From Classical to Quantum Codes

Matilde Marcolli

Ma148b: Algebraic and Categorical Information
Caltech, Winter 2025

This lecture is based on:

- A.R. Calderbank, E.M. Rains, P.W. Shor, N.J.A. Sloane, *Quantum error correction and orthogonal geometry*, Phys. Rev. Lett. 78 (1997), no. 3 405.
- M. Heydeman, M. Marcolli, S. Parikh, I. Saberi, *Nonarchimedean holographic entropy from networks of perfect tensors*, Adv. Theor. Math. Phys. 25 (2021), no. 3, 591–721.
- S. Gurevich and R. Hadani, *Quantization of symplectic vector spaces over finite fields*, Journal of Symplectic Geometry 7 (2009), no. 4 475–502.
- M. Marcolli, C. Perez, *Codes as fractals and noncommutative spaces*, Math. Comput. Sci. 6 (2012), no. 3, 199–215.
- N. Combé, Yu.I. Manin, M. Marcolli, *Moufang patterns and Geometry of Information*, Pure Appl. Math. Q. 19 (2023), no. 1, 149–189..

Classical codes

- alphabet finite set $\mathfrak{A}$ of cardinality $q \geq 2$
- classical (unstructured) code: subset $C \subset \mathfrak{A}^n$
- elements of C are code words: $x = (a_1, \ldots, a_n)$ in $C \subset \mathfrak{A}^n$
- $k = k(C) = \log_q \# C$ with $\lfloor k \rfloor$ integer part of k
- transmission rate: ratio $R = k/n$
- Hamming distance between code words $x = (a_i)$ and $y = (b_i)$

$$d(x, y) = \#\{i \,|\, a_i \neq b_i\}$$

- relative minimum distance: ratio $\delta = d/n$ with $d(C) = \min\{d(x, y) \,|\, x, y \in C, \, x \neq y\}$
- classical code C with these parameters: $[n, k, d]_q$ code

Classical linear codes

- finite field $\mathfrak{A} = \mathbb{F}_q$ of cardinality $q = p^r$ characteristic $p > 0$
- code is linear if $C \subset \mathbb{F}_q^n$ is an $\mathbb{F}_q$-linear subspace of vector space $\mathbb{F}_q^n$
- $k = \lfloor k \rfloor$ is an integer for linear codes $=$ dim C as vector space
- given $\mathbb{F}_q$-bilinear form $\langle \cdot, \cdot \rangle$ on $\mathbb{F}_q^n$, self-orthogonal code C if all code words $x, y \in C$ have $\langle x, y \rangle = 0$
- dual code $C^\perp$: vectors v in $\mathbb{F}_q^n$ with $\langle v, x \rangle = 0$ for all $x \in C$
- self-orthogonal: $C \subseteq C^\perp$

Central extensions: groups from linear codes

- ilnear code $C \subset \mathbb{F}_q^n$ with $\dim C = q^k$ so $C \simeq \mathbb{F}_q^k$
- cocycle $\theta : C \times C \to \mathbb{F}_q$

$$\theta(v,w) - \theta(u+v,w) + \theta(u,v+w) - \theta(u,v) = 0$$

- central extension

$$0 \to \mathbb{F}_q \to G_\theta \to C \to 0$$

- multiplication

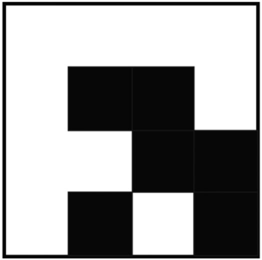
$$(v,x)\cdot(w,y) = (v+w, x+y+\theta(v,w))$$

- associativity from cocycle condition
- when $\mathbb{F}_q = \mathbb{F}_2$ view $\theta : C \times C \to \mathbb{F}_2$ as "QR code diagram" $\theta : \mathbb{F}_2^k \times \mathbb{F}_2^k \to \mathbb{F}_2$

Example

- quaternion units group $Q_8 = \{1, \pm i, \pm j, \pm k\}$ relations $i^2 = j^2 = k^2 = -1$ and $ij = k$
- $C = \mathbb{F}_2^2$, extension $0 \to \mathbb{F}_2 \to Q_8 \to C \to 0$ with cocycle θ

$v \setminus w$	00	10	01	11
00	0	0	0	0
10	0	1	1	0
01	0	0	1	1
11	0	1	0	1



Quantum codes

- qbit = a vector in finite dimensional Hilbert space $\mathbb{C}^2$
- binary qbit spaces $(\mathbb{C}^2)^{\otimes n}$
- q-ary qbit = a vector in $\mathbb{C}^q$ and q-ary qbit spaces $(\mathbb{C}^q)^{\otimes n}$
- q-ary quantum code of *length* n and *size* k = a k-dimensional $\mathbb{C}$-linear subspace of $\mathbb{C}^{q^n} = (\mathbb{C}^q)^{\otimes n}$
- quantum error: a linear map $E \in \mathrm{End}_{\mathbb{C}}(\mathbb{C}^{q^n})$
- for quantum errors of the form $E = E_1 \otimes \cdots \otimes E_n$, the weight is $w(E) = \#\{i \,|\, E_i \neq id\}$
- quantum error E is detectable by a quantum code Q if

$$P_Q\, E\, P_Q = \lambda_E P_Q$$

with P_Q orthogonal projection onto $Q \subset \mathbb{C}^{q^n}$ and $\lambda_E \in \mathbb{C}$ constant depending only on E

- for $q = p^m$ consider field $\mathbb{F}_q$ as an $\mathbb{F}_p$-vector space, $\mathbb{F}_p^m$
- for $x \in \mathbb{F}_q^n$, $x = (a_1, \ldots, a_n)$ write each coefficient $a_i \in \mathbb{F}_q$ as vectors $a_i = (a_{i1}, \ldots, a_{im})$ with a_{ij} in $\mathbb{F}_p$
- elements of $\mathbb{Z}/p\mathbb{Z}$, integer numbers $0 \leq a_{ij} \leq p - 1$
- given a linear operator $L \in \mathrm{End}_{\mathbb{C}}(\mathbb{C}^p)$ with $L^p = id$, can consider integer powers $L^{a_{ij}}$

Fundamental error operators

- T and R on $\mathbb{C}^p$ given by matrices

$$T = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & & & & & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & 0 & \cdots & 0 & 0 \end{pmatrix}$$

$$R = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & \xi & 0 & \cdots & 0 & 0 \\ 0 & 0 & \xi^2 & \cdots & 0 & 0 \\ \vdots & & & & & \vdots \\ 0 & 0 & 0 & \cdots & \xi^{p-2} & 0 \\ 0 & 0 & 0 & \cdots & 0 & \xi^{p-1} \end{pmatrix},$$

where $\xi = \exp(2\pi i/p)$

Relations and basis

- power and commutation relations

$$T^p = R^p = id \qquad \text{and} \qquad TR = \xi RT$$

- these imply composition relations

$$T^k R^\ell = \xi^{k\ell} R^\ell T^k$$

$$(T^k R^\ell)(T^r R^s) = \xi^{-r\ell} T^{r+k} R^{s+\ell} = \xi^{sk-r\ell} (T^r R^s)(T^k R^\ell)$$

- the operators $T^k R^\ell$ form an orthonormal basis of $M_p(\mathbb{C}) = \mathrm{End}_{\mathbb{C}}(\mathbb{C}^p)$ with respect to the inner product $\langle A, B\rangle = \mathrm{Tr}(A^* B)$

Composite error operators

- x and y are elements in $\mathbb{F}_q$, written as vectors $x = (a_1, \dots, a_m)$, $y = (b_1, \dots, b_m)$ with coeffs $a_i, b_i \in \mathbb{F}_p$
- linear maps $E = E_1 \otimes \cdots \otimes E_n$ in $\mathrm{End}_{\mathbb{C}}(\mathbb{C}^{q^n})$, with $q = p^m$, where the factors E_i are of the form $E_i = T_x R_y$

$$T_x = T^{a_1} \otimes \cdots \otimes T^{a_n}$$

$$R_y = R^{b_1} \otimes \cdots \otimes R^{b_n}$$

- for $v = (x_1, \dots, x_n)$ and $w = (y_1, \dots, y_n)$ vectors in $\mathbb{F}_q^n$, corresponding error operator

$$E_{v,w} = T_{x_1} R_{y_1} \otimes \cdots \otimes T_{x_n} R_{y_n}$$

- T and R relations imply commutation relation

$$E_{v,w} E_{v',w'} = \xi^{\langle v, w' \rangle - \langle w, v' \rangle} E_{v',w'} E_{v,w}$$

- for $v, w \in \mathbb{F}_q^n$, the bilinear form $\langle v, w \rangle$

$$\langle v, w \rangle = \sum_{i=1}^{n} \sum_{j=1}^{m} a_{ij} b_{ij}$$

Group laws

- also get composition relation

$$E_{v,w}E_{v',w'} = \xi^{-\langle w,v'\rangle} E_{v+v',w+w'}$$

- $\mathcal{E}$ subgroup of $\mathrm{Aut}_{\mathbb{C}}(\mathbb{C}^{q^n})$ given by invertible linear maps of the form

$$\mathcal{E} = \{\xi^k E_{v,w} \,|\, v,w \in \mathbb{F}_q^n,\, 0 \leq k \leq p-1\}$$

- finite group of order p^{2mn+1}
- center $\mathcal{Z}$ of $\mathcal{E}$ is the subgroup $\{\xi^k\, id\}$ isomorphic to $\mathbb{Z}/p\mathbb{Z}$
- We'll see this is related to Heisenberg groups and symplectic spaces over finite fields

Quantum stabilizer codes

- quantum stabilizer code is a quantum code is obtained as joint eigenspace of all the linear transformations in a commutative subgroup of $\mathcal{E}$
- $\mathcal{S} \subset \mathcal{E}$ commutative subgroup with $\#\mathcal{S} = p^{r+1}$
- $\chi : \mathcal{S} \to U(1)$ character trivial on $\mathcal{Z}$
- quantum stabilizer code $Q = Q_{\mathcal{S},\chi}$ is linear subspace of $\mathbb{C}^{q^n}$

$$Q_{\mathcal{S},\chi} = \{\psi \in \mathbb{C}^{q^n} \,|\, A\psi = \chi(A)\psi, \ \forall A \in \mathcal{S}\}$$

- dimension p^{mn-r}

CRSS algorithm: classical–quantum correspondence

- given classical linear self-orthogonal code $C \subset \mathbb{F}_q^{2n}$, with $\# C = p^r$
- linear maps $E_{v,\varphi(w)}$, for (v,w) an $\mathbb{F}_p$-basis of C, together with elements $\xi^k id$, generate a subgroup $\mathcal{S} \subset \mathcal{E}$
- composition relation and self-orthogonality imply subgroup $\mathcal{S}$ is abelian
- by construction of order $\#\mathcal{S} = p^{r+1}$
- this determines a quantum stabilizer codes $Q_{\mathcal{S},\chi}$ with parameters $[[n, n-r/m, d^\perp]]_q$
- minimum distance d_Q of the quantum stabilizer code $Q_{\mathcal{S},\chi}$ satisfies

$$d_Q = d^\perp = d_{C^\perp \smallsetminus C}$$

$$d_{C^\perp \smallsetminus C} := \min \#\{ i \,|\, v_i \neq 0 \ \text{ or } \ w_i \neq 0, \ (v,w) \in \mathbb{F}_q^{2n}, (v,w) \in C^\perp \smallsetminus C \}$$

