Boolean functions and quantum stabilizer codes related to Narain CFTs

京都大学 数理解析研究所・古田悠馬
Yuma FURUTA
Research Institute for Mathematical Sciences,
Kyoto University

概要

共形場理論と誤り訂正符号の間には深いつながりがあり，古典的な誤り訂正符号を用いた正則な共形場理論の構成が知られていた。この構成を用いると共形場理論の物理的な量を誤り訂正符号によって記述できるなどのメリットがある。今回は近年発見された量子誤り訂正符号による Narain CFT という非正則な共形場理論の構成について紹介する。この構成を考えることの理論物理的な動機やブール関数による上の構成の記述とその数学的な意味について発表する予定である。

1　導入

まず，先行研究である Dymarsky, Shapere の結果 [1] を大まかにレビューすることで量子誤り訂正符号を用いた Narain CFT の構成について紹介する。

1.1　Narain CFT

まず簡単に Narain CFT を導入する。まず共形不変な場の量子論で，作用

$$\mathcal{S} = \frac{1}{4\pi\kappa} \iint \mathrm{d}\sigma\, \mathrm{d}\tau \left(h^{\alpha\beta} \partial_\alpha X^I \partial_\beta X_I + 2 B_{IJ} \dot{X}^I X'^J \right)$$

を考える。ただし $h^{\alpha\beta} = \begin{pmatrix} 1 & \\ & -1 \end{pmatrix}$, $I = 0, \ldots, n-1$。さらに場 $\vec{X}(\tau, \sigma)$ に，ある格子 Γ による同一視

$$\vec{X} \sim \vec{X} + 2\pi\vec{e}, \quad \vec{e} \in \Gamma$$

をすることで得られる共形場理論を Narain CFT という。これは各状態をラベルするベクトルを

$$\vec{p}_L = \frac{2\vec{P} + (B + I)\vec{e}}{2}$$
$$\vec{p}_R = \frac{2\vec{P} + (B - I)\vec{e}}{2}$$

で定義される $(\vec{p}_L, \vec{p}_R)$ ととることができる。さらにこれらのベクトルが張る格子は偶自己双対であることが分かる。ただし，計量は Lorentz 型計量 $g = \begin{pmatrix} I & 0 \\ 0 & -I \end{pmatrix}$。すなわち，偶自己双対格子を構成すれば Narain CFT が構成できるのである。言い換えれば，Narain CFT とは Lorentz 計量をもつ偶自己双対格子から作られる Lattice CFT ともいえる。[*1]

1.2 量子誤り訂正符号

次に，量子誤り訂正符号について述べる。これは量子情報通信において用いられる技術であり，通信において発生するエラーをある程度訂正することができる。

今回は特にスタビライザ符号という種類の符号を用いる。これは以下のように定められる。n-qubit からなる Hilbert 空間 $\mathcal{H} = (\mathbb{C}^2)^{\otimes n}$ の k 次元部分空間 $\mathcal{H}_\mathcal{C}$ をひとつ定め，符号空間と呼ぶ。符号空間の固定化群 $\mathscr{S}_\mathcal{C}$ を

$$\mathscr{S}_\mathcal{C} \coloneqq \left\{ s : \mathcal{H} \to \mathcal{H} \mid s\,|\psi\rangle = |\psi\rangle \text{ for } {}^\forall\, |\psi\rangle \in \mathcal{H}_\mathcal{C} \right\}$$

で定義する。ここで，各演算子 $\mathcal{H} \to \mathcal{H}$ は Pauli 演算子で生成されると仮定している。すると各生成子 s_i は Pauli 演算子を用いて

$$s_i = i^{\alpha\cdot\beta} \epsilon \left(X^{\alpha_1} \otimes \cdots \otimes X^{\alpha_n}\right) \left(Z^{\beta_1} \otimes \cdots \otimes Z^{\beta_n}\right),\ \alpha, \beta \in \{0,1\}^n$$

