Title: Quantum codes, lattices, and CFTs

Speakers: Anatoly Dymarsky

Series: Quantum Fields and Strings

Date: November 25, 2020 - 11:00 AM

URL: http://pirsa.org/20110066

Abstract: There is a deep relation between classical error-correcting codes, Euclidean lattices, and chiral 2d CFTs. We show this relation extends to include quantum codes, Lorentzian lattices, and non-chiral CFTs. The relation to quantum codes provides a simple way to solve modular bootstrap constraints and identify interesting examples of conformal theories. In particular we construct many examples of physically distinct isospectral theories, examples of "would-be" CFT partition function -- non-holomorphic functions satisfying all constraints of the modular bootstrap, yet not associated with any

known CFT, and find theory with the maximal spectral gap among all Narain CFTs with the central charge c=4. At the level of code theories the problem of finding maximal spectral gap reduces to the problem of finding optimal code, leading to "baby bootstrap" program. We also discuss averaging over the ensemble of all CFTs associated with quantum codes, and its possible holographic interpretation. The talk is based on arXiv:2009.01236 and arXiv:2009.01244.

Codes & CFTs
Nov 11, 2020 at 12:00 PM

Quantum codes, lattices, and CFTs

Anatoly Dymarsky

University of Kentucky

in collaboration with Al Shapere

QI/Strings seminar,
PI, November 25, 2020

Plan of the talk

- Classical codes, Euclidean lattices, chiral CFTs
- Quantum codes, Lorentzian lattices, non-chiral CFTs
- Applications: specific examples, "baby bootstrap," averaging over codes and AdS/CFT

What is code?

$n(n-1)/2$

$A \to$ Apple

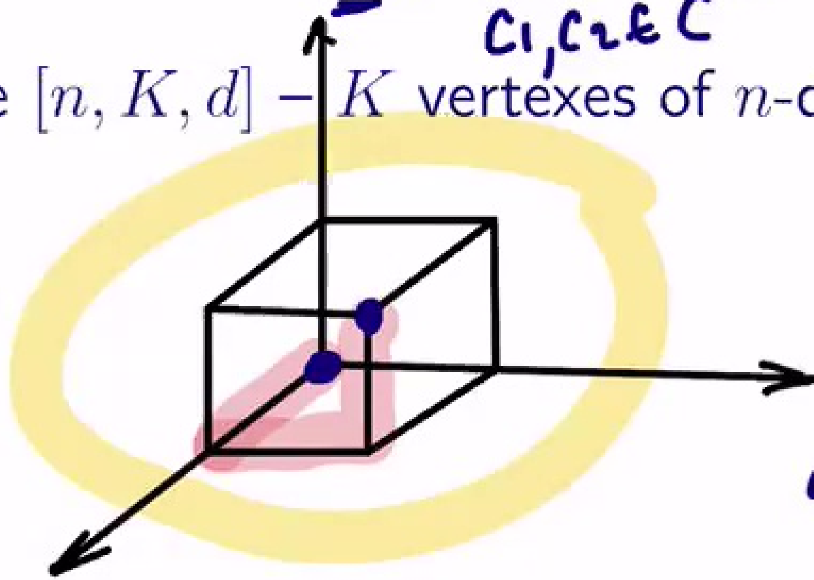
- examples: $\boxed{\text{Morse code}}$, NATO phonetic alphabet

$B \to$ BRAVO

- binary code $[n, K, d]$ – K codewords, each is a binary string of length n

$d = \min_{c_1, c_2 \in C} d(c_1, c_2)$: 2 –

- binary code $[n, K, d]$ – K vertexes of n-dimensional cube



$3 = d((0,0,0),(1,1,1))$

$\shortparallel$

e^2

$\underbrace{0 \ldots 1 \ldots 1}$

$d(c_1, c_2) = \#$ bit to flip

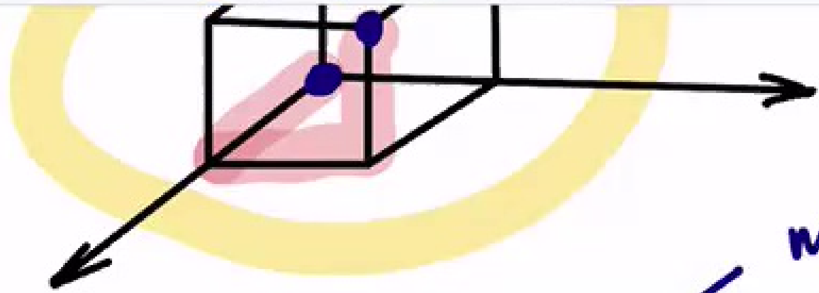
- binary linear code $\mathcal{C} \ni c(x) = G\,x$, $c \in (\mathbb{Z}_2)^n$, $x \in (\mathbb{Z}_2)^k$

