての元 x に対して $\mathrm{wt}(x) \equiv 0 \pmod{\Delta}$ となる整数 $\Delta \geq 2$ が存在するときに C を Δ-divisible とよぶ.

2 Type I, II, III, IV code と Gleason の定理

次の結果は Gleason–Pierce による[1] formally self-dual Δ-divisible code の特徴付けである.

[1] [24] ではこの結果は Gleason–Pierce–Turyn によるとされている.

Theorem 1 (Gleason–Pierce)**.** C を formally self-dual Δ-divisible $\mathbb{F}_q$-code とする. 次のうちの 1 つが成り立つ.

(I) $q = 2$, $\Delta = 2$,
(II) $q = 2$, $\Delta = 4$, このとき C は self-dual になる,
(III) $q = 3$, $\Delta = 3$, このとき C は self-dual になる,
(IV) $q = 4$, $\Delta = 2$,
(V) q は任意で $\Delta = 2$ かつ $W_C(x, y) = (x^2 + (q-1)y^2)^{n/2}$.

C が上の (I), (II), (III), (IV) を満たす場合をそれぞれ Type I, II, III, IV code とよぶ. (V) の場合は長さ 2 の code の直和になり自明なケースとして通常通り取り扱わないことにして, Type I, II, III, IV code を中心に考えていく.

Remark 2. Type II code と Type III code は自動的に self-dual になるが, self-dual でない Type I code は実際に存在する. 一般には Type IV code は self-dual にならないが, 別の内積に関して self-dual になる (第 4 節の最後の部分を参照).

C を Type X (ここで X は I, II, III または IV) code とする. まず Type X code の weight enumerator についての考察を与える. 詳細は, 例えば [24, Chap. 19], [32, Section 6] などを参照していただきたい.

Lemma 3. C を Type X code とする. このとき次が成り立つ.

(1) $W_C(x, y) = W_C\Big(\dfrac{x + (q-1)y}{\sqrt{q}}, \dfrac{x - y}{\sqrt{q}}\Big)$.
(2) $W_C(x, y) = W_C(x, \omega y)$, ただし ω は 1 の原始 Δ 乗根を表す.

Proof. C の長さを n とする.
(1) MacWilliams 恒等式より $W_{C^\perp}(x, y) = \frac{1}{|C|} W_C(x+(q-1)y, x-y)$ が成り立つ. $C = C^\perp$ より

$$W_C(x, y) = W_{C^\perp}(x, y) = \frac{1}{q^{n/2}} W_C(x + (q-1)y, x - y) = W_C\Big(\frac{x + (q-1)y}{\sqrt{q}}, \frac{x - y}{\sqrt{q}}\Big).$$

(2) 全ての $c \in C$ に対して $\mathrm{wt}(c) \equiv 0 \pmod{\Delta}$ なので

$$W_C(x, \omega y) = \sum_{c \in C} x^{n - \mathrm{wt}(c)} (\omega y)^{\mathrm{wt}(c)} = \sum_{c \in C} x^{n - \mathrm{wt}(c)} y^{\mathrm{wt}(c)} = W_C(x, y)$$

が成り立つ. □

Lemma 3 から次が成り立つ:

$$\frac{1}{\sqrt{q}} \begin{pmatrix} 1 & q-1 \\ 1 & -1 \end{pmatrix} \circ W_C(x, y) = W_C(x, y), \begin{pmatrix} 1 & 0 \\ 0 & \omega \end{pmatrix} \circ W_C(x, y) = W_C(x, y),$$

ただし, 行列 $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ と多項式 $f(x, y)$ に対して $A \circ f(x, y) = f(ax + by, cx + dy)$ とする. 各 X に対して, この 2 つの行列で生成される群を考える:

$$G_{\mathrm{X}} = \Big\langle \frac{1}{\sqrt{q}} \begin{pmatrix} 1 & q-1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & \omega \end{pmatrix} \Big\rangle \ (\subset GL(2, \mathbb{C})).$$

ちなみに, これらの群の位数は $|G_{\mathrm{I}}| = 16, |G_{\mathrm{II}}| = 192, |G_{\mathrm{III}}| = 48, |G_{\mathrm{IV}}| = 12$ となる. $W_C(x,y)$ は G_{X} によって不変な多項式全体

$$\mathbb{C}[x,y]^{G_{\mathrm{X}}} = \{f(x,y) \in \mathbb{C}[x,y] \mid A \circ f(x,y) = f(x,y)\ (\forall A \in G_{\mathrm{X}})\}$$

に含まれる. さらに, Gleason の定理として知られている次の結果が成り立つ (ただし, Type IV の場合は MacWilliams–Mallows–Sloane [22] によって示されている).