と書ける（ϵ はある定数)。つまり各生成子を長さ $2n$ のバイナリベクトル (α, β) とみなせる。さらに，$\mathscr{S}_\mathcal{C}$ の生成子同士の積は (α, β) の $\mathbb{F}_2$ 上の和であるから，スタビライザ符号 $\mathcal{C}$ は生成行列

$$H = \begin{pmatrix} \alpha_1 & \beta_1 \\ \cdots & \cdots \\ \alpha_{n-k} & \beta_{n-k} \end{pmatrix} \tag{1}$$

を持つ長さ $2n$，k 次元の $\mathbb{F}_2$ 上の符号とみなせる。以下ではこのスタビライザ符号を用いて，つまり上記の生成行列 (1) により実自己双対符号を構成することを考える。

1.3 Narain CFT の構成

次に，この量子スタビライザ符号を用いて Narain CFT を構成する方法を紹介する。それには 1.1 章で述べたように偶自己双対格子を構成すればよい。そこで，量子スタビライザ符号 $\mathcal{C}$ を用いて以下のように格子 $\Lambda(\mathcal{C})$ を構成する。

$$\Lambda(\mathcal{C}) \coloneqq \left\{ v \in \mathbb{Z}^{2n} \mid v \equiv^\exists c \bmod 2,\ c \in \mathcal{C} \right\} / \sqrt{2}$$

とすると，$\mathcal{C}$ が実自己双対であることと $\Lambda(\mathcal{C})$ が偶自己双対であることが同値になることが分かる。すなわち，偶自己双対格子を構成すれば Narain CFT が構成できることが分かった。この構成に基づくと，符号の量と CFT の物理量が表 1 のように対応することが分かる。

[*1] 知られている事実として，(n, n) 型の計量を持つ偶自己双対格子は同型を除いて唯一つしか存在しないが，同じ同型類に属す lattice から作られる CFT でも物理的には異なるものになることがある。これにより，物理ではより弱い同値関係である “T-duality” を用いる。

符号	CFT
長さ	中心電荷
重み多項式	分配関数
binary distance	spectral gap

表 1　符号と CFT の対応関係

例えば，CFT の分配関数 $\mathcal{Z}(\tau,\bar{\tau})$ は次のように書ける。

$$\mathcal{Z}(\tau,\bar{\tau}) = \frac{1}{|\eta(\tau)|^{2n}} W_{\mathcal{C}}\left(\frac{b\bar{b}+c\bar{c}}{2}, \frac{b\bar{b}-c\bar{c}}{2}, \frac{a\bar{a}}{2}\right)$$

ここで

$$a(\tau) = \sum_{n=-\infty}^{\infty} q^{(n+1/2)^2/2},\ b(\tau) = \sum_{n=-\infty}^{\infty} q^{(n^2/2)},\ c(\tau) = \sum_{n=-\infty}^{\infty} (-1)^n q^{n^2/2}$$

はヤコビテータ関数で，$W_{\mathcal{C}}(x,y,z)$ は量子スタビライザ符号の重み多項式。今回は CFT の spectral gap という量に着目する。これは符号の binary distance という量に対応することが [1] により分かった。従って spectral gap が大きい CFT を得るには binary distance が大きい符号を得ればよいことになる。しかし binary distance を大きくする構成法はいまだ知られていない。そこで本研究ではこの binary distance をブール関数によって表し，binary distance を大きくする構成を探る。

1.4　ブール関数

まず実自己双対スタビライザ符号はある 2 次斉次ブール関数と 1:1 に対応することを説明する。実自己双対符号 $\mathcal{C}$ の生成行列は $n \times 2n$ 行列で，同値変形により

$$\begin{pmatrix} B & I \end{pmatrix}$$

の形にできることが分かっている。ただし B, I はそれぞれ $n \times n$ 行列である。ここで $\mathcal{C}$ が実自己双対であるという条件から B はあるグラフの隣接行列とみなせることがいえる。この隣接行列を用いて $f(x_1,\ldots,x_n) = \sum_{i<j} B_{ij}x_ix_j$ という多項式を定義する。この多項式を $\mathbb{Z}_2^n$ から $\mathbb{Z}_2$ への関数とみなしたとき，f は $\mathcal{C}$ に付随したブール関数と呼ぶ。このブール関数を用いて binary distance を表したのが本研究の主結果である。

