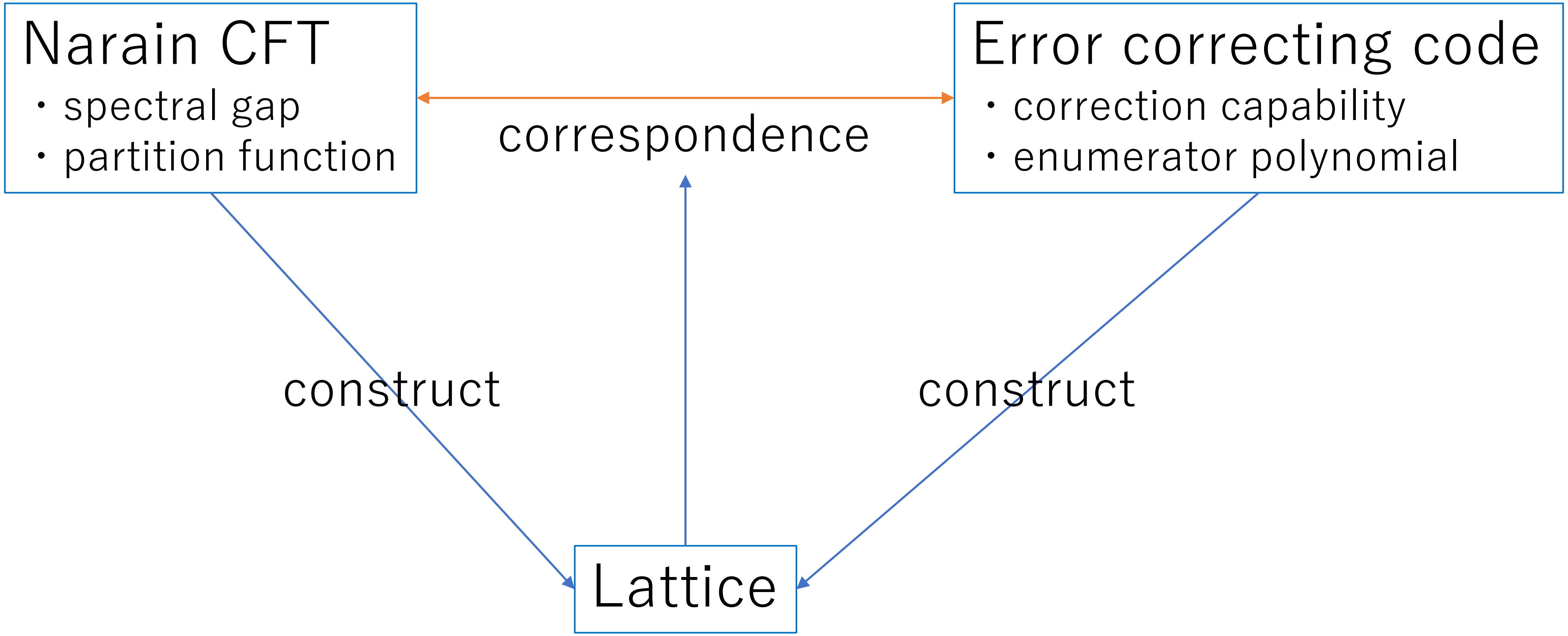
Narain CFTs and error correcting codes

Shinichiro Yahagi (Tokyo U.)

based on arXiv: 2203.10848

Overview


Narain CFT
・spectral gap
・partition function
Error correcting code
・correction capability
・enumerator polynomial
correspondence
construct
construct
Lattice

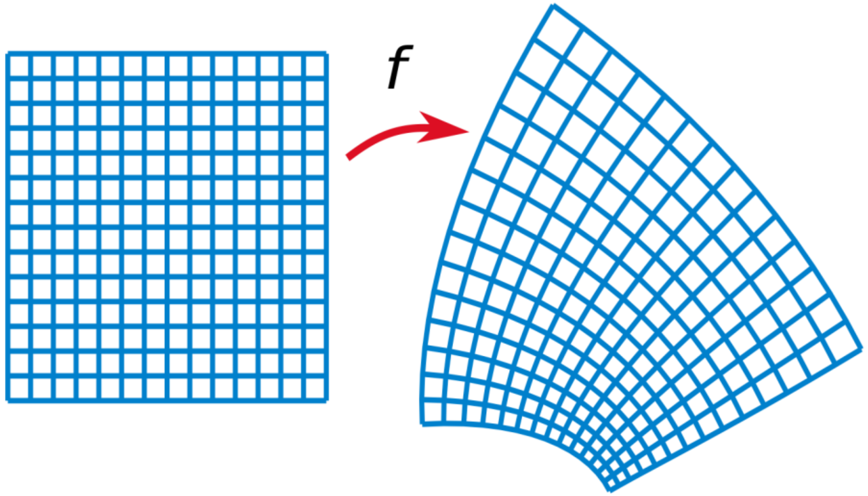
contents

1. Narain CFT

CFT

- A conformal field theory (CFT) is a quantum field theory that is invariant under conformal transformations.

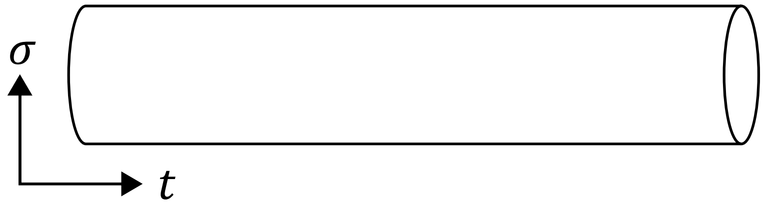
= angle preserving :



- A two-dimensional CFT has rich mathematical structure and is used to describe condensed matter, critical phenomena, and string theory.