Theorem 4 ([13], [22])**.** C を Type X code とする. このとき

$$W_C(x,y) \in \mathbb{C}[x,y]^{G_{\mathrm{X}}} = \mathbb{C}[f_{\mathrm{X}}, g_{\mathrm{X}}]$$

が成り立つ, ただし

X	f_{X}	g_{X}
I	x^2+y^2	$x^8+14x^4y^4+y^8$
II	$x^8+14x^4y^4+y^8$	$x^4y^4(x^4-y^4)^4$
III	x^4+8xy^3	$y^3(x^3-y^3)^3$
IV	x^2+3y^2	$y^2(x^2-y^2)^2$

である.

Gleason の定理より直ちに次が得られる:

Corollary 5. 長さ n の Type X code が存在すれば, n は次数 $\deg(f_{\mathrm{X}})$ で割り切れる.

さらに minimum weight に関する上限を得ることが出来る. 証明については Type I, II, III の場合は Mallows–Sloane [26] を, Type IV の場合は MacWilliams–Odlyzko–Sloane–Ward [23] を見ていただきたい.

Theorem 6 ([23], [26])**.** C を長さ n の Type X code とすると

$$d(C) \le \Delta\left\lfloor \frac{n}{\deg(g_{\mathrm{X}})} \right\rfloor + \Delta$$

が成り立つ, ただし $\lfloor\ \rfloor$ はガウス記号を表す.

C を長さ n の Type X code とする. $d(C) = \Delta\lfloor \frac{n}{\deg(g_{\mathrm{X}})} \rfloor + \Delta$ であるときに *extremal* とよぶ. 次の節では extremal Type X code の存在についての結果を紹介する.

3 Extremal Type I, II, III, IV code の存在

この節で扱う extremal Type X code (X は I, II, III または IV) の存在結果および次の節で扱う Type X code の分類結果については, 2005 年の Huffman [21] の概説が詳しい. この原稿では, [21] の出版後の進展についても述べたい.

- 長さ n の extremal Type I self-dual code が存在する必要十分条件は

$$n = 2, 4, 6, 8, 12, 14, 22, 24$$

で, さらに全ての非同値な extremal Type I self-dual code が Ward [34] により決定されている.

さらに self-dual にならない場合も含めて, 長さ n の extremal Type I code が存在する必要十分条件は

$$n = 2, 4, 6, 8, 10, 12, 14, 18, 20, 22, 24, 28, 30$$

であることが知られている. self-dual でない場合の extremal Type I code の分類も進められていて, 今年になって最後に未解決だった長さ 30 の場合の分類が終わったので ([5] を参照), extremal Type I code の分類は完成したことになる.

- extremal Type II code の場合は, 次の長さ n において存在することが分かっている:

$$n = 8, 16, \ldots, 64, 80, 88, 104, 112, 136.$$

$n = 112$ 以外での存在については [10, p. 194] または [32, p. 213] を参照していただきたい. $n = 112$ の存在は最近まで分かっていなかったが, 著者 [14] によって構成された. 次の長さでは存在しないことが分かっている ([32, Theorem 29] を参照):

$$n = 24k \ (k \geq 154), 24k + 8 \ (k \geq 159), 24k + 16 \ (k \geq 164).$$

それ以外の長さでは存在するかどうか分かっていない. 長さ $n \leq 64$ については存在が古くから分かっていたこともあり, 1973 年には Sloane [33] は長さ 72 での存在について気にしており, その存在性を決めることを提案している.

Problem A (Sloane [33])**.** 長さ 72 の extremal Type II code は存在するか？

- extremal Type III code の場合は, 長さ $n = 4, 8, \ldots, 60, 64$ において存在することが分かっている ([21, Table 6] を参照). また, $n = 24k \ (k \geq 3)$, $12k \ (k \geq 70), 12k + 4 \ (k \geq 75), 12k + 8 \ (k \geq 78)$ では存在しないことが分かっている ([32, Theorem 29] を参照). 存在の分かっていない最小の長さは 68 である. 長さ 64 までは必ず存在し, 長さ 72 では存在しないことが分かっているので, 長さ 68 での extremal Type III code が存在するかどうかは判断が難しいところである. 過去に著者自身も構成を試みたことがあるが, 見付けることは出来なかった.

Problem B. 長さ 68 の extremal Type III code は存在するか？

- extremal Type IV code の場合は, 長さ $n = 2, \ldots, 10, 14, \ldots, 22, 28, 30$ において存在することが分かっていて, $n = 12, 24, 26, 6k \ (k \geq 17), 6k+2 \ (k \geq 20), 6k+4 \ (k \geq 22)$ では存在しないことが分かっている ([21, Table 7], [32, Theorem 29] を参照). 存在の分かっていない最小の長さは 32 である. Type IV code は Type I, II, III code に比べてあまり調べられていないと思われるので, 新たな長さで extremal Type IV code の存在が分かるはずである.

