Golay code を用いた Leech lattice の構成

竹内光　　京都大学　修士二回

code とは

(binary linear)code（符号）とは、$\mathbb{F}_2^n$ の subspace$C(\cong \mathbb{F}_2^k)$ のことである。

$c \in C$（code word と呼ばれる）に対して $w(c)$ を「$c \in \mathbb{F}_2^n$ の n 個の桁の中で、成分が 1 である桁の個数」と定める。(c の weight という。)

例. A を正四面体の接触行列、I_n を n 次単位行列として、

$$\mathbb{F}_2^8 \supset \tilde{H} := \mathbb{F}_2^4[I_4, A]$$

を考える。この $\tilde{H}$ は extended Hamming code と呼ばれる。

code から lattice を作る

$\mathbb{R}^n$ の lattice（格子）とは、$\mathbb{R}^n$ の basis$\{v_1, v_2, \cdots, v_n\}$ を使って $\mathbb{Z}v_1 + \mathbb{Z}v_2 + \cdots \mathbb{Z}v_n$ と書かれる集合のこと。code$C \subset \mathbb{F}_2^n$ があると、各桁を mod2 する写像

$$\begin{aligned} \rho : \mathbb{Z}^n &\longrightarrow \mathbb{F}_2^n \\ (a_1, a_2, \cdots, a_n) &\rightarrow (a_1 \mathrm{mod} 2, a_2 \mathrm{mod} 2, \cdots, a_n \mathrm{mod} 2) \end{aligned}$$

の引き戻し $\rho^{-1}(C)$ は lattice。$\Gamma_c := \frac{1}{\sqrt{2}}\rho^{-1}(C)$ を C から作られる lattice という。

例. extended Hamming code$\tilde{H}$ に対する latticeΓ は E_8lattice と呼ばれるものになる。

用語の定義

C を linear code、Γ を lattice とする。

- C:doubly even $\overset{\text{def}}{\iff} w(c) \equiv 0 \bmod 4 (\forall c \in C)$
- C:self dual $\overset{\text{def}}{\iff} C = C^{\perp}$
- Γ:integral $\overset{\text{def}}{\iff} x \cdot y \in \mathbb{Z} (\forall x, y \in \Gamma)$
- Γ:even $\overset{\text{def}}{\iff} x \cdot y \in 2\mathbb{Z} (\forall x, y \in \Gamma)$
- Γ:unimodular $\overset{\text{def}}{\iff} \mathrm{vol}(\mathbb{R}^n/\Gamma) = 1$

すると C と Γ_C の間には関係があって、

命題. *1.* C:doubly even$\iff \Gamma_C$:even

2. $C \subset C^{\perp} \iff \Gamma_C$:integral

3. $C = C^{\perp} \iff \Gamma_C$:unimodular

extended Golay code の構成

B を正 20 面体の接触行列、J 全ての成分が 1 の 12×12 行列として

$$\mathbb{F}_2^{24} \supset \tilde{G} := \mathbb{F}_2^{12}[I_{12}, J - B]$$

を考える。この $\tilde{G}$ は extended Golay code と呼ばれる。

Golay code の性質

- $\tilde{G}$:doubly even,self dual
- $\tilde{G}$ は $\mathbf{0}$、759 個の weight8 の元、2576 個の weight12 の元、759 個の weight16 の元、$\mathbf{1}$ の合計 4096 個の元から成っている。($\mathbf{0}, \mathbf{1}$ は 24 桁全てが $0, 1$ であるベクトルを表す。)

Leech lattice は $\mathbb{R}^{24}$ の even unimodular lattice で、root($x^2 = 2$ となる元) を含まない。このような lattice は同型を除いて一つであることが知られている。以下 Golay code を使って構成してみよう。