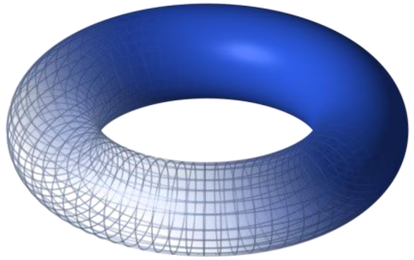
Narain CFT

- We consider "a closed string" : $X(t,\sigma),\ \sigma \cong \sigma + 2\pi$



- A Narain CFT is a 2d CFT that describes a closed string on the compactified space :

$$X^i \cong X^i + 2\pi R,\ R : \text{radius},\ i = 1, \dots, n$$



$T^{n=2}$

- The action :

$$S = \frac{1}{4\pi\alpha'} \int dt \int_0^{2\pi} d\sigma \left[G_{ij} \left(\partial_t X^i \partial_t X^j - \partial_\sigma X^i \partial_\sigma X^j \right) - 2 B_{ij} \partial_t X^i \partial_\sigma X^j \right]$$

G_{ij} : metric, B_{ij} : antisymmetric background

Effects of the compactification

- The center-of-mass momentum P

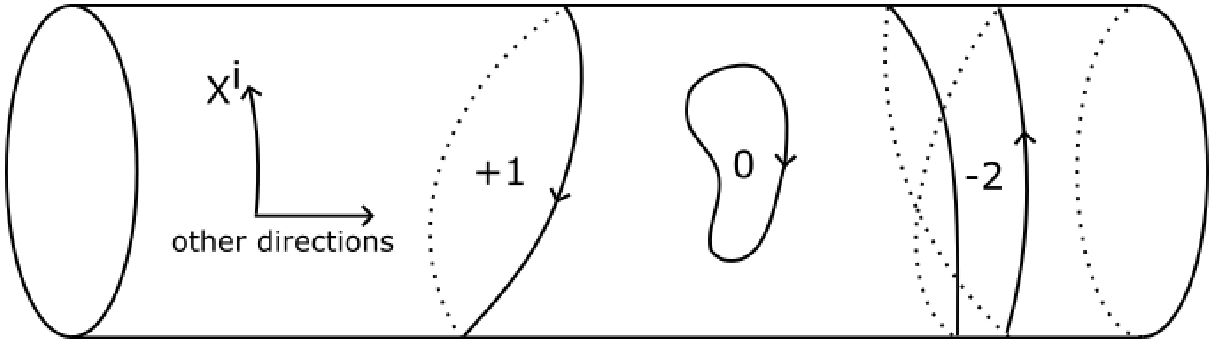
- The operator $\exp(2\pi i R\widehat{P_i})$, which translates strings once around the i-th direction, must be the identity for states.

$$P_i := \frac{\partial L}{\partial(\partial_t X^i)} = \frac{1}{R} m_i, \qquad m_i \in \mathbb{Z} \qquad ①$$

- winding number w

- A string can wind around the compact direction.

$$X^i(t,\sigma) - X^i(t,\sigma + 2\pi) = 2\pi R w^i, \qquad w^i \in \mathbb{Z} \qquad ②$$



Momentum

- From the equation of motion, the mode expansion of X^i is

$$X^i(t,\sigma) = X_L^i(t-\sigma) + X_R^i(t+\sigma),$$

$$X_L^i(t-\sigma) = \hat{x}_L^i + \frac{\alpha'}{2}\hat{p}_L^i(t-\sigma) + i\sqrt{\frac{\alpha'}{2}}\sum_{n\in\mathbb{Z}\setminus\{0\}}\frac{\hat{\alpha}_n^i}{n}e^{-in(t-\sigma)},$$

$$X_R^i(t+\sigma) = \hat{x}_R^i + \frac{\alpha'}{2}\hat{p}_R^i(t+\sigma) + i\sqrt{\frac{\alpha'}{2}}\sum_{n\in\mathbb{Z}\setminus\{0\}}\frac{\hat{\tilde{\alpha}}_n^i}{n}e^{-in(t+\sigma)}$$

- By substituting these for ①②, eigenvalues of $\hat{p}_L, \hat{p}_R$ on orthogonal basis are

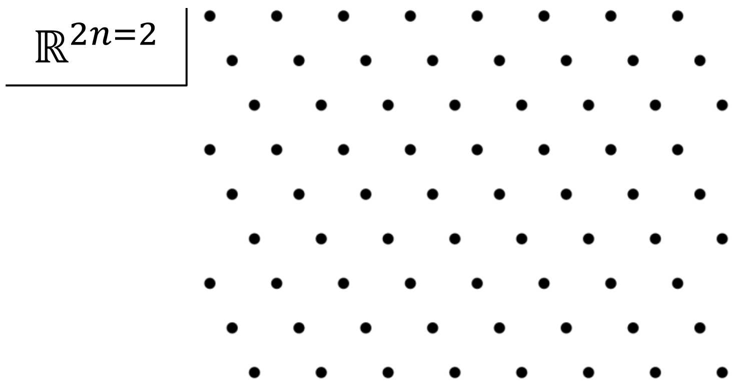
$$k_{L\mu} = e_\mu^i\left[\frac{1}{R}m_i + \frac{R}{2}(B+G)_{ij}w^j\right],\quad k_{R\mu} = e_\mu^i\left[\frac{1}{R}m_i + \frac{R}{2}(B-G)_{ij}w^j\right],$$

e_μ^i : tetrad $\left(G_{ij}e_\mu^i e_\nu^j = \delta_{\mu\nu}\right)$

A lattice from a Narain CFT

- The momenta form a lattice :

$$\Lambda(R,G,B) = \left\{ \begin{pmatrix} \overrightarrow{k_L} \\ \overrightarrow{k_R} \end{pmatrix} \middle| \vec{m}, \vec{w} \in \mathbb{Z}^n \right\} \subset \mathbb{R}^{2n}$$



