Narain CFTs from Error-Correcting Codes via Integers of Cyclotomic Field

Takumi Oikawa

The Graduate University for Advanced Studies, SOKENDAI

Based on arXiv:2410.12488 with Shun'ya Mizoguchi

Introduction

- **Error-correcting code** is useful for the construction of CFTs.

  Indeed, some 2d chiral CFTs can be constructed from a certain class of CECCs via Eucledean lattices. [Dolan-Goddard-Montague '90, '96]

Introduction

- **Error-correcting code** is useful for the construction of CFTs.

  Indeed, some 2d chiral CFTs can be constructed from a certain class of CECCs via Eucledean lattices.

  [Dolan-Goddard-Montague '90, '96]

  CECCs → Eucledean Lattices → Chiral CFTs

- In recent years, this construction was generalized to the case of QECCs.

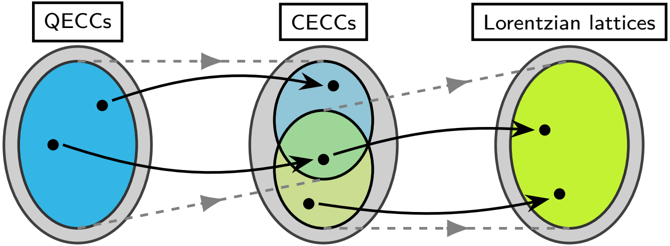
  [Dymarsky-Shapere '20]

  QECCs → Lorentzian Lattices → Non-chiral CFTs

Overview (1/2)

- We focus on the **Narain CFT**, which is the theory of n free bosons $X^i(\tau, \sigma)$ compactified on an n-dimensional torus. [Narain '86] [Narain-Sarmadi-Witten '87]
- The momentum $(\vec{p}_L, \vec{p}_R)$ forms the **Lorentzian even self-dual lattice** $\Lambda \subset \mathbb{R}^{n,n}$.

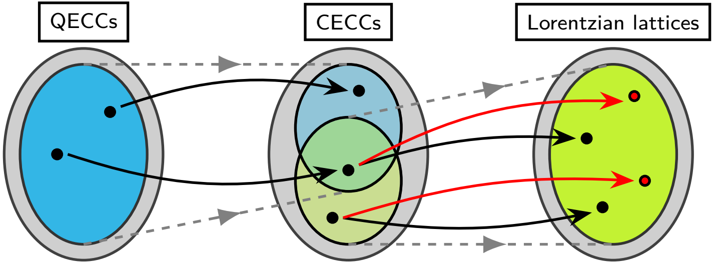
$\Longrightarrow$ They can be constructed from CECCs, and then related to QECCs.
[Dymarsky-Shapere '20] [Kawabata-Nishioka-Okuda '23]



Overview (2/2)

- However, the way to associate Euclidean lattices with CECCs is not unique.
  [Conway-Sloane '87] [Ebeling '94] . . .
- Inspired by the earlier works, we construct the Lorentzian lattice from CECCs using **integers of cyclotomic field**.

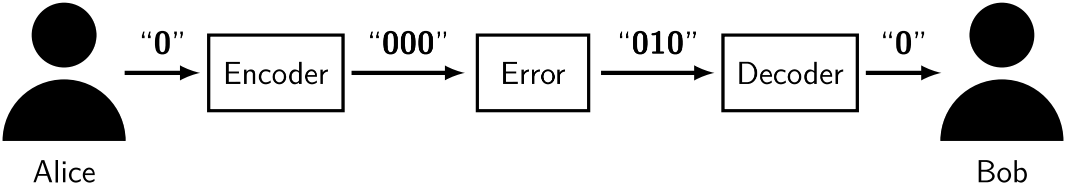
  $\Longrightarrow$ We obtain a broader class of corresponding Narain CFTs. [Mizoguchi-TO '24]



Classical error correction

- The important point of CECC is to add the **redundancy** into original messages.
- A simple example is to repeat each bit three times (**repetition code**).

  Then, $\mathbb{F}_2 = \{0, 1\}$ is embedded into $\mathbb{F}_2^3$ as $\mathcal{C} = \{000, 111\} \subset \mathbb{F}_2^3$.