$d \sim n$ $\quad \log_2 K/n$ – fixed $\quad n \to \infty \quad \max d/n$

$3 = d((0,0,0),(1,1,1))$

$\shortparallel$

e^2



mod 2

- binary linear code $\mathcal{C} \ni c(x) = Gx$, $c \in (\mathbb{Z}_2)^n$, $x \in (\mathbb{Z}_2)^k$

over $GF_2 \equiv \{0, 1\}$

$c_1, c_2 \in C$

$2^k = K$

$c_1 + c_2 \in C$

$1 \quad 2^k$

Code technicalities

$$c = (x_1 c_1 + \ldots + x_k c_k) \bmod 2$$

$x = \{0, 1\}$

- enumerator polynomial

$$W_{\mathcal{C}}(x, y) = \sum_{c \in \mathcal{C}} x^{n - \mathrm{w}(c)} y^{\mathrm{w}(c)}$$

counts number of codewords of given weight $\mathrm{w}(c)$

3 / 20

6:27 PM Wed Nov 25

$c_1, c_2 \in C$

$c_1 + c_2 \in C$

$2^k = K$

Code technicalities

- enumerator polynomial

$$W_{\mathcal{C}}(x,y) = \sum_{c \in \mathcal{C}} x^{n-\mathrm{w}(c)} y^{\mathrm{w}(c)}$$

counts number of codewords of given weight $\mathrm{w}(c)$

- even code: $\mathrm{w}(c)$ are even; double-even code: $\mathrm{w}(c) \vdots 4$

- self-dual code $\mathcal{C}^* = \mathcal{C}$

$$W_{\mathcal{C}}(x,y) = W_{\mathcal{C}}\left(\frac{x+y}{\sqrt{2}}, \frac{x-y}{\sqrt{2}}\right)$$

3 / 20

$c_1 + c_2 \in C$

Code technicalities

$\vec{c}^{\,2}$ - even.

- enumerator polynomial

$y^2, y^4, \ldots$

$$W_{\mathcal{C}}(x,y) = \sum_{c\in\mathcal{C}} x^{n-\mathrm{w}(c)} y^{\mathrm{w}(c)}$$

counts number of codewords of given weight $\mathrm{w}(c) = \vec{c}^{\,2}$

$W(x,y) = W(x,-y)$

- even code: $\mathrm{w}(c)$ are even; double-even code: $\mathrm{w}(c) \vdots 4$

$W(x,y) = W(x,iy)$

- self-dual code $\mathcal{C}^* = \mathcal{C}$

$(\vec{c}_1 \cdot \vec{c}_2 \bmod 2)$

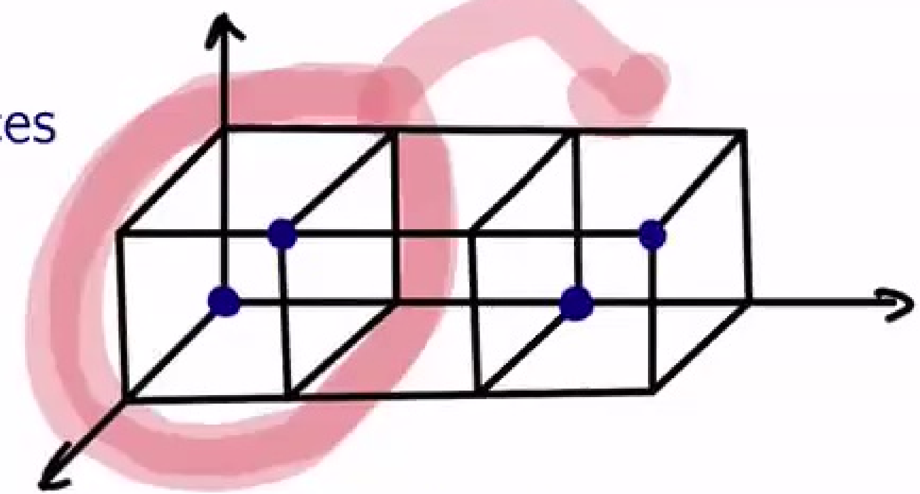
$$\boxed{W_{\mathcal{C}}(x,y) = W_{\mathcal{C}}\left(\frac{x+y}{\sqrt{2}}, \frac{x-y}{\sqrt{2}}\right)}$$