- For later convenience, we define another lattice.

$$\Lambda_N(R,G,B) = \left\{ \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \middle| \vec{m}, \vec{w} \in \mathbb{Z}^n \right\} \subset \mathbb{R}^{2n},$$

← We will associate a code with this lattice

$$\alpha_\mu = \frac{k_{L\mu} + k_{R\mu}}{\sqrt{2}} = e_\mu^i \left[\frac{\sqrt{2}}{R} m_i + \frac{R}{\sqrt{2}} B_{ij} w^j \right],$$

$$\beta_\mu = \frac{k_{L\mu} - k_{R\mu}}{\sqrt{2}} = e_\mu^i \frac{R}{\sqrt{2}} G_{ij} w^j.$$

Even self-duality

- **Prop.** The lattice $\Lambda_N(R,G,B)$ is even and self-dual with a metric

$$g = \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix}.$$

● Even

- A lattice Λ is even $:\Leftrightarrow \forall x \in \Lambda, x \cdot x \in 2\mathbb{Z}$

● Self-dual

- A dual lattice of $\Lambda \subset \mathbb{R}^n$: $\Lambda^* = \{x' \in \mathbb{R}^n | \forall x \in \Lambda, x \cdot x' \in \mathbb{Z}\}$
- A lattice Λ is self-dual $:\Leftrightarrow \Lambda = \Lambda^*$

- We can verify these properties directly.

Proof (even)

- (A lattice Λ is even $:\Leftrightarrow \forall x \in \Lambda, x \cdot x \in 2\mathbb{Z}$)

$$\alpha_\mu = \frac{k_{L\mu}+k_{R\mu}}{\sqrt{2}} = e_\mu^i \left[\frac{\sqrt{2}}{R} m_i + \frac{R}{\sqrt{2}} B_{ij} w^j\right],$$
$$\beta_\mu = \frac{k_{L\mu}-k_{R\mu}}{\sqrt{2}} = e_\mu^i \frac{R}{\sqrt{2}} G_{ij} w^j.$$

- For $\forall x = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \in \Lambda_N(R, G, B)$,

$$x \cdot x = (\alpha^T \quad \beta^T) \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = 2\alpha^T \beta = 2m_i G_{ij} w^j + R^2 B_{ij} w^i w^j = 2m_i w^i$$

B is antisymmetric → vanishes

Spectrum

$\alpha_\mu = \frac{k_{L\mu}+k_{R\mu}}{\sqrt{2}}$,
$\beta_\mu = \frac{k_{L\mu}-k_{R\mu}}{\sqrt{2}}$

- We can describe important quantities of the CFT in the language of the lattice.
- The spectral gap (of primary states) = the energy difference between its ground state and first excited state :

$$\Delta = \min_{\substack{(\vec{k_L},\vec{k_R})\in\Lambda(R,G,B) \\ (\vec{k_L},\vec{k_R})\neq 0}} \frac{\vec{k_L}^2 + \vec{k_R}^2}{2} = \min_{\substack{(\alpha,\beta)\in\Lambda_N(R,G,B) \\ (\alpha,\beta)\neq\vec{0}}} \frac{\alpha^2+\beta^2}{2}$$

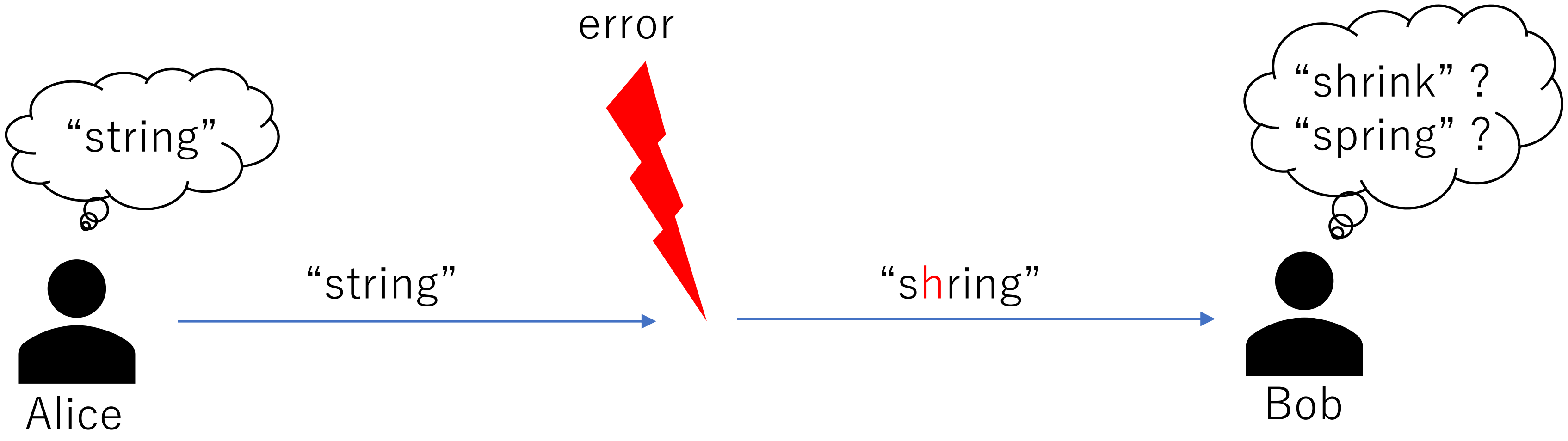
- The partition function $= \mathrm{Tr}_{\mathrm{states}}[\exp(2\pi i\tau_1 P - 2\pi\tau_2 H)]$:

$$Z(\tau) = |\eta(\tau)|^{-2n} \sum_{(\vec{k_L},\vec{k_R})\in\Lambda(R,G,B)} q^{\vec{k_L}^2/2}\bar{q}^{\vec{k_R}^2/2}$$
$$= |\eta(\tau)|^{-2n} \sum_{(\alpha,\beta)\in\Lambda_N(R,G,B)} q^{(\alpha+\beta)^2/4}\bar{q}^{(\alpha-\beta)^2/4}$$

$\eta(\tau)$: Dedekind eta function,
$q = e^{2\pi i\tau}, \qquad \bar{q} = e^{-2\pi i\bar{\tau}}$

2. Error correcting code

Error correcting code



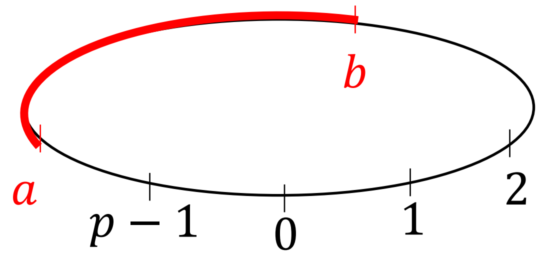
- An error correcting code is a concept in information theory for transmitting information correctly in spite of errors.

Finite field

- A finite field F is a field that contains a finite number of elements, which is a prime p or a prime power p^l.

- For a prime p, $F_p = \mathbb{Z}/p\mathbb{Z} = \{0,1,\dots,p-1\}$
- We define a distance d between $a, b \in F_p^n$ by

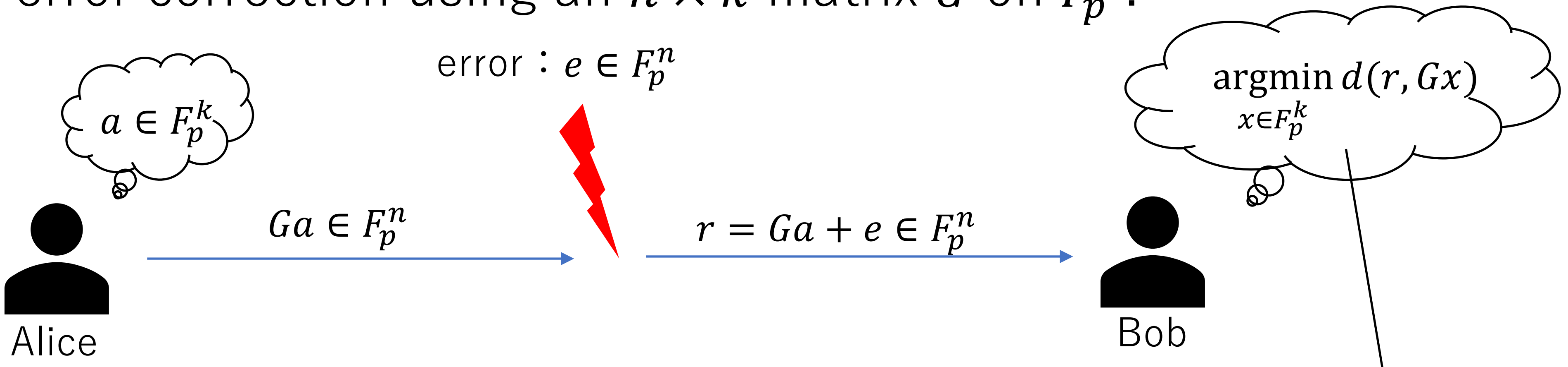
$$d(a,b) = \sqrt{\sum_{i=1}^{n} |a_i - b_i|^2}, \qquad |a_i - b_i| = \min\{a_i - b_i, b_i - a_i\}\,(\in \mathbb{Z})$$



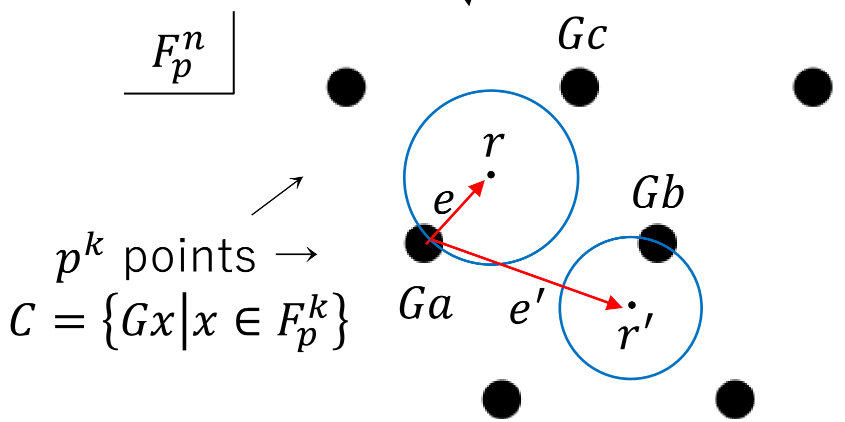
Error correction

$n > k$

- The error correction using an $n \times k$ matrix G on F_p :



- We call $C = \{Gx | x \in F_p^k\} \subset F_p^n$ a code.