- In this case, Bob can correct one bit-flip error by majority vote.

Classical error-correcting code

- We consider length-n CECCs over $\mathbb{F}_p = \{0, 1, \cdots, p-1\}$.

  Thus, we encode k-bit original messages $x \in \mathbb{F}_p^k$ into n-bit **codewords** $c \in \mathbb{F}_p^n$.

Classical error-correcting code

- We consider length-n CECCs over $\mathbb{F}_p = \{0, 1, \cdots, p-1\}$.

  Thus, we encode k-bit original messages $x \in \mathbb{F}_p^k$ into n-bit **codewords** $c \in \mathbb{F}_p^n$.

Definition: $[n, k]_p$ code

A **p-ary linear code** $\mathcal{C} \subset \mathbb{F}_p^n$ is defined as a set of codewords $c \in \mathbb{F}_p^n$ generated by the $\mathbb{F}_p$-valued $k \times n$ matrix G,

$$\mathcal{C} = \left\{ c \in \mathbb{F}_p^n \,\middle|\, c = xG,\ x \in \mathbb{F}_p^k \right\}.$$

Dual code

- For the construction of even self-dual lattices, we introduce dual codes.

Definition: Dual code

For an $[n,k]_p$ code $\mathcal{C}$, the **dual code** of $\mathcal{C}$ is defined as

$$\mathcal{C}^\perp = \left\{ c' \in \mathbb{F}_p^n \,\middle|\, c \cdot c' = 0 \mod p,\ c \in \mathcal{C} \right\}.$$

Here, the inner product is the standard Euclidean norm $c \cdot c' = \sum_{i=1}^n c_i c_i'$.

Dual code

- For the construction of even self-dual lattices, we introduce dual codes.

Definition: Dual code

For an $[n, k]_p$ code $\mathcal{C}$, the **dual code** of $\mathcal{C}$ is defined as

$$\mathcal{C}^{\perp} = \left\{ c' \in \mathbb{F}_p^n \,\middle|\, c \cdot c' = 0 \mod p,\ c \in \mathcal{C} \right\}.$$

Here, the inner product is the standard Euclidean norm $c \cdot c' = \sum_{i=1}^{n} c_i c_i'$.

- If $\mathcal{C}$ satisfies $\mathcal{C} \subset \mathcal{C}^{\perp}$, then $\mathcal{C}$ is called **self-orthogonal**.

  Especially, $\mathcal{C}$ is called **self-dual** if and only if $\mathcal{C}$ satisfies $\mathcal{C} = \mathcal{C}^{\perp}$.

Construction A

- We construct the Euclidean lattice from CECCs via the **Construction A**.

[Leech-Sloane '71]

Definition: Construction A

For an $[n,k]_p$ code $\mathcal{C}$, we define the Construction A lattice $\Lambda(\mathcal{C})$ as

$$\Lambda(\mathcal{C}) \coloneqq \frac{1}{\sqrt{p}}\rho^{-1}(\mathcal{C}), \text{ where } \rho\colon \mathbb{Z}^n \to (\mathbb{Z}/p\mathbb{Z})^n = \mathbb{F}_p^n.$$

Construction A

- We construct the Euclidean lattice from CECCs via the **Construction A**.

[Leech-Sloane '71]

Definition: Construction A

For an $[n, k]_p$ code $\mathcal{C}$, we define the Construction A lattice $\Lambda(\mathcal{C})$ as

$$\Lambda(\mathcal{C}) := \frac{1}{\sqrt{p}}\rho^{-1}(\mathcal{C}), \text{ where } \rho\colon \mathbb{Z}^n \to (\mathbb{Z}/p\mathbb{Z})^n = \mathbb{F}_p^n.$$

- The lattice vectors $\lambda \in \Lambda(\mathcal{C})$ are given by identifying with $c \in \mathcal{C}$ under $\bmod p$,

$$\lambda = \frac{c + pm}{\sqrt{p}}, \text{ for } c \in \mathcal{C},\ m \in \mathbb{Z}^n.$$

Construction A (example)

- Consider $\mathcal{C} = \{00, 11\} \subset \mathbb{F}_2^2$ and then, construct the Construction A lattice $\Lambda(\mathcal{C})$.

