Quantum Error Correcting Codes and Matrix Factorisations

Will Troiani

May 3, 2023

1 Quantum Error Correcting Codes

Definition 1.0.1. A qubit is a copy of the \mathbb{C} -Hilbert space \mathbb{C}^2 .

The **state** of a qubit \mathbb{C}^2 is a vector $|\psi\rangle \in \mathbb{C}^2$ of norm 1.

A pair $(\mathbb{C}^2, |\psi\rangle)$ consisting of a qubit \mathbb{C}^2 and a state $|\psi\rangle \in \mathbb{C}^2$ is a **prepared qubit** and we say \mathbb{C}^2 has been **prepared** to $|\psi\rangle$.

Definition 1.0.2. Let $\mathcal{H}_1, \mathcal{H}_2$ be two state spaces. The **composite state** space is $\mathcal{H}_1 \otimes \mathcal{H}_2$. A **state** of a composite system is a vector $|\psi\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2$ which can be written as a linear combination of pure tensors

$$\alpha_1 |\psi_1\rangle + \ldots + \alpha_n |\psi_n\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2$$

where the coefficients satisfy $|\alpha_1|^2 + \ldots + |\alpha_n|^2 = 1$.

We define a measurement as a family of possible outcomes with assocaited probabilities. We allow for the possibility that measurements effect the state, and so measurements are operators upon the state space.

Definition 1.0.3. A measurement on a state space \mathcal{H} is a finite family of linear operators $\{M_m : \mathcal{H} \longrightarrow \mathcal{H}\}_{m \in \mathcal{M}}$ satisfying the completeness condition.

$$\sum_{m \in \mathcal{M}} M_m^{\dagger} M_m = I \tag{1}$$

An element $m \in \mathcal{M}$ is an **outcome**.

The **resulting state** after measurement $\{M_m\}_{m\in\mathcal{M}}$ and outcome m is:

$$\frac{M_m |\psi\rangle}{\sqrt{p(m)}}\tag{2}$$

Remark 1.0.4. Associated to every measurement and state vector $|\psi\rangle$ there is a value

$$p(m) := \langle \psi | M_m^{\dagger} M_m | \psi \rangle = || M_m | \psi \rangle ||^2$$
(3)

It follows from (1) that $p(m) \leq 1$ for all $m, |\psi\rangle$. We understand p(m) as the probability of outcome m on the measurement $\{M_m\}_{m\in\mathcal{M}}$.

Definition 1.0.5. A linear transformation P is a **projector** if $P^2 = P$.

Definition 1.0.6. A quantum error correcting code (QECC) is a pair $Q = (\mathcal{H}, S)$ consisting of a state space \mathcal{H} along with a set of operators S on \mathcal{H} . The elements of S are the **stabilisers**. The **codespace** \mathcal{H}^S of \mathcal{Q} is the maximal subspace of \mathcal{H} invariant under all the operators in S.

See Appendix A for an example of a simple QECC.

2 Matrix factorisations

2.1 Koszul Complex

Recall that a \mathbb{Z}_2 -graded ring R comes equipt with a choice of isomorphism $R \cong R_0 \oplus R_1$ where R_0, R_1 are subgroups of R. The elements of R_1 are **odd**.

Definition 2.1.1. Let E be a \mathbb{Z}_2 -graded ring and consider a set of odd elements $\theta_1, \ldots, \theta_n, \theta_1^*, \ldots, \theta_n^* \in E$. These **satisfy the canonical anticommutation relations** if the following hold for all $i, j = 1, \ldots, n$.

- $\bullet \ \theta_i \theta_j + \theta_j \theta_i = 0$
- $\bullet \ \theta_i^* \theta_j^* + \theta_j^* \theta_i^* = 0$
- $\bullet \ \theta_i \theta_j^* + \theta_j \theta_i^* = \delta_{ij}$