4 / 20

MacWilliams identity

Codes and lattices

- binary codes $\to$ lattices



placing unit cubes at each even coordinate points

$$\Lambda(\mathcal{C}) = \{ v/\sqrt{2} \,|\, v \bmod 2 \in \mathcal{C} \}$$

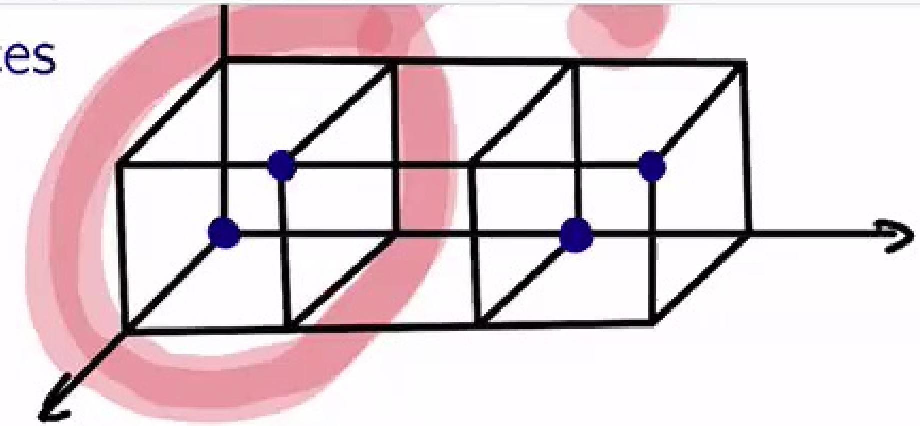
Construction A

$v = (v_1 \ldots v_n) \bmod 2$

$(0, 1, \ldots)$

- double-even code $\to$ even lattice

- binary codes $\to$ lattices



placing unit cubes at each even coordinate points

$$\Lambda(\mathcal{C}) = \{v/\sqrt{2}\,|\,v \bmod 2 \in \mathcal{C}\}$$

Construction A

$v = (v_1 \ldots v_n) \bmod 2$

$(0, 1, \ldots)$

- double-even code $\to$ even lattice
- self-dual code $\to$ self-dual lattice

$(\vec{x})^2$ - integer $\times 2$

even $\to$ $x \in \Lambda$

$\Lambda = \Lambda^*$

Codes and lattices, and CFTs

$\Lambda = \{ a_1 \vec{e}_1 + \dots + a_n \vec{e}_n ,\ a_i \in \mathbb{Z} \}$

$\vec{e}_1, \dots, \vec{e}_n \in R^n$

- lattice theta-function

$\Lambda^* \ni \vec{y}$

$$\Theta_\Lambda = \sum_{v \in \Lambda} q^{v^2/2}, \qquad q = e^{2\pi i \tau}$$

$\vec{x} \in \Lambda$ $\quad |\vec{x}|^2$ - even

- for Construction A lattices

$\vec{y} \cdot \vec{x} \in \mathbb{Z}$ $\quad \vec{x} \in \Lambda$

$$\Theta_{\Lambda(\mathcal{C})} = W_{\mathcal{C}}(\theta_3(q^2), \theta_2(q^2))$$

$\Lambda \subset \Lambda^*$

$x, y \in \Lambda$ $\quad \vec{x} \cdot \vec{y} \in \mathbb{Z}$

- double-even s.-d. codes $\to$ even s.-d. lattices $\to$ chiral CFTs

enumerator $\to$ theta-function $\to$ partition function

modular invariance:

$\tau \to \tau + 1: \quad W_{\mathcal{C}}(x, y) = W_{\mathcal{C}}(x, iy)$

$y \cdot x \in \mathbb{Z}$

$\Theta_{\Lambda(\mathcal{C})} = W_{\mathcal{C}}(\theta_3(q^2), \theta_2(q^2))$

$\vec{x} \in \Lambda$

- double-even s.-d. codes → even s.-d. lattices → chiral CFTs

  enumerator → theta-function → partition function

  modular invariance:

  $\tau \to \tau + 1$: $W_{\mathcal{C}}(x, y) = W_{\mathcal{C}}(x, iy)$

  $\tau \to -1/\tau$: MacWilliams identity

$PSL_2(\mathbb{Z})$

A few examples

- n=8: unique Hamming $[8, 4, 4]$ code e_8,
  unique root lattice E_8,
  unique $W_{e_8}(x, y) = x^8 + 14x^4y^4 + y^8$,
  unique modular form $E_4 = W_{e_8}(\theta_3(q^2), \theta_2(q^2))$

A few examples

- n=8: unique Hamming $[8,4,4]$ code e_8,
  unique root lattice E_8,
  unique $W_{e_8}(x,y) = x^8 + 14x^4y^4 + y^8$,
  unique modular form $E_4 = W_{e_8}(\theta_3(q^2), \theta_2(q^2))$

- n=16: two codes $e_8 \oplus e_8$, d_{16}^+,
  two lattices $E_8 \oplus E_8$, D_{16}^+,
  unique invariant polynomial $W = W_{e_8}^2$,
  unique modular form E_4^2

- n=24: 9 codes, 24 lattices, two linearly independent modular forms E_4^3, E_6^2, and many dozens of invariant polynomials (mostly "fake")