  The lattice vectors $\lambda \in \Lambda(\mathcal{C})$ are given by identifying with $c \in \mathcal{C}$ under $\bmod 2$:

$$\lambda = \frac{c + 2m}{\sqrt{2}}, \quad \text{for } c \in \mathcal{C},\ m \in \mathbb{Z}^2$$

Construction A (example)

- Consider $\mathcal{C} = \{00, 11\} \subset \mathbb{F}_2^2$ and then, construct the Construction A lattice $\Lambda(\mathcal{C})$.

  The lattice vectors $\lambda \in \Lambda(\mathcal{C})$ are given by identifying with $c \in \mathcal{C}$ under $\bmod 2$:

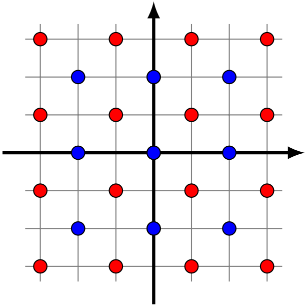
$$\lambda = \frac{c + 2m}{\sqrt{2}}, \quad \text{for } c \in \mathcal{C},\ m \in \mathbb{Z}^2$$

- Then, $\Lambda(\mathcal{C})$ consists of two types of points:

$$(0, 0) + \sqrt{2}m \quad \text{and} \quad \left(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}\right) + \sqrt{2}m.$$

  Therefore,

$$\Lambda(\mathcal{C}) = \left[\sqrt{2}\mathbb{Z}^2\right] \bigcup \left[\left(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}\right) + \sqrt{2}\mathbb{Z}^2\right].$$



Narain CFT

- We focus on the **Narain CFT**, which is the theory of n free bosons $X^i(\tau, \sigma)$ compactified on an n-dimensional torus $\mathbb{R}^n/(2\pi\Gamma)$; [Narain '86] [Narain-Sarmadi-Witten '87]

$$S = \frac{1}{8\pi}\int \mathrm{d}t \int_0^{2\pi} \mathrm{d}\sigma \Big[G_{ij}\Big(\partial_t X^i\, \partial_t X^j - \partial_\sigma X^i\, \partial_\sigma X^j\Big) - 2B_{ij}\, \partial_t X^i\, \partial_\sigma X^j\Big],$$

where G (and B) are $n \times n$ constant (anti-) symmetric matrix, respectively.

- The set of momentum $(\vec{p}_L, \vec{p}_R)$ forms a lattice $\tilde{\Lambda} = \{(\vec{p}_L, \vec{p}_R) \mid \vec{m}, \vec{w} \in \mathbb{Z}^n\} \subset \mathbb{R}^{2n}$,

$$\vec{p}_{L_i} = \frac{m_i}{R} + \frac{R}{2}(B_{ij} + G_{ij})w^j, \quad \vec{p}_{R_i} = \frac{m_i}{R} + \frac{R}{2}(B_{ij} - G_{ij})w^j.$$

Lorentzian even self-dual lattice

- We introduce another convention of $(\vec{p}_L, \vec{p}_R)$ as

$$\Lambda \coloneqq (\lambda_1, \lambda_2) = \left\{ \left(\frac{\vec{p}_L - \vec{p}_R}{\sqrt{2}}, \frac{\vec{p}_L + \vec{p}_R}{\sqrt{2}} \right) \;\middle|\; \vec{m}, \vec{w} \in \mathbb{Z}^n \right\}.$$

Lorentzian even self-dual lattice

- We introduce another convention of $(\vec{p}_L, \vec{p}_R)$ as

$$\Lambda := (\lambda_1, \lambda_2) = \left\{ \left(\frac{\vec{p}_L - \vec{p}_R}{\sqrt{2}}, \frac{\vec{p}_L + \vec{p}_R}{\sqrt{2}} \right) \,\middle|\, \vec{m}, \vec{w} \in \mathbb{Z}^n \right\}.$$

- This **Narain lattice** $\Lambda \subset \mathbb{R}^{n,n}$ forms the **even self-dual lattice** w.r.t. Lorentzian off-diagonal metric $\eta = \begin{pmatrix} 0 & I_n \\ I_n & 0 \end{pmatrix}$.