2　主結果

まずブール関数の Extended Propagation Criteria (EPC) を次で定義する。

定義 1. $a,\mu,k \in \mathbb{Z}_2^n$ とする。

$$v(a,\mu,k) = \sum_{x \in k+V_{\bar{\mu}}} (-1)^{f(x)+f(x+a)}, \quad k \preceq \mu$$

d\ n	2	3	4	5	6	7	8	9	10	11	12
2	1	2	2,3	3,4	3-5	3-6	3-7	4-8	4-9	4-10	4-11
3				2	3	3,4	3,4	3-5	4-6	4-7	4-8
4					2		3,4	3,4	3-5	4-6	4-7
5										4	4
6											4

表 2　Ref. [3] L.E.Danielsen (2005)

をブール関数の *fixed-extended autocorrelation function* という。ただし $x \succeq y \Leftrightarrow x_i \geq y_i$ for $^\forall i \in \{1, \ldots, n\}$, $V_a \coloneqq \{x \in \mathbb{Z}_2^n \mid x \preceq a\}$。$f(x)$ が q 次の $EPC(l)$ をみたすとは，$k \preceq \mu$ かつ $1 \leq w(a) \leq l$, $0 \leq w(\mu \& \bar{a}) \leq q$ なる全ての a, μ, k に対し $v(a, \mu, k) = 0$ となること。

またブール関数の EPC 距離を次で定義する。

定義 2. ブール関数の *EPC* 距離が d であるとは, $l + q < d$ で $(l, q) \neq 0$ なる全ての整数 $l \geq 1$, $q \geq 0$ に対して $f(x)$ が q 次の *EPC(l)* をみたすこととである。

このとき，次が成り立つことが分かった。[2]

定理 1 (主結果)**.** 実自己双対スタビライザ符号 $\mathcal{C}$ の *binary distance* はそれに付随したブール関数の *EPC* 距離に一致する。

証明の概略. EPC 距離は以下を満たすような長さ $2n$ の nonzero ベクトル $(a, b) \in \mathbb{Z}_2^{2n}$ の重み（値が 1 の成分の数）の最小値に等しい。

$$\sum_{x \in \mathbb{Z}_2^n} (-1)^{f(x)+f(x+a)+b \cdot x} \neq 0 \tag{2}$$

一方，a の値が 1 の成分に対応する qubit に σ_x，b の値が 1 の成分に対応する qubit に σ_z をかけるエラー演算子を $\mathcal{E}$ とする。$|\psi'\rangle = \mathcal{E}|\psi\rangle$ の各係数を並べると $s' = (-1)^{f(x+a)+b \cdot x}$ となる。ここで式 (2) の左辺は $s \cdot s'$ つまり $|\psi\rangle$ と $|\psi'\rangle$ の内積を表している。従って演算子 $\mathcal{E}$ によるエラー状態 $\mathcal{E}|\psi\rangle$ の誤りが復元できることと $|\psi\rangle$ と $\mathcal{E}|\psi\rangle$ が直交することが同値になる。よって式 (2) を満たす (a, b) は $\mathbb{F}_2$ 上の符号としての $\mathcal{C}$ の元とみなせる。つまり式 (2) を満たす (a, b) の重みの最小値 $= w_b$ の最小値，すなわち符号の binary distance に一致する。 □

以上の定理から，binary distance を大きくする代わりに EPC 距離を大きくすればよいことが分かる。そこで Danielsen 氏によって調べられた APC 距離と PAR の関係 [3] を利用する。それは，APC 距離と PAR の間には負の相関関係にある，すなわち APC 距離が大きいほど PAR は小さくなる傾向にあるという関係である。