When $A \cong A_0 \oplus A_1$, $B \cong B_1 \oplus B_2$ are \mathbb{Z}_2 -graded modules (over a graded ring R, say), a homomorphism $\varphi : A \longrightarrow B$ can be written as a matrix

$$\begin{pmatrix} \varphi_{00} & \varphi_{01} \\ \varphi_{10} & \varphi_{11} \end{pmatrix} \tag{4}$$

where $\varphi_{00}(A_0) \subseteq B_0, \varphi_{01}(A_0) \subseteq B_1, \varphi_{10}(A_1) \subseteq B_0, \varphi_{11}(A_1) \subseteq B_1$. Writing this matrix as a sum yields respectively an even and odd component of φ

$$\begin{pmatrix} \varphi_{00} & \varphi_{01} \\ \varphi_{10} & \varphi_{11} \end{pmatrix} = \begin{pmatrix} \varphi_{00} & 0 \\ 0 & \varphi_{11} \end{pmatrix} + \begin{pmatrix} 0 & \varphi_{01} \\ \varphi_{10} & 0 \end{pmatrix}$$
 (5)

In this way, Hom(A, B) is also a \mathbb{Z}_2 -graded module over R.

When E is a \mathbb{Z}_2 -graded ring of the form E = End(A) for some \mathbb{Z}_2 -graded ring A, then E admitting a set of odd elements satisfying the anticommutation relations is sufficient for A to admit a Clifford algebra representation [1, Lemma 5.6.2].

Definition 2.1.2. The Clifford Algebra C_n is generated by elements $\mu_1, \ldots, \mu_n, \nu_1, \ldots, \nu_n$ subject to:

$$[\mu_i, \mu_j] = -2\delta_{ij} \quad [\nu_i, \nu_j] = 2\delta_{ij} \quad [\mu_i, \nu_j] = 0$$

where
$$[\xi, \zeta] = \xi \zeta + \zeta \xi$$
 for $\xi, \zeta \in \{\mu_1, \dots, \mu_n, \nu_1, \dots, \nu_n\}$.

There is a C_m action on S_m and hence on $S_m \otimes_{\mathbb{C}} (Y \otimes X)$. This is induced by two canonical endomorphisms which exist on S_m . The **wedge** and **contraction** maps.

$$\theta_i: \bigwedge^{d-1} (\mathbb{C}\theta_1 \oplus \ldots \oplus \mathbb{C}\theta_n) \longrightarrow \bigwedge^{d} (\mathbb{C}\theta_1 \oplus \ldots \oplus \mathbb{C}\theta_n)$$
$$\theta_{j_1} \wedge \ldots \wedge \theta_{j_{d-1}} \longmapsto \theta_i \wedge \theta_{j_1} \wedge \ldots \wedge \theta_{j_{d-1}}$$

and

$$\theta_i^* : \bigwedge^d (\mathbb{C}\theta_1 \oplus \ldots \oplus \mathbb{C}\theta_n) \longrightarrow \bigwedge^{d-1} (\mathbb{C}\theta_1 \oplus \ldots \oplus \mathbb{C}\theta_n)$$
$$\theta_{j_1} \wedge \ldots \wedge \theta_{j_d} \longmapsto \sum_{k=1}^d (-1)^{k+1} \delta_{j_k=i} \theta_{j_1} \wedge \ldots \wedge \hat{\theta}_{j_k} \wedge \ldots \wedge \theta_{j_d}$$

Given a free R-module $A = R\theta_1 \oplus \ldots \oplus R\theta_r$ of rank r, the multiplication and contraction operators satisfy the canonical anticommutation relations. Thus, A admits a Clifford algebra representation.

2.2 Matrix factorisations

Let k denote a ring.

Recall that if A, B are \mathbb{Z} -graded k-modules then Hom(A, B) is also \mathbb{Z} -graded [3]. We have a similar definition for \mathbb{Z}_2 -graded modules.

Definition 2.2.1. Let A, B be \mathbb{Z}_2 -graded k-modules. A homomorphism $f: A \longrightarrow B$ is **even** if $f(A_0) \subseteq B_0$ and $f(A_1) \subseteq A_1$. The homomorphism f is **odd** if $f(A_0) \subseteq B_1$ and $f(A_1) \subseteq B_0$.

Remark 2.2.2. If $f: A \longrightarrow B$ is any module homomorphism then f can be written as a matrix

 $\begin{pmatrix} f_{00} & f_{01} \\ f_{10} & f_{11} \end{pmatrix} \tag{6}$

The morphism f is thus even if $f_{01} = f_{10} = 0$ and is odd if $f_{00} = f_{11} = 0$. This also shows that the morphism f can be written as the sum of an even and an odd component.

