Quantum Codes & Quadratic forms.

Definition 13. An *involution* on an additive category $\mathcal{A}$ is an additive contravariant functor

$$* : \mathcal{A}^{\mathrm{op}} \to \mathcal{A}$$

together with a natural isomorphism

$$\eta : \mathrm{id}_{\mathcal{A}} \xrightarrow{\sim} * \circ *^{\mathrm{op}}$$

such that, for every object $A \in \mathcal{A}$, $(\eta_A)^* \circ \eta_{A^*} = \mathrm{id}_{A^*}$, i.e., the double dual is naturally isomorphic to the identity functor and the involution is of order two up to isomorphism.

We denote such a structure by the pair $(\mathcal{A}, *)$.

Example 14. Let R be an associative ring equipped with a ring involution

$$\overline{(\cdot)} : R \to R, \quad \overline{ab} = \bar{b}\bar{a}, \quad \bar{\bar{a}} = a.$$

Let $\mathcal{A}$ be the additive category whose objects are finitely generated, free left R-modules, and whose morphisms are R-linear maps.

Define a contravariant functor

$$* : \mathcal{A}^{\mathrm{op}} \to \mathcal{A}$$

as follows:

- For each object $M \in \mathcal{A}$, let

  $$M^* := \mathrm{Hom}_R(M, R),$$

  with the structure of a left R-module defined by

  $$(r \cdot f)(m) := f(m) \cdot \bar{r} \quad \text{for } r \in R, f \in M^*, m \in M.$$

- For a morphism $f : M \to N$, define

  $$f^* : N^* \to M^*, \quad f^*(\phi) := \phi \circ f.$$

There is a natural isomorphism $\eta_M : M \to M^{**}$, given by

$$\eta_M(m)(\phi) := \overline{\phi(m)} \quad \text{for } m \in M, \phi \in M^*.$$

Thus, $(\mathcal{A}, *)$ is an additive category with involution.

Ex. $R = R_0[\pi]$ where R_0 is commutative

$\bar{\cdot} : R \to R$

$g \mapsto g^{-1} \quad \forall g \in \pi$

Definition 15. Let $\mathcal{A}$ be an additive category with involution. For objects $M, N \in \mathcal{A}$, define a duality isomorphism

$$T_{M,N} : \mathrm{Hom}_{\mathcal{A}}(M, N^*) \to \mathrm{Hom}_{\mathcal{A}}(N, M^*), \quad \psi \mapsto \psi^* \circ \eta_N.$$

In particular, when $M = N$, we obtain a duality involution

$$T := T_{M,M} : \mathrm{Hom}_{\mathcal{A}}(M, M^*) \to \mathrm{Hom}_{\mathcal{A}}(M, M^*), \quad \psi \mapsto \psi^* \circ \eta_M.$$

Definition 16. For $\varepsilon = \pm 1$ and $M \in \mathcal{A}$, define the ε-duality involution

$$T_\varepsilon := \varepsilon T : \mathrm{Hom}_{\mathcal{A}}(M, M^*) \to \mathrm{Hom}_{\mathcal{A}}(M, M^*), \quad \psi \mapsto \varepsilon\psi^* \circ \eta_M.$$

Example 17. Let R be an associative ring equipped with a ring involution $\overline{(\cdot)} : R \to R$. Let $\mathcal{A}$ be the category of finitely generated, free left R-modules. For any $M, N \in \mathcal{A}$ and $\psi \in \mathrm{Hom}_{\mathcal{A}}(M, N^*)$, we have $\psi^*(y)(x) = \overline{\psi(x)(y)}$ for all $x \in M, y \in N$. If $M = N$, by writing $\psi(x)(y) =: \langle x, y\rangle \in R$

$$(T_\varepsilon(\psi)(x))(y) = \varepsilon\overline{\langle y, x\rangle},$$

for all $x, y \in M$.

Definition 18. Let $\mathcal{A}$ be an additive category with involution. An ε-quadratic form in $\mathcal{A}$ is a pair (M, ψ), where $M \in \mathcal{A}$ is an object together with an element

$$\psi \in Q_\varepsilon(M) := \mathrm{coker}(1 - T_\varepsilon : \mathrm{Hom}_{\mathcal{A}}(M, M^*) \to \mathrm{Hom}_{\mathcal{A}}(M, M^*)).$$

The form (M, ψ) is said to be *non-singular* if the morphism

$$(1 + T_\varepsilon)\psi = \psi + \varepsilon\psi^* : M \to M^*$$

is an isomorphism in $\mathcal{A}$.

