数理解析研究所講究録 1228 巻 2001 年 35-42

Type II Codes over $\mathbb{Z}_{2k}$ and the Leech Lattice

山形大学 理学部 原田 昌晃 (Masaaki Harada)
Department of Mathematical Sciences
Yamagata University

本講演では、Leech lattice に関係のある $\mathbb{Z}_{2k}$ 上の長さ 24 の Type II code についての最近の二つの結果を紹介した。前半は Leech lattice の norm $2k$ の orthogonal frame の存在と同値な $\mathbb{Z}_{2k}$ 上の extremal Type II code の存在についての結果であり、これは T.A. Gulliver との共同研究 [6] で、後半は北詰正顕氏との共同研究 [7] で、Niemeier lattice と Leech lattice に関係した $\mathbb{Z}_4$ 上の Type II code を考えることによって得られる Dong-Li-Mason-Norton [5] の結果の別証明を紹介した。

1 準備

1.1 $\mathbb{Z}_{2k}$ 上の Type II Code

$\mathbb{Z}_{2k} = \{0, 1, 2, \ldots, 2k-1\}$ を位数 $2k$ の整数の剰余環とする。$\mathbb{Z}_{2k}^n$ の $\mathbb{Z}_{2k}$-部分加群を $\mathbb{Z}_{2k}$ 上の長さ n の code C とよぶ。通常 coding theory においては Hamming weight を考えるが lattice との関係でここでは Euclidean weight と呼ばれる weight を考える。$x = (x_1, x_2, \ldots, x_n)$ に対しての Euclidean weight $wt_E(x)$ は $\sum_{i=1}^n \min\{x_i^2, (2k-x_i)^2\}$ で定義される。C の minimum Euclidean weight d_E は 0 でない最小の Euclidean weight のことである。C の dual code $C^\perp$ は通常通り定義される：つまり、$C^\perp = \{x \in \mathbb{Z}_{2k}^n | x \cdot y = 0 \ (\forall y \in C)\}$ である、ここで $x = (x_1, \ldots, x_n)$ と $y = (y_1, \ldots, y_n)$ の内積は $x \cdot y = x_1y_1 + \cdots + x_ny_n$ で与えられる。$C = C^\perp$ のとき C は *self-dual* とよばれる。$\mathbb{Z}_{2k}$ 上の self-dual code の全ての codeword の Euclidean weight が $4k$ の倍数であるとき Type II code と呼ばれる。$\mathbb{Z}_{2k}$ の上の Type II codes は [1] で導入された self-dual code の even unimodular lattice に関係したクラスである。$k = 1$ の場合は古くから知られている binary Type II code の定義と一致することに注意しておきたい。

1.2 Construction A、Leech lattice と Niemeier lattice

次に紹介する code を用いた even unimodular lattice の構成方法は Construction A と呼ばれるもので binary code に関しては古くから知られている ([4, 第 7 章] を参照)。$\mathbb{Z}_{2k}$ の場合には [1] で与えられている。

命題 1 (Construction A). C を $\mathbb{Z}_{2k}$ 上の Type II code とし C の minimum Euclidean weight を d_E で表すことにする。このとき

$$A_{2k}(C) = \frac{1}{\sqrt{2k}}\{(x_1,\ldots,x_n) \in \mathbb{Z}^n \mid (x_1 \pmod{2k},\ldots,x_n \pmod{2k}) \in C\}$$

は minimum norm $\min\{d_E/2k, 2k\}$ の even unimodular lattice になる。

lattice に関しての用語等の詳しい説明は割愛させていただくことにするが、未定義な用語に関しては [4] を参照していただきたい。

24 次元の even unimodular lattice は同型を除いて 24 種類あることが知られておりこれらは Niemeier [8] によって分類されたので Niemeier lattice と呼ばれている。また、minimum norm が 4 の場合は同型を除いて唯一つしか存在せず Leech lattice と呼ばれる [3]。ここでは全体を通して Λ で表すことにする。Λ の norm m の互いに直交する 24 個のベクトルを norm m の *orthogonal frame* と呼ぶことにする。Λ の norm $2k$ の orthogonal frame の存在と $\mathbb{Z}_{2k}$ 上の長さ 24 の extremal Type II code の存在は同値であることが分かっている [2]。ここで、長さ 24 の extremal Type II code とは minimum Euclidean weight が $8k$ である場合を指す。このとき extremal Type II code から Construction A で得られる lattice は Leech lattice であることが直ちに分かる。