Definition 2.2.3. Let $f \in k$ be a non-zero divisor. A linear factorisation of $f \in k$ over k is a pair (X, ∂_X) consisting of a \mathbb{Z}_2 -graded k-module $X = X_0 \oplus X_1$ and an odd homomorphism $\partial_X : X \longrightarrow X$ satisfying

$$\partial_X^2 = f \cdot \mathrm{id}_X \tag{7}$$

If X is free then (X, ∂_X) is a matrix factorisation.

The theory of Matrix factorisations is motivated by the search for square roots to operators. As a toy example, multiplication by $x^2 - y^2$ in $\mathbb{C}[x, y]$ does not admit a square root, but it does if we allow matrix solutions.

$$\begin{pmatrix} 0 & x - y \\ x + y & 0 \end{pmatrix}^2 = (x^2 - y^2) \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$
 (8)

A more serious example is given by the square root of the Laplacian operator, see the Introduction of [4].

Our interest in matrix factorsations comes from the fact that appropriate homotopy categories of matrix factorsations form the homoategories of the bicategory of Landau-Ginzburg models, which we anticipate to find within a model of multiplicative linear logic (proofs as hypersurface singularities).

Definition 2.2.4. A morphism of linear factorisations

$$\alpha: \left(X = X_0 \oplus X_1, d_X = \begin{pmatrix} 0 & p_X \\ q_X & 0 \end{pmatrix}\right) \longrightarrow \left(Y = Y_0 \oplus Y_1, d_Y = \begin{pmatrix} 0 & p_Y \\ q_Y & 0 \end{pmatrix}\right)$$

of $f \in R$ is a pair of morphisms $\alpha_0 : X_0 \longrightarrow Y_0, \alpha_1 : X_1 \longrightarrow Y_1$ rendering the following diagram commutative.

$$X_{0} \xrightarrow{p_{X}} X_{1} \xrightarrow{q_{X}} X_{0}$$

$$\downarrow^{\alpha_{0}} \qquad \downarrow^{\alpha_{1}} \qquad \downarrow^{\alpha_{0}}$$

$$Y_{0} \xrightarrow{p_{Y}} Y_{1} \xrightarrow{q_{Y}} Y_{0}$$

$$(9)$$

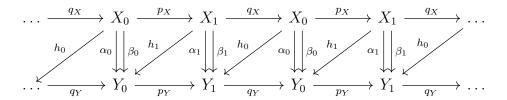
Given a matrix factorisation $(X = X_0 \oplus X_1, d_X) = \begin{pmatrix} 0 & p_X \\ q_X & 0 \end{pmatrix}$ there is a sequence

 $\dots \xrightarrow{p_X} X_1 \xrightarrow{q_X} X_0 \xrightarrow{p_X} X_1 \xrightarrow{q_X} \dots \tag{10}$

however, we note that in general $d_X^2 = f \cdot I \neq 0$ and so strictly speaking this is not a chain complex.

Definition 2.2.5. We use the notation of Definition 2.2.4. Let $\beta = (\beta_0, \beta_1)$ be another morphism of linear factorisations $(X, d_X) \longrightarrow (Y, d_Y)$. The morphisms α, β are **homotopic** if there exists a pair of morphisms $h_0: X_0 \longrightarrow Y_1, h_1: X_1 \longrightarrow Y_0$ such that the following holds

$$\alpha_0 - \beta_0 = q_Y h_0 + h_1 p_X, \qquad \alpha_1 - \beta_1 = h_0 q_X + p_Y h_1$$
 (11)



The relation of homotopy defines an equivalence relation on the set of morphisms of linear factorisations.

Definition 2.2.6. A linear transformation whose underlying \mathbb{Z}_2 -graded k-module is free and of finite rank is a **matrix factorisation**. There is a category $\text{hmf}(k[\underline{x}], f)$ where the objects are matrix factorisations of f and the morphisms are homotopy equivalence classes of morphisms of matrix factorisations.