Definition 19. A morphism of ε-quadratic forms

$$f : (M, \psi) \to (M', \psi')$$

is a morphism $f : M \to M'$ in $\mathcal{A}$ such that

$$f^*\psi' f = \psi \in Q_\varepsilon(M).$$

Definition 33. Let $\mathcal{A}$ be an additive category with involution. An ε-symmetric form in $\mathcal{A}$ is a pair (M, ψ), where $M \in \mathcal{A}$ is an object together with an element

$$\psi \in Q^\varepsilon(M) := \ker(1 - T_\varepsilon : \mathrm{Hom}_{\mathcal{A}}(M, M^*) \to \mathrm{Hom}_{\mathcal{A}}(M, M^*)).$$

The form (M, ψ) is said to be *non-singular* if the morphism

$$\psi : M \to M^*$$

is an isomorphism in $\mathcal{A}$.

Remark 34. If $\mathcal{A}$ is a category of modules over a ring where 2 is invertible, symmetric and quadratic forms coincide.

Modern terminology is Poincare objects.

Origin is probably Poincare duality.

M manifold $\rightsquigarrow$ chain complex over $R = R_0[\![\pi]\!]$
with (graded) symmetric form.

framing $\longrightarrow$ quadratic refinement

Classify the RHS:

1. Up to Witt equivalences related to surgery.

2. Up to isomorphism classes $\boxed{\text{Hard}}$

3. 2. + coarse-graining.

Coarse-graining: restriction of scalar to $R_0[H]$
with $H \leq \pi$ finite index subgroup.

LHS: Pass to finite cover

Dramatically easier classification.

Also most relevant to me.

Ex. $R = \mathbb{F}_p[x, x^{-1}]$

There are a lot of nonsingular skew-symmetric forms on free modules. But with coarse-graining it becomes the direct sum of

$$\left(R^2, \begin{pmatrix} & 1 \\ -1 & \end{pmatrix}\right) \quad \text{and} \quad \left(R^2, \begin{pmatrix} & x-1 \\ -x^{-1}+1 & \end{pmatrix}\right)$$

Quantum Codes

$R = \mathbb{Z}_n[G]$ or some other Ω

$$P = \left(R^{2q}, \begin{pmatrix} & I_q \\ -I_q & \end{pmatrix}\right)$$

LCP submodule with $L^\perp = \{ p \in P,\ \omega(p, l) = 0\ \forall l \in L \}$
$= L$

$\longrightarrow$ $\boxed{\text{G-invariant commuting local Hamiltonian on a Cayley graph of G.}}$

Most commonly $G = \mathbb{Z}^D$ for some D.

$D=2$: Toric code All Witt trivial abelian anyon theories

$D=3$: Fractons show up.

$D \geq 4$: Wilder things.

Ex. $R = \mathbb{F}_2[x, x^{-1}, y, y^{-1}]$

$$\sigma_{\text{2D-toric}} = \begin{pmatrix} y+xy & 0 \\ x+xy & 0 \\ \hline 0 & 1+y \\ 0 & 1+x \end{pmatrix} \cong \begin{pmatrix} 1+\bar{x} & 0 \\ 1+\bar{y} & 0 \\ \hline 0 & 1+y \\ 0 & 1+x \end{pmatrix}.$$

$P = R^4$ and $L = \mathrm{im}\, \sigma_{\text{2D-toric}}$

$Q^0 \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2$ e and m anyons.

Invariants of Phase

Definition: $Q^i = \mathrm{Ext}_R^{i+1}(P/L, R)$

Q^0 point excitations$/\sim$

Q^i Extented excitations$/\sim$

7.1. 3D $\mathbb{Z}_n$-toric code. We take $\Lambda = \mathbb{Z}^3$ and denote generators of R corresponding to three basis vectors by x, y, z, so that R is a Laurent polynomial ring in three variables x, y, z. 3D toric code is defined by $P = R^6$, $L = \mathrm{im}(\sigma)$ with

$$\sigma = \begin{pmatrix} 1-\bar{x} & 0 & 0 & 0 \\ 1-\bar{y} & 0 & 0 & 0 \\ 1-\bar{z} & 0 & 0 & 0 \\ 0 & 0 & z-1 & y-1 \\ 0 & z-1 & 0 & 1-x \\ 0 & 1-y & 1-x & 0 \end{pmatrix}. \tag{68}$$

$$\mathrm{Ext}_R^1(\overline{P/L}, R) \cong \mathbb{Z}_n,$$
$$\mathrm{Ext}_R^2(\overline{P/L}, R) \cong \mathbb{Z}_n,$$

Full Classification in 2+1 D.