4 Type I, II, III, IV code の分類について

この節では Type X code (ここで X は I, II, III または IV) の分類についての結果を紹介する. なお, この節では extremal に限らない code も対象とすることに注意する.

Type II, Type III, Type IV code と Type I self-dual code に対しては, mass formula とよばれる分類結果を確認する等式が知られており, 分類を行なう際に非常に役立つ. 以下, この節では Type I code は self-dual code のみを考えることにし, 混乱がない場合はそのことを明記しない. まず $T_{\mathrm{X}}(n)$ を長さ n の Type X code の (集合として) 異なる個数とすると, 次が成り立つ ([32, Section 2] を参照):

$$T_{\mathrm{X}}(n) = \begin{cases} \prod_{i=1}^{n/2-1}(2^i+1) & \text{Type I self-dual の場合,} \\ 2\prod_{i=1}^{n/2-2}(2^i+1) & \text{Type II の場合,} \\ 2\prod_{i=1}^{n/2-1}(3^i+1) & \text{Type III の場合,} \\ \prod_{i=0}^{n/2-1}(2^{2i+1}+1) & \text{Type IV の場合.} \end{cases}$$

長さ n の Type X code C に同値な Type X code の個数は $\frac{N_{\mathrm{X}}(n)}{|\operatorname{Aut}(C)|}$ で与えられる, ただし $N_{\mathrm{I}}(n) = n!$, $N_{\mathrm{II}}(n) = n!$, $N_{\mathrm{III}}(n) = 2^n n!$, $N_{\mathrm{IV}}(n) = 3^n n!$. したがって, $\mathcal{C}_{\mathrm{X}}(n)$ で長さ n の非同値な Type X code 全体を表すことにすると,

$$T_{\mathrm{X}}(n) = \sum_{C \in \mathcal{C}_n} \frac{N_{\mathrm{X}}(n)}{|\operatorname{Aut}(C)|} \tag{1}$$

が成り立ち, (1) を mass formula とよぶ.

表 1: Type II でない Type I self-dual code と Type II code の分類について

長さ n	$\#_{\mathrm{I}}(n)$	$\#_{\mathrm{II}}(n)$	文献	長さ n	$\#_{\mathrm{I}}(n)$	$\#_{\mathrm{II}}(n)$	文献
2	1	-	[29]	20	16	-	[29]
4	1	-	[29]	22	25	-	[30]
6	1	-	[29]	24	46	9	[30]
8	1	1	[29]	26	103	-	[8]
10	2	-	[29]	28	261	-	[8]
12	3	-	[29]	30	731	-	[8]
14	4	-	[29]	32	3210	85	[3], [8]
16	5	2	[29]	34	24147	-	[2]
18	9	-	[29]				

では, 現時点で知られている Type X code の分類結果を紹介する. まず, 長さ n の非同値な Type X code の個数を $\#_{\mathrm{X}}(n)$ で表す. ただし, $\#_{\mathrm{I}}(n)$ は Type II code でない Type I self-dual code のみを考えることにする. 表 1 に $\#_{\mathrm{I}}(n)$ と $\#_{\mathrm{II}}(n)$ の結果を, 表 2 と表 3 にそれぞれ $\#_{\mathrm{III}}(n)$ と $\#_{\mathrm{IV}}(n)$ の結果を, 分類を完成した文献とともに与える.

分類を行なう道筋を簡単に説明しよう. 出来るだけ多くの非同値な Type X code を構成し, $\frac{N_{\mathrm{X}}(n)}{|\operatorname{Aut}(C)|}$ の和が (1) の左辺の値に一致するかどうかを確認し, もし足りない場合は,

表 2: Type III code の分類について

長さ n	$\#_{\mathrm{III}}(n)$	文献	長さ n	$\#_{\mathrm{III}}(n)$	文献
4	1	[25]	16	7	[7]
8	1	[25]	20	24	[31]
12	3	[25]	24	338	[18]

表 3: Type IV code の分類について

長さ n	$\#_{\mathrm{IV}}(n)$	文献	長さ n	$\#_{\mathrm{IV}}(n)$	文献
2	1	[23]	12	10	[23]
4	1	[23]	14	21	[23]
6	2	[23]	16	55	[7]
8	3	[23]	18	245	[16]
10	5	[23]	20	3427	[19]

一致するまで新しい code を探せば良いことになる. 古くから, Conway, Pless, Sloane を中心に分類が行なわれ, 分類の際に code を構成する方法としては, 主に gluing とよばれる方法が採用されてきた. 最近完成した分類は, 効率良く code を構成する必要があり別の方法で分類に必要な code を構成し, 分類が完成されている. 例えば, 長さ 24 の Type III code の分類は Harada–Munemasa [18] によって最近行なわれたが, 用いられた方法を第 5.1 節で紹介する.