- self-dual code $\longrightarrow$ self-dual lattice

even $\rightarrow$ $\vec{x} \in \Lambda$ $\quad (\vec{x})^2$ – integer × 2

$\Lambda = \Lambda^*$

Codes and lattices, and CFTs

$Z = \dfrac{\Theta_\Lambda}{\eta(\tau)^n}$

- lattice theta-function

$\Lambda^* \ni \vec{y}$

$$\Theta_\Lambda = \sum_{v \in \Lambda} q^{v^2/2}, \qquad q = e^{2\pi i \tau}$$

- for Construction A lattices

$\vec{y} \cdot \vec{x} \in \mathbb{Z}$

$\vec{x} \in \Lambda$

$$\Theta_{\Lambda(\mathcal{C})} = W_\mathcal{C}(\theta_3(q^2), \theta_2(q^2))$$

- double-even s.-d. codes $\rightarrow$ even s.-d. lattices $\rightarrow$ chiral CFTs

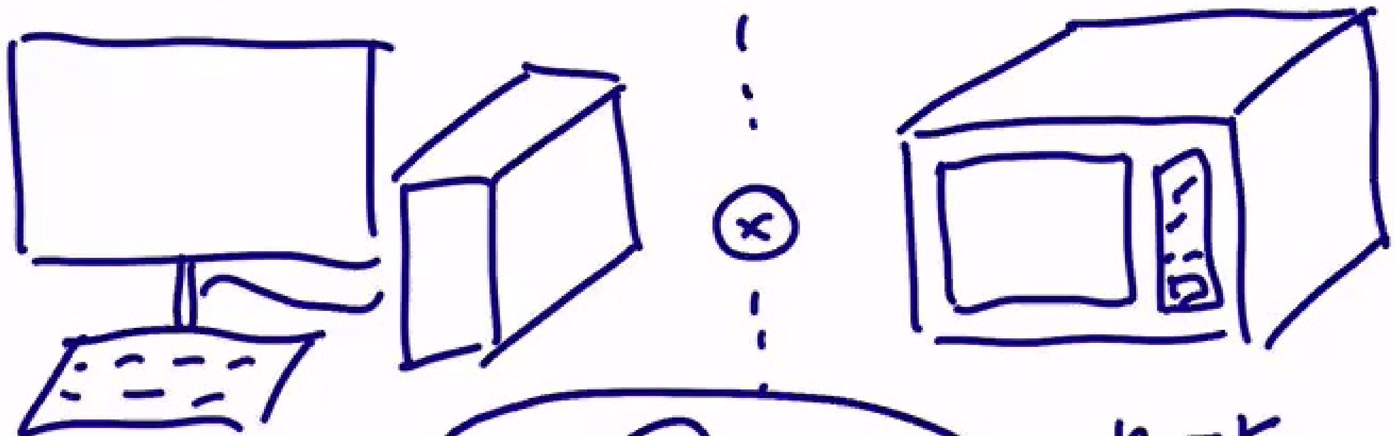
enumerator $\rightarrow$ theta-function $\rightarrow$ partition function

What is quantum code?

$|0\rangle \equiv |\uparrow\rangle$

$|1\rangle \equiv |\downarrow\rangle$

- consider a quantum computer and auxiliary qubits



k $\qquad$ $n-k$

$$|\psi\rangle = |\psi_l\rangle \otimes |0\ldots0\rangle \equiv \mathcal{H}_c$$

- decoherence affects auxiliary qubits

$$|\psi\rangle = |\psi_l\rangle \otimes |s_{k+i}\ldots s_n\rangle$$

$n-k+1 \ldots n$

- but this can be trivially fixed by syndrome measurement

σ_z^{k+i} $\quad$ 6x

6:49 PM Wed Nov 25

What is quantum code?

$|\psi\rangle \in$ n spin

- syndrome measurement operators $\sigma_z^{k+i} \to g_i = U\sigma_z^{k+i}U^\dagger$

  $(n-k)$

- code subspace

$$\mathcal{H}_{\text{code}} \ni U(|\psi_l\rangle \otimes |0\ldots\rangle)$$

stabilizer codes

- g_i generate abelian stabilizer group

$$g_i\, g_j = g_j\, g_i, \qquad g_i^2 = 1,$$

$$g_i \mathcal{H}_{\text{code}} = \mathcal{H}_{\text{code}}$$

- generators g_i belong to Pauli group

$$g_i = g(\vec{\alpha}_i, \vec{\beta}_i) = \epsilon \left((\sigma_x)^{\alpha_i^1} \otimes (\sigma_x)^{\alpha_i^n} \right) \left((\sigma_z)^{\beta_i^1} \otimes (\sigma_z)^{\beta_i^n} \right)$$

