「双対符号に対する Assmus-Mattson 定理の拡張」

Strengthening of the Assmus-Mattson theorem for some dual codes

神戸学院大学　中空　大幸
Hiroyuki Nakasora
Kobe Gakuin University

1　序文

X を v 個の点集合とし，$\mathcal{B}$ は X の k 点の部分集合の族 (ブロックの集合) で，性質として任意の t 個の点は丁度 λ 個のブロックに含まれるとする。このとき，$(X, \mathcal{B})$ を t-(v, k, λ)design と呼ぶ。次に，C を $\mathbb{F}_q$ 上の $[n, k, d]$ code とする。$c = (c_1, c_2, \ldots, c_n) \in C$, $(c_i \in \mathbb{F}_q)$ に対して，$supp(c) = \{i : c_i \neq 0\}$ を c の support と呼ぶ。$X = \{1, 2, \ldots, n\}$，$\mathcal{B}$ を weight w のコードワード全体の support とする。すると，結合構造 $D_w = (X, \mathcal{B})$ を C の weight w に対する support design という。この support design について次の Assmus-Mattson の定理[1] [1] が重要である。

Theorem 1.1 (Assmus–Mattson [1])**.** *Let C be an $[n, k, d]$ linear code over $\mathbb{F}_q$ and $C^\perp$ be the dual $[n, n-k, d^\perp]$ code. Let t be an integer less than d. Let v_0 be the largest integer satisfying $v_0 - \lfloor \frac{v_0+q-2}{q-1} \rfloor < d$, and w_0 be the largest integer satisfying $w_0 - \lfloor \frac{w_0+q-2}{q-1} \rfloor < d^\perp$, where, if $q = 2$, we take $v_0 = w_0 = n$. Let $C^\perp$ have at most $d - t$ non-zero weights less than or equal to $n - t$. Then, for each weight v with $d \leq v \leq v_0$, the support design in C is a t-design, and for each weight w with $d^\perp \leq w \leq \min\{n - t, w_0\}$, the support design in $C^\perp$ is a t-design.*

ある linear code C の support design D_w が Assmus-Mattson の定理によって t-design $(t > 0)$ となるならば，その符号を applicable to the Assmus–Mattson theorem と呼ぶ。

ここで，D_w について次のような定義を与える。

$$\delta(C) := \max\{t \in \mathbb{N} \mid \forall w, D_w \text{ is a } t\text{-design}\}$$
$$s(C) := \max\{t \in \mathbb{N} \mid \exists w, \text{ s.t. } D_w \text{ is a } t\text{-design}\}$$

この定義から明らかに $\delta(C) \geq t$ と $\delta(C) \leq s(C)$ である。2016 年の我々の論文 [8] において次のような問題を提起した。

Problem 1.2. $s(C)$ の上限を求めよ。

Problem 1.3. $\delta(C) < s(C)$ となる場合はどこで起こり得るか？

Problem 1.2 について，$t \geq 6$ の t-design の実例は現在知られていない。Problem 1.2 は，重要な符号のクラスである extremal Type II code について調べる過程で発生した。

[1] 松尾厚先生のご指摘通り，講演では $\exists t \in \mathbb{N}$ と t を固定して定理の説明をしましたが正しくないです。本稿はオリジナルに近い形で書きました。また，t を固定した形で書かれている文献も幾つかあります。

2 Extremal Type II codeのサポートデザイン

2.1 $\delta(C)$ と $s(C)$ について

長さ n の extremal Type II code を C とする。ここで C の minimum weight は $d(C) = 4[n/24]+4$ である。また，Zhang [13] より (i) $n = 24m$ の場合 $m \geq 154$, (ii) $n = 24m+8$ の場合 $m \geq 159$, (iii) $n = 24m+16$ の場合 $m \geq 164$ で非存在が知られている。

このコードの系列からは Assmus-Mattson の定理によって (i) n=$24m$ の場合 5-design, (ii) $n = 24m+8$ の場合 3-design, (iii) $n = 24m+16$ の場合 1-design が得られる。

$\delta(C)$ と $s(C)$ の値の可能性について N. Horiguchi, T. Miezaki and H. Nakasora [6] と T. Miezaki and H. Nakasora [8] から次の結果を得ている。

Theorem 2.1. *Let C be an extremal Type II code of length n.*

(1) *If $n = 24m$, then $\delta(C) = s(C) = 5$ or $\delta(C) = s(C) = 7$.*

(2) *If $n = 24m+8$, then $\delta(C) = s(C) = 3$ or $5 \leq \delta(C) \leq s(C) \leq 7$.*