この節の最後に Type IV code についての注意とその分類の応用について述べたい. まず $\mathbb{F}_4 = \{0, 1, \omega, \omega^2\}$ とする, ただし $\omega^2 + \omega = 1$ とする. 別の内積 (Hermitian 内積とよばれる) を $x * y = \sum_{i=1}^{n} x_i y_i^2$ で定義し, この内積に関する dual code を $C^* = \{x \in \mathbb{F}_4^n \mid x * y = 0\ (\forall y \in C)\}$ とする. $C = C^*$ であるとき Hermitian self-dual, $C \subset C^*$ であるとき Hermitian self-orthogonal とよぶ. 実は, C が Type IV code であることと Hermitian self-dual code であることが同値である [23]. 次に Calderbank–Rains–Shor–Sloane [6] による $\mathbb{F}_4$-code と quantum code (量子符号) の関係についての重要な結果を紹介する. Hermitian self-orthogonal code C で $C^* \setminus C$ には weight $< d$ の元を含まないものが存在すれば C が quantum $[[n, n-2k, d]]$ code を与える, ただし, ここで k は C の部分空間としての次元を表す[2]. 任意の Hermitian self-orthogonal code はある Hermitian self-dual code に含まれるので, Hermitian self-dual code の分類が完成すれば, 理論上は同じ長さの Hermitian self-orthogonal code が全て分かったことになる (実際に分類が出来るかどうかは別). したがって, 良い quantum $[[n, k, d]]$ code の構成[3] への応用を目論むと Hermitian self-dual code の分類は役立つと思われる. 例えば, 現時点では quantum $[[20, 2, 7]]$ code

[2] この結果は C が部分空間でなくても加法部分群であれば成り立つことを注意しておく. 詳細は [6] を見ていただきたい.

[3] quantum code においても n と k を固定したときに d がどれだけ大きくなるかが基本的な問題とされる.

の存在は分かっていない[4]. [19] で行なわれた長さ 20 の Hermitian self-dual code の分類から 9 次元部分空間で上の条件を満たすものがあるかどうか, 調べてみる価値はありそうである.

5 Type II lattice と Type II $\mathbb{Z}_{2k}$-code

この節では, 今までとは話題を変えて, Type II lattice とそれに関係した Type II $\mathbb{Z}_{2k}$-code について考える.

5.1 Construction A, self-dual $\mathbb{Z}_{2k}$-code と k-frame

標準的な内積 (x, y) が定義されたユークリッド空間 $\mathbb{R}^n$ の部分集合 L が n 次元の lattice であるとは $\mathbb{R}^n$ の基底 $v_1, v_2, \ldots, v_n$ で $L = \{k_1v_1 + k_2v_2 + \cdots + k_nv_n \mid k_i \in \mathbb{Z}\}$ となるものが存在するときのことをいう. L の dual lattice $L^* = \{x \in \mathbb{R}^n \mid (x, y) \in \mathbb{Z}\ (\forall\ y \in L)\}$ と L が一致するとき L は unimodular とよばれ, L の全ての元 x に対して norm (x, x) が偶数になるとき L は even とよばれる. L の minimum norm は $\min(L) = \min\{(x, x) \mid \mathbf{0} \neq x \in L\}$ で定義される. even unimodular lattice のことを Type II lattice とよぶ. 2 つの unimodular lattice L, L' に対して $L = L'A$ となる n 次直交行列 A が存在するときに同型とよび, $L \cong L'$ と表す. $L = LA$ である直交行列 A の集合を L の自己同型群 $\mathrm{Aut}(L)$ とよぶ.

n 次元の Type II lattice L が存在するとき $n \equiv 0 \pmod 8$ であり, さらに

$$\min(L) \leq 2\left\lfloor \frac{n}{24} \right\rfloor + 2 \tag{2}$$

が成り立つことが知られている (例えば [10, Chap. 7] を参照). $\min(L) = 2\lfloor n/24 \rfloor + 2$ を満たす n 次元の Type II lattice L を extremal とよぶ.