$\mathrm{PAR}_{I,H,N} = 2^\lambda$ となる λ の値を APC 距離 d で分類して $n = 12$ までまとめたものが表 [**?**] である。APC 距離は EPC 距離の定義とほぼ同じものであるため，EPC 距離も PAR と同様の関係にあると考えた。しかしこれはあくまで相関関係にすぎないので，PAR が小さい構成をしても

実際に binary distance が大きいかは実証してみなければいけない。そこで，まず次の Parker 氏, Tellambura 氏の結果 [4] を用い，PAR が小さくなるような構成を通じて EPC 距離が大きいかどうか考察する。

定理 2. $n = Lt$,θ_j, γ_j は $\mathbb{Z}_2^t$ 内の置換で

$$p(x) = \sum_{j=0}^{L-2} \theta_j(\mathbf{x}_j)\gamma_j(\mathbf{x}_j) + \sum_{j=0}^{L-1} g_j(\mathbf{x}_j)$$

とすると，$s = (-1)^{p(x)}$ に対し $\mathrm{PAR}_{LUUT}(s) \leq 2^t$ となる。

この構成は nested clique graph というグラフを含んでいる。これは t 次の完全グラフを t 次の完全グラフの構造でネストしたもので，$[K_t[K_t]]$ と書く。これは各完全グラフの繋ぎ方に自由度があり，$\frac{1}{2}(t-1)(t-2)$ 個の t 次の置換を選ぶ。そこで本研究では t を奇素数とし，次のように構成した。

$$\sigma_k = \begin{pmatrix} 1 & 2 & \cdots & t \\ m & m+l & \cdots & m+(t-1)l \end{pmatrix} \tag{3}$$

この構成を $t = 3, 5, 7, 11$ のとき実際行い，対応するブール関数の EPC 距離を計算した。すると EPC 距離は $d = 4, 8, 12, 21$ となり，全て $2t-2$ を超えることが分かった。これは長さに対して平方根程度の大きさを持っており，現状得られる実自己双対符号の中では比較的性質が良いといえる。従ってこの関係は一般の奇素数 t で成り立つという予想を設定した。

予想. t を奇素数とする。式 (3) に従って構成した *nested clique graph* から作られる実自己双対スタビライザ符号は長さ t^2 で *binary distance* は $2t-2$ 以上。

3　結論

本研究では，Narain CFT の spectral gap が量子スタビライザ符号の binary distance と関係することを動機に，大きい spectral gap を得るために binary distance を大きくする方法を探索した。そこで量子スタビライザ符号の binary distance はそれに付随したブール関数の EPC 距離に等しいことを示した。すると EPC 距離と PAR の間の負の相関関係を利用することができ，Parker 氏, Tellambura 氏の結果より PAR が小さくなるような構成を参考にできるようになった。本研究ではその中でも nested clique graph に着目し，式 (3) のように構成した。そしてこの構成では長さの平方根程度の binary distance が得られることをいくつかの t で検証した。そこで一般の奇素数 t でも同程度の binary distance が得られると予想した。今後の課題としてはこの予想を証明・反証を行うことが挙げられる。また PAR をより小さくするような構成を考え，さらに性質の良い量子スタビライザ符号を構成することも今後の課題である。

参考文献

[1] Anatony Dymarsky and Alfred Shapere. Quantum stabilizer codes and lattices and CFTs. *J High Energ Phys 2021 160*, 2020.

[2] Yuma Furuta. Relation between spectra of Narain CFTs and properties of associated boolean functions. *JHEP*, Vol. 2022, No. 146, 2022.

[3] Lars Eirik Danielsen. On Self-Dual Quantum Codes, Graphs, and Boolean Functions. *ArXivquant-Ph0503236*, March 2005.

[4] M.G. Parker and C. Tellambura. A construction for binary sequence sets with low peak-to-average power ratio. In *Proc. IEEE Int. Symp. Inf. Theory*, p. 239, Lausanne, Switzerland, 2002. IEEE.