(3) *If $n = 24m+16$, then $\delta(C) = s(C) = 1$ or $3 \leq \delta(C) \leq s(C) \leq 5$.*

Problem 1.2 について，extremal Type II code において $s(C) \leq 7$ である。Problem 1.3 について，Theorem 2.1(1) の n が 24 の倍数のときは $\delta(C) < s(C)$ となる場合が起きないことが分かる。次の命題で $\delta(C) < s(C)$ が起きる可能性がある場合について述べる。

Proposition 2.2. *If the case $\delta(C) < s(C)$ occurs, then one of the following holds:*

(1) *$n = 24m+8$, $m = 58$, $\delta(C) = 6$ and $s(C) = 7$ with $w = n/2$;*

(2) *$n = 24m+16$, $m \in \{10, 23, 79, 93, 118, 120, 123, 125, 142\}$, $\delta(C) = 4$ and $s(C) = 5$ with $w = n/2$.*

Extremal Type II code において，$\delta(C) < s(C)$ となる実例は知られていなく未解決問題である。

2.2 Extremal Type II lattice と spherical t-design

$\delta(C) < s(C)$ の場合の重要性は,「符号とサポートデザインの関係」と「格子と spherical t-design の関係」との類似性によることが挙げられる。

Theorem 2.3 ([12])**.** *Let L be an extremal Type II lattice of rank n and $L_{2m} := \{x \in L : (x,x) = 2m\}$. If $L_{2m} \neq \phi$, then L_{2m} is a spherical*

$$\begin{cases} 11\text{-}design & (n \equiv 0 \pmod{24}), \\ 7\text{-}design & (n \equiv 8 \pmod{24}), \\ 3\text{-}design & (n \equiv 16 \pmod{24}). \end{cases}$$

例えば，$(E_8)_{2m}$ は spherical 7-design である。そして，次の Ramanujan τ 函数との関係がある。

Theorem 2.4 ([12]). *$(E_8)_{2m}$ is a spherical 8-design if and only if $\tau(m) = 0$, where*

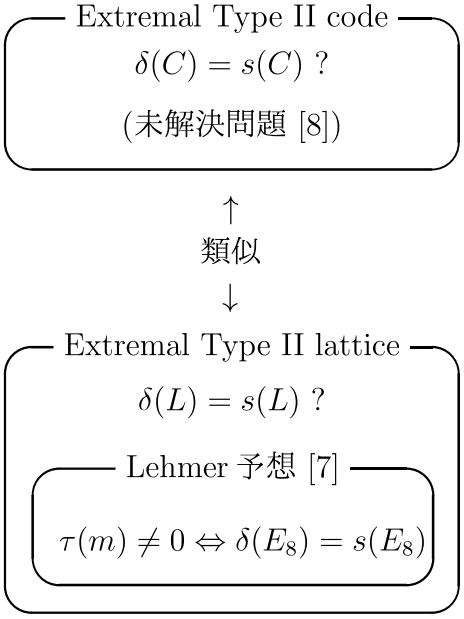
$$q\prod_{m=1}^{\infty}(1-q^m)^{24} = \sum_{m=0}^{\infty}\tau(m)q^m.$$

すると，有名な Lehmer 予想が関係している。

Conjecture 2.5 ([7]). For all m,

$$\tau(m) \neq 0.$$

「符号と support t-design の関係」と「格子と spherical t-design の関係」との類似性をまとめると右図の通りである



3 長さ 48 の triply even binary code のサポートデザイン

3.1 $\delta(C) < s(C)$ の例

我々は [9] で $\delta(C) < s(C)$ の例を長さ 48 の Triply even binary codes の中で見つけた。長さ 48 の triply even binary codes は Betsumiya and Munemasa [4] で分類がされている。すべてで 7647 個のコードのデータが別宮先生のウェブサイト [3] で与えられている。そこで用いられている記号 ⟨Dimension, Code Id, [Generators]⟩ を本稿では ⟨Dimension, [Code Id]⟩ で表す。

Proposition 3.1. *If a triply even binary code of length 48 C is applicable to the Assmus–Mattson theorem, then one of the following:*

(*A*) $\langle 7, [144]\rangle$, $\langle 8, [129, 130, 131, 132, 133]\rangle$,
$\langle 9, [59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 1109, 1712, 1714, 1716, 1960]\rangle$,
$\langle 10, [16, 17, 18, 19, 20, 21, 22, 549, 550, 554, 1001, 1245, 1246, 1247]\rangle$,
$\langle 11, [6, 7, 154, 520]\rangle$, $\langle 12, [3]\rangle$, $\langle 13, [1]\rangle$.