CRSS algorithm: classical–quantum correspondence

- conversely given quantum stabilizer code $Q = Q_{\mathcal{S},\chi}$
- given $\mathbb{F}_p$-linear automorphism $\varphi \in \mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_p^m)$
- get $\mathbb{F}_p$-linear code of length $2n$, with $\#C = p^r$ for $\#\mathcal{S} = p^{r+1}$

$$C = C_{Q,\varphi} = \{(v, \varphi^{-1}(w)) \,|\, E_{v,w} \in \mathcal{S}\}$$

- C is self-orthogonal with respect to bilinear form

$$\langle v, \varphi(w')\rangle - \langle v', \varphi(w)\rangle$$

with $\langle v, w\rangle = \sum_{i=1}^n \sum_{j=1}^m a_{ij} b_{ij}$

- role of automorphism φ: field extension $\mathbb{F}_q$ of $\mathbb{F}_p$ is identified with the vector space $\mathbb{F}_p^m$ (loose track of field structure); can use field automorphism φ to remember the remaining structure

Symplectic vector spaces and Heisenberg groups

- Symplectic vector space (V, ω) over a finite field $\mathbb{F}_q$ (char$\neq 2$):
  - ω closed: cocycle condition

$$d\omega(u, v, w) = \omega(v, w) - \omega(u + v, w) + \omega(u, v + w) - \omega(u, v) = 0$$

  - ω non-degenerate: given $u \in V$ find v with $\omega(u, v) \neq 0$
- Heisenberg group central extension determined by cocycle ω

$$0 \to \mathbb{F}_q \to \mathrm{Heis}(V, \omega) \to V \to 0$$

$$(v, x) \cdot (w, y) = (v + w, x + y + \frac{1}{2}\omega(v, w))$$

- $H(\mathbb{F}_q^{2n}) = \mathrm{Heis}(\mathbb{F}_q^{2n}, \omega)$ with ω standard Darboux form
- Darboux form: sum $\mathbb{F}_q^{2n} = \oplus_i \mathbb{F}_q^2$ on each $\mathbb{F}_q^2$ symplectic form

$$\omega((x_1, y_1), (x_2, y_2)) = y_1 x_2 - y_2 x_1$$

- the error operators $E_{ab} = T_a R_b$ give the explicit representation matrices of the Heisenberg group $H(\mathbb{F}_q^{2n})$ with respect to the central character specified by ξ with $\xi^p = 1$
- Darboux basis for (V, ω) direct sum of 2-dim symplectic spaces over $\mathbb{F}_q$
    - using ω non-degen can find a first $\mathbb{F}_q^2 = \mathrm{span}\{u, v\}$ with $\omega(u, v) = 1$
    - using closed can decompose $V = \mathbb{F}_q^2 \oplus W$ with $W = \{w \in V \,|\, \omega(u, w) = \omega(v, w) = 0\}$
    - then repeat

Heisenberg groups and CRSS quantum codes

- unique irreducible complex representation $\mathcal{H} = \mathcal{H}_\chi(V,\omega)$ of $\mathrm{Heis}(V,\omega)$ with central character $\chi : \mathbb{F}_q \to \mathbb{C}^*$
- functorial geometric quantization over finite fields (Gurevich–Hadani) $\Rightarrow$ decomposition of $\mathcal{H} = (\mathbb{C}^q)^{\otimes n}$ as tensor product of q-ary qbits $\mathbb{C}^q$
- representation matrices $E_{ab} = T_a R_b$ of $\mathrm{Heis}(V,\omega)$ additive basis of $\mathrm{End}(\mathcal{H})$
- isotropic subspace $C \subset V \Rightarrow$ abelian subgroup of $\mathrm{Heis}(V,\omega)$ $\Rightarrow$ mutually diagonalizable, $\mathcal{H}$ sum of $\#C = q^k$ eigenspaces of dimension q^{n-k}
- Each such joint eigenspace of C of dimension q^{n-k} is a quantum code $\mathcal{Q}_C \simeq (\mathbb{C}^q)^{\otimes(n-k)}$ that encodes $n-k$ qbits to n qbits (CRSS quantum code associated to classical code C)

Algebro-geometric codes

- algebraic points $X(\mathbb{F}_q)$ of a curve X over a finite field $\mathbb{F}_q$
- set $A \subset X(\mathbb{F}_q)$ and divisor D on X with $supp(D) \cap A = \emptyset$
- code $C = C_X(A, D)$ by evaluation at A of rational functions $f \in \mathbb{F}_q(X)$ with poles at D
- bound on order of pole of f at D determines dimension of the linear code

Reed-Solomon codes case $X(\mathbb{F}_q) = \mathbb{P}^1(\mathbb{F}_q)$

- $C = \{(f(x_1), \cdots, f(x_n)) \,:\, f \in \mathbb{F}_q[x], \deg(f) < k\}$ gives an $[n, k, n-k+1]_q$ with $n \leq q$
- or homogeneous polynomials at points $x_i = (u_i : v_i) \in \mathbb{P}^1(\mathbb{F}_q)$

$$\hat{C} = \{(f(u_1, v_1), \ldots, f(u_n, v_n)) \,:\, f \in \mathbb{F}_q[u, v], \text{homog. } \deg(f) < k\}$$

- generalized Reed-Solomon codes: $w = (w_1, \ldots, w_n) \in \mathbb{F}_q^n$

$$C_{w,k} = \{(w_1 f(x_1), \cdots, w_n f(x_n)) \,:\, f \in \mathbb{F}_q[x], \deg(f) < k\}$$

$$\hat{C}_{w,k} = \{(w_1 f(u_1, v_1), \ldots, w_n f(u_n, v_n)) \,:\, f \in \mathbb{F}_q[u, v], \text{homog.} \deg(f) < k\}$$

CRSS of Reed-Solomon codes

- Hermitian self-dual case: $\langle v, w \rangle_H = \sum_{i=1}^n v_i w_i^q$, with $v, w \in \mathbb{F}_{q^2}^n$
- Hermitian-self-dual length n over $\mathbb{F}_{q^2}$ gives self-dual code $\tilde{C}$ length $2n$ over $\mathbb{F}_q$ then CRSS
- Hermitian self-duality conditions for generalized Reed–Solomon codes with $w = (w_1, \ldots, w_n) \in (\mathbb{F}_{q^2}^*)^n$
- For $w_i = 1$ and $n = q^2$ with $k = q$, Hermitian-self-dual Reed-Solomon code $C = C_{1,q}$ and associated $[[q^2 + 1, q^2 - 2q + 1, q + 1]]_q$-quantum Reed-Solomon code $\mathcal{C}$

Symplectic vector spaces and perfect tensors $(p > 2)$

- perfect tensor: $T \in \mathcal{V}^{\otimes m}$ ($\mathcal{V}$ with inner prod to identify with dual, here qbit $\mathcal{V} = \mathbb{C}^q$) such that all splittings (tensor/Hom) for $j \leq m/2$ are *isometries*

$$\mathcal{V}^{\otimes j} \to \mathcal{V}^{\otimes(m-j)}$$

- when isometric injection of the $(n-k)$-qbits code space $\mathcal{Q}_C$ inside the n-qbit space $\mathcal{H}$ is obtained from a partition of the indices of a $(2n-k)$-index tensor into $(n-k)$-qbits (to be encoded), together with n-qbits (encoding space)
- even number of indices of perfect tensor when $\dim C = k$ even
- procedure to produce directly perfect tensors via a version of CRSS algorithm and quantization of symplectic vector spaces over finite fields

Lagrangians

- Symplectic vector space (V,ω) of dim $2n$ over $\mathbb{F}_q$; Lagrangian subspace $L \subset V$ (of dim n)
- Irreducible rep of $\mathrm{Heis}(V,\omega)$ can be realized through a choice of Lagrangian $L \subset V$ (in classical construction of quantum mechanical Hilbert space that identifies position vs momentum repres L, $L^\vee$) $\quad \mathcal{H}_L = \mathcal{H}_\chi(V,L,\omega)$ (invariants under $L^\vee$)
- L chosen in "general position" means that intersection with Darboux decomposition as small as possible, so a basis of $\mathcal{H}_L$ is as far as possible from being a tensor-product basis in the Darboux decomposition

$$(\dim V = 4n) \quad V = \oplus_i V_i \Rightarrow (\mathbb{C}^q)^{\otimes 2n} = \mathcal{H} = \otimes_i \mathcal{H}_i = \otimes_i \mathbb{C}^q$$

$$V = W \oplus W' \text{ splitting of } 2n \text{ indices } k \leq n \text{ and } 2n-k$$

$$\dim(L \cap W) \geq 2(k-n), \quad \dim(L \cap W') \geq 2(n-k)$$

for $k = n$ general position if both zero-dimensional

Lagrangians and perfect tensors

- geometrically maximal rank of perfect tensors with respect to decomposition into groups of qbits corresponds to a "general position" of the Lagrangian (with respect to a given symplectic splitting of V into 2-dim Darboux pieces)
- most non-general position: L' sum of 1-dim Lagrangians in each 2-dim Darboux subspace (maximally decomposable)
- (functorial quantization): symplectomorphism $\psi : W_1 \to W_2 \Rightarrow \mathcal{H}(\psi) : \mathcal{H}(W_1) \to \mathcal{H}(W_2)$
- if Lagrangian L in general position then symplectomorphism $\psi : \bar{W} \to W'$ (with opposite $(\bar{W}, \bar{\omega}) = (W, -\omega)$)
- $\mathcal{H}(\psi) : \mathcal{H}(W)^\vee \to \mathcal{H}(W')$ same as tensor $T \in \mathcal{H}(W) \otimes \mathcal{H}(W') = \mathcal{H}(V)$ is perfect tensor

Example: 3-qtrit quantum code

- quantum Reed–Solomon code with perfect tensor condition
- start with classical $[n, k, n-k+1]_{q^2}$ Reed–Solomon code
- choose parameters $n = q = 3$, $k = (q-1)/2 = 1$
- $X = \mathbb{P}^1(\mathbb{F}_3) \smallsetminus \{\infty\} = \{[1:0], [1:1], [1:2]\}$
- $[3, 1, 3]_9$-code

$$\{(f_a(1,0), f_a(1,1), f_a(1,2)) \,|\, a \in \mathbb{F}_9, \;\; f_a \in \mathbb{F}_9[u, v]\}$$

- $k = 1$ so homogeneous polynomials just $f_a(u, v) = a_0 \in \mathbb{F}_9$

$$\{(a_0, a_0, a_0) \,|\, a_0 \in \mathbb{F}_9\}$$

- self-orthogonal code: $\langle a, b \rangle = 3 a_0 b_0^3 = 0$
- $d_Q = \min\{\mathrm{weight}(v) \,|\, v \in D^\perp \smallsetminus D\} = 2$ from

$$D^\perp = \{\langle a, b\rangle = a_0(b_1^3 + b_2^3 + b_3^3) = 0\} = \{(2b_2 + 2b_3, b_2, b_3) \,|\, b_i \in \mathbb{F}_9\}$$

- take then classical $[2n, 2k, 2n-2k+1]_q$ Reed–Solomon code same parameters $n = q = 3$, $k = (q-1)/2 = 1$
- inputs $a = (a_0, b_0) \in \mathbb{F}_3^2$ and code

$$C = \{(f_{a_0}(1,0), f_{b_0}(1,0), f_{a_0}(1,1), f_{b_0}(1,1), f_{a_0}(1,2), f_{b_0}(1,2))\}$$

- again because $k = 1$ just

$$C = \{((a_0, b_0), (a_0, b_0), (a_0, b_0)) \,|\, (a_0, b_0) \in \mathbb{F}_3^2\}$$