2 Leech lattice の orthogonal frame の存在について

最近 Chapman [2] が Leech lattice Λ の orthogonal frame の存在について次のような問題を考えた。

問題 A 全ての $2k \geq 4$ に関して、Leech lattice には norm $2k$ の orthogonal frame は存在するのか？

まず Chapman は Λ に norm m の orthogonal frame が存在すれば、全ての自然数 l に対して norm lm の orthogonal frame が存在することを確かめた。そして全ての素数 $p \neq 11$ に対して norm $2p$ の orthogonal frame を構成して、$k \neq 11^r$ なる全ての偶数 $2k \geq 4$ に対して norm $2k$ の orthogonal frame が存在することを示した。したがって、問題 A は次のようになる：

問題 B Leech lattice には norm $k = 22$ の orthogonal frame は存在するのか？

上に述べたように、norm $2k$ の orthogonal frame が Λ に存在することと長さ 24 の $\mathbb{Z}_{2k}$ 上の extremal Type II code の存在は Construction A を介して同値であることが言えるので、$\mathbb{Z}_{22}$ 上の extremal Type II code が構成出来れば、Leech lattice における orthogonal frame の存在問題が完全に解決される。

ここでは $\mathbb{Z}_{2k}$ 上の extremal Type II code C_{22} の構成が出来たことを報告する。構成方法は quasi-twisted construction と呼ばれるもので、一般に良い code を構成するときに使われるものである。C_{22} の生成行列 (I, A) は

$$A = \begin{pmatrix}
13 & 21 & 3 & 12 & 19 & 15 & 3 & 1 & 1 & 1 & 1 & 1 \\
21 & 13 & 21 & 3 & 12 & 19 & 15 & 3 & 1 & 1 & 1 & 1 \\
21 & 21 & 13 & 21 & 3 & 12 & 19 & 15 & 3 & 1 & 1 & 1 \\
21 & 21 & 21 & 13 & 21 & 3 & 12 & 19 & 15 & 3 & 1 & 1 \\
21 & 21 & 21 & 21 & 13 & 21 & 3 & 12 & 19 & 15 & 3 & 1 \\
21 & 21 & 21 & 21 & 21 & 13 & 21 & 3 & 12 & 19 & 15 & 3 \\
19 & 21 & 21 & 21 & 21 & 21 & 13 & 21 & 3 & 12 & 19 & 15 \\
7 & 19 & 21 & 21 & 21 & 21 & 21 & 13 & 21 & 3 & 12 & 19 \\
3 & 7 & 19 & 21 & 21 & 21 & 21 & 21 & 13 & 21 & 3 & 12 \\
10 & 3 & 7 & 19 & 21 & 21 & 21 & 21 & 21 & 13 & 21 & 3 \\
19 & 10 & 3 & 7 & 19 & 21 & 21 & 21 & 21 & 21 & 13 & 21 \\
1 & 19 & 10 & 3 & 7 & 19 & 21 & 21 & 21 & 21 & 21 & 13
\end{pmatrix}$$

で定義される。C_{22} が self-dual であることは $A \cdot A^T = -I$ であることを確認すれば示される、ただし、ここで A^T は A の転置を表す。また、生成行列の全ての行の Euclidean weight が 44 の倍数なので C_{22} の全ての codeword の Euclidean weight が 44 の倍数であることが分かる。minimum Euclidean weight は計算機によって確認した。特に今回は

MAGMA というソフトを利用した。以上から C_{22} が extremal Type II code であることが確認された。

補題 2. $\mathbb{Z}_{22}$ 上の長さ 24 の extremal Type II code が存在する。また、Leech lattice において norm 22 の orthogonal frame が存在する。

Chapman [2] の結果と併せて、問題 A の答えを得る：

定理 3. 全ての自然数 $k \geq 2$ に対して、Leech lattice において norm $2k$ の orthogonal frame が存在する。

この結果を code の言葉で書き直すと以下のようになる。ただし、binary のケースは extended Golay code が extremal になることは良く知られている。