(*B*) $\langle 2, [1]\rangle, \langle 3, [4]\rangle, \langle 4, [7]\rangle, \langle 5, [12]\rangle$

$\delta(C) < s(C)$ の例は次の定理による結果である。

Theorem 3.2. *Let C be a triply even binary code length 48 in Proposition 3.1. Let D_w and $D_w^{\perp}$ be the support t-design of weight w of C and $C^{\perp}$.*

(1) *For all w, D_w and $D_w^{\perp}$ are 1-designs.*

(2) *If C is a code in Proposition 3.1 (A) except for $\langle 13, [1]\rangle$, $D_6^{\perp}$ (and also $D_{42}^{\perp}$) is a 2-design but is not a 3-design. For the other cases, D_w and $D_w^{\perp}$ are not 2-designs.*

41 個の $\delta(C) < s(C)$ の例の中でも，最も有名なコードを次に挙げる。

Example 3.3. Proposition 3.1 (A) の 1 つである $\langle 7, [144]\rangle$ の triply even code を C とする。その weight enumerator は

$$W_C(x,y) = x^{48} + 3x^{32}y^{16} + 120x^{24}y^{24} + 3x^{16}y^{32} + y^{48}$$

である。C の双対符号 $C^\perp$ は Miyamoto's moonshine code [11] と呼ばれる。

Proposition 3.1 と Theorem 3.2 から，すべての weight w に対して，D_w と $D_w^\perp$ は 1-design である。さらに，双対符号の weight 6 は特別で $D_6^\perp$ は 2-$(48, 6, 2520)$ design となっている。($D_{42}^\perp$ は 2-$(48, 6, 2520)$ design の complement である。)

Theorem 3.2 (2) で除いた 1 個のコードについて述べる。

Example 3.4. $\langle 13, [1]\rangle$ の triply even code は extended doubling $\mathcal{D}(\mathcal{G}_{24})$ である。また，$\mathrm{Aut}\,\mathcal{D}(\mathcal{G}_{24}) = 2^{12}.M_{24}$ である。$\mathcal{D}(\mathcal{G}_{24}) = C'$ とおく。その weight enumerator は

$$W_{C'}(x,y) = x^{48} + 759x^{32}y^{16} + 6672x^{24}y^{24} + 759x^{16}y^{32} + y^{48}$$

である。

MacWilliams 恒等式

$$W_{C'^\perp}(x,y) = 2^{-13}W_{C'}(x+y, x-y)$$

から双対符号の $C'^\perp$ のコードワードの個数を計算すると weight 6 のコードワードの個数が $A_6^\perp = 0$ である。よって，$D_6^\perp$ はブロックの集合が空集合である自明なデザインであることが分かる。双対符号の weight 6 を除いたすべての weight w に対して，Proposition 3.1 と Theorem 3.2 から，D_w と $D_w^\perp$ は 1-design である。

表 1 には Theorem 3.2 で得られる双対符号の weight 6 の support 2-deign についてまとめている[2]。

3.2 Theorem 3.2 の証明

Theorem 3.2 の証明について述べる。まず，準備として harmonic weight enumerator の定義から始める。

Definition 3.5. 長さ n の binary code を C，$f \in \mathrm{Harm}_k$ とする。C と f に関する harmonic weight enumerator は

$$W_{C,f}(x,y) = \sum_{\mathbf{c}\in C} \widetilde{f}(\mathbf{c}) x^{n-\mathrm{wt}(\mathbf{c})} y^{\mathrm{wt}(\mathbf{c})}$$

である。

次に harmonic weight enumerator と t-design の関係は次の Delsarte [5] による。

[2]田邊顕一朗先生から質問がありましたが，これら 41 個の 2-design はすべて非同型である。

表 1: weight 6 の support 2-deign について

次元	[Code Id] Weight distribution (i, A_i) for $A_i \neq 0$	2-(v, k, λ) 個数
7	[144] $(0,1),(16,3),(24,120),(32,3),(48,1)$	2-$(48,6,2520)$ 1
8	[129,130,131,132,133] $(0,1),(16,15),(24,224),(32,15),(48,1)$	2-$(48,6,1240)$ 5
9	[59,60,61,62,63,64,65,66,67,68,69,1109,1712,1714,1716,1960] $(0,1),(16,39),(24,432),(32,39),(48,1)$	2-$(48,6,600)$ 16
10	[16,17,18,19,20,21,22,549,550,554,1001,1245,1246,1247] $(0,1),(16,87),(24,848),(32,87),(48,1)$	2-$(48,6,280)$ 14
11	[6,7,154,520] $(0,1),(16,183),(24,1680),(32,183),(48,1)$	2-$(48,6,120)$ 4
12	[3] $(0,1),(16,375),(24,3344),(32,375),(48,1)$	2-$(48,6,40)$ 1
13	[1] $(0,1),(16,759),(24,6672),(32,759),(48,1)$	- 0