- self-orthogonality for inner product

$$\langle (a, b), (a', b') \rangle = 3a_0 b_0' - 3a_0' b_0 = 0$$

- for $(a,b) \in C$ group elements $\xi^i E_{a,b}$ with $0 \leq i \leq 2$

$$E_{a,b} = T_{a_0} R_{b_0} \otimes T_{a_0} R_{b_0} \otimes T_{a_0} R_{b_0}$$

- matrices $T_{a_0} R_{b_0}$

$$T_0R_0 = \begin{pmatrix} 1 & & \\ & 1 & \\ & & 1 \end{pmatrix} \quad T_0R_1 = \begin{pmatrix} 1 & & \\ & \xi & \\ & & \xi^2 \end{pmatrix} \quad T_0R_2 = \begin{pmatrix} 1 & & \\ & \xi^2 & \\ & & \xi \end{pmatrix}$$

$$T_1R_0 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \quad T_1R_1 = \begin{pmatrix} 0 & \xi & 0 \\ 0 & 0 & \xi^2 \\ 1 & 0 & 0 \end{pmatrix} \quad T_1R_2 = \begin{pmatrix} 0 & \xi^2 & 0 \\ 0 & 0 & \xi \\ 1 & 0 & 0 \end{pmatrix}$$

$$T_2R_0 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \quad T_2R_1 = \begin{pmatrix} 0 & 0 & \xi^2 \\ 1 & 0 & 0 \\ 0 & \xi & 0 \end{pmatrix} \quad T_2R_2 = \begin{pmatrix} 0 & 0 & \xi \\ 1 & 0 & 0 \\ 0 & \xi^2 & 0 \end{pmatrix}.$$

- orthonormal basis of qbits $|a_0\rangle$ with $a_0 \in \mathbb{F}_3$

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \qquad |1\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \qquad |2\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$$

- common eigenvectors of the matrices $T_{a_0} R_{b_0}$

$$\begin{array}{lll} |A\rangle = |000\rangle + |111\rangle + |222\rangle & |B\rangle = |012\rangle + |120\rangle + |201\rangle & |C\rangle = |021\rangle + |210\rangle + |102\rangle \\ |D\rangle = |001\rangle + |112\rangle + |220\rangle & |E\rangle = |010\rangle + |121\rangle + |202\rangle & |F\rangle = |100\rangle + |211\rangle + |022\rangle \\ |G\rangle = |002\rangle + |110\rangle + |221\rangle & |H\rangle = |020\rangle + |101\rangle + |212\rangle & |I\rangle = |200\rangle + |011\rangle + |122\rangle \end{array}$$

with $|ijk\rangle = |i\rangle \otimes |j\rangle \otimes |k\rangle \in (\mathbb{C}^3)^{\otimes 3}$

- eigenvalues and eigenvectors $\xi^i E_{a,b}$ (with notation $a_0^3 := (a_0, a_0, a_0)$)

	$E_{0^3,0^3}$	$E_{0^3,1^3}$	$E_{0^3,2^3}$	$E_{1^3,0^3}$	$E_{1^3,1^3}$	$E_{1^3,2^3}$	$E_{2^3,0^3}$	$E_{2^3,1^3}$	$E_{2^3,2^3}$
$\|A\rangle$	1	1	1	1	1	1	1	1	1
$\|B\rangle$	1	1	1	1	1	1	1	1	1
$\|C\rangle$	1	1	1	1	1	1	1	1	1
$\|D\rangle$	1	ξ^2	ξ	1	ξ^2	ξ	1	ξ^2	ξ
$\|E\rangle$	1	ξ^2	ξ	1	ξ^2	ξ	1	ξ^2	ξ
$\|F\rangle$	1	ξ^2	ξ	1	ξ^2	ξ	1	ξ^2	ξ
$\|G\rangle$	1	ξ	ξ^2	1	ξ	ξ^2	1	ξ	ξ^2
$\|H\rangle$	1	ξ	ξ^2	1	ξ	ξ^2	1	ξ	ξ^2
$\|I\rangle$	1	ξ	ξ^2	1	ξ	ξ^2	1	ξ	ξ^2

- from table see that invariant subspaces for group $\mathcal{S}$ are $\mathrm{span}\{|A\rangle, |B\rangle, |C\rangle\}$ or $\mathrm{span}\{|D\rangle, |E\rangle, |F\rangle\}$ or $\mathrm{span}\{|G\rangle, |H\rangle, |I\rangle\}$
- can equivalently take one: say $Q_C = \mathrm{span}\{|A\rangle, |B\rangle, |C\rangle\}$
- resulting quantum code $[[3,1,2]]_3$ quantum Reed-Solomon 3-qtrit code is a 4-index perfect tensor
- see as an isometric map $T : \mathbb{C}^3 \to (\mathbb{C}^3)^{\otimes 3}$

$$|0\rangle \mapsto \frac{1}{\sqrt{3}}|A\rangle, \quad |1\rangle \mapsto \frac{1}{\sqrt{3}}|B\rangle, \quad |2\rangle \mapsto \frac{1}{\sqrt{3}}|C\rangle$$

Characteristic 2 case: Symplectic spaces and quantization

- S. Gurevich, R. Hadani, *The Weil representation in characteristic two*, Adv. Math. 230 (2012), no. 3, 894–926

Setting:

- finite field $k = \mathbb{F}_{2^r}$
- residue field $\mathcal{O}_K/\mathfrak{m}_K = \mathbb{F}_{2^r}$ of an unramified extension K of degree r of $\mathbb{Q}_2$, with $\mathcal{O}_K \subset K$ ring of integers, $\mathfrak{m}_K$ maximal ideal
- ring $R = \mathcal{O}_K/\mathfrak{m}_K^2$
- $(\tilde{V}, \tilde{\omega})$ free R-module with a symplectic form
- $\mathbb{F}_{2^r}$-vector space $V = \tilde{V}/\mathfrak{m}_K$ with R-valued non-degenerate skew-symmetric form (almost-symplectic) $\omega = 2\tilde{\omega}$

- polarization of symplectic form $\tilde{\omega}$: bilinear form $\tilde{\beta} : \tilde{V} \times \tilde{V} \to R$ with

$$\tilde{\beta}(\tilde{v}, \tilde{w}) - \tilde{\beta}(\tilde{w}, \tilde{v}) = \tilde{\omega}(\tilde{v}, \tilde{w})$$

- bilinearity implies cocycle condition

$$\tilde{\beta}(\tilde{v}, \tilde{w} + \tilde{u}) - \tilde{\beta}(\tilde{v}, \tilde{w}) - \tilde{\beta}(\tilde{v} + \tilde{w}, \tilde{u}) + \tilde{\beta}(\tilde{w}, \tilde{u}) = 0$$

- on V $\beta = 2\tilde{\beta}$ induces an R-valued cocycle with

$$\beta(v, w) - \beta(w, v) = \omega(v, w)$$

Heisenberg groups in characteristic 2

- Heisenberg group is the extension determined by cocycle β

$$0 \to R \to \mathrm{Heis}(V, \beta) \to V \to 0$$

- multiplication

$$(v, r) \star (w, s) = (r + s + \beta(v, w), v + w)$$

- choice of a character $\chi : R \to \mathbb{C}^*$ determines an irreducible complex representation $\mathcal{H}_\chi(V, \beta)$ of $\mathrm{Heis}(V, \beta)$

Weil Heisenberg groups in characteristic 2

- $\mathbb{F} = \mathbb{F}_{2^d}$, central extension of a symplectic $\mathbb{F}_{2^d}$-vector space (V, ω) by $\mathbb{F}$-valued cocycle $\beta : V \times V \to \mathbb{F}$ with $\beta(u, v) - \beta(v, u) = \omega(u, v)$

$$0 \to \mathbb{F} \to \mathrm{Heis}_{Weil}(V, \beta) \to V \to 0$$

- advantage of version with R instead of $\mathbb{F}$: better symmetries

Comparison

- automorphisms in $\mathrm{Aut}(\mathrm{Heis}(V,\beta))$ acting trivially on center: affine symplectic group

$$0 \to V^\vee \to \mathrm{ASp}(V) \to \mathrm{Sp}(V) \to 1$$

  extension of symplectic group: solutions (α, g) of

$$\alpha(v+w) - \alpha(v) - \alpha(w) = \beta(gv, gw) - \beta(v,w)$$

- automorphisms in $\mathrm{Aut}(\mathrm{Heis}_{Weil}(V,\beta))$ acting trivially on center: pseudo-symplectic group

$$0 \to V^\vee \to \Psi(V) \to O(Q) \to 1$$

  $O(Q) \subset \mathrm{Sp}(V)$ orthogonal group of quadratic form $Q(v) = \beta(v,v)$: solutions (α, g) of above

- $\Psi(V)$ not an extension of symplectic group but $\mathrm{ASp}(V)$ yes

enhanced Lagrangians

- pair (L, α) with $L \subset V$ Lagrangian and $\alpha : L \to R$ satisfying

$$\alpha(v + w) - \alpha(v) - \alpha(w) = \beta(v, w)$$

- this $\alpha : L \to R$ defines section $\tau : L \to \mathrm{Heis}(V, \beta)$ of the projection $\mathrm{Heis}(V, \beta) \to V$ by $\tau : \ell \mapsto (\ell, \alpha(\ell))$

$$\tau(\ell + \ell') = (\ell + \ell', \alpha(\ell + \ell')) =$$

$$(\ell + \ell', \alpha(\ell) + \alpha(\ell') + \beta(\ell, \ell')) = \tau(\ell) \star \tau(\ell')$$

- realization of irreducible Heisenberg representation: $\mathcal{H}_{(V,L,\beta,\chi)}$ subspace of $\mathbb{C}[\mathrm{Heis}(V, \beta)]$ functions with

$$f((0, x) \cdot (w, y)) = \chi(x) f(w, y), \quad \forall x \in k, \ \forall (w, y) \in V \times k$$

$$f(\tau(\ell) \cdot (w, y)) = f(w, y), \quad \forall \ell \in L, \ \forall (w, y) \in V \times k$$

with action of $\mathrm{Heis}(V, \beta)$ by right translations

Tensor Networks, Quantum Codes, and Geometry from Information

- Fernando Pastawski, Beni Yoshida, Daniel Harlow, John Preskill, *Holographic quantum error-correcting codes: Toy models for the bulk/boundary correspondence*, JHEP 06 (2015) 149 [HaPPY]

Main Idea: Bulk spacetime geometry is the result of *entanglement* of quantum states in the boundary through a network of quantum error correcting codes

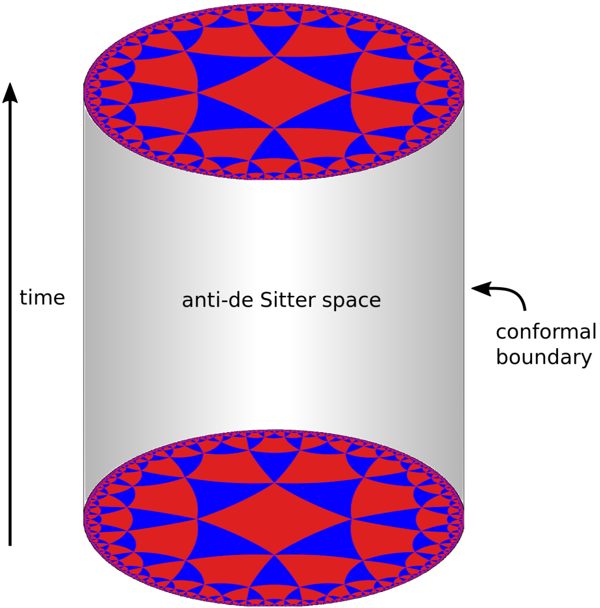
- quantum codes by perfect tensors: maximal entanglement across bipartitions
- network of perfect tensors with contracted legs along a tessellation of hyperbolic space
- uncontracted legs at the boundary (physical spins), and at the center of each tile in the bulk (logical spins)
- holographic state: pure state of boundary spins
- logical inputs on the bulk: encoding by the tensor network (holographic code)

AdS/CFT Holographic Correspondence

- bulk/boundary spaces
- hyperbolic geometry in the bulk (Lorentzian AdS spaces, Euclidean hyperbolic spaces $\mathbb{H}^{d+1}$)
- conformal boundary at infinity:
  $\partial\mathbb{H}^3 = \mathbb{P}^1(\mathbb{C})$ (AdS_3/CFT_2) or
  $\partial\mathbb{H}^2 = \mathbb{P}^1(\mathbb{R})$ (AdS_2/CFT_1)
- AdS/CFT correspondence: a d-dimensional conformal field theory on the boundary related to a gravitational theory on the $d+1$ dimensional bulk