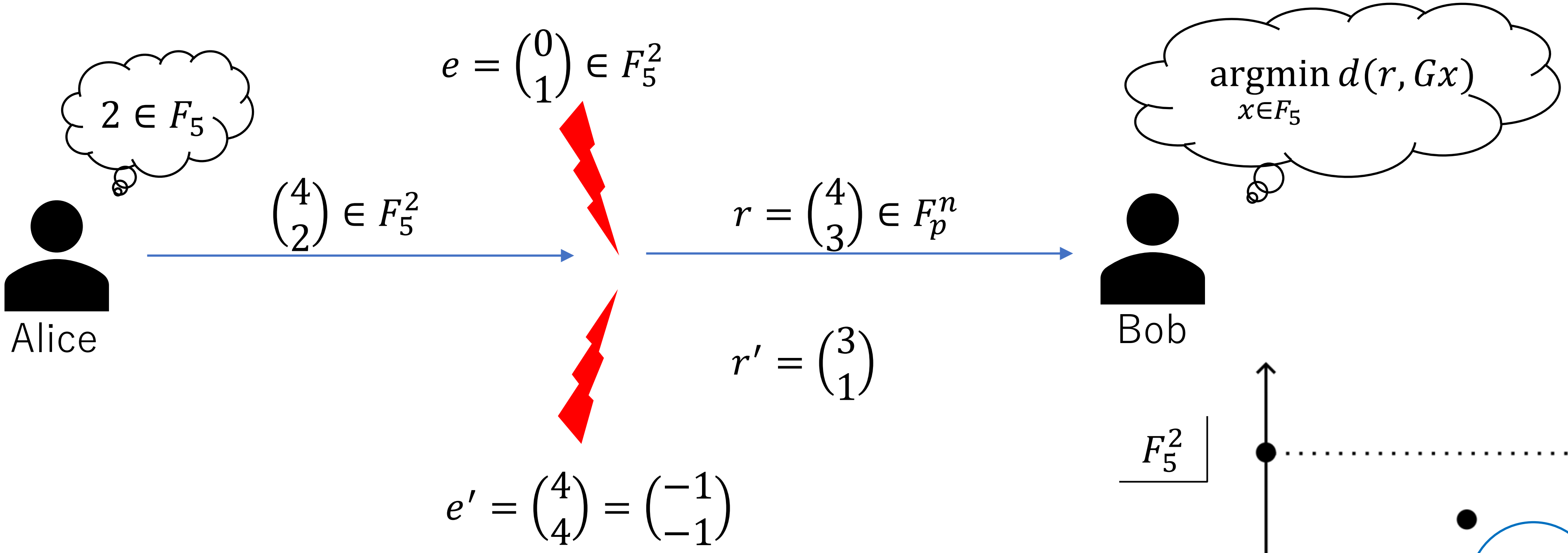
- Bob can get the correct message if

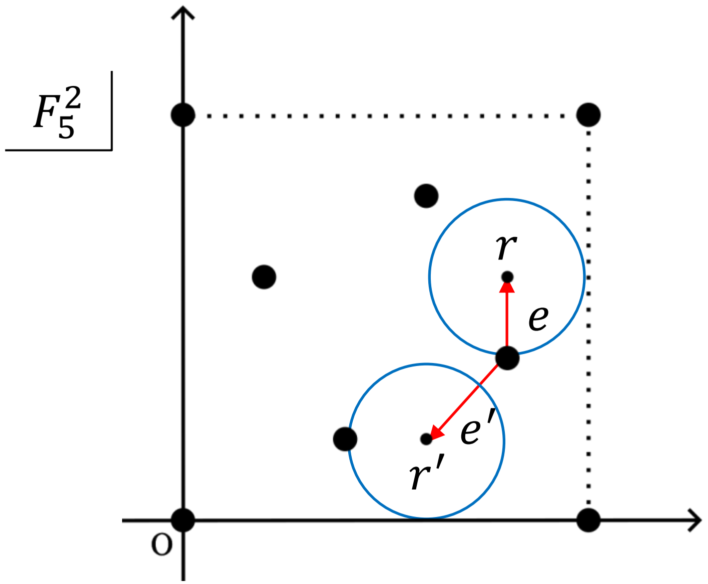
$$2d(e, 0) < D(C) \coloneqq \min_{c, c' \in C, c \neq c'} d(c, c')$$

→ $D(C)$: error correction capability

Example : A code on $\boldsymbol{F_5}$

- $G = \begin{pmatrix}2\\1\end{pmatrix} \to C = \left\{\begin{pmatrix}0\\0\end{pmatrix}, \begin{pmatrix}2\\1\end{pmatrix}, \begin{pmatrix}4\\2\end{pmatrix}, \begin{pmatrix}1\\3\end{pmatrix}, \begin{pmatrix}3\\4\end{pmatrix}\right\} \subset F_5^2, \quad D(C) = \sqrt{2^2 + 1^2} = \sqrt{5}$