Definition 2.2.7. If (X, d_X) is a matrix factorisation then so is $(X[1], -d_X)$. If we denote this by $\Psi(X, d_X)$ then $\Psi : \operatorname{hmf}(k[\underline{x}], f) \longrightarrow \operatorname{hmf}(k[\underline{x}], f)$ is extends to an endofunctor which induces a supercategorical structure on $\operatorname{hmf}(k[\underline{x}], f)$ if we take $\xi : \Psi^2 \longrightarrow 1_{\operatorname{hmf}(k[\underline{x}], f)}$ to be the identity.

Definition 2.2.8. Let (X, ∂_X) be a linear factorisation of $f \in k$ over k and (Y, ∂_Y) a linear factorisation of $g \in k$ also over k. Then the **tensor product** of (X, ∂_X) and (Y, ∂_Y) consists of the following data:

$$X \otimes_k Y, \qquad \partial_{X \otimes_k Y} = d_X \otimes 1 + 1 \otimes d_Y$$
 (12)

where $X \otimes_k Y$ is the *graded* tensor product, which satisfies the following for all $x_1, x_2 \in X, y_1, y_2 \in Y$.

$$(x_1 \otimes y_1)(x_2 \otimes y_2) = (-1)^{\deg(x_2)\deg(y_1)}(x_1 x_2 \otimes y_1 y_2)$$
(13)

Lemma 2.2.9. The tensor product $(X \otimes_k Y, \partial_{X \otimes_k Y})$ is a linear factorisation of f + g.

Proof. See [1][Page 35].
$$\Box$$

In the special case where there exists $f \in k[\underline{x}], g \in k[\underline{y}], h \in k[\underline{z}]$ and (X, ∂_X) is a linear factorisation of $f - g \in k[\underline{x}, \underline{y}]$ and (Y, ∂_Y) is a linear factorisation of $g - h \in k[\underline{y}, \underline{z}]$ then we also have the *cut* of (X, ∂_X) and (Y, ∂_Y) .

Definition 2.2.10. For each $y_1, \ldots, y_n \in \underline{y}$ let $\partial_{y_i} g$ denote the formal partial derivative of g with respect to y_i . Denote by J_g the following k[y]-module.

$$J_g := k[\underline{y}]/(\partial_{y_1}g, \dots, \partial_{y_n}g) \tag{14}$$

The **cut** of $(X, \partial_X), (Y, \partial_Y)$ is the data of

$$X|Y := (X \otimes_{k[\underline{y}]} J_g \otimes_{k[\underline{y}]} Y), \qquad \partial_{X|Y} = d_X \otimes 1 \otimes 1 + 1 \otimes 1 \otimes d_Y \qquad (15)$$

Lemma 2.2.11. The cut X|Y is a matrix factorisation of f-h.

Proof. Check this.
$$\Box$$

We will use the following Lemma to indirectly talk about matrix factorisations using \mathbb{Z}_2 -graded modules over Clifford algebras.

Definition 2.2.12. Let $k[\underline{x}], k[\underline{y}]$ denote polynomial rings over variables x_1, \ldots, x_n and y_1, \ldots, y_n respectively. Let $U(\underline{x}) = \sum_{i=1}^n x_i^2$.

We let C_U denote the \mathbb{Z}_2 -graded k-algebra with multiplicative generators $\mu_1, \ldots, \mu_n, \nu_1, \ldots, \mu_n$ satisfying the relations

$$[\mu_i, \mu_j] = -2\delta_{ij}$$
 $[\mu_i, \nu_j] = 0$ $[\nu_i, \nu_j] = 2\delta_{ij}$ (16)

where $\delta_{ij} = 1$ if and only if i = j and $\delta_{ij} = 0$ otherwise is the Kronecker delta.

Lemma 2.2.13. Let \tilde{X} be a \mathbb{Z}_2 -graded C_U -module which is free and finitely generated over k. Then $X := \tilde{X} \otimes_k k[\underline{x},\underline{y}]$ coupled with the map

$$\partial_X = \sum_{i=1}^n \mu_i x_i + \sum_{j=1}^n \nu_j y_j \tag{17}$$

is a matrix factorisation of $U(y) - U(\underline{x}) \in k[\underline{x}, y]$.