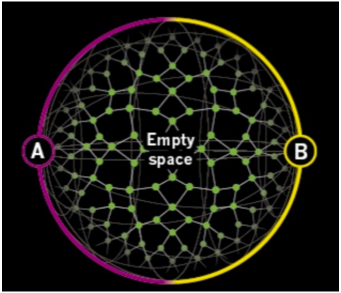
AdS/CFT Holography developed in String Theory since the 1990s

- E. Witten, *Anti-de Sitter space and holography*, arXiv:hep-th/9802150


time
anti-de Sitter space
conformal
boundary

More recent view of AdS/CFT: **Quantum Information**

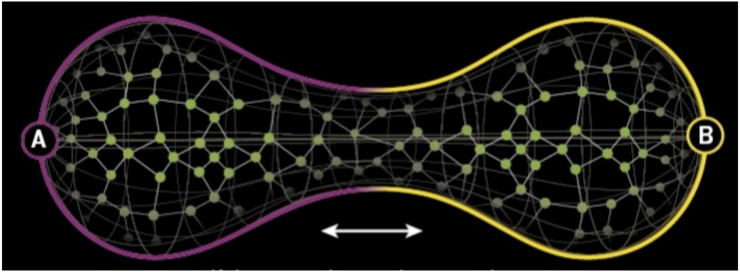
- relation between CFT on the boundary and gravity on the bulk with focus on Information (Entanglement Entropy) of quantum states on the boundary and geometry (gravity) on the bulk.



from R.Cowen, "The quantum source of space-time", Nature 527 (2015) 290–293

Spacetime geometry emerges from quantum entanglement

Entanglement between quantum fields in regions A and B decreases when corresponding regions of bulk space are pulled apart: dynamics of spacetime geometry (= gravity) constructed from quantum entanglement



from R.Cowen, "The quantum source of space-time", Nature 527 (2015) 290–293

Ryu–Takayanagi Formula:
Entanglement Entropy and Bulk Geometry

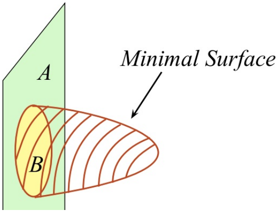
- Entanglement Entropy: $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$

$$\rho_A = \mathrm{Tr}_{\mathcal{H}_B}(|\Psi\rangle\langle\Psi|), \quad \mathcal{S}_A = -\mathrm{Tr}(\rho_A \log \rho_A)$$

- Entanglement and Geometry: (conjecture)

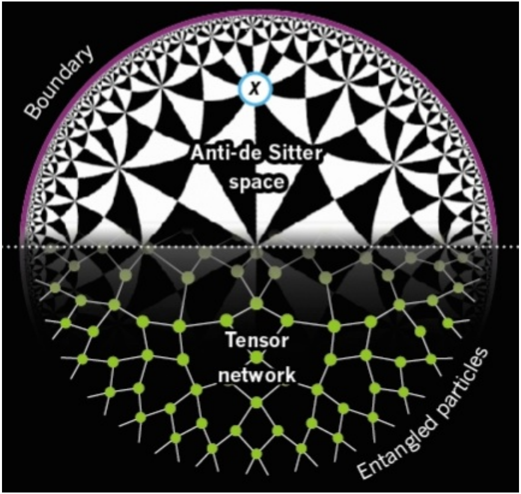
$$\mathcal{S}_A = \frac{\mathcal{A}(\Sigma_{\min})}{4G}$$

area of minimal surface in the bulk with given boundary $\partial A = \partial B$



from T.Nishioka,S.Ryu,T.Takayanagi, "Holographic entanglement entropy: an overview", J.Phys.A 42 (2009) N.50, 504008

tensor networks as discretization of the bulk space



from R.Cowen, "The quantum source of space-time", Nature 527 (2015) 290–293

Pentagon tile holographic code [HaPPY]

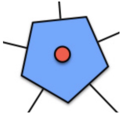
• perfect tensors: $T_{i_1,\ldots,i_n}$ such that, for $\{1,\ldots,n\} = A \cup A^c$ with $\#A \leq \#A^c$, isometry $T : \mathcal{H}_A \to \mathcal{H}_{A^c}$; perfect code (encodes one qbit to $n-1$)

• six legs perfect tensor $T_{i_1\ldots,i_6}$: five qbit perfect code $[[5,1,3]]_2$-quantum code:

$$\mathcal{C} \subset \mathcal{H}^{\otimes 5}, \quad \mathcal{C} = \{\psi \in \mathcal{H}^{\otimes 5} \,:\, S_j \psi = \psi\}$$

$$S_1 = X \otimes Z \otimes Z \otimes X \otimes I$$

X, Y, Z Pauli gates and $S_2, S_3, S_4, S_5 = S_1 S_2 S_3 S_4$ cyclic perms, with $\mathcal{H} = \mathbb{C}^2$ one qbit Hilbert space



5-ary qbits perfect tensor codes generalize case of 3-qtrit with 6-legs perfect tensor

- Example of perfect tensor codes
  - single 3-ary qubit (qutritt) encodes to three 3-ary qubits

$$
\begin{array}{lcl}
|0\rangle & \mapsto & |000\rangle + |111\rangle + |222\rangle \\
|1\rangle & \mapsto & |012\rangle + |120\rangle + |201\rangle \\
|2\rangle & \mapsto & |021\rangle + |102\rangle + |210\rangle
\end{array}
$$

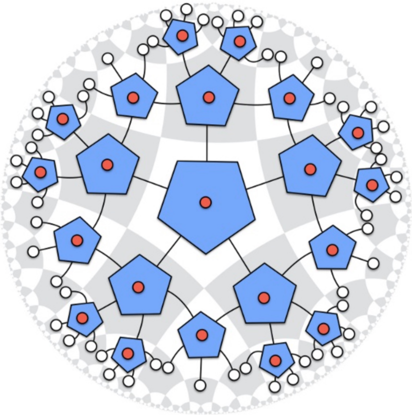
  - polynomial codes $f_a(x) = ax^d + b_{d-1}x^{d-1} + \cdots + b_1 x + b_0$

$$
|a\rangle \mapsto \sum_{b\in\mathbb{F}_q^d} \left(\otimes_{x\in\mathbb{F}_q} |f_a(x)\rangle\right)
$$

  - example: $q = 5$ [HaPPY] code case

$$
|a\rangle \mapsto \sum_{b_0,b_1\in\mathbb{F}_5} |b_0, b_0+b_1+a, b_0+2b_1+4a, b_0+3b_1+4a, b_0+4b_1+a\rangle
$$

  - in general $[n, k, n-k+1]_q$ Reed–Solomon code $\Rightarrow$ quantum $[[n, n-2k, k+1]]_q$ code; for $n = q$ and $k+1 = n-k$ perfect tensor $[[q, 1, (q+1)/2]]_q$ code



from F.Pastawski, B.Yoshida, D.Harlow, J.Preskill, *Holographic quantum error-correcting codes: Toy models for the bulk/boundary correspondence*, JHEP 06 (2015) 149

Properties of the [HaPPY] code

- quantum error-correcting codes with a tensor network structure as *discretized version* of spacetime
- bulk and boundary degrees of freedom (logical/physical)
- exact prescription for mapping bulk operators to boundary operators
- Ryu–Takayanagi: entanglement entropy in the CFT is computed by the area of a certain minimal surface in the bulk geometry (cutting legs in the tensor network cuts out the bulk region)

Bulk discretization via tensor networks depend on a choice of tessellation and construction of a network of perfect tensors along the tessellation: is there a natural bulk discretization that works?

- Some more results on the [HaPPY] code:
  - Elliott Gesteau, Monica Jinwoo Kang, *The infinite-dimensional HaPPY code: entanglement wedge reconstruction and dynamics*, arXiv:2005.05971
  - Elliott Gesteau, Monica Jinwoo Kang, *Thermal states are vital: Entanglement Wedge Reconstruction from Operator-Pushing*, arXiv:2005.07189

Passing to the limit of an infinite tessellation in the [HaPPY] construction shows some limitations as a model of AdS/CFT holography (lack of long-range entanglement in the boundary and CFT behavior, but good properties of entanglement wedge reconstruction)

Tensor networks: general setup

Graphs

- finite graph $G = (F, V, \partial, j)$
- F set of flags (half-edges) and V set of vertices
- boundary map $\partial : F \to V$ identifies root vertex of each flag
- structure involution $j : F \to F$, $j^2 = id$ described how half-edges are glued together into edges of G
- internal edges $E_{int}(G)$ are pairs $e = (f, f')$ with $j(f) = f'$ and $f \neq f'$
- external edges $E_{ext}(G)$ are fixed points $j(f) = f$
- cut set $C \subset E_{in}(G)$ set of internal edges such that if all the edges $e \in C$ are cut get exactly two non-empty connected components

$$G \smallsetminus C = G_{C,1} \sqcup G_{C,2}$$

tensor network on a graph: tensor network $(G, \mathcal{H}, T)$

- (finite) graph G without multiple edges (in general want to extend to infinite graph)
- vertices $v \in V$ are decorated by pairs $(\mathcal{H}_v, T^{(v)})$ of a complex vector space $\mathcal{H}_v = (\mathbb{C}^q)^{\otimes \deg(v)}$, for some $q = p^r > 0$ a power of some prime p, with $\deg(v)$ the valence of the vertex, and a $T^{(v)} \in \mathcal{H}_v$
- tensor $T^{(v)} = (T^{(v)})_{i_1,\ldots,i_{\deg(v)}}$, with indices $i_f \in \mathbb{F}_q$, labelled by the flags $f \in F$ with $\partial(f) = v$
- edge $e = (f, f')$, $f' = j(f)$, with $\partial e = \{v, v'\}$ corresponds to a contraction of indices of $T^{(v)}$ and $T^{(v')}$

$$\sum_{i_f, i'_{f'} \in \mathbb{F}_q} \delta^{i_f, i'_{f'}} \, T^{(v)}_{i_1,\ldots,i_{\deg(v)}} \, T^{(v')}_{i'_1,\ldots,i'_{\deg(v')}}$$

  δ^{ij} the Kronecker delta function
- *bonds* = internal edges of G, *dangling legs* = external edges of G
- graph G is called the *support* of the tensor network

Entangled state

- tensor network $\mathcal{T} = (G, \mathcal{H}, T)$ computes an entangled state $|\psi_{\mathcal{T}}\rangle$ in $\mathcal{H}_{\mathcal{T}} = (\mathbb{C}^q)^{\otimes |E_{ext}(G)|}$
- standard basis $|a_1 \dots a_N\rangle$ of the space $(\mathbb{C}^q)^{\otimes N}$ with $a = (a_1, \dots, a_N) \in \mathbb{F}_q^N$
- at vertex $v \in V(G)$ entangled state

$$|\psi_v\rangle = \sum_{a_1,\dots,a_{\deg(v)} \in \mathbb{F}_q} T^{(v)}_{a_1,\dots,a_{\deg(v)}} |a_1 \dots a_{\deg(v)}\rangle$$

  superposition of the pure states $|a_1\rangle \otimes \cdots \otimes |a_{\deg(v)}\rangle$
- along an edge $e \in E_{int}(G)$

$$|\psi_e\rangle = \sum_{a_i, b_j \in \mathbb{F}_q} \delta^{a_f, b_{f'}} \, T^{(v)}_{a_1,\dots,a_{\deg(v)}} \, T^{(v')}_{b_1,\dots,b_{\deg(v')}} |\hat{a}^{(f)}, \hat{b}^{(f')}\rangle,$$

  with $\hat{a}^{(f)} = (a_1, \dots, \hat{a}_f, \dots, a_{\deg(v)})$ and $\hat{b}^{(f')} = (b_1, \dots, \hat{b}_{f'}, \dots, b_{\deg(v')})$, and $\hat{a}_f$ and $\hat{b}_{f'}$ with this entry removed
- after performing all edge contractions on the $|\psi_v\rangle$ get $|\psi_{\mathcal{T}}\rangle$ (remaining qubits of external edges)

case with no external edges

- same computation gives a complex number: amplitude $\alpha_{\mathcal{T}}$
- for any cut-set C an entangled states $|\psi_{C,i}\rangle$ in $(\mathbb{C}^q)^{\otimes |C|}$
- amplitude $\alpha_{\mathcal{T}}$ is obtained from these by contracting the indices corresponding to the pairs $e = (f_1, f_2)$ cut set

density matrix

- density matrix of the entangled state $|\psi_{\mathcal{T}}\rangle$

$$\rho = \frac{1}{\langle \psi_{\mathcal{T}} | \psi_{\mathcal{T}} \rangle} \, |\psi_{\mathcal{T}}\rangle \, \langle \psi_{\mathcal{T}}|$$