8 / 20

6:55 PM Wed Nov 25

stabilizer codes

- g_i generate abelian stabilizer group

$1 = (\sigma_x)^0 (\sigma_z)^0$

$\sigma_x = (\sigma_x)^1 (\sigma_z)^0$

$$g_i\, g_j = g_j\, g_i, \quad g_i^2 = 1,$$

$$g_i \mathcal{H}_{\text{code}} = \mathcal{H}_{\text{code}}$$

$g_i =$

$\sigma \otimes \ldots \otimes \sigma$

4^n

- ~~generators g_i belong to Pauli group~~

α, β

$$\boxed{g_i = g(\vec{\alpha}_i, \vec{\beta}_i) = \epsilon \left((\sigma_x)^{\alpha_i^1} \otimes (\sigma_x)^{\alpha_i^n} \right) \left((\sigma_z)^{\beta_i^1} \otimes (\sigma_z)^{\beta_i^n} \right)}$$

- stabilizer group is a vector space of binary "codewords" $\vec{\alpha}_i, \vec{\beta}_i$

$g(\alpha_1, \beta_1)\, g(\alpha_2, \beta_2) = \# g(\alpha_1 + \alpha_2, \beta_1 + \beta_2)$

mod 2

over GF:

$(\vec{\alpha}, \vec{\beta})$

Quantum stabilizer codes

- quantum $[[n, k, d]]$ stabilizer code: $(n-k)$-dimensional binary vector space inside $(\mathbb{Z})^{2n}$, self-orthogonal under

9 / 20

Quantum stabilizer codes

$2n$ over $GF2$

- quantum $[[n,k,d]]$ stabilizer code: $(n-k)$-dimensional binary vector space inside $(\mathbb{Z})^{2n}$, self-orthogonal under scalar product

$\vec{\alpha}_i \cdot \vec{\beta}_j + \vec{\alpha}_j \cdot \vec{\beta}_i \bmod 2 = 0$

$$g_{\mu\nu} = \left(\begin{array}{c|c} 0 & 1 \\ \hline 1 & 0 \end{array}\right)$$

stab. group =

$= \left\{ \begin{array}{l} \text{linear bin. code} \\ \text{length } 2n\ + \\ \text{self-orth.} \end{array} \right.$

- new construction A: $[[n,k,d]]$ stabilizer code $\to$ lattice in $\mathbb{R}^{n,n}$ space

  code is self-dual when $k=0$; self-dual code $\to$ self-dual lattice

  code is real when all g_i are real; real code $\to$ even lattice

$$\begin{pmatrix} + & & & & & \\ & + & & & & \\ & & + & & & \\ & & & - & & \\ & & & & - & \\ & & & & & - \end{pmatrix}$$

lin. code over $GF(4)$

self-cond.

- real self-dual $[[n,0,d]]$ code $\to$ even self-dual lattice in $\mathbb{R}^{n,n}$ $\to$ Narain CFT

Θ_Λ - S. theta fun.

- refined enumerator polynomial $W_{\mathcal{C}}(x,y,z)$ counts codewords: i) affecting p qubits ii) with q matrices σ_y

$$W_{\mathcal{C}}(x,y,z) = \sum_{c=(\vec{\alpha},\vec{\beta})\in C} x^{n-p} y^q z^{p-q}$$

$2^0 = 1$

$Z = \frac{\Theta_\Lambda}{|\eta|^{24}}$

self-dual codes $W_{\mathcal{C}}(x,y,z) = W_{\mathcal{C}}(x',y',z')$ $\quad \tau \to -1/\tau$

real codes $W_{\mathcal{C}}(x,y,z) = W_{\mathcal{C}}(x,-y,z)$ $\quad \tau \to \tau + 1$

- CFT partition function

$$Z(\tau,\bar{\tau}) = \underbrace{W_{\mathcal{C}}\left(b\,\bar{b} + c\,\bar{c}, b\,\bar{b} - c\,\bar{c}, a\,\bar{a}\right)}_{\Theta_\Lambda} / |\eta(\tau)|^{2n}$$

$$g_i = \sigma_x^i \prod_{j=1} (\sigma_z^j)^{\mathrm{B}_{ij}},$$

$$\psi_{\mathcal{C}} = \sum_{\vec{\alpha}} (-1)^{\sum_{i>j} \mathrm{B}_{ij}\alpha_i\alpha_j} |\alpha_1 \ldots \alpha_n\rangle$$