$\Gamma_{\tilde{G}} = \frac{1}{\sqrt{2}} \rho^{-1}(\tilde{G})$,$\Gamma := \rho^{-1}(\tilde{G})$ とおく。$x \in \Gamma$ の元は $x = c + 2z (c \in \tilde{G}, z \in \mathbb{Z}^{24})$ と表せる。$\tilde{G}$:doubly even より $\sum x_i \in 2\mathbb{Z}$ なので次の準同型を考える。

$$\begin{aligned} \alpha : \Gamma &\longrightarrow \mathbb{F}_2 \\ x &\to \frac{1}{2} \sum x_i \equiv \frac{1}{2} \sum y_i \bmod 2 \end{aligned}$$

$L := \alpha^{-1}(0)$ とおくと、L は Γ の index2 の sublattice で、$x^2 = 4$ となる元を含まない。なぜなら Γ に含まれる $x^2 = 4$ となる元は type$(\pm 2)^1 0^{23}$ のものしかなく、これは α で 1

に写るので L に入っていないから。(ベクトルが type$a_1^{b1}a_2^{b2}\cdots a_k^{bk}$ とは、$b_1+b_2+\cdots+b_k$ 桁のうち a_1 が b_1 桁、a_2 が b_2 桁、$\cdots$、a_k が b_k 桁から成っていることを表している。)

そこで $N := \alpha^{-1}(1)$ とおき、$L \sqcup (\frac{1}{2}\mathbf{1}+N)$ という集合を考えると、これも lattice になっている。($\mathbf{1}$ は全ての成分が 1 であるベクトル)

定義. $\Lambda_{24} := \frac{1}{\sqrt{2}}(L \sqcup (\frac{1}{2}\mathbf{1}+N))$:Leech lattice

even であること

$\frac{1}{\sqrt{2}}L$ に含まれるベクトル $x = \frac{1}{2}(c+2z)$ に関しては、

$x^2 = \frac{1}{2}(c^2+4cy+4y\ 2) = \frac{c^2}{2} = 0\mathrm{mod}2$ ($\because$ C:doubly even)

$\frac{1}{\sqrt{2}}(\frac{1}{2}\mathbf{1}+N)$ に含まれるベクトル $x = \frac{1}{\sqrt{2}}(\frac{1}{2}\mathbf{1}+c+2y)$ に関しては、

$x^2 = \frac{1}{2}(6+2(\mathbf{1}\cdot y)) \equiv 3+\sum y_i \equiv 0\mathrm{mod}2$

unimodular であること

$\frac{1}{\sqrt{2}}L$ は $\Gamma_{\tilde{G}}$ の index2 の sublattice、同時に Λ_{24} の index2 の sublattice でもある。

$\tilde{G}$:self dual $\therefore$ $\Gamma_{\tilde{G}}$:unimodular を使えば、

$$\mathrm{vol}(\mathbb{R}^{24}/\Lambda_{24}) = \frac{1}{2}\mathrm{vol}(\mathbb{R}^{24}/\frac{1}{\sqrt{2}}L) = \mathrm{vol}(\mathbb{R}^{24}/\Gamma_{\tilde{G}}) = 1$$

$\therefore$ Λ_{24}:unimodular

root を含まないこと

L は $x^2=4$ となる元を含まないので、$\frac{1}{\sqrt{2}}L$ は root を含まない。

$\frac{1}{\sqrt{2}}(\frac{1}{2}\mathbf{1}+N) \subset \frac{1}{\sqrt{2}}(\frac{1}{2}\mathbf{1}+\mathbb{Z}^{24})$ の中で最も短いベクトルは $\frac{1}{\sqrt{2}}(\pm\frac{1}{2},\pm\frac{1}{2},\cdots,\pm\frac{1}{2})$ だが、

$\{\frac{1}{\sqrt{2}}(\pm\frac{1}{2},\pm\frac{1}{2},\cdots,\pm\frac{1}{2})\}^2 = 3 > 2$

$\therefore$ $\frac{1}{\sqrt{2}}(\frac{1}{2}\mathbf{1}+N)$ も root を含まない。

参考文献

[1] Wolfgang Ebeling,"Lattices and Codes: A Course Partially Based on Lectures by F. Hirzebruch",Advanced lectures in mathematics