- partition $A \sqcup B$ of the set of external edges of G:

$$\rho_A = \mathrm{Tr}_B(\rho)$$

with $\mathrm{Tr}_B : \mathcal{H}_A \otimes \mathcal{H}_B \to \mathcal{H}_A$, tracing out (contracting indices) dangling legs in B

Entanglement entropy

- assignment
$$A \mapsto S_{\mathcal{T}}(A) := \mathrm{Tr}(\rho_A \log \rho_A),$$
for $A \subset E_{ext}(G)$ ranging over all subsets of external edges
- connected graph G with no external edges:
$$A_i \mapsto S_{\mathcal{T},C,i}(A_i) := \mathrm{Tr}(\rho_{C,A_i} \log \rho_{C,A_i}),$$
for C ranging over cut-sets and $A_i \subset E_{ext}(G_{C,i})$
$$\rho_{C,A_i} = \mathrm{Tr}_{C \smallsetminus A_i}(\rho_{C,i})$$
with $\rho_{C,i}$ density matrix of entangled state $|\psi_{C,i}\rangle$

More general: can have more legs of tensor $T^{(v)}$ at vertices: $\deg(v)$ outputs and some inputs, then tensor network as quantum code

Other geometric aspects of CRSS quantum codes
Twisted group rings

- discrete group G, group ring $\mathbb{C}[G]$ associative noncommutative algebra
- (reduced) C^*-completion $C^*_r(G)$: closure of $\mathbb{C}[G]$ operator norm of algebra of bounded operators $\mathcal{B}(\ell^2(G))$ using right (or left) regular representation
- right regular representation: action of $\mathbb{C}[G]$ on $\ell^2(G)$ by $r_g f(g') = f(g'g)$

- multiplier $\sigma : G \times G \to U(1)$ is a 2-cocycle

$$\sigma(g,1) = \sigma(1,g) = 1$$

$$\sigma(g_1,g_2)\sigma(g_1g_2,g_3) = \sigma(g_1,g_2g_3)\sigma(g_2,g_3)$$

- twisted group ring $\mathbb{C}[G,\sigma]$ is generated by the twisted translations $r_g^\sigma f(g') = f(g'g)\,\sigma(g',g)$
- cocycle property implies associativity of $\mathbb{C}[G,\sigma]$ (and unital)
- composition relation

$$r_g^\sigma r_{g'}^\sigma = \sigma(g,g') r_{gg'}^\sigma$$

- twisted (reduced) group C^*-algebra $C_r^*(G,\sigma)$ norm closure of $\mathbb{C}[G,\sigma]$ in $\mathcal{B}(\ell^2(G))$

Matrix algebras

- matrix algebra $M_{q^n}(\mathbb{C})$ for $q = p^m$ identified with twisted group C^*-algebra $C^*((\mathbb{Z}/p\mathbb{Z})^{2mn}, \sigma)$
- multiplier $\sigma : (\mathbb{Z}/p\mathbb{Z})^{2m} \times (\mathbb{Z}/p\mathbb{Z})^{2m} \to U(1)$

$$\sigma((v,w),(v',w')) = \xi^{-\langle w,v' \rangle}$$

with $\xi = \exp(2\pi i/p)$ and

$$\langle v,w \rangle = \sum_{i=1}^{n} \sum_{j=1}^{m} a_{ij} b_{ij}$$

- cocycle condition $\sigma((v,w),(0,0)) = \sigma((0,0),(v,w)) = 1$ and

$$\sigma((v,w),(v',w'))\sigma((v+v',w+w'),(v'',w'')) = \xi^{-\langle w,v' \rangle - \langle w,v'' \rangle - \langle w',v'' \rangle}$$

$$= \sigma((v,w),(v'+v'',w'+w''))\sigma((v',w'),(v'',w''))$$

- generators $r^\sigma_{(v,w)}$ such that $r^\sigma_{(v,w)} r^\sigma_{(v',w')} = \xi^{-\langle w,v' \rangle} r^\sigma_{(v+v',w+w')}$
- same as generated by transformations $\xi^i E_{v,w}$

Noncommutative tori

- (rational or irrational) rotation algebras aka noncommutative tori
- rotation algebra $\mathcal{A}_\theta$ is C^*-algebra generated by two unitaries U and V with commutation relation

$$UV = \xi VU$$

  with $\xi = \exp(2\pi i\theta)$
- rational case, $\theta \in \mathbb{Q}$ these algebras are Morita equivalent (bimodule identifying categories of modules, isom for NC spaces) to functions $C(\mathbb{T}^2)$ on ordinary commutative torus $\mathbb{T}^2$
- irrational case $\theta \in \mathbb{R} \smallsetminus \mathbb{Q}$, the Morita equivalence classes correspond to the orbits of the action of $\mathrm{SL}_2(\mathbb{Z})$ on the real line by fractional linear transformations

Rational noncommutative tori

- rational case with $\xi = \exp(2\pi i/p)$

$$\mathcal{A}_{1/p} \ni a = \sum_{k,\ell} f_{k,\ell}(\mu, \lambda)\, T^k R^\ell$$

- $f_{k,\ell}(\mu, \lambda)$ continuous functions of $(\lambda, \mu) \in S^1 \times S^1 = \mathbb{T}^2$
- T and R fundamental error matrices of quantum codes
- finite sum for $0 \leq k, \ell \leq p-1$ since $T^p = R^p = id$
- generators U and V are $U = \mu T$ and $V = \lambda R$, with $\mu = \exp(2\pi it)$ and $\lambda = \exp(2\pi is)$ in S^1

Quantum codes and vector bundles

- rational NC torus $\mathcal{A}_{n/m}$ isomorphic to the algebra $\Gamma(T^2, \mathrm{End}(E_m))$ of sections of the endomorphisms bundle of a rank m vector bundle E_m over torus T^2
- start with trivial bundle on T^2 with fiber $M_m(\mathbb{C})$
- action of $(\mathbb{Z}/m\mathbb{Z})^2$ by

$$\tau_{1,0} : (\mu, \lambda, M) \mapsto (\mu, e^{-2\pi i n/m}\lambda, TMT^{-1})$$

$$\tau_{0,1} : (\mu, \lambda, M) \mapsto (e^{2\pi i n/m}\mu, \lambda, RMR^{-1})$$

- quotient gives a non-trivial bundle over T^2, which is endomorphisms bundle $\mathrm{End}(E_m)$ of a vector bundle E_m of rank m: bundle with fiber $M_m(\mathbb{C})$
- algebra of sections $\Gamma(T^2, \mathrm{End}(E_m))$ is fixed point subalgebra of $C(T^2, M_m(\mathbb{C})) = C(T^2) \otimes M_m(\mathbb{C})$ (endomorphisms of trivial bundle) under $(\mathbb{Z}/m\mathbb{Z})^2$-action

- action on algebra $C(T^2, M_m(\mathbb{C})) = C(T^2) \otimes M_m(\mathbb{C})$

$$\alpha_{1,0} : f(\mu, \lambda) \otimes M \mapsto f(\mu, e^{-2\pi i n/m}\lambda) \otimes TMT^{-1},$$
$$\alpha_{0,1} : f(\mu, \lambda) \otimes M \mapsto f(e^{2\pi i n/m}\mu, \lambda) \otimes RMR^{-1}$$

- fixed point subalgebra then generated by $\mu \otimes T$ and $\lambda \otimes R$ with commutation relation of the NC torus
- C^*-algebra homomorphism $\mathcal{A}_{n/m} \to M_m(\mathbb{C})$ sending generators U and V to the matrices T and R.

Quantum stabilizer codes

- E_p rank p bundle over T^2 with $\mathcal{A}_{1/p} = \Gamma(T^2, \mathrm{End}(E_p))$
- q-ary quantum stabilizer code $Q_{\mathcal{S},\chi}$ (for $q = p^m$) of length n and size k $\Rightarrow$ commutative subalgebra $\mathcal{A}_{\mathcal{S}} \subset \mathcal{A}_{1/p}^{\otimes r}$, with $r = nm$, and subbundle $\mathcal{F}_{\mathcal{S},\chi}$ of external tensor product $E_p^{\boxtimes mn}$ over $T^{2r} = T^2 \times \cdots \times T^2$
- elements of the algebra $\mathcal{A}_{\mathcal{S}}$ act as scalars on $\mathcal{F}_{\mathcal{S},\chi}$
- these data equivalent to assigning $Q_{\mathcal{S},\chi}$
- here action of $(\mathbb{Z}/p\mathbb{Z})^{2r}$ on $C(T^{2r}, M_{q^n}(\mathbb{C}))$

$$\alpha_{v,w} : f(\underline{\mu}, \underline{\lambda}) \otimes M \mapsto f(\xi^v \underline{\mu}, \xi^{-w} \underline{\lambda}) \otimes E_{v,w} M E_{v,w}^{-1}$$

- matrix algebra $M_{q^n}(\mathbb{C})$ identified with $C^*(\mathcal{E}/\mathcal{Z}) = C^*((\mathbb{Z}/p\mathbb{Z})^{2mn}, \sigma)$ generated by the $E_{v,w}$

- algebra $\mathcal{A}_{\mathcal{S}} = C(X_{\mathcal{S}})$ algebra of functions of a space $X_{\mathcal{S}} = \cup_{\chi \in \hat{\mathcal{S}}} T_\chi$
- T_χ is a quotient of the torus T^{2r}
- over T_χ the bundle $\mathcal{F}_{\mathcal{S},\chi}$ becomes direct sum $\mathcal{L}_{\mathcal{S},\chi}^{\oplus k}$ of k-copies of a line bundle
- if quantum code $Q_{\mathcal{S},\chi}$ from classical linear code $C \subset \mathbb{F}_q^n$ via CRSS algorithm can see some properties of classical code from algebra $\mathcal{A}_{\mathcal{S}}$
- for $c \in C$ Hamming weight $\varpi(c)$ number of non-zero coordinates of $c \in \mathbb{F}_q^n$
- algebra $\mathcal{A}_{\mathcal{S}} = C(X_{\mathcal{S}})$ has natural filtration by Hamming weight of words in classical code C

Moufang loops and codes

- a loop is a set L with an operation $\star : L \times L \to L$ that is not associative, a unit element e with $e \star a = a \star e = a$ for all $a \in L$ and such that the left and right multiplication maps $r_x(y) = y \star x$ and $\ell_x(y) = x \star y$ are bijections $L \to L$
- last condition shows existence of unique left and right inverses x_ℓ^{-1}, x_r^{-1} of $x \in L$
- in this very general form there is not much structure, but can impose a stronger condition
- Moufang loop: loop L satisfying near-associativity relation (Moufang identity)

$$x \star (y \star (x \star z)) = ((x \star y) \star x) \star z, \quad \forall x, y, z \in L$$

Some properties of Moufang loops

- any subloop (closed under $\star$ containing e) generated by two elements x, y is a group (i.e. associative)
- powers of a single element are well defined: $x^3 = (x \star x) \star x = x \star (x \star x)$ etc
- left and right inverse agree $x_\ell^{-1} = x_r^{-1} = x^{-1}$
- other equivalent forms of the Moufang identity

$$x \star (y \star (z \star y)) = ((x \star y) \star z) \star y, \quad \forall x, y, z \in L$$

$$(y \star (x \star z)) \star y = (y \star x) \star (z \star y) = y \star ((x \star z) \star y) \quad \forall x, y, z \in L$$

- commutator $[a,b]$ and associator $[a,b,c]$ in loop L:

$$a \star b = b \star a \star [a,b] \quad \text{and} \quad (a \star b) \star c = (a \star (b \star c)) \star [a,b,c]$$

- nucleus $N(L)$ of loop L: set of all elements $a \in L$ such that $[a,b,c] = [b,a,c] = [b,c,a] = 1$ for all $b,c \in L$
- Moufang center $C(L)$ of Moufang loop L: set of elements $a \in L$ such that $[a,b] = 1$ for all $b \in L$
- center $Z(L)$ of Moufang loop L: intersection $Z(L) = N(L) \cap C(L)$
- nucleus $N(L)$ is a subgroup of L and center $Z(L)$ is an abelian subgroup

Code loops

- $C \subset \mathbb{F}_q^n$ linear code
- *twisted cocycle* $\theta : C \times C \to \mathbb{F}_q$ with

$$\theta(v, w) - \theta(u + v, w) + \theta(u, v + w) - \theta(u, v) = \delta(u, v, w)$$

  (2-cochain that is not a cocycle)
- loop $L(C, \theta) = C \ltimes_\theta \mathbb{F}_q$ instead of group
- conditions under which this is a Moufang loop?