系 4. 全ての自然数 k に対して $\mathbb{Z}_{2k}$ 上の extremal Type II code が存在する。

3 Dong–Li–Mason–Norton の結果について

定理 5 (Dong, Li, Mason and Norton [5]). Λ を Leech lattice とし N を Niemeier lattice の一つとすると

$$\sqrt{2}N \subseteq \Lambda \tag{1}$$

が成り立つ。

原田–北詰 [7] は (1) を満たすように Neimier lattice を $\mathbb{Z}_4$ 上の Type II code から Construction A で構成することによって、上の結果の別証明を得ることが出来た。ここではその結果を紹介する。Type II code の生成行列を明白に与えることによってどのように Niemeier lattice が Leech lattice の中に埋め込まれているかが分かるという利点があると思われる。

(1) を満たすような Neimier lattice N を Construction A を通して $\mathbb{Z}_4$ 上の Type II code から構成した。その方法を簡単に述べることにする (詳しくは原論文 [7] を見て頂きたい)。

1. N が Leech lattice でなければその root 系から $\mathbb{Z}_4$ 上の self-orthogonal code の生成行列 (つまりは求めたい self-dual code の生成行列の一部をなす) を作る。(Leech lattice の場合は次のステップに進む)。もちろん $\frac{\sqrt{2}}{2}g \in \Lambda$ となるようにする、ただし、g は生成行列の行を表す。

2. この生成行列を Leech lattice の元を上手く利用することによって self-dual になるまで拡大させる。このときも $\frac{\sqrt{2}}{2}g \in \Lambda$ となるように選ぶ。

ここでの Leech lattice の元は MOG によって求められる extedned Golay code の元を利用して得られるものを用いる ([4, 第 11 章])。[4] の 133 ページにこのような方法で構成された Leech lattice の生成行列が与えられている。

全ての場合をここで載せることは出来ないので、例としてルート系が D_8^3 である Niemeier lattice の場合についてどのように構成されたかを詳しく述べることをにする。まず最初に Construction A で D_8^3 を構成するような $\mathbb{Z}_4$ 上の Type II code の生成行列 $G(D_8^3)$ を与える：

$$G(D_8^3) = \begin{pmatrix}
0220 & 0000 & 0000 & 0000 & 0000 & 0000 \\
0022 & 0000 & 0000 & 0000 & 0000 & 0000 \\
0002 & 2000 & 0000 & 0000 & 0000 & 0000 \\
0000 & 2200 & 0000 & 0000 & 0000 & 0000 \\
0000 & 0220 & 0000 & 0000 & 0000 & 0000 \\
0000 & 0022 & 0000 & 0000 & 0000 & 0000 \\
0000 & 0000 & 0220 & 0000 & 0000 & 0000 \\
0000 & 0000 & 0022 & 0000 & 0000 & 0000 \\
0000 & 0000 & 0002 & 2000 & 0000 & 0000 \\
0000 & 0000 & 0000 & 2200 & 0000 & 0000 \\
0000 & 0000 & 0000 & 0220 & 0000 & 0000 \\
0000 & 0000 & 0000 & 0022 & 0000 & 0000 \\
0000 & 0000 & 0000 & 0000 & 0220 & 0000 \\
0000 & 0000 & 0000 & 0000 & 0022 & 0000 \\
0000 & 0000 & 0000 & 0000 & 0002 & 2000 \\
0000 & 0000 & 0000 & 0000 & 0000 & 2200 \\
0000 & 0000 & 0000 & 0000 & 0000 & 0220 \\
0000 & 0000 & 0000 & 0000 & 0000 & 0022 \\
3111 & 1111 & 3111 & 1111 & 0000 & 0000 \\
0000 & 0000 & 3111 & 1111 & 3111 & 1111 \\
1111 & 1111 & 1111 & 1111 & 1111 & 1111
\end{pmatrix}$$

まずルート系 D_8^3 からどのように self-orthogonal code が得られるかを述

べることにする。

$$
\begin{aligned}
a_1 &= (1,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0),\\
a_2 &= (\bar{1},1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0),\\
a_3 &= (0,\bar{1},1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0),\\
a_4 &= (0,0,\bar{1},1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0),\\
a_5 &= (0,0,0,\bar{1},1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0),\\
a_6 &= (0,0,0,0,\bar{1},1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0),\\
a_7 &= (0,0,0,0,0,\bar{1},1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0),\\
a_8 &= (0,0,0,0,0,0,\bar{1},1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0),
\end{aligned}
$$