- Bob can correct e but not e'.

$$2d(e) = 2 \ < \ D(C) = \sqrt{5} \ < \ 2d(e') = 4$$

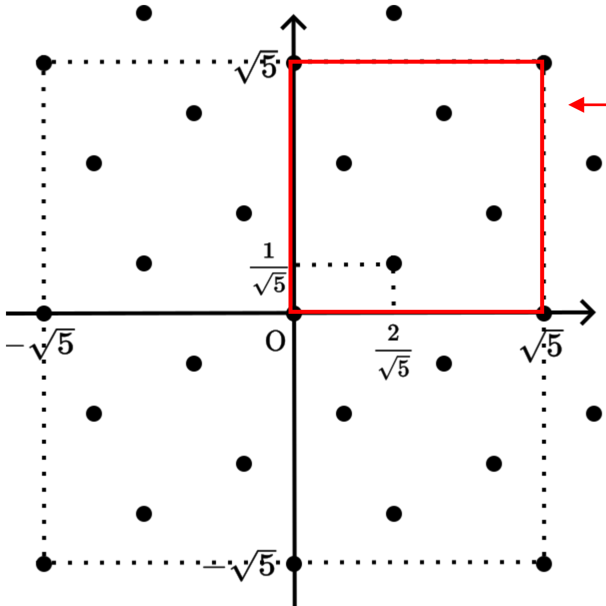
A lattice from a code

- We construct a lattice from a code $C \subset F_p^n$ by

$$\Lambda_p(C) = \left\{ \frac{c + pm}{\sqrt{p}} \,\middle|\, c \in C, m \in \mathbb{Z}^n \right\} \subset \mathbb{R}^n$$

- e.g. For $C = \left\{ \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \end{pmatrix}, \begin{pmatrix} 4 \\ 2 \end{pmatrix}, \begin{pmatrix} 1 \\ 3 \end{pmatrix}, \begin{pmatrix} 3 \\ 4 \end{pmatrix} \right\} \subset F_5^2$,

$\Lambda_5(C) =$



corresponds to F_5^2

Even self-duality

- The case $p = 2$ was studied by Dymarsky and Shapere [1].
- **Prop.** For $p > 2$, the lattice $\Lambda_p(C)$ is even and self-dual with the metric $g = \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix}$ if and only if C is self-dual.

● Self-dual

on F_p ↙

- A dual code of $C \subset F_p^n$: $C^* = \left\{ c' \in F_p^n \middle| \forall c \in C, c \cdot c' = 0 \right\}$
- A code C is self-dual :⇔ $C = C^*$
- e.g. A code on F_5 generated by $G = \begin{pmatrix} 1 & 2 \\ 2 & 3 \\ 4 & 1 \\ 3 & 1 \end{pmatrix}$ is self-dual.

$$\because \begin{pmatrix} 1 \\ 2 \\ 4 \\ 3 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 2 \\ 4 \\ 3 \end{pmatrix} = 1*4+2*3+4*1+3*2 = 0, \quad \begin{pmatrix} 1 \\ 2 \\ 4 \\ 3 \end{pmatrix} \cdot \begin{pmatrix} 2 \\ 3 \\ 1 \\ 1 \end{pmatrix} = 1*1+2*1+4*2+3*3 = 0 \text{ etc.}$$

Proof (self-dual)

- The dual lattice of the code is the lattice of the dual code.

$$
\begin{aligned}
\because \quad & x' \in (\Lambda_p(\mathcal{C}))^* \\
& \Leftrightarrow \forall x \in \Lambda_p(\mathcal{C}), x \cdot x' \in \mathbb{Z} \\
& \Leftrightarrow \forall c \in \mathcal{C}, \forall m \in \mathbb{Z}^{2n}, \frac{1}{\sqrt{p}}(R(c) + pm) \cdot x' \in \mathbb{Z} \\
& \Leftrightarrow \exists c' \in F_p^{2n}, \exists m' \in \mathbb{Z}^{2n}, x' = \frac{1}{\sqrt{p}}(R(c') + pm') \text{ and} \\
& \quad \forall c \in \mathcal{C}, \forall m \in \mathbb{Z}^{2n}, \frac{1}{p}(R(c) + pm) \cdot (R(c') + pm') \in \mathbb{Z} \\
& \Leftrightarrow \exists c' \in \mathcal{C}^*, \exists m' \in \mathbb{Z}^{2n}, x' = \frac{1}{\sqrt{p}}(R(c') + pm') \\
& \Leftrightarrow x' \in \Lambda_p(\mathcal{C}^*)
\end{aligned}
$$

R is a map : $F_p \to \mathbb{Z}$

- Thus, $\left(\Lambda_p(C)\right)^* = \Lambda_p(C) \Leftrightarrow C^* = C$.

Self-dual code

- **Prop.** A code $C \subset F_p^n$ is self-dual if and only if n is even and C is generated by

$$G = \begin{pmatrix} I \\ X \end{pmatrix}$$

(up to swapping rows)

where X is an $\frac{n}{2} \times \frac{n}{2}$ matrix s.t. $X + X^T = 0$ on F_p

- For the example on the previous page,

$$C = \left\{ \begin{pmatrix} 1 & 2 \\ 2 & 3 \\ 4 & 1 \\ 3 & 1 \end{pmatrix} x \,\middle|\, x \in F_5^2 \right\} = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 2 \\ 3 & 0 \end{pmatrix} y \,\middle|\, y \in F_5^2 \right\} \subset F_5^4$$

3. Relation

Relation through lattices

- Now, we constructed even self-dual lattices from a Narain CFT and a self-dual code.
- The simplest relation is the case where they form the same lattice.