Some code loops references

- R.L. Griess, *Code Loops*, J. of Algebra, 100 (1986) 224–234
- T. Hsu, *Explicit constructions of code loops as centrally twisted products*, Math. Proc. Camb. Phil. Soc. 128 (2000), 223–232
- B. Nagy, D.M. Roberts, *(Re)constructing Code Loops*, The American Mathematical Monthly, 128 (2021) N.2, 151–161

Code loop construction: doubly even codes

- binary linear codes $C \subset \mathbb{F}_2^n$
- doubly even code: weight $|v| = \#\{v_i = 1\} = v_1 + \cdots + v_n$, the number of ones in the word, is divisible by 4
- logical AND operation: $u\&v := (u_1 v_1, \ldots, u_n v_n)$
- twisted cocycle θ with twisting function

$$\delta(u,v,w) = |u\&v\&w| \mod 2$$

- θ satisfies

$$\theta(v,w) + \theta(w,v) = \frac{1}{2}|v\&w| \mod 2$$

$$\theta(v,v) = \frac{1}{4}|v| \mod 2$$

- (Griess): loop codes obtained in this way are Moufang loops

Examples of doubly even codes: Hamming and Golay codes

- Hamming code $C \subset \mathbb{F}_2^8$ subspace spanned by the four row vectors

$$\begin{matrix} 1\,0\,0\,0\,0\,1\,1\,1 \\ 0\,1\,0\,0\,1\,0\,1\,1 \\ 0\,0\,1\,0\,1\,1\,0\,1 \\ 0\,0\,0\,1\,1\,1\,1\,0 \end{matrix}$$

- extended binary Golay code $C \subset \mathbb{F}_2^{24}$ linear subspace spanned by row vectors

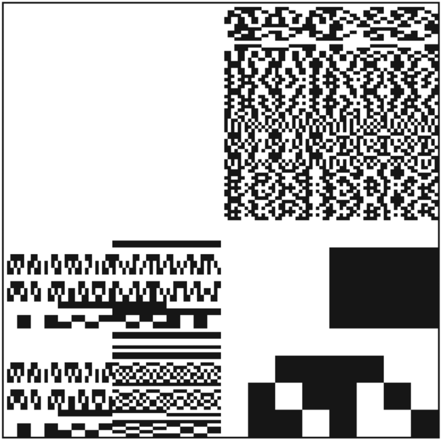
000110000000010110100011	101001011100111001111111
101001111101101111110001	100000011100001001001100
000100000000100100111110	000001000000111001001110
010000000010000110101101	100000001000111000111000
000000000010010101010111	100000000100101000010111
100000000000100111110001	011011000001111011111111

- decomposition into complementary subspaces $C = V \oplus W$
- to determine θ enough to evaluate on complementary subspaces

$$\begin{aligned}
\theta(v_1 + w_1, v_2 + w_2) = {} & \theta(v_1, v_2) + \theta(w_1, w_2) + \theta(v_1, w_1) \\
& + \theta(w_2, v_2) + \theta(v_1 + v_2, w_1 + w_2) \\
& + \tfrac{1}{2}|v_2 \,\&\, (w_1 + w_2)| + |v_1 \,\&\, v_2 \,\&\, (w_1 + w_2)| \\
& + |w_1 \,\&\, w_2 \,\&\, v_2| + |v_1 \,\&\, w_1 \,\&\, (v_2 + w_2)| \pmod 2
\end{aligned}$$

Example: Golay code and Parker loop

- for Golay code take $C = V \oplus W$ with two left/right columns of basis vectors above
- θ then completely determined by $2^{14} - 2^8 + 1 = 16129$ values



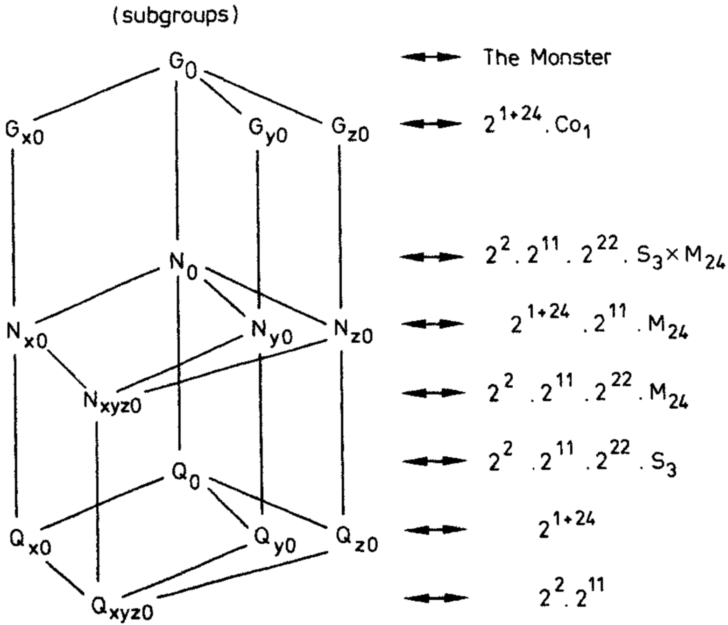
- Parker loop $L(C, \theta) = C \ltimes_\theta \mathbb{F}_2$

Parker loop and the Monster group

- J.H. Conway, *A simple construction for the Fischer–Griess monster group*, Invent. Math. 79 (1985), 513–540

Sketch of main idea

- Monster group: simple group constructed by Griess as automorphism group of a certain algebra in a 196884-dimensional space
- Conway obtained a simpler construction from the Parker loop
- symmetries of Golay code: permutations of a set Ω of size 24 that fix C seen as subset of the set of parts $P = P(\Omega)$ identifying $\mathbb{F}_2$-valued vectors with characteristic functions of subsets
- the Golay code has symmetries M_{24} the Mathieu group
- using sets of ordered triples in $P \cup \{0\}$ and self-maps of these sets construct various subgroups of the Monster group


(subgroups)
G0
Gx0
Gy0
Gz0
N0
Nx0
Ny0
Nz0
Nxyz0
Q0
Qx0
Qy0
Qz0
Qxyz0
The Monster
2^{1+24}.Co1
2^2.2^11.2^22.S3×M24
2^{1+24}.2^11.M24
2^2.2^11.2^22.M24
2^2.2^11.2^22.S3
2^{1+24}
2^2.2^11

Code loops and cubic symplectic structures

- T. Hsu, *Moufang loops of class 2 and cubic forms*, Math. Proc. Camb. Phil. Soc. 128 (2000), 197–222

Setting:

- Moufang loops L that are central extensions

$$0 \to Z \to L \to C \to 0$$

  with abelian groups $Z = Z(L)$ and $C = L/Z(L)$
- associated cubic symplectic structure

$$\chi : C \times C \to Z, \quad \alpha : C \times C \times C \to Z$$

$$\chi(\bar{a}, \bar{b}) = [a, b], \quad \alpha(\bar{a}, \bar{b}, \bar{c}) = [a, b, c]$$

  for $a, b, c \in L$ with $\bar{a}, \bar{b}, \bar{c}$ in C
- expressions well defined as values of $[a, b]$ and $[a, b, c]$ do not change when shifting entries by elements of center $Z = Z(L)$
- Note: commutators and associators take values center $Z(L)$ as quotient $L/Z(L)$ is an abelian group

- $\alpha : C \times C \times C \to Z$ is antisymmetric and multilinear (hence also a cocycle)
- $\chi : C \times C \to Z$ is antisymmetric and satisfies

$$\chi(\bar{a} + \bar{b}, \bar{c}) = \chi(\bar{a}, \bar{c}) + \chi(\bar{b}, \bar{c}) + 3\,\alpha(\bar{a}, \bar{b}, \bar{c})$$

- from identity (where terms in rhs can be associated in any way)

$$[a \star b, c] = [a, c] \star [[a, c], b] \star [b, c] \star [a, b, c]^3$$

  that holds when associators are central
- Note special role of characteristic $p = 3$

- also consider function $\sigma : C \to Z$ with $\sigma(\bar{a}) = a^p = \overbrace{a \star \cdots \star a}^{p-\text{times}}$
- this satisfies

$$\sigma(\bar{a} + \bar{b}) = \sigma(\bar{a}) + \sigma(\bar{b}) + \chi(a, b), \qquad \text{when } p = 2$$

$$\sigma(\bar{a} + \bar{b}) = \sigma(\bar{a}) + \sigma(\bar{b}), \qquad \text{when } p > 2$$

- $(a \star b)^p = \overbrace{(a \star b) \star \cdots \star (a \star b)}^{p-\text{times}} = a^p \star b^p \star [a, b]^{p(p-1)/2}$
- writing Z additively: $\sigma(\bar{a}) + \sigma(\bar{b}) + \frac{p(p-1)}{2}\chi(\bar{a}, \bar{b})$, for $p > 2$ coefficient multiple of characteristic p so zero, for $p = 2$ coefficient $\frac{p(p-1)}{2} = 1$
- Note special role of characteristic $p = 2$

Loops from cubic symplectic structures

- O. Chein, E. Goodaire. *Moufang loops with a unique nonidentity commutator (associator, square).* J. Alg. 130 (1990), 369–384.
- proved that (in characteristic 2) all loops obtained in this way are code loops of doubly even codes
- data of Hsu's cubic symplectic structure can be chosen arbitrarily: for any data $\sigma_i, \chi_{ij}, \alpha_{ijk} \in \mathbb{F}_2$, $\exists$ binary linear code C with basis $\{c_i\}$ such that

$$\sigma(c_i) = \sigma_i, \quad \chi_{ij} = \chi(c_i, c_j), \quad \alpha(c_i, c_j, c_k) = \alpha_{ijk}$$

- the case of doubly even codes is a cubic symplectic structure in Hsu's sense
- any small Frattini extension is a code loop of a doubly even code

$$\sigma_i = |c_i|/4, \ \ \chi(c_i, c_j) = |c_i \& c_j|/2, \ \ \alpha(c_i, c_j, c_k) = |c_i \& c_j \& c_k|.$$

Another construction: Almost-symplectic code loops

Almost-symplectic structure (p odd)

- finite dimensional vector space V over $\mathbb{F}_q$ (q odd) with non-degenerate skew-symmetric form $\omega : V \times V \to \mathbb{F}_q$.
  - $\omega(u, v) = -\omega(v, u)$, with $\omega(u, 0) = \omega(0, u) = 0$
  - for any $u \neq 0$ in V, there is some $v \in V$ satisfying $\omega(u, v) \neq 0$
- ω is not required to be closed
- nontrivial coboundary $d\omega = \delta$

$$d\omega(u, v, w) = \omega(v, w) - \omega(u+v, w) + \omega(u, v+w) - \omega(u, v) = \delta(u, v, w)$$

- Note: ω is *not* bilinear, otherwise $d\omega = 0$ would follow

Almost-symplectic structure ($p = 2$)

- $q = 2^r$, consider ring $R = \mathcal{O}_K/\mathfrak{m}_K^2$, where $\mathbb{F}_{2^r} = \mathcal{O}_K/\mathfrak{m}_K$
- (V, ω) with almost-symplectic $\omega : V \times V \to R$
- polarization: $\beta : V \times V \to R$

$$\beta(u, v) - \beta(v, u) = \omega(u, v)$$

- coboundary

$$d\beta(u, v, w) = \beta(v, w) - \beta(u+v, w) + \beta(u, v+w) - \beta(u, v) = \gamma(u, v, w),$$

with

$$\delta(u, v, w) = \gamma(u, v, w) + \gamma(w, v, u).$$

- polarization satisfies $\beta(v, 0) = \beta(0, v)$ since $\omega(0, v) = \omega(v, 0) = 0$
- polarization $\beta(u, v) - \beta(v, u) = \omega(u, v)$ is normalized if also satisfies $\beta(v, 0) = 0$ for all $v \in V$.