Definition: Even self-dual lattice

A **dual lattice** is defined as $\Lambda^* = \{x' \in \mathbb{R}^n \mid x \odot x' \in \mathbb{Z},\ \forall x \in \mathbb{Z}\}$ w.r.t. η.
Then a lattice Λ is **self-dual** iff $\Lambda = \Lambda^*$, and **even** iff $x \odot x \in 2\mathbb{Z}$ for $\forall x \in \Lambda$.

CECC $\to$ Lattice

- For a length-$2n$ code $\mathcal{C} \subset \mathbb{F}_p^{2n}$, we associate the Construction A lattice $\Lambda(\mathcal{C})$ by

$$\Lambda(\mathcal{C}) = \left\{ \left(\frac{\alpha + pk_1}{\sqrt{p}}, \frac{\beta + pk_2}{\sqrt{p}} \right) \;\middle|\; c = (\alpha, \beta) \in \mathcal{C},\ \ k_1, k_2 \in \mathbb{Z}^n \right\}.$$

CECC $\to$ Lattice

- For a length-$2n$ code $\mathcal{C} \subset \mathbb{F}_p^{2n}$, we associate the Construction A lattice $\Lambda(\mathcal{C})$ by

$$\Lambda(\mathcal{C}) = \left\{ \left(\frac{\alpha + pk_1}{\sqrt{p}}, \frac{\beta + pk_2}{\sqrt{p}} \right) \,\middle|\, c = (\alpha, \beta) \in \mathcal{C},\ k_1, k_2 \in \mathbb{Z}^n \right\}.$$

- For odd prime p, the Construction A lattice $\Lambda(\mathcal{C})$ is **even self-dual** with Lorentzian metric η if CECC $\mathcal{C}$ is **self-dual** w.r.t. η.

[Yahagi '22] [Kawabata-Nishioka-Okuda '23]

CECC $\to$ Lattice

- For a length-$2n$ code $\mathcal{C} \subset \mathbb{F}_p^{2n}$, we associate the Construction A lattice $\Lambda(\mathcal{C})$ by

$$\Lambda(\mathcal{C}) = \left\{ \left(\frac{\alpha + pk_1}{\sqrt{p}}, \frac{\beta + pk_2}{\sqrt{p}} \right) \,\middle|\, c = (\alpha, \beta) \in \mathcal{C},\ \ k_1, k_2 \in \mathbb{Z}^n \right\}.$$

- For odd prime p, the Construction A lattice $\Lambda(\mathcal{C})$ is **even self-dual** with Lorentzian metric η if CECC $\mathcal{C}$ is **self-dual** w.r.t. η.

[Yahagi '22] [Kawabata-Nishioka-Okuda '23]

- For example, the $[2n, n]_p$ code $\mathcal{C}$ generated by $n \times 2n$ matrix $(I_n \mid B_n)$, where B_n is $\mathbb{F}_p$-valued antisymmetric matrix (**B-form code**).

  $\Longrightarrow \Lambda(\mathcal{C})$ corresponds to the Narain lattice with $G = I_n$ and $B = B_n$.

Motivation

- The Constructin A is based on a “hypercubic lattice” $\mathbb{Z}^n$:

$$\Lambda(\mathcal{C}) = \left\{ \left(\frac{\alpha + pk_1}{\sqrt{p}}, \frac{\beta + pk_2}{\sqrt{p}} \right) \;\middle|\; c = (\alpha, \beta) \in \mathcal{C},\ k_1, k_2 \in \mathbb{Z}^n \right\}.$$

But there is no reason to restrict to “square” lattice. $\Longrightarrow$ triangular, ADE, etc.

Motivation

- The Constructin A is based on a "hypercubic lattice" $\mathbb{Z}^n$:

$$\Lambda(\mathcal{C}) = \left\{ \left(\frac{\alpha + pk_1}{\sqrt{p}}, \frac{\beta + pk_2}{\sqrt{p}} \right) \middle| \, c = (\alpha, \beta) \in \mathcal{C}, \; k_1, k_2 \in \mathbb{Z}^n \right\}.$$

  But there is no reason to restrict to "square" lattice. $\Longrightarrow$ triangular, ADE, etc.