- (code equivalences) T-duality at the level of graphs is edge local complementation (ELC)

$$\Gamma \to \Gamma * i * j * i$$

where $\Gamma \to \Gamma * i$ is local complementation

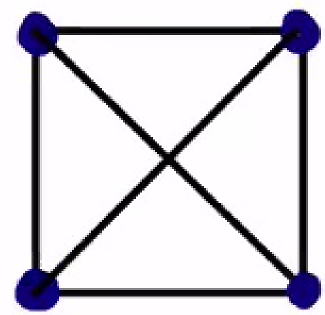
13 / 20

Local complementation and edge local complementation

Application: interesting lattices, special theories

- $n = 4$ code specified by the following graph

$$B = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$$



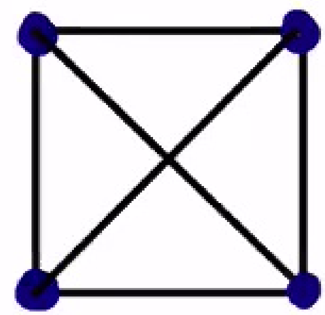
$n=12$

- corresponding lattice is root lattice E_8 understood as even self-dual Lorentzian lattice in $\mathbb{R}^{4,4}$
- corresponding "non-chiral E_8" Narain CFT has maximal spectral gap $\Delta_1 = 1$ among all Narain theories with $c = \bar{c} = 4$
- this is the same theory as 8 free Majorana fermions with the diagonal GSO projection, or $SO(8)_1$ WZW theory

Application: interesting lattices, special theories

- $n = 4$ code specified by the following graph

$$\mathrm{B} = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$$



$\cancel{2^4}$

$n = 12$

$\mathbb{R}^{12,12}$

- corresponding lattice is root lattice E_8 understood as even self-dual Lorentzian lattice in $\mathbb{R}^{4,4}$
- corresponding "non-chiral E_8" Narain CFT has maximal spectral gap $\Delta_1 = 1$ among all Narain theories with $c = \bar{c} = 4$
- this is the same theory as 8 free Majorana fermions with the diagonal GSO projection, or $SO(8)_1$ WZW theory

Application: solving modular bootstrap constraints $z \to W$

- any polynomial W invariant under MacWilliams identity and $y \to -y$ defines modular-invariant $Z(\tau, \bar{\tau})$
- all such $W = \mathcal{P}(W_1, W_2, W_3)$
- starting from $n = 3$ there are many "fake" polynomials not associated with any code, hence many "would-be" partition functions likely not associated with any CFT

$$W = x^3 + 2x^2z + 3xz^2 + y^2z + z^3, \quad (1)$$
$$W = x^3 + x^2z + 3xz^2 + 2y^2z + z^3, \quad (2)$$
$$W = x^3 + 2x^2z + xy^2 + 2xz^2 + 2z^3, \quad (3)$$
$$W = x^3 + xy^2 + 2xz^2 + 2y^2z + 2z^3, \quad (4)$$

constraints $z \to W$

- any polynomial W invariant under MacWilliams identity and $y \to -y$ defines modular-invariant $Z(\tau, \bar{\tau})$
- all such $W = \mathcal{P}(W_1, W_2, W_3)$

$n = 3$

- starting from $n = 3$ there are many "fake" polynomials not associated with any code, hence many "would-be" partition functions likely not associated with any CFT

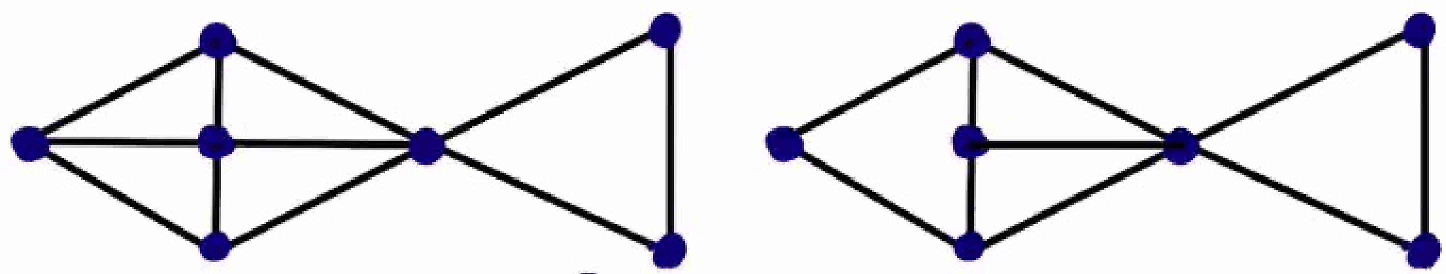
$$
\left\{
\begin{aligned}
W &= x^3 + 2x^2 z + 3xz^2 + y^2 z + z^3, && (1)\\
W &= x^3 + x^2 z + 3xz^2 + 2y^2 z + z^3, && (2)\\
W &= x^3 + 2x^2 z + xy^2 + 2xz^2 + 2z^3, && (3)\\
W &= x^3 + xy^2 + 2xz^2 + 2y^2 z + 2z^3, && (4)\\
W &= x^3 + x^2 z + 2xy^2 + xz^2 + 3z^3, && (5)\\
W &= x^3 + 2xy^2 + xz^2 + y^2 z + 3z^3, && (6)
\end{aligned}
\right.
$$