Lack of linearity

- lack of linearity of β in the left/right variable:

$$\gamma_\ell(u,v,w) := \beta(u+v,w) - \beta(u,w) - \beta(v,w)$$

$$\gamma_r(u,v,w) := \beta(u,v+w) - \beta(u,w) - \beta(v,w),$$

- so can write

$$\gamma(u,v,w) = \gamma_r(u,v,w) - \gamma_\ell(u,v,w),$$

- similarly for $\delta_\ell(u,v,w)$ and $\delta_r(u,v,w)$, lack of linearity of ω.

Almost-symplectic code loops

- *p* odd: code loops $\mathcal{L}(V,\omega)$ given by extension

$$0 \to \mathbb{F}_q \to \mathcal{L}(V,\omega) \to V \to 0$$

- non-associative multiplication

$$(u,x) \star (v,y) = (u+v, x+y+\frac{1}{2}\omega(u,v))$$

$u, v \in V$ and $x, y \in \mathbb{F}_q$

- *p* even: code loops $\mathcal{L}(V,\beta)$ given by extensions

$$0 \to R \to \mathcal{L}(V,\beta) \to V \to 0$$

- non-associative multiplication

$$(u,x) \star (v,y) = (u+v, x+y+\beta(u,v))$$

$u, v \in V$ and $x, y \in R$

Moufang identity

- Moufang identity for the loop $\mathcal{L}(V, \beta)$ iff

$$\gamma(u, v, u + w) = \gamma(v, w, u) \quad \forall u, v, w \in V$$

- same for $\mathcal{L}(V, \omega)$ for $p > 2$

$$\delta(u, v, u + w) = \delta(v, w, u) \quad \forall u, v, w \in V$$

- by direct computation from Moufang identity

$$(a \star b) \star (c \star a) = a \star ((b \star c) \star a)$$

with $a = (u, x)$, $b = (v, y)$, $c = (w, z)$

Cyclic and Hochschild cochains

- function $\eta : V \times \cdots \times V \to R$ is cyclic if $(1-\lambda)\eta = 0$ with
$$\lambda\eta(v_0, \ldots, v_n) = (-1)^n \eta(v_n, v_0, \ldots, v_{n-1})$$
- function $\eta : V \times \cdots \times V \to R$ is multilinear if $\delta_i \eta = 0$ for all $i = 0, \ldots, n$ with $\delta_i \eta(v_0, \ldots, v_n) =$
$$\eta(v_0, \ldots, v_i + w_i, \ldots, v_n) - \eta(v_0, \ldots, v_i, \ldots, v_n) - \eta(v_0, \ldots, w_i, \ldots, v_n)$$
- function $\eta : V \times \cdots \times V \to R$ Hochschild cocycle if $d\eta = 0$ with Hochschild coboundary
$$d\eta(v_0, \ldots, v_{n+1}) = \eta(v_1, \ldots, v_{n+1}) - \eta(v_0 + v_1, v_2, \ldots, v_{n+1}) + \cdots$$
$$+ (-1)^i \eta(v_0, \ldots, v_{i=1} + v_i, \ldots, v_{n+1}) + \cdots$$
$$+ (-1)^{n-1} \eta(v_0, \ldots, v_{n-1}, v_n + v_{n+1} + (-1)^n \eta(v_0, \ldots, v_n).$$
- multilinearity implies $d\eta = 0$
$$d\eta = \sum_{i=0}^{n} (-1)^i \delta_i \eta$$

Moufang condition and cyclic property

- If β is normalized and $\gamma = d\beta$ is multilinear, then the Moufang identity is equivalent to γ being cyclic
- same for $p > 2$: if $\delta = d\omega$ multilinear then Moufang condition equivalent to δ being cyclic

Linear representations of loops

- E.K. Loginov, *On linear representations of Moufang loops.* Commun. Algebra, 21 (1993) N.7, 2527–2536.
- loop $\mathcal{L}$ and vector space $\mathcal{H}$ over a field F
- left and right composition maps $\ell, \rho : \mathcal{L} \to Aut(\mathcal{H})$,

$$\ell_a(h) = a \star h, \quad \rho_a(h) = h \star a$$

- these should satisfy $a \star (h + h') = a \star h + a \star h'$, $(h + h') \star a = h \star a + h' \star a$, $a \star (\lambda h) = \lambda\, a \star h$, $(\lambda h) \star a = \lambda\, h \star a$, for all $a \in \mathcal{L}$, $h, h' \in \mathcal{H}$, $\lambda \in F$
- associate to a loop $\mathcal{L}$ the non-associative algebra $F[\mathcal{L}]$
- maps ℓ, ρ extend by linearity to $F[\mathcal{L}]$ (Eilenberg's notion of representation of nonassociative algebras)
- if loop is Moufang maps $\ell, \rho : \mathcal{L} \to Aut(\mathcal{H})$ satisfy
  - associator $[a, b, h]$ is skew-symmetric for all $a, b \in F[\mathcal{L}]$ and $h \in \mathcal{H}$
  - identities $h \star (b \star (a \star b)) = ((h \star b) \star a) \star b$ and $((a \star b) \star a) \star h = a \star (b \star (a \star h))$ hold, for all $a, b \in F[\mathcal{L}]$ and all $h \in \mathcal{L}$.

Isotropic and polarizable subspaces

- (V, ω) almost-symplectic in characteristic 2 with normalized polarization β
- isotropic subspace $C \subset V$ linear subspace where $\omega|_C \equiv 0$
- polarizable subspace $P \subset V$ linear subspace for which there is a map $\alpha : P \to R$ satisfying

$$\alpha(u+v) - \alpha(u) - \alpha(v) = \beta(u,v), \quad \forall u, v \in P$$

- polarized subspace: pair (P, α)
- polarization relation is just Hochschild coboundary $\beta = d\alpha$ so it implies $\gamma|_P = d\beta|_P = 0$.

Polarizations and sections

- polarized subspace (P, α) determines a section $\tau : P \to \mathcal{L}(V, \beta)$ of the projection $\mathcal{L}(V, \beta) \to V$, with image $\tau(P) \subset \mathcal{L}(V, \beta)$ a subgroup of the loop $\mathcal{L}(V, \beta)$
- if P also isotropic, then $\tau(P) \subset \mathcal{L}(V, \beta)$ is an abelian subgroup
- take $\tau(v) = (v, \alpha(v))$ for $v \in P$

$$(v, \alpha(v)) \star (w, \alpha(w)) = (v+w, \alpha(v)+\alpha(w)+\beta(v, w)) = (v+w, \alpha(v+w))$$

- associative since $d\beta|_P = 0$
- on an isotropic subspace polarization β is symmetric, hence multiplication also commutative

CRSS quantum codes from code loops

- $\mathcal{L}=$ almost-symplectic loops $\mathcal{L}(V,\omega)$ for $p>2$ and $\mathcal{L}(V,\beta)$ for $p=2$
- $\mathcal{H}=\mathbb{C}[\mathcal{L}]$ with left and right composition maps
- $|a\rangle$ with $a\in\mathcal{L}$ for the canonical basis of $\mathcal{H}$
- character $\chi: Z(\mathcal{L})\to\mathbb{C}^*$ (that is, a character $\chi: R\to\mathbb{C}^*$ for $p=2$ or $\chi:\mathbb{F}_q\to\mathbb{C}^*$ for $p>2$) gives subspace $\mathcal{H}_\chi\subset\mathcal{H}$: functions that transform like $\ell_{(0,x)}f(u,y)=\chi(x)f(u,y)$, for $x\in Z(\mathcal{L})$ and $(u,y)\in\mathcal{L}$
- An isotropic subspace $C\subset V$ determines a commuting family of error operators $\chi(\tau(v))E_v$, with $v\in C$, and an associated error correcting quantum code $\mathcal{C}_C\subset\mathcal{H}_\chi$ given by a joint eigenspace of these operators.
- $C\mapsto\mathcal{C}_C$ almost-symplectic CRSS algorithm.

Wedge product

- $\theta : V \to \mathbb{F}_q$ for q odd, or $\theta : V \to R$ in characteristic 2, and $\omega : V \times V \to \mathbb{F}_q$ for q odd, or $\omega : V \times V \to R$ in characteristic 2
- wedge product $\theta \wedge \omega$

$$(\theta \wedge \omega)(u, v, w) := \theta(u)\,\omega(v, w) + \theta(w)\,\omega(u, v)$$

- uniquely defined by compatibility with wedge product of two 1-forms θ_1, θ_2 as

$$(\theta_1 \wedge \theta_2)(v, w) := \theta_1(v)\theta_2(w) - \theta_1(w)\theta_2(v),$$

through relation

$$d(\theta_1 \wedge \theta_2) = d\theta_1 \wedge \theta_2 - \theta_1 \wedge d\theta_2$$

Locally conformally symplectic structures

- (V, ω) over $\mathbb{F}_q$ almost-symplectic space
- ω is *locally conformally symplectic structure* if there is a closed 1-form θ such that

$$d\omega = \theta \wedge \omega$$

- in characteristic 2 the form θ has values in R instead of $\mathbb{F}_q$

Darboux decomposition

- Darboux decomposition $V \simeq \oplus_i \mathbb{F}_q^2$ for a symplectic vector space uses $d\omega = 0$
- almost-symplectic case in general does *not* have Darboux decomposition
- if almost-symplectic ω is *locally conformally symplectic* then again have Darboux decomposition
- $d\theta = 0$ means θ is linear:

$$d\theta(u, v) = \theta(v) - \theta(u + v) + \theta(u) = 0$$

- So $V = \mathrm{Ker}(\theta) \oplus \mathbb{F}_q$ and $d\omega|_K \equiv 0$
- $\exists$ pair of vectors u, v in K with $\omega(u, v) = 1$: copy of $\mathbb{F}_q^2$ with Darboux symplectic form
- continue on complement until get $\oplus_{i=1}^{n-1} \mathbb{F}_q^2$ plus one $\mathbb{F}_q$
- combining all $V = \oplus_{i=1}^{n} \mathbb{F}_q^2$
- under quantization, corresponding decomposition of $\mathcal{H}$ into tensor product of q-ary qubits