ここで $\bar{1}$ は -1 を表すことにする。$a_1,\ldots,a_8$ はルート系 D_8 を生成することが分かる。ここで $\mathbb{Z}_4$ 上のベクトルとして考えると $2a_1 = 2a_2$ であり

$$
\begin{aligned}
&(2,2,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0)\\
&= 2(1,1,1,1,1,1,1,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0) + 2(a_4 + a_6 + a_8)
\end{aligned}
$$

となる。また

$$2(1,1,1,1,1,1,1,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0)$$

は $G(D_8^3)$ の最後の二つの行から求まる。以上によって $G(D_8^3)$ の最初の 6 行が求まった。同様にして最初の 18 行が求まりまたこれがルート系 D_8^3 に対応していることが分かる。残りの 3 行は Leech lattice の元を用いて self-dual code になるように足されたものである。以上によって $G(D_8^3)$ が得られた。残りの 23 個の Niemeier lattice についての求める $\mathbb{Z}_4$ 上の Type II code の生成行列に関しては原論文の [7] をご覧いただきたい。

4 $\mathbb{Z}_4$ と $\mathbb{Z}_6$ 上の extremal Type II code

本講演の中心はすでに述べた第 2 節と第 3 節に書かれてある結果であったが、講演の最後に $\mathbb{Z}_4$ と $\mathbb{Z}_6$ 上の extremal Type II code の存在について分かっていることを簡単に述べたので、ここでその報告をしてこの小論を終えることにする。

まず、最初に extremal の定義を復習することにする。$\mathbb{Z}_4$ の場合、長さ n の Type II code が $d_E = 8[n/24] + 8$ となるとき extremal とよび、長さ 64 以下の場合に限られるが $\mathbb{Z}_6$ 上の長さ n の Type II code が $d_E = 12[n/24] + 12$ となるとき extremal とよばれる。どちらの場合も

この長さにおいて minimum Euclidean weight が最大になる場合に相当する。

$\mathbb{Z}_4$ 上の extremal Type II code の同値を除いた数は以下の様になっている。ここで二つの $\mathbb{Z}_{2k}$ 上の Type II code C, C' が同値とは、C' の座標を入れ替え、必要があればある座標に -1 を掛けることによって C に一致する場合を指す。

長さ	8	16	24	32	40	48	56	64
個数	4	5	many	many	≥ 2	≥ 1	?	?

長さ 24 と 32 に関しては既にたくさんの extremal Type II code が知られている。

続いて $\mathbb{Z}_6$ 上の extremal Type II code の存在については以下のようなことが知られている：

長さ	8	16	24	32	40	48	56	64
個数	≥ 1	≥ 2	≥ 10	≥ 10	≥ 9	≥ 3	≥ 1	≥ 1

講演では長さ 56 と 64 に関してはまだ存在するかどうか分かっていないと述べたが、集会の後、北詰正顕氏との共同研究において構成することに成功したことを報告しておく。

最後に、講演の終わりに全ての Niemeier lattice が $\mathbb{Z}_6$ 上の Type II code から構成出来るかという質問を受けたが、これについても構成出来ることが北詰氏との共同研究で分かったことを報告しておく。

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), 257–269.

[2] R. Chapman, Double circulant constructions of the Leech lattice, *J. Aust. Math. Soc. Ser. A* **69** (2000), 287–297.

[3] J.H. Conway, A characterisation of Leech's lattice, *Invent. Math.* **7** (1969), 137–142.

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

[5] C. Dong, H. Li, G. Mason and S.P. Norton, Associative subalgebras of the Griess algebra and related topics, *The Monster and Lie Algebras*, Ohio State Univ. Math. Res. Inst. Publ., 7, de Gruyter, Berlin, 1998, 27–42.

[6] T.A. Gulliver and M. Harada, Orthogonal frames in the Leech lattice and a Type II Code over $\mathbb{Z}_{22}$, *J. Combin. Theory Ser. A*, (to appear).

[7] M. Harada and M. Kitazume, $\mathbb{Z}_4$-code constructions for the Niemeier lattices and their embeddings in the Leech lattice, *Eurp. J. Combin.* **21** (2000), 473–485.

[8] H.-V. Niemeier, Definete quadratische Formen der Dimension 24 und Diskriminante 1, *J. Number Theory* **5** (1973), 142–178.