Theorem 3.6 ([5]). D_w が *t-design* になることと，任意の $f \in \mathrm{Harm}_k$, $1 \leq k \leq t$ に対して $\sum_{b \in D_w} \widehat{f}(b) = 0$ を満たすことは同値である。

Bachoc [2] は次のような MacWilliams 型の恒等式を示した。

Theorem 3.7 ([2]). $W_{C,f}(x,y)$ を *binary code* C と *degree* k の *harmonic function* f に関する *harmonic weight enumerator* とする。

$$W_{C,f}(x,y) = (xy)^k Z_{C,f}(x,y)$$

そこで，$Z_{C,f}$ は *degree* $n-2k$ の *homogeneous polynomial* である。すると，次を満たす。

$$Z_{C^\perp,f}(x,y) = (-1)^k \frac{2^{n/2}}{|C|} Z_{C,f}\left(\frac{x+y}{\sqrt{2}}, \frac{x-y}{\sqrt{2}}\right)$$

Proof. C を Proposition 3.1 (A) の triply even code とする。ただし $\langle 13, [1] \rangle$ を除く。すると，Assmus-Mattson の定理よりすべての weight w に対して，D_w と $D_w^\perp$ は 1-design である。この時 $D_6^\perp$ が 2-design になることを示す。

$W_{C,f}(x,y)$ を C と degree 2 の harmonic function f に関する harmonic weight enumerator とする。

$$\begin{aligned} W_{C,f}(x,y) &= \sum_{\mathbf{c} \in C} \widetilde{f}(c) x^{48-wt(c)} y^{wt(c)} \\ &= ax^{32}y^{16} + bx^{24}y^{24} + ax^{16}y^{32} \\ &= (xy)^2(ax^{30}y^{14} + bx^{22}y^{22} + ax^{14}y^{30}) \\ &= (xy)^2 Z_{C,f}(x,y) \end{aligned}$$

ここで，$a, b \neq 0$ である。

Theorem 3.7 より，つぎの等式をみたす係数 a', b' が存在する。

$$\begin{aligned} Z_{C^\perp,f}(x,y) &= (-1)^2 \frac{2^{24}}{|C|} Z_{C,f}\left(\frac{x+y}{\sqrt{2}}, \frac{x-y}{\sqrt{2}}\right) \\ &= a'(x+y)^{30}(x-y)^{14} + b'(x+y)^{22}(x-y)^{22} + a'(x+y)^{14}(x-y)^{30} \end{aligned}$$

$C^\perp$ は minimum weight 4 より，$Z_{C^\perp,f}$ の中の x^{44} の係数は 0 である。よって，$b' = -2a'$ を得る。ゆえに，

$$\begin{aligned} &W_{C^\perp,f}(x,y) \\ &= (xy)^2 \left(a'(x+y)^{30}(x-y)^{14} - 2a'(x+y)^{22}(x-y)^{22} + a'(x+y)^{14}(x-y)^{30}\right) \end{aligned}$$

すると，直接的な計算により $W_{C^\perp,f}$ の中の $x^{42}y^6$ の係数は 0 であることを得る。Theorem 3.6 より，$D_6^\perp$ は 2-design である。

□

4 Theorem 3.2 の一般化

長さ 48 の Triply even binary codes の中で起きた現象である $\delta(C) < s(C)$ の例を一般化した結果 [10] を述べる。

C を binary $[n,k,d]$ code として $\mathbf{1}_n \in C$ とする。C の双対符号 $C^\perp$ のパラメータは $[n, n-k, d^\perp]$ である。すると，$d^\perp$ は偶数であることに注意しておく。Assmus–Mattson の定理 (Theorem 1.1) の条件から，次の等式をみたす $d^\perp$ と t について考える。

$$d^\perp - t = \sharp\{u \mid C_u \neq \emptyset, 0 < u \leq n-t\}. \tag{4.1}$$

ここで，$C_u := \{c \in C \mid \mathrm{wt}(c) = u\}$ である。

D_u と $D_w^\perp$ をそれぞれ C の weight u と $C^\perp$ の weight w の support design とする。すると，Assmus–Mattson の定理より，D_u と $D_w^\perp$ は t-design である。そのようにして，符号 C は applicable to the Assmus–Mattson theorem である。

まず，$d^\perp$ と t について次のような制限が得られた。

Theorem 4.1. (1) *If C is applicable to the Assmus–Mattson theorem with $d^\perp - t = 1$, then $(d^\perp, t) = (2,1)$ or $(4,3)$.*

Moreover, we have $\delta(C) = s(C) = \delta(C^\perp) = s(C^\perp) = 1$ or 3.