次に Construction A として知られている self-dual $\mathbb{Z}_k$-code から unimodular lattice を構成する方法を述べる. C を長さ n の self-dual $\mathbb{Z}_k$-code とする. このとき

$$A_k(C) = \frac{1}{\sqrt{k}}\{x \in \mathbb{Z}^n \mid x \bmod k \in C\}\ (\subset \mathbb{R}^n)$$

は n 次元の unimodular lattice になることが, C が self-dual であることより分かる. n 次元の unimodular lattice L の部分集合 $\{f_1, f_2, \ldots, f_n\}$ が $(f_i, f_j) = k\delta_{ij}$ を満たすとき k-frame とよぶ, ここで δ_{ij} はクロネッカーのデルタを表す. 明らかに $A_k(C)$ は標準的な k-frame $\{\sqrt{k}e_1, \sqrt{k}e_2, \ldots, \sqrt{k}e_n\}$ を含む, ただし $e_i = (\delta_{i1}, \delta_{i2}, \ldots, \delta_{in})$ $(i = 1, 2, \ldots, n)$. さらに n 次元の unimodular lattice L が k-frame $\{f_1, f_2, \ldots, f_n\}$ を含むとき, f_i を第 i 行とする n 次正方行列を F とすると $L \cdot (\frac{1}{\sqrt{k}}F^T)$ は標準的な k-frame をもつ. この標準的な k-frame から self-dual $\mathbb{Z}_k$-code C が得られる, つまり $A_k(C) = L \cdot (\frac{1}{\sqrt{k}}F^T)$ となる.

[4]講演では quantum $[[18, 4, 6]]$ code の存在性についても触れた. その後, 東北大の宗政昭弘氏との計算により長さ 18 の Hermitian self-dual code の分類を用いて 7 次元の Hermitian self-orthogonal code からは quantum $[[18, 4, 6]]$ code は得られないことが分かった.

したがって, L が k-frame を含むことと $A_k(C) \cong L$ となる self-dual $\mathbb{Z}_k$-code C が存在することが同値であることが分かる.

さらに self-dual $\mathbb{Z}_k$-code の分類を unimodular lattice の k-frame の分類に帰着させたのが Harada–Munemasa–Venkov [20] である. $\{f_1, f_2, \dots, f_n\}$, $\{g_1, g_2, \dots, g_n\}$ を unimodular lattice L の k-frame とし, 上のようにしてこれらの k-frame から得られる self-dual $\mathbb{Z}_k$-code を C, D とする. C と D が同値であることと

$$\{\pm f_1, \pm f_2, \dots, \pm f_n\} = \{\pm g_1, \pm g_2, \dots, \pm g_n\} \cdot P$$

となる $P \in \mathrm{Aut}(L)$ が存在することが同値であることを示した. これを用いることで L の k-frame 全体の $\mathrm{Aut}(L)$-軌道分解を与えることが $A_k(C) \cong L$ となる self-dual $\mathbb{Z}_k$-code C の分類を導くことが分かる. 実際に [20] では既に分類されていた全ての非同型な 28 次元の minimum norm 3 の unimodular lattice の 3-frame を分類することで長さ 28 の extremal Type III code は同値を除いて 6931 個存在することが示された. また, 同様に 24 次元の全ての非同型な unimodular lattice の 3-frame を分類することで長さ 24 の Type III code の分類を行なうことが出来た (表 2 を参照).

5.2 Extremal Type II $\mathbb{Z}_{2k}$-code

C を長さ n の self-dual $\mathbb{Z}_{2k}$-code とする. $x \in \mathbb{Z}_{2k}^n$ に対して成分が $\pm j$ である成分の個数を $n_j(x)$ で表すとき x の Euclidean weight $\mathrm{wt}_E(x)$ を $n_1(x) + 2^2 n_2(x) + \cdots + k^2 n_k(x)$ で定義する. C の minimum Euclidean weight を $d_E(C) = \min\{\mathrm{wt}_E(x) \mid \mathbf{0} \neq x \in C\}$ とする. 次に, 既に定義されている Type II code の一般化として Type II $\mathbb{Z}_{2k}$-code を定義しよう. self-dual $\mathbb{Z}_{2k}$-code の全ての元 x が $\mathrm{wt}_E(x) \equiv 0 \pmod{4k}$ を満たすとき Type II とよぶ. $k = 2$ のときは Bonnecaze–Solé–Bachoc–Mourrain [4][5] で, 一般の k に対しては Bannai–Dougherty–Harada–Oura [1] で定義された. $k = 1$ のときは既に定義している Type II code と一致することに注意しておく. また Euclidean weight の定義から C が Type II $\mathbb{Z}_{2k}$-code であれば $A_{2k}(C)$ は Type II lattice になることが分かる. これらが Type II という名前が付いた理由である. Type II lattice の存在条件から, 長さ n の Type II $\mathbb{Z}_{2k}$-code が存在すれば $n \equiv 0 \pmod 8$ であることが分かる. また $\min(A_{2k}(C)) = \min\{d_E(C)/2k, 2k\}$ が成り立つ (詳細は [1] を参照).