Remark 2.2.14. The map (17) is odd because we consider $k[\underline{x}, \underline{y}]$ to admit the \mathbb{Z}_2 -grading

$$k[\underline{x}, y] \oplus 0 \tag{18}$$

That is, $k[\underline{x}, \underline{y}]$ has $k[\underline{x}, \underline{y}]$ entirely in degree 0, and the zero module 0 in degree 1. For example, if \underline{x}, y are both singleton sets $\underline{x} = \{x\}, y = \{y\}$ then

$$\deg(\partial_X(x \otimes p)) = \deg(\mu x \otimes xp + \nu x \otimes y_j p)$$
$$= \deg(\mu x) \ (= \deg(\nu x))$$
$$= \deg(x) + 1$$

Example 2.2.15. Let \underline{x} be a set of variables $\{x_1, \ldots, x_n\}$ and $\sigma \in S_n$ a permutation on this set. Let \tilde{X} denote the \mathbb{Z}_2 -graded k-algebra

$$\tilde{X} := \bigwedge (k\theta_1 \oplus \ldots \oplus k\theta_n) \tag{19}$$

which is a C_U -algebra (Definition 2.2.12) with C_U -action induced by the following

$$\mu_i = \theta_{\sigma^{-1}i} + \theta_{\sigma^{-1}i}^*$$
$$\nu_i = \theta_i - \theta_i^*$$

Thus, by Lemma 2.2.13 we obtain a matrix factorisation $(X = \tilde{X} \otimes k[\underline{x}, \underline{y}], \partial_X)$. Now say we had another similar matrix factorisation; let $\underline{y} = \{y_1, \dots, y_m\}$ be another set of variables and let τ be a permutation on this set. Let \tilde{Y} denote the \mathbb{Z}_2 -graded k-algebra

$$\tilde{Y} := \bigwedge (k\psi_1 \oplus \ldots \oplus k\psi_m) \tag{20}$$

This is a C_U -module with C_U -action induced by the following

$$\overline{\nu_i} = \psi_{\tau^{-1}i} + \psi_{\tau^{-1}i}^*$$

$$\omega_i = \psi_i - \psi_i^*$$

This induces a matrix factorisation $(Y = \tilde{Y} \otimes k[\underline{y}, \underline{z}], \partial_Y)$ of $U(\underline{y}) - U(\underline{z})$ where

$$\partial_Y := \sum_{i=1}^n \overline{\nu}_i y_i + \sum_{i=1}^n \omega_i z_i \tag{21}$$

and $\underline{z} = \{z_1, \dots, z_n\}$ is another set of variables.

We will first consider the cut X|Y. The sequence of partial derivatives $(\partial_{u_1}U(y),\ldots,\partial_{u_n}U(y))=(2y_1,\ldots,2y_n)$ and so

$$J_{U(y)} = k[y]/(y_1, \dots, y_n) = k$$
 (22)

as a k[y]-module with trivial k[y]-action. We thus have

$$X|Y = X \otimes_{k[x,y]} k \otimes_{k[y,z]} Y, \qquad \partial_{X|Y} = d_X \otimes 1 \otimes 1 + 1 \otimes 1 \otimes d_Y \qquad (23)$$

Say R is a commutative ring. We will consider an element $f \in R$ of the following particular form: say we have $a_1, \ldots, a_n, b_1, \ldots, b_n \in R$ such that $f = \sum_{i=1}^n a_i b_i$. The guiding example of such an element is when R is a polynomial ring and f is a quadratic form.

Lemma 2.2.16. Suppose M is a \mathbb{Z}_2 -graded R-module with odd R-linear maps $\theta_i, \theta_i^* : M \longrightarrow M, i = 1, \ldots, n$ satisfying the canonical anticommutation relations. Then, setting $\delta_+ = \sum_{i=1}^n a_i \theta_i$ and $\delta_- = \sum_{i=1}^n b_i \theta_i^*$ we have that $(M, \delta_- + \delta_+)$ is a linear factorisation of f.

Proof. See [1, Lemma
$$4.2.3$$
].

Therefore, $(\bigwedge R^n, \delta_- + \delta_+)$ is a matrix factorisation of f. This is the Koszul matrix factorisation of f.