16 / 20

$n \to \dots$

we find non-equivalent graphs/codes with the same W, hence isospectral code CFTs

- analog of Milnor's example, $n = 7$



- many dozens of pairs and triples for $n = 8$, and beyond

60 pairs 5 triplets

$n = 11$ groups 11

Application: "baby bootstrap"

- for code CFTs spectral gap is controlled by binary Hamming distance

7:13 PM Wed Nov 25 37%

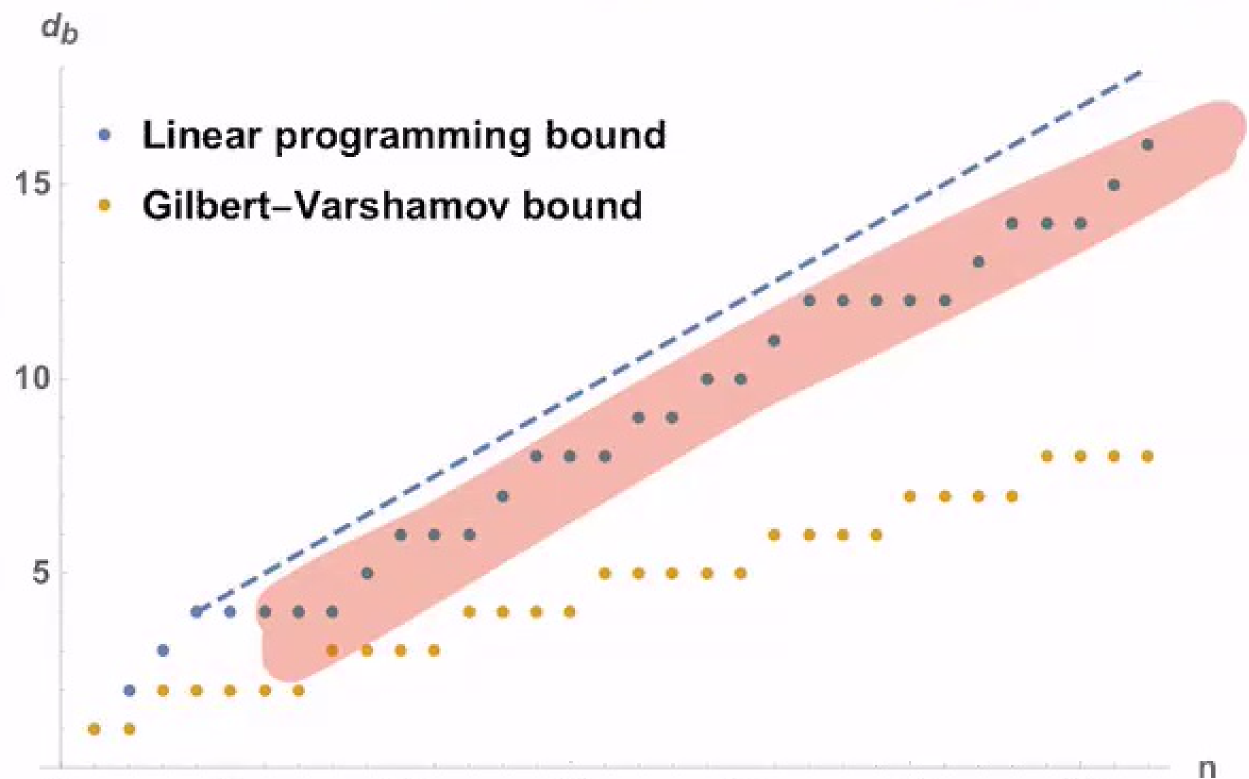
Application: "baby bootstrap"

- for code CFTs spectral gap is controlled by binary Hamming distance

$$d_\mathrm{b} = \min_{c=(\vec{\alpha},\vec{\beta})\in\mathcal{C},c\neq 0} \alpha^2+\beta^2$$