Proposition 7. C を長さ n の Type II $\mathbb{Z}_{2k}$-code とする. $k \leq 6$ であれば

$$d_E(C) \leq 4k \left\lfloor \frac{n}{24} \right\rfloor + 4k \tag{3}$$

が成り立つ.

$k = 1$ の場合は既に Theorem 6 で述べられている結果であり, $k = 2$ の場合は [4] で示されている. $k = 3, 4, 5, 6$ の場合は, 最近 Harada–Miezaki [17] で示された. $k = 2, 3, \dots, 6$ の場合の証明は, 本質的に (2) に依存しており, 一般の k に対しても同じ上限が成り立つと著者は思っている.

[5] 成分が ± 1 であるベクトルを含むことが定義に含まれていたが, この条件は自然に導かれることがその後分かった.

Problem C. $k \geq 7$ でも (3) が成り立つことを示せ.

$k = 1$ の場合と同じように, $d_E(C) = 4k\lfloor \frac{n}{24} \rfloor + 4k$ を満たす長さ n の Type II $\mathbb{Z}_{2k}$-code C を extremal とよぶことにしよう ($k \leq 6$). なお, $k \leq 6$ で $m \leq 8$ であれば長さ $8m$ の extremal Type II $\mathbb{Z}_{2k}$-code が存在することが分かっている [17]. したがって Problem A を含む形で, 新たな問題が与えられる.

Problem D. $k \leq 6$ で長さ 72 の extremal Type II $\mathbb{Z}_{2k}$-code が存在するか？

$k \leq 6$ かつ $n \leq 24k - 8$ と仮定. このとき C を長さ n の extremal Type II $\mathbb{Z}_{2k}$-code とすると $\min(A_{2k}(C)) = \min\{d_E(C)/2k, 2k\} = 2\lfloor \frac{n}{24} \rfloor + 2$ であることから $A_{2k}(C)$ は n 次元の extremal Type II lattice になる. 特に, $k = 4, 5, 6$ のときは長さ 72 の extremal Type II $\mathbb{Z}_{2k}$-code が存在すれば, 72 次元の extremal Type II lattice が構成されることになる[6].

6 Moonshine VOA に関係した code

講演の最後に, 最近の Harada–Lam–Munemasa [15] による moonshine VOA $V^\natural$ と関係した (self-dual) code についての結果を紹介した. moonshine VOA $V^\natural$ は Frenkel–Lepowsky–Meurman [12] によって構成され, その自己同型群はモンスター単純群となることが分かっている興味ある VOA である. ここでは, これまでに述べた結果との関連を強調して [15] の結果の 1 部を簡単に紹介したい.

$V^\natural$ の Virasoro frame に関係した moonshine code の定義を与える. なお, 未定義な用語や記号などと基本的な結果については Dong–Griess–Höhn [11] と Miyamoto [27] (または [15]) を見ていただくことにする. T ($\subset V^\natural$) を $V^\natural$ の Virasoro frame とする. このとき T-加群として

$$V^\natural \cong \bigoplus_{h_i \in \{0, \frac{1}{2}, \frac{1}{16}\}} m_{h_1,\ldots,h_{48}} \bigotimes_{i=1}^{48} L\Big(\frac{1}{2}, h_i\Big)$$

と分解される. $\alpha = (\alpha_1, \ldots, \alpha_{48}) \in \mathbb{F}_2^{48}$ に対して V^α で $h_i = \frac{1}{16}$ となるのが $\alpha_i = 1$ に限られる T-部分加群 $\bigotimes_{i=1}^{48} L(\frac{1}{2}, h_i)$ の和を表すことにする. このとき $D = \{\alpha \in \mathbb{F}_2^{48} \mid V^\alpha \neq 0\}$ は長さ 48 の binary code つまり $\mathbb{F}_2$-code になり $V^\natural = \bigoplus_{\alpha \in D} V^\alpha$ となることが分かっている. この D を T に関する *moonshine code* とよぶ. $V^\natural$ を理解するために Virasoro frame にどのようなものがあるかが分かることが役立つと思われ, また, Virasoro frame の分類に moonshine code の分類が役立つと思われる. 実際, [11] と [27] では $V^\natural$ を構成するために 7 次元の moonshine code が与えられている.