(2) *If C is applicable to the Assmus–Mattson theorem with $d^\perp - t = 3$, then $(d^\perp, t) = (4,1), (6,3)$, or $(8,5)$.*

この Theorem 4.1 から，$d^\perp - t = 1$ のとき，$\delta(C) < s(C)$ と $\delta(C^\perp) < s(C^\perp)$ の場合は起きないことが分かる。$d^\perp - t = 3$ のとき，$\delta(C^\perp) < s(C^\perp)$ の場合が起きる n と d の基準を次の定理で与える。

Theorem 4.2. *Let C be applicable to the Assmus–Mattson theorem with $(d^\perp, t) = (4, 1)$ or $(6, 3)$. If the equation*

$$\left(\sum_{i=0}^{w}(-1)^{w-i}\binom{d-(t+1)}{w-i}\binom{n-2d}{2i}\right)+(-1)^{w+1}\binom{n/2-(t+1)}{w}=0$$

is satisfied, then $D^\perp_{2w+t+1}$ is a $(t+1)$-design.

この Theorem 4.2 は特定の場合に対して Assmus–Mattson の定理の強化版を与えている。[10] の Appendix B に，$(d^\perp, t) = (4, 1)$ のとき，$n \leq 10000$ に対して，この Theorem 4.2 をみたす具体的な n, d と weight w の表を載せている。$(d^\perp, t) = (6, 3)$ のときは $n \leq 10000$ に対して，Theorem 4.2 をみたす n と d は存在しないことを注意しておく。

$(d^\perp, t) = (8, 5)$ のとき，$\delta(C^\perp) < s(C^\perp)$ の場合が起こる可能性はない。事実として次の定理が得られる。

Theorem 4.3. *Let C be applicable to the Assmus–Mattson theorem with $(d^\perp, t) = (8, 5)$. Then C is the extended Golay code $\mathcal{G}_{24}$.*

$\delta(C^\perp) < s(C^\perp)$ の場合が起きる可能性を探索する一連の流れで，extended Golay code $\mathcal{G}_{24}$ の新しい特徴付けを与えられることは興味深い。

参考文献

[1] E. F. Assmus, Jr. and H. F. Mattson, Jr., New 5-designs, *J. Combin. Theory Ser. A* **6** (1969), 122-151.

[2] C. Bachoc, On harmonic weight enumerators of binary codes, *Des. Codes Cryptogr.* **18** (1999), no. 1-3, 11-28.

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

[4] K. Betsumiya and A. Munemasa, On triply even binary codes, *J. Lond. Math. Soc.* **86 (1)** (2012), 1-16.

[5] P. Delsarte, Hahn polynomials, discrete harmonics, and t-designs, *SIAM J. Appl. Math.* **34** (1978), no. 1, 157-166.

[6] N. Horiguchi, T. Miezaki and H. Nakasora, On the support designs of extremal binary doubly even self-dual codes, *Des. Codes Cryptogr.*, **72** (2014), 529-537.

[7] D. H. Lehmer, The vanishing of Ramanujan's $\tau(n)$, *Duke Math. J.* **14** (1947), 429–433.

[8] T. Miezaki and H. Nakasora, An upper bound of the value of t of the support t-designs of extremal binary doubly even self-dual codes, *Des. Codes Cryptogr.*, **79** (2016), 37-46.

[9] T. Miezaki and H. Nakasora, The support designs of the triply even binary codes of length 48, *J. Combin. Designs*, **27** (2019), 673-681.

[10] T. Miezaki and H. Nakasora, Strengthening of the Assmus–Mattson theorem for some dual codes, arXiv:2004.03396.(2020)

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

[12] B. B. Venkov, Even unimodular extremal lattices (Russian), *Algebraic geometry and its applications. Trudy Mat. Inst. Steklov.* **165** (1984), 43–48; translation in *Proc. Steklov Inst. Math.* **165** (1985) 47–52.

[13] S. Zhang, On the nonexistence of extremal self-dual codes, *Discrete Appl. Math.* **91** (1999), 277-286.