W

- d_b can be constrained using Linear Programming



18 / 20

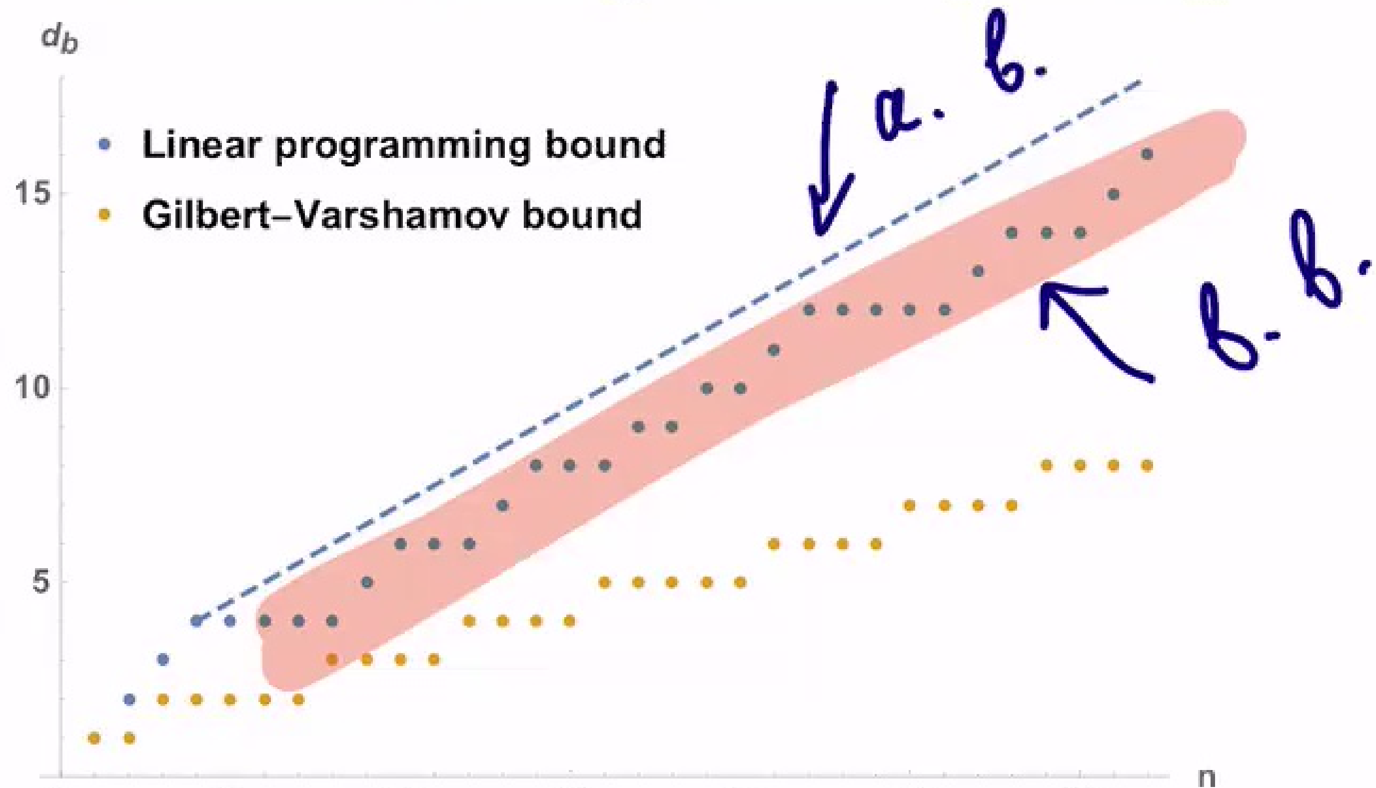
Application: "baby bootstrap"

- for code CFTs spectral gap is controlled by binary Hamming distance

W

$$d_{\mathrm{b}} = \min_{c=(\vec{\alpha},\vec{\beta})\in\mathcal{C},c\neq 0} \alpha^2+\beta^2$$

- d_{b} can be constrained using Linear Programming



- averaging over all Narain theories (random Narain theory) $=$ CS in AdS_3

  Afkhami-Jeddi, Cohn, Hartman, Tajdini; Maloney, Witten

- averaging over all codes (choosing random code) is known to produce a good code; the same applies to lattices

- averaging over all code CFTs yields the partition function $\overline{W}$ with linear spectral gap

$$\Delta_1 \sim c\frac{p^*}{2}, \qquad p^* \approx 0.11, \quad H(p^*) = \ln(2)/2$$

- $\overline{Z}$ admits representation as a sum over handlebodies, suggesting holographic interpretation

Conclusions

- quantum codes $\rightarrow$ Lorentzian lattices $\rightarrow$ non-chiral CFTs

- "baby bootstrap": "an ansatz" to reduce modular bootstrap constrains to algebraic relations on $W(x, y, z)$

open questions:

- insights about spectral gap of Narain theories when $c \gg 1$

- random/averaged (code) CFT and holography

- quantum error correction at the level of CFT Hilbert space

7:19 PM Wed Nov 25 40%

- quantum codes $\rightarrow$ Lorentzian lattices $\rightarrow$ non-chiral CFTs
- "baby bootstrap": "an ansatz" to reduce modular bootstrap constrains to algebraic relations on $W(x, y, z)$

open questions:

- insights about spectral gap of Narain theories when $c \gg 1$
- random/averaged (code) CFT and holography
- quantum error correction at the level of CFT Hilbert space

20 / 21