長さ n の Type II $\mathbb{Z}_4$-code C の residue code C_0 を $\{x \bmod 2 \mid x \in C\}$ ($\subset \{0,1\}^n$) と定義し binary code とみなす. C_0 は $\mathbf{1} = (1, 1, \ldots, 1)$ を含み, かつ doubly even code となる, つまり全ての $x \in C_0$ に対して $\mathrm{wt}(x) \equiv 0 \pmod 4$ が成り立つ [9]. binary doubly

[6]講演では, 72 次元の extremal Type II lattice の存在は分かっていないと紹介したが, 講演後の 8 月 18 日に G. Nebe が構成することに成功したという非常に衝撃的なニュースを本人から受け取った (preprint は [28]). この lattice は 8-frame を含むことが分かるので, 長さ 72 の extremal Type II $\mathbb{Z}_8$-code の存在を導く.

even code C_0 は self-orthogonal, つまり $C_0 \subset C_0^{\perp}$ となることに注意. したがって, その次元は $\dim(C_0) \leq n/2$ となる. また, $d(C_0^{\perp}) \geq d_E(C)/4$ が成り立つ.

B を長さ 24 の binary doubly even code とする. B を residue code とする長さ 24 の extremal Type II $\mathbb{Z}_4$-code が存在するときに B を *realizable* とよぶ (extremal の定義は第 5.2 節を参照). $\mathrm{dou}(B) = \{(x_1, x_1, \ldots, x_{24}, x_{24}) \in \mathbb{F}_2^{48} \mid (x_1, \ldots, x_{24}) \in B\}$ としたとき B の *doubling* $D(B)$ を $\langle \mathrm{dou}(B), (1,0,1,0,\ldots,1,0)\rangle$ と定義する. このとき, [15] では次を示すことが出来た.

Theorem 8. $D(B)$ が moonshine code になる必要十分条件は B が realizable となることである.

実際に realizable code B の分類結果を与えよう. 今までの議論より realizable code B は次の条件を満たすことが分かる:

$$\text{doubly even code, } \mathbf{1} \in B, \ d(B^{\perp}) \geq 4. \tag{4}$$

長さ 24 で minimum weight 4 以上の binary code が存在する場合, その次元 k は $k \leq 18$ となることが知られているので, $6 \leq \dim(B) \leq 12$ となることに注意しておく. k 次元の binary doubly even code は必ずある $k+1$ 次元の binary doubly even code に含まれることが知られている ($k \leq 11$). 表 1 で紹介した通り, 長さ 24 の Type II code, つまり, binary doubly even self-dual code は同値を除いて 9 個存在することが知られている. 9 個それぞれの 11 次元の部分空間を考えることで, 条件 (4) を満たす 11 次元の binary doubly even code の分類が出来る. 以下, 同様に次元を下げていけば, 条件 (4) を満たす binary doubly even code の分類を得る. 表 4 の 2 列目に条件 (4) を満たす k 次元の非同値な code の個数 $\#_k$ を与える. ここで Type II code の分類が役立ったことが分かって貰えると思う.

表 4: 条件 (4) を満たす長さ 24 の binary doubly even code

次元 k	$\#_k$	$\#^{\mathrm{r}}_{k,8}$	$\#^{\mathrm{r}}_{k,4}$	$\#^{\mathrm{n}}_{k,8}$	$\#^{\mathrm{n}}_{k,4}$
12	9	1	8	0	0
11	21	1	20	0	0
10	49	3	44	0	2
9	60	6	40	4	10
8	32	4	16	8	4
7	7	3	2	2	0
6	1	1	0	0	0

次に, 条件 (4) を満たす各 binary doubly even code B が realizable であるか, つまり B を residue code とする extremal Type II $\mathbb{Z}_4$-code が存在するかどうかを決めた. $\#^{\mathrm{r}}_{k,d}$ が各次元 k での minimum weight d の非同値な realizable code の個数を, $\#^{\mathrm{n}}_{k,d}$ が各次元での minimum weight d の非同値な realizable でない code の個数を表す ($d = 4, 8$). Theorem 8 により doubling code が moonshine code となるものの分類が完成したことになる. 今回, doubling code が moonshine code となるものが binary doubly even code や

extremal Type II $\mathbb{Z}_4$-code と関連することが分かり, self-dual code の専門家として, 非常に興味ある結果に辿り着いたことを嬉しく思う.

参考文献

[1] E. Bannai, S.T. Dougherty, M. Harada and M. Oura, Type II codes, even unimodular lattices, and invariant rings, *IEEE Trans. Inform. Theory* **45** (1999), 1194–1205.

[2] R.T. Bilous, Enumeration of the binary self-dual codes of length 34, *J. Combin. Math. Combin. Comput.* **59** (2006), 173–211.

[3] R.T. Bilous and G.H.J. van Rees, An enumeration of binary self-dual codes of length 32, *Des. Codes Cryptogr.* **26** (2002), 61–86.