- **Prop.** If a code $C \subset F_p^{2n}$ is generated by $G = \binom{I}{X}$ where X is an $n \times n$ matrix s.t. $X + X^T = 0$,

$$\Lambda_N\left(R = \sqrt{\frac{2}{p}}, G = I, B = X\right) = \Lambda_p(C) \subset \mathbb{R}^{2n}$$

$\nearrow$ compactification radius $\quad\uparrow$ metric $\quad\nwarrow$ antisymmetric background

$\because$ Both lattices can be written as $\left\{\begin{pmatrix}\sqrt{p}I & \frac{1}{\sqrt{p}}X \\ 0 & \frac{1}{\sqrt{p}}I\end{pmatrix} y \,\middle|\, y \in \mathbb{Z}^{2n}\right\}$.

Correspondence in both theories

- Using this relation, we can consider the spectrum and the symmetries of the CFT in the language of the code.

- (rough summary in [3])

	CFT	Lattice Λ	Code $\mathcal{C}$
	modular invariance	even self-dual	self-dual
n	central charge	dimension	length
p	compactification radii $\sqrt{2/p}$	$\sqrt{p}\mathbb{Z}^{2n} \subset \Lambda$	on the finite field with p elements
	spectral gap	minimum length	correction capability
	partition function		enumerator polynomial

Partition function

- The partition function $Z(\tau)$ of the CFT can be written as the extended enumerator polynomial of the code.

$$Z(\tau) = |\eta(\tau)|^{-2n} \sum_{c \in C} \prod_{x,y \in F_p} \left(t_{x,y}\right)^{w_{x,y}(c)},$$

$$t_{x,y} = \sum_{m,l \in \mathbb{Z}} q^{\left(x+y+p(m+l)\right)^2/4p} \, \bar{q}^{\left(x-y+p(m-l)\right)^2/4p},$$

$$w_{x,y}(c) = |\{i \in \{1, \dots, n\} | (c_i, c_{i+n}) = (x, y)\}|$$

← code dependency

If $c = (1,2,2,3,1,1)^T \subset F_p^6$,
$w_{1,3}(c) = 1, w_{2,1}(c) = 2,$
the others : 0

- We can relate

  a symmetry of the CFT that keeps $Z(\tau)$ invariant to

  a symmetry of the code that keeps polynomial invariant,

which have been studied separately.

Proof

$$
\begin{aligned}
&|\eta(\tau)|^{2n} Z(\tau) \\
&= \sum_{x\in\Lambda_N(r,I,B)} q^{\sum_{i=1}^{n}(x_i+x_{i+n})^2/4}\bar{q}^{\sum_{i=1}^{n}(x_i-x_{i+n})^2/4} \\
&= \sum_{y\in\Lambda_p(\mathcal{C})} q^{\sum_{i=1}^{n}(y_i+y_{i+n})^2/4}\bar{q}^{\sum_{i=1}^{n}(y_i-y_{i+n})^2/4} \\
&= \sum_{c\in\mathcal{C}} \sum_{m\in\mathbb{Z}^{2n}} \prod_{i=1}^{n} q^{(R(c_i)+pm_i+R(c_{i+n})+pm_{i+n})^2/4p}\bar{q}^{(R(c_i)+pm_i-R(c_{i+n})-pm_{i+n})^2/4p} \\
&= \sum_{c\in\mathcal{C}} \prod_{i=1}^{n} \sum_{m,l\in\mathbb{Z}} q^{(R(c_i)+R(c_{i+n})+p(m+l))^2/4p}\bar{q}^{(R(c_i)-R(c_{i+n})+p(m-l))^2/4p}.
\end{aligned}
$$

Spectral gap

- The spectral gap Δ of the CFT and the error correction capability $D(C)$ of the code satisfy

$$\Delta = \frac{1}{2p}\min\{D(C)^2, p^2\}$$

← In most cases, $D(C)^2 < p^2$

- → Searching for the code with high correction capability
  = Searching for the Narain CFT with large spectral gap

include CFTs not related to codes ↙

- The largest spectral gap among all Narain CFTs with n scalars is not well known for general n.
- Is this relation helpful?

Proof

$$\Delta = \min_{\substack{x \in \Lambda_N(r,I,B) \\ x \neq 0}} \frac{1}{2} x^T x = \min_{\substack{y \in \Lambda_p(\mathcal{C}) \\ y \neq 0}} \frac{1}{2} y^T y$$

$$= \min_{\substack{c \in \mathcal{C}, m \in \mathbb{Z}^{2n} \\ R(c)+pm \neq 0}} \frac{1}{2} \sum_{i=1}^{2n} \left(\frac{R(c_i) + pm_i}{\sqrt{p}} \right)^2$$