A Quantum error correcting codes examples

Definition A.0.1 (Bit flip correction). Input: a received message $|\psi\rangle$,

1. perform the following projective measurements:

$$\langle \psi | Z_1 Z_2 | \psi \rangle$$
 with resulting state $| \psi' \rangle$, (24)

followed by

$$\langle \psi' | Z_2 Z_3 | \psi' \rangle \tag{25}$$

let (r_1, r_2) be the pair of results from these measurements.

- 2. It will be shown that $r_1, r_2 \in \{1, -1\}$, and the resulting state of the second measurement is $|\psi\rangle$.
- 3. Now retrieve $|\varphi\rangle$ based on the values of r_1, r_2 :
 - if $(r_1, r_2) = (1, 1)$, return $|\psi\rangle$,
 - if $(r_1, r_2) = (-1, 1)$, return $X_1 | \psi \rangle$,
 - if $(r_1, r_2) = (1, -1)$, return $X_3 | \psi \rangle$,
 - if $(r_1, r_2) = (-1, -1)$, return $X_2 | \psi \rangle$

We now prove correctness of Algorithm A.0.1:

Proof. It will be helpful to first notice:

$$Z_1 Z_2 |000\rangle = |000\rangle$$
 $Z_1 Z_2 |001\rangle = |001\rangle$ $Z_1 Z_2 |010\rangle = -|010\rangle$ $Z_1 Z_2 |011\rangle = -|011\rangle$ $Z_1 Z_2 |100\rangle = -|100\rangle$ $Z_1 Z_2 |101\rangle = -|101\rangle$ $Z_1 Z_2 |110\rangle = |110\rangle$ $Z_1 Z_2 |111\rangle = |111\rangle$

Let $|\psi\rangle := a\,|010\rangle + b\,|101\rangle$ be a state, ie, an element of $\mathbb{H}^{\otimes 3}$. We perform the measurement Z_1Z_2 followed by Z_2Z_3 :

$$\langle \psi | Z_1 Z_2 | \psi \rangle = (a \langle 010| + b \langle 101|) Z_1 Z_2 (a | 010 \rangle + b | 101 \rangle)$$

= $(a \langle 010| + b \langle 101|) (-a | 010 \rangle - b | 101 \rangle)$
= $-a^2 - b^2 = -1$

and

$$\langle \psi | Z_2 Z_3 | \psi \rangle = (a \langle 010| + b \langle 101|) Z_1 Z_2 (a | 010 \rangle + b | 101 \rangle)$$

$$= (a \langle 010| + b \langle 101|) (-a | 010 \rangle - b | 101 \rangle)$$

$$= -a^2 - b^2 = -1$$

We can infer from the fact that both of these came out as -1 that it was the second bit which was flipped, and so we can correct this. However, what is the impact of this measurement on the state? Again we calculate:

$$Z_1 Z_2(a |010\rangle + b |101\rangle) = Z_1(-a |010\rangle + b |101\rangle)$$

= $-a |010\rangle - b |101\rangle$

and

$$Z_2 Z_3(-a|010\rangle - b|101\rangle) = Z_2(-a|010\rangle + b|101\rangle)$$

= $a|010\rangle + b|101\rangle$

and so the measurements (in the end) did not impact our state.

References

- [1] R. Hitchcock. Differentiation, Division and the Bicategory of Landau-Ginzburg Models. Master's thesis. http://therisingsea.org/notes/MScThesisRohanHitchcock.pdf
- [2] F. Borceux. *Handbook of Categorical Algebra 1: Basic Category Theory*. Vol. 50. Encyclopedia of Mathematics and its Applications. Cambridge University Press, 1994.
- [3] W. Troiani. Secondary Commutative Algebra.
- [4] T. Friedrich, Dirac Operators in Riemannian Geometry 20MathematicsSubjectClasification.Primary58Jx; Secondary 53C27, 53C28, 57R57, 58J05, 58J20, 58J50, 81R25.
- [5] D. Murfet. The cut operation on matrix factorisations
- [6] M. Nielsen, I. Chuang Quantum Computation and Quantum Information tenth anniversary Cambridge University Press, 09 December 2010
- [7] W. Troiani *Elementary Commutative Algebra* https://williamtroiani.github.io/pdfs/CommutativeAlgebraWithLin.pdf
- [8] J. Baez. https://math.ucr.edu/home/baez/quantum/node4.html