- Such **Euclidean** lattices can be constructed from CECCs using "integers" of **cyclotomic field** $\mathbb{Q}(\zeta_p)$ instead of $\mathbb{Z}^n \subset \mathbb{R}^n$

  [Conway-Sloane '87] [Ebeling '94] [Montague '93] [Dolan-Goddard-Montague '94]...

- We use these facts to construct **Lorentzian** lattices, and identify the corresponding Narain CFTs.

  [Mizoguchi-TO '24]

Example: $\mathbb{Q}(\zeta_3)$ and $\mathbb{Z}[\zeta_3]$

- **The third cyclotomic field $\mathbb{Q}(\zeta_3)$** is a number field by adjoining ζ_3 to $\mathbb{Q}$,

$$\mathbb{Q}(\zeta_3) = \{a_0 + a_1\zeta_3 \mid a_0, a_1 \in \mathbb{Q}\} \quad \text{where} \quad \zeta_3 = \frac{-1+\sqrt{-3}}{2}.$$

  This is a two-dimensional vector space over $\mathbb{Q}$ with basis 1 and ζ_3.

Example: $\mathbb{Q}(\zeta_3)$ and $\mathbb{Z}[\zeta_3]$

- **The third cyclotomic field $\mathbb{Q}(\zeta_3)$** is a number field by adjoining ζ_3 to $\mathbb{Q}$,

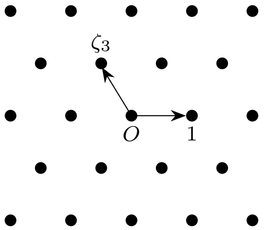
$$\mathbb{Q}(\zeta_3) = \{a_0 + a_1\zeta_3 \mid a_0, a_1 \in \mathbb{Q}\} \quad \text{where} \quad \zeta_3 = \frac{-1+\sqrt{-3}}{2}.$$

  This is a two-dimensional vector space over $\mathbb{Q}$ with basis 1 and ζ_3.

- The **integers** of $\mathbb{Q}(\zeta_3)$ are defined as

$$\mathbb{Z}[\zeta_3] = \{m_0 + m_1\zeta_3 \mid m_0, m_1 \in \mathbb{Z}\}.$$

  $\mathbb{Z}[\zeta_3]$ forms an equilateral triangular lattice in $\mathbb{C} \simeq \mathbb{R}^2$.



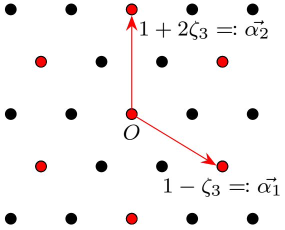
Lattices over $\mathbb{Z}[\zeta_3]$

- Consider the set of "multiple" of $1-\zeta_3 \in \mathbb{Z}[\zeta_3]$ as

$$\mathfrak{P} := (1-\zeta_3)\mathbb{Z}[\zeta_3] = \{(1-\zeta_3)\xi \mid \xi \in \mathbb{Z}[\zeta_3]\}.$$

- Since $\mathbb{Z}[\zeta_3]/\mathfrak{P} \cong \mathbb{F}_3$, $\mathbb{Z}[\zeta_3]$ is partitioned as

$$\mathbb{Z}[\zeta_3] = \bigcup_{i=0}^{2}[i+\mathfrak{P}] \quad \text{where} \quad i \in \mathbb{F}_3.$$



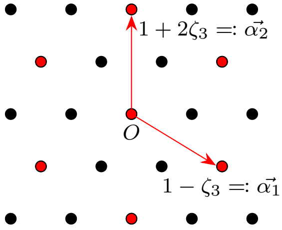
Lattices over $\mathbb{Z}[\zeta_3]$

- Consider the set of "multiple" of $1 - \zeta_3 \in \mathbb{Z}[\zeta_3]$ as

$$\mathfrak{P} := (1 - \zeta_3)\mathbb{Z}[\zeta_3] = \{(1 - \zeta_3)\xi \mid \xi \in \mathbb{Z}[\zeta_3]\}.$$

- Since $\mathbb{Z}[\zeta_3]/\mathfrak{P} \cong \mathbb{F}_3$, $\mathbb{Z}[\zeta_3]$ is partitioned as

$$\mathbb{Z}[\zeta_3] = \bigcup_{i=0}^{2} [i + \mathfrak{P}] \quad \text{where} \quad i \in \mathbb{F}_3.$$



- Then, identify elements of $\mathbb{Z}[\zeta_3]$ with $\mathbb{F}_3$-valued codewords $c \in \mathbb{F}_3^n$ under "$\mathrm{mod}\ \mathfrak{P}$".