[4] A. Bonnecaze, P. Solé, C. Bachoc and B. Mourrain, Type II codes over $\mathbb{Z}_4$, *IEEE Trans. Inform. Theory* **43** (1997), 969–976.

[5] S. Bouyuklieva and I. Bouyukliev, Classification of the extremal formally self-dual even codes of length 30, *Advances Math. Communications* **4** (2010), 433–439.

[6] A.R. Calderbank, E.M. Rains, P.W. Shor and N.J.A. Sloane, Quantum error correction via codes over GF(4), *IEEE Trans. Inform. Theory* **44** (1998), 1369–1387.

[7] J.H. Conway, V. Pless and N.J.A. Sloane, Self-dual codes over $GF(3)$ and $GF(4)$ of length not exceeding 16, *IEEE Trans. Inform. Theory* **25** (1979), 312–322.

[8] J.H. Conway, V. Pless and N.J.A. Sloane, The binary self-dual codes of length up to 32: a revised enumeration, *J. Combin. Theory Ser. A* **60** (1992), 183–195.

[9] J.H. Conway and N.J.A. Sloane, Self-dual codes over the integers modulo 4, *J. Combin. Theory Ser. A* **62** (1993), 30–45.

[10] J.H. Conway and N.J.A. Sloane, *Sphere Packing, Lattices and Groups (3rd ed.)*, Springer-Verlag, New York, 1999.

[11] C. Dong, R.L. Griess, Jr. and G. Höhn, Framed vertex operator algebras, codes and the moonshine module, *Commun. Math. Phys.* **193** (1998), 407–448.

[12] I.B. Frenkel, J. Lepowsky and A. Meurman, *Vertex Operator Algebras and the Monster*, Academic Press, New York, 1988.

[13] A.M. Gleason, Weight polynomials of self-dual codes and the MacWilliams identities, *Act. Congr. Int. Math.*, Vol. 3, pp. 211–215, Gauthier-Villars, Paris, 1971.

[14] M. Harada, An extremal doubly even self-dual code of length 112, *Electron. J. Combin.* **15** (2008), Note 33, 5 pp.

[15] M. Harada, C.H. Lam and A. Munemasa, On the structure codes of the moonshine vertex operator algebra, (submitted), ArXiv:math.QA/1005.1144.

[16] M. Harada, C. Lam, A. Munemasa and V.D. Tonchev, Classification of generalized Hadamard matrices $H(6,3)$ and quaternary Hermitian self-dual codes of length 18, (submitted), ArXiv:math.CO/1007.2555.

[17] M. Harada and T. Miezaki, An upper bound on the minimum weight of Type II $\mathbb{Z}_{2k}$-codes, *J. Combin. Theory Ser. A*, (to appear).

[18] M. Harada and A. Munemasa, A complete classification of ternary self-dual codes of length 24, *J. Combin. Theory Ser. A* **116** (2009), 1063–1072.

[19] M. Harada and A. Munemasa, Classification of quaternary Hermitian self-dual codes of length 20, (submitted).

[20] M. Harada, A. Munemasa and B. Venkov, Classification of ternary extremal self-dual codes of length 28, *Math. Comput.* **78** (2009), 1787–1796.

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

[22] F.J. MacWilliams, C.L. Mallows and N.J.A. Sloane, Generalizations of Gleason's theorem on weight enumerators of self-dual codes, *IEEE Trans. Inform. Theory* **18** (1972), 794–805.

[23] F.J. MacWilliams, A.M. Odlyzko, N.J.A. Sloane and H.N. Ward, Self-dual codes over $GF(4)$, *J. Combin. Theory Ser. A* **25** (1978), 288–318.

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

[25] C.L. Mallows, V. Pless and N.J.A. Sloane, Self-dual codes over GF(3), *SIAM J. Appl. Math.* **31** (1976), 649–666.

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

[27] M. Miyamoto, A new construction of the moonshine vertex operator algebra over the real number field, *Ann. of Math.* **159** (2004), 535–596.

[28] G. Nebe, An even unimodular 72-dimensional lattice of minimum 8, (preprint).

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

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

[31] V. Pless, N.J.A. Sloane and H.N. Ward, Ternary codes of minimum weight 6 and the classification of length 20, *IEEE Trans. Inform. Theory* **26** (1980), 305–316.

[32] E.M. Rains and N.J.A. Sloane, Self-dual codes, in *Handbook of Coding Theory*, V.S. Pless and W.C. Huffman, eds., Elsevier, Amsterdam, (1998), 177–294.

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

[34] H.N. Ward, A restriction on the weight enumerator of a self-dual code, *J. Combin. Theory Ser. A* **21** (1976), 253–255.