Theorem (Haah, Ruba–Y.)

$D=2$. • Q^0 is <u>finite</u> and $Q^i=0$ $i \geq 1$

There is a non-singular quadratic form

• $\theta: Q^0 \longrightarrow \mathbb{Q}/\mathbb{Z}$.

Moreover, θ is Witt trivial.

(Q^0, θ) corresponds to the abelian anyon theory the local Hamiltonian is meant to realize on $\mathbb{Z}^2$ lattice!

Coarse-graining amounts to forgetting the R-module structure on Q^0 because Q^0 is finite.

Theorem 78 (Theorem 8.4.12 in [7]). *There are equivalences of categories:*

$$\{\textit{pointed braided fusion categories}\} \longleftrightarrow \{\textit{pre-metric groups}\}, \tag{217a}$$

$$\{\textit{pointed modular tensor categories}\} \longleftrightarrow \{\textit{metric groups}\}. \tag{217b}$$

Modular tensor categories correspond to (2+1)-dimensional topological quantum field theories via the Reshetikhin–Turaev construction [31], which assigns a TQFT to each MTC. Freed and Teleman [8] show that such a TQFT can support a gapped boundary if and only if the underlying MTC is equivalent to the Drinfeld center of a fusion category—that is, when the theory also arises from a Turaev–Viro model [36]. In the case of pointed MTCs, their condition for supporting a gapped boundary translates to the corresponding metric group being metabolic. This criterion has a natural counterpart in abelian Chern–Simons theory, where gapped boundaries correspond to Lagrangian subgroups of the charge lattice, as studied by Kapustin and Saulina [16].

What about higher dimensions $D \geq 3$.

Braiding

Let $\hat{R}$ be the module $R_0[[G]]$

Corollary 9. *Let M be a finitely generated R-modules, for all $i \geq 0$, there is a canonical isomorphism*

$$\mathrm{Tor}_i^R(M, \widehat{R}) \cong \mathrm{Hom}_R(\mathrm{Ext}_R^i(M, R), \widehat{R}). \tag{37}$$

In particular,

$$\mathrm{Tor}_i^R(M, \widehat{R}) = 0 \text{ if and only if } \mathrm{Ext}_R^i(M, R) = 0. \tag{38}$$

Proof. Let $A = M, B = R$ and $C = \widehat{R}$ in the proposition above. Then (38) is deduced from the fact that $\widehat{R}$ is a cogenerator. □

By Corollary 9, $\mathbb{Z}_n$-duals of charge modules of a stabilizer code described by a Lagrangian $L \subset P$ are given by Tor modules:

$$\mathrm{Tor}_{i+1}^R(P/L, \widehat{R}) \cong \mathrm{Hom}_R(Q_L^i, \widehat{R}) \cong \mathrm{Hom}_{\mathbb{Z}_n}(Q_L^i, \mathbb{Z}_n). \tag{39}$$

Free resolution:

$$\cdots \to F' \to P \to P/L \to 0$$

- $\_ \otimes \hat{R}$:

$$\cdots \to F' \otimes \hat{R} \to P \otimes \hat{R} \to 0$$

- $\mathrm{Hom}(\_, R)$:

$$0 \to \mathrm{Hom}(P, R) \to \mathrm{Hom}(F', R) \to \cdots$$

Dualize:

$$\begin{tikzcd}
\cdots \arrow[r] & \mathrm{Hom}(\mathrm{Hom}(F^1,R),\hat{R}) \arrow[r] & \mathrm{Hom}(\mathrm{Hom}(P,R),\hat{R}) \arrow[r] & 0 \\
\cdots \arrow[r] & F^1\otimes\hat{R} \arrow[r] \arrow[u] & P\otimes\hat{R} \arrow[r] \arrow[u] & 0
\end{tikzcd} \Bigg\} \beta$$

β is a quasi-isomorphism.

In other words, $R\mathrm{Hom}(P/L, R)$ and $P/L\otimes^{\mathbb{L}}\hat{R}$ are dual.

Fully mobile case (Topological order?)

Fully mobile $\Leftrightarrow$ Q^i finite.

Coarse-graining is forgetting R-module structure

Duality collapse to duality between Q^i and Q^{D-i-2} looking like Poincare duality.

Aspiration

Stabilizer codes	Manifolds.
Lattice with symmetry.	Fundamental group
Charge modules Q^i	Homology modules
Braiding.	Poincare duality
Spin Statistics	quadratic refinement
Coarse - graining	lifting to a finite cover