$\Longrightarrow$ we can construct $2n$-dim. lattice from length-n ternary codes $\mathcal{C} \subset \mathbb{F}_3^n$,

$$\Lambda_{\mathbb{C}}(\mathcal{C}) := \{c + (1 - \zeta_3)\xi \mid c \in \mathcal{C},\ \xi \in \mathbb{Z}[\zeta_3]^n\}.$$

Narain Lattices via $\mathbb{Z}[\zeta_3]$

- Similarly to the Construction A, we construct Narain lattice from CECC via $\mathbb{Z}[\zeta_3]$:
[Mizoguchi-TO '24]

$$\Lambda(\mathcal{C}) := \{\alpha + (1-\zeta_3)k_1, \beta + (1-\zeta_3)k_2 \mid (\alpha,\beta) \in \mathcal{C},\ k_1, k_2 \in \mathbb{Z}[\zeta_3]^n\}.$$

cf. Construction A: $\Lambda(\mathcal{C}) = \left\{ \left(\frac{\alpha+pk_1}{\sqrt{p}}, \frac{\beta+pk_2}{\sqrt{p}} \right) \,\middle|\, (\alpha,\beta) \in \mathcal{C},\ k_1, k_2 \in \mathbb{Z}^n \right\}.$

$\Longrightarrow$ As a result, $[2n, n]_p$ B-form codes give even self-dual lattice $\Lambda(\mathcal{C}) \subset \mathbb{R}^{2n,2n}$.

Narain Lattices via $\mathbb{Z}[\zeta_3]$

- Similarly to the Construction A, we construct Narain lattice from CECC via $\mathbb{Z}[\zeta_3]$:

[Mizoguchi-TO '24]

$$\Lambda(\mathcal{C}) := \{\alpha + (1-\zeta_3)k_1, \beta + (1-\zeta_3)k_2 \mid (\alpha,\beta) \in \mathcal{C},\ k_1, k_2 \in \mathbb{Z}[\zeta_3]^n\}.$$

cf. Construction A: $\Lambda(\mathcal{C}) = \left\{ \left(\frac{\alpha+pk_1}{\sqrt{p}}, \frac{\beta+pk_2}{\sqrt{p}} \right) \,\middle|\, (\alpha,\beta) \in \mathcal{C},\ k_1, k_2 \in \mathbb{Z}^n \right\}.$

$\Longrightarrow$ As a result, $[2n,n]_p$ B-form codes give even self-dual lattice $\Lambda(\mathcal{C}) \subset \mathbb{R}^{2n,2n}$.

- From the direct calculation, the corresponding Narain CFT is

$$G = I_n \otimes C_3^{-1}, \quad B = B_n \otimes C_3^{-1}, \quad C_3 : \text{Gram matrix of } A_2 \text{ root lattice.}$$

Conclusions and Outlook

- We construct Narain lattices $\Lambda(\mathcal{C}) \subset \mathbb{R}^{n(p-1),n(p-1)}$ by identifying CECCs over $\mathbb{F}_p$ with $\mathbb{Z}[\zeta_p]$-valued vectors since $\mathbb{Z}[\zeta_p]/\mathfrak{P} \cong \mathbb{F}_p$.
- From $[2n, n]_p$ B-form codes, we obtain the corresponding Narain CFTs

$$G = I_n \otimes C_p^{-1}, \quad B = B_n \otimes C_p^{-1}, \quad C_p : \text{Gram matrix of } A_{p-1}.$$

- Our approach is the generalization of Construction A and gives the systematical way to obtain broader class of Narain CFTs.
- Generalization to other number field (e.g. quadratic field, subfield of $\mathbb{Q}(\zeta_p)$, etc.) and general CECCs over $\mathbb{F}_{p^l}$ or $\mathbb{Z}_n$ will be interesting.