Lagrangians and perfect tensors

- loop $\mathcal{L}$ (that is, $\mathcal{L}(V,\omega)$ for characteristic $p > 2$ and $\mathcal{L}(V,\beta)$ in characteristic $p = 2$)
- $L \subset V$ be a Lagrangian with respect to ω (an enhanced Lagrangian (L,α) for $p = 2$)
- $\tau(L) \subset \mathcal{L}$ section $\tau(L) = \{(v,\alpha(v)) \,|\, v \in L\}$ for $p = 2$ ($\tau(L) = \{(v,0) \,|\, v \in L\}$ for $p > 2$): abelian group
- Lagrangian L in *general position* with respect to the Darboux decomposition of locally conformally symplectic structure determines a perfect tensor $T_L \in \mathcal{H}$

Moufang loops and Latin square designs

- Latin square design is a pair $\mathcal{D} = (P, A)$ of a set P of points and a set A of lines
- $\#P = 3N$ with a splitting $P = P_1 \sqcup P_2 \sqcup P_3$ into points of three types, with $\#P_i = N$, for $i = 1, 2, 3$
- set A of lines, with $\#A = N^2$
- each line in A contains exactly 3 points, one from each of the three subsets of P
- any two points from two different subsets of P belong to exactly one line in A

Latin square

- Latin square of the design $\mathcal{D}$ is an $N \times N$ matrix
- entries corresponding to the N^2 lines in A and with (x_1, x_2)-entry equal to x_3 if the line containing $x_1 \in P_1$ and $x_2 \in P_2$ has $x_3 \in P_3$ as the third point
- order of Latin square is number N of points of each type

Category

- Latin square designs form a category
- objects $\mathcal{D} = (P, A)$
- morphisms $\mathcal{D} \to \mathcal{D}'$ given by triples of maps $\alpha_i : P_i \to P_i'$ such that, if (x_1, x_2, x_3) is a line in A then $(\alpha_1(x_1), \alpha_2(x_2), \alpha_3(x_3))$ is a line in A'

Thomsen loop and design

- for a loop $\mathcal{L}$, the *Thomsen design* $\mathcal{D}(\mathcal{L})$ has $P = \mathcal{L}_1 \sqcup \mathcal{L}_2 \sqcup \mathcal{L}_3$, three copies of $\mathcal{L}$ labelled $i = 1, 2, 3$, and $A = \{(x_1, x_2, x_3) \,|\, (x_1 \star x_2) \star x_3 = 1 \in \mathcal{L}\}$
- conversely for a Latin square design $\mathcal{D}$ have *Thomsen loop* $\mathcal{L}(\mathcal{D})$
- $\mathcal{D} \mapsto \mathcal{L}(\mathcal{D})$ is functorial and gives an equivalence of categories
- category of loops with morphisms *isotopisms*: triples of maps $(\alpha, \beta, \gamma) : \mathcal{L} \to \mathcal{L}'$ satisfying $\alpha(x) \star' \beta(y) = \gamma(x \star y)$ for all $x, y \in \mathcal{L}$

Automorphisms and Moufang condition

- automorphism of a Latin square design $\mathcal{D} = (P, A)$ is a permutation of P that sends lines to lines
- central automorphism τ_x of $\mathcal{D}$, centered at $x \in P$: fixes x and exchanges other two points on each line in A containing x
- *central Latin square design*: admits a central automorphism at every point $x \in P$
- equivalence between the category of central Latin square designs and the category of *Moufang loops*

Graph of the Thomsen design

- loops $\mathcal{L}(V,\omega)$ for p odd and $\mathcal{L}(V,\beta)$ for $p=2$
- Thomsen designs $\mathcal{D}(\mathcal{L}(V,\omega))$ and $\mathcal{D}(\mathcal{L}(V,\beta))$ associated graphs $G = G_{\mathcal{L}(V,\omega)}$ or $G = G_{\mathcal{L}(V,\beta)}$
- describing how points of the design are connected by lines
- $N = \#\mathcal{L}$ order $N = q^{2n+2}$ for $q = 2^r$ and $N = q^{2n+1}$ for q odd
- panel $\Pi_{(u,x)_i}$ of lines through a point $(u,x)_i$ ($i = 1,2,3$ type index) contains N lines, each containing two other points
- panels $\Pi_{(u,x)_i}$ and $\Pi_{(v,y)_j}$ with types $i \neq j$ intersect in a single line
- so graph with $\#V(G) = 3N$ and uniform valence $\deg(v) = 2N$, so $\#E(G) = 3N^2$
- $N = q^{2n+1}$ for $q = p^r$ with p odd and $N = q^{2n+2}$ for $q = 2^r$
- subgraph $G_{\tau(C)}$ with $3q^k$ vertices and $3q^{2k}$ edges for subdesign $\mathcal{D}(\tau(C))$

Tensor network from the Thomsen design

- Lagrangian (L, α) in general position and corresponding perfect tensor T_L
- subgraph $G \subset G_{\tau(L)}$ with same vertex set as $G_{\tau(L)}$ and only edges between points u_i and $(u + e_r)_j$, for $\{e_r\}_{r=1,\dots,n}$ with e_r standard basis of $\mathbb{F}_q^n \simeq L$
- $T = T_{\ell_1,\dots,\ell_{2n}}$ indices labelled by vectors $\ell = (\ell_1, \dots, \ell_{2n}) \in \mathbb{F}_q^{2n} \simeq V$ in the Darboux basis
- entangled state associated to corolla of vertex u_i in G

$$|\psi_{u_i}\rangle = \sum_{\ell} T_\ell \, |\ell\rangle$$

with $|\ell\rangle$ standard basis of $\mathcal{H}$

Chamber systems

- chamber system of type I on a set Ω (set of chambers) is a family $\{\rho_i\}_{i\in I}$ of equivalence relations on Ω
  1. if $\omega \sim_i \omega'$ and $\omega \sim_j \omega'$, for some $i \neq j \in I$, then $\omega = \omega'$
  2. the I-graph (vertex set Ω and edges $e_{\omega,\omega'}$, for $\omega \sim_i \omega'$ for some ρ_i) is connected
- subset $J \subset I \Rightarrow$ *residue of type J* is a connected component of J-graph
- number of colors $\#I$ is *rank* of chamber system
- panels $=$ connected components of the monochromatic subgraphs
- Latin chamber system is a chamber system of rank 3 where any two panels of different colors intersect in a unique chamber

Latin square designs and Latin chamber systems

- Latin square design determines a Latin chamber system
- Ω given by the set of the N^2 cells of the Latin square
- equivalences: same row, same column, same symbol in the cell
- set of chambers of Latin chamber system = set of lines of the Latin square design
- set of panels = set of points of the Latin square design
- a panel = set of lines that contain a given point

Buildings: Coxeter groups

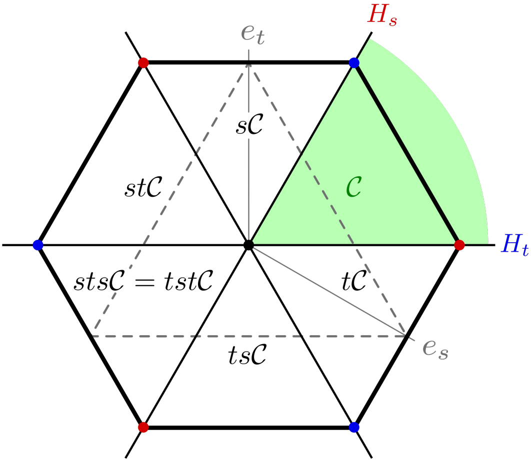
- best known class of chamber systems are buildings
- Coxeter group: group defined by a presentation

$$G = \langle x_i,\ i \in I \mid x_i^2 = 1\,\forall i,\ (x_i x_j)^{m_{ij}} = 1\,\forall i,j \in I\}$$

  with $m_{ij} \geq 2$ integers or $m_{ij} = \infty$ (ie no such relation)
- G always isomorphic to group generated by reflections in a family of hyperplanes H_i in Euclidean or hyperbolic space with mutual angles π/m_{ij} (parallel for $m_{ij} = \infty$)
- Coxeter complex: cell complex where images under G of reflecting hyperplanes decompose ambient space into pieces that give the cells
- chamber system with chambers the max dim cells of the complex and related by one of the equivalence relations ρ_i if obtained by reflection along the hyperplanes H_i

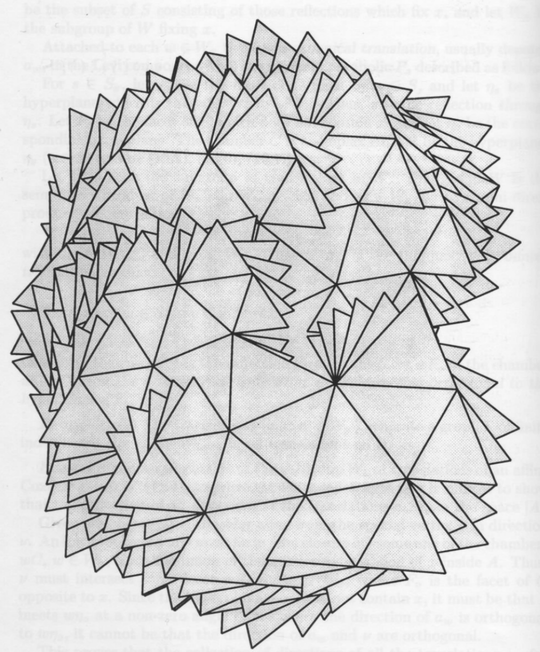
Example

- dihedral group $D_n = \langle s, t \,|\, s^2 = 1,\ t^2 = 1,\ (st)^n = 1 \}$
- chambers and Coxeter complex



Buildings

- n-dimensional building: simplicial complex B that is a union of subcomplexes called apartments with
  1. every k-simplex with $k < n$ is in at least three n-simplices
  2. any $(n-1)$-simplex in an apartment A lies in exactly two adjacent n-simplices of A
  3. the graph of adjacent n-simplices is connected
  4. any two simplices lie in a common apartment
  5. if two simplices σ, τ are in both A and A' apartments, $\exists$ simplicial isomorphism $A \simeq A'$ fixing σ, τ
- n-simplices are the chambers
- G-building: apartments are isomorphic to the Coxeter complex of G
- $\exists\ d : B \times C \to G$ (a kind of G-valued "metric") with $\rho_i = \{(b, b') \,|\, d(b, b') = 1 \text{ or } d(b, b') = x_i\}$ equivalence relations of the chamber system



Latin chamber systems and buildings

- Latin chamber systems are not themselves buildings
- but... a Latin chamber system has universal 2-cover that is a building iff the associated Thomsen loop is a group
- U. Meierfrankenfeld, G. Stroth, R.M. Weiss, *Local identification of spherical buildings and finite simple groups of Lie type*, Math. Proc. Camb. Phil. Soc., Vol.154 (2013) 527–547.

2-coverings

- path (gallery) in (the graph of) a chamber system is 2-homotopically trivial if it can be reduced to trivial path through a sequence of replacements of subgalleries lying in rank 2 residues by other galleries in same residue
- collection $\mathcal{C}$ of closed walks in a graph Δ: a $\mathcal{C}$-covering $\tilde{\Delta} \to \Delta$ is covering where every closed walk in $\mathcal{C}$ lifts to a closed walk in $\tilde{\Delta}$: $\exists$ universal $\mathcal{C}$-cover
- 2-covering of a chamber system is a $\mathcal{C}$-covering for $\mathcal{C} =$ all closed walks in rank 2 residues

General question: construction and properties of tensor networks on buildings

- What classes of buildings (or more general chamber systems) have interesting tensor networks?
- What holographic properties can one expect these tensor networks to have?
  - causal wedge and entanglement wedge reconstruction, complementary recovery (Coxeter complex structure is relevant here)
  - geodesic lengths in the bulk and boundary measure (Patterson–Sullivan measure, $CAT(0)$ property)
  - Ryu–Takayanagi formula for entanglement entropy in terms of bulk minimal areas/lengths (expect here stronger hyperbolicity needed, $CAT(-1)$ property)
- Elliott Gestaeu, Matilde Marcolli, and Sarthak Parikh, *Holographic tensor networks from hyperbolic buildings*, J. High Energy Phys. 2022, no. 10, Paper No. 169, 28 pp.