R is a map : $F_p \to \mathbb{Z}$

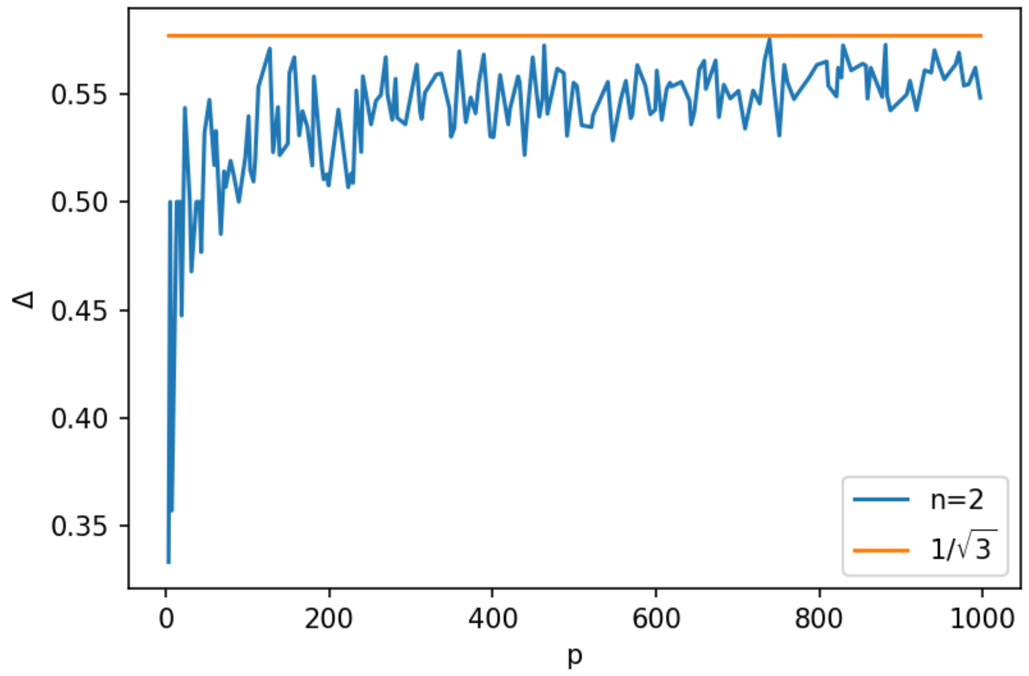
$$= \frac{1}{2p} \min \left\{ \min_{\substack{c \in \mathcal{C}, m \in \mathbb{Z}^{2n} \\ c \neq 0}} \sum_{i=1}^{2n} (R(c_i) + pm_i)^2, \min_{\substack{m \in \mathbb{Z}^{2n} \\ m \neq 0}} \sum_{i=1}^{2n} (pm_i)^2 \right\}$$

$$= \frac{1}{2p} \min \left\{ \min_{\substack{c \in \mathcal{C} \\ c \neq 0}} \sum_{i=1}^{2n} \min\{R(c_i)^2, (R(c_i) - p)^2\}, p^2 \right\}$$

$$= \frac{1}{2p} \min \left\{ D(\mathcal{C})^2, p^2 \right\}.$$

Spectral gap, $n = 2$

- From numerical calculations, the largest spectral gap of Narain CFTs corresponding to codes on F_p^2 is as follows :



- The values suggest that $1/\sqrt{3}$ is their upper bound, which can be checked analytically by reducing to the sphere packing in two dim.

Spectral gap, $n = 3$

- For $a \in \mathbb{Z}$ s.t. $p = (a^4 + 1)/2$ is a prime number, we consider a code C on F_p generated by

$$G = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & -a & -a^2 \\ a & 0 & -a^3 \\ a^2 & a^3 & 0 \end{pmatrix}.$$

- The error correction capability :

$$D(C) = \left| G \begin{pmatrix} (a-1)/2 \\ (a-1)/2 \\ 0 \end{pmatrix} \right| = \sqrt{(3a^4 - 4a^3 + 6a^2 - 4a + 3)/4}$$

- The spectral gap of the corresponding CFT :

$$\Delta = \frac{1}{2p} \min\{D(C)^2, p^2\} = \frac{(3a^4 - 4a^3 + 6a^2 - 4a + 3)}{4(a^4 + 1)} \xrightarrow[a \to \infty]{} \frac{3}{4}$$

← The largest known spectral gap for $n = 3$ [2] !

4. Future prospects

Code on finite field F_{p^l}

- We considered only finite fields with prime elements.

- For a prime power p^l, $F_{p^l} = F_p[x]/(f_{p,l}(x)) = \{\sum_{t=0}^{l-1} a_t x^t \mid a_t \in F_p\}$

  ↗ polynomial ring on F_p ↖ Conwey polynomial

- E.g. $F_{3^2} = F_3[x]/(x^2 + 2x + 2) = \{a_2 x^2 + a_1 x + a_0 \mid a_2, a_1, a_0 \in F_3\}$

  $(x^2 + 1) \times (x + 2) = x^3 + 2x^2 + x + 2 = 2x + 2$

- It is difficult to relate a code on F_{p^l} to a self-dual lattice than on F_p.

  → Can it correspond to a more general CFT?

Spectral gap for large $\boldsymbol{n}$

- Through the correspondence between quantum gravity and CFT, the spectral gap corresponds to the energy difference in gravity theory.

- We do not know

  the largest spectral gap and

  how to construct a CFT with large spectral gap

  for large n.

- Can we answer these using the relation between CFTs and codes?

Thank you for listening.

References

[1] A. Dymarsky and A. Shapere, *Quantum stabilizer codes, lattices, and CFTs*, J. High Energ. Phys. 2021, 160 (2021) [arXiv:2009.01244].

[2] N. Afkhami-Jeddi, H. Cohn, T. Hartman and A. Tajdini, *Free partition functions and an averaged holographic duality*, J. High Energ. Phys. 2021, 130 (2021) [arXiv:2006.04839].

[3] Shinichiro Yahagi, *Narain CFTs and error-correcting codes on finite fields*, arXiv:2203.10848.