Hypermap-Homology Quantum Codes

Martin Leslie

Department of Mathematics
University of Arizona
Advisor: Dr. Marek Rychlik

May 10, 2013

Quantum computing

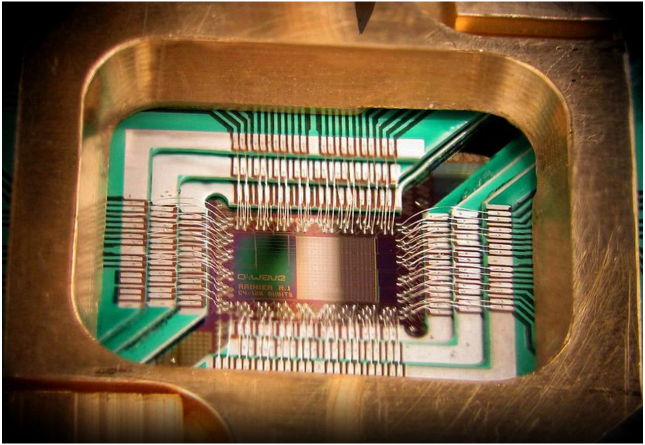


Figure 1 : A 128-qubit superconducting adiabatic quantum optimization processor from D-Wave Systems Inc.

Quantum states and Pauli matrices

- We work with a system of n qubits, the state of which is given by an element $|\psi\rangle \in \mathcal{H}_n = (\mathbb{C}^2)^{\otimes n}$.
- We insist that $|\psi\rangle = \sum_{\vec{\imath} \in \mathbb{F}_2^n} a_{\vec{\imath}} |\vec{\imath}\rangle$ is normalized so that $\sum |a_{\vec{\imath}}|^2 = 1$ and consider states differing by $e^{i\theta}$ with $\theta \in \mathbb{R}$ to be equivalent.
- Define the Pauli operators X, Y, Z by

$$X(a|0\rangle + b|1\rangle) = a|1\rangle + b|0\rangle,$$

$$Z(a|0\rangle + b|1\rangle) = a|0\rangle - b|1\rangle$$

  and $Y = iXZ$.
- We think of I, X, Y and Z as errors that can occur to a single qubit.

Quantum errors and error correction

- Assume we have encoded a k-qubit state into an n-qubit state $|\psi\rangle$.
- Define the group

$$G_n = \left\{ c \bigotimes_{i=1}^{n} A_i \mid c \in \{\pm 1, \pm i\}, A_i \in \{I, X, Y, Z\} \right\}.$$

- Assume that an error $E \in G_n$ occurs so that the state is now $E|\psi\rangle$. To correct the error we need to measure $E|\psi\rangle$ in such a way that we only learn E not $|\psi\rangle$.
- A quantum (error-correcting) code is a method for encoding states and correcting errors. A quantum code has parameters $[n, k, d]$ where a code with *minimum distance* d can correct any errors on at most $\lfloor (d-1)/2 \rfloor$ qubits.

CSS codes

- A CSS (Calderbank-Shor-Steane) code is defined by two binary matrices H_X and H_Z such that $H_X H_Z^T = 0$.
- We think of H_X and H_Z as being parity check matrices for classical codes C_X and C_Z. Thus

$$C_X = \ker H_X, \quad C_Z = \ker H_Z, \quad C_X^\perp = \operatorname{im} H_X^T, \quad C_Z^\perp = \operatorname{im} H_Z^T.$$

- It can be shown that a CSS code has parameters $[n, k, d]$ where H_X and H_Z have n columns,

$$k = n - \dim C_X^\perp - \dim C_Z^\perp \text{ and}$$

$$d = \min\{\operatorname{wt}(c) \colon c \in (C_X \setminus C_Z^\perp) \cup (C_Z \setminus C_X^\perp)\}.$$

Some families of CSS codes

- Calderbank and Shor [CS96] showed that there exist a family of CSS codes with $d \sim c_1 n$ and $k \sim c_2 n$.
- Codes using sparse matrices are of interest because they can be efficiently decoded. However there are no known sparse CSS codes with performance as good as Calderbank and Shor's codes.
- Most practically well-performing families of sparse codes (for example MacKay, Mitchison and McFadden's 'bicycle codes' [MMM04]) have minimum distances that are bounded above as n increases.
- Codes based on homological ideas such as embedding graphs on surfaces have achieved $d \sim c\sqrt{n}$ or $d \sim c\sqrt{n \log n}$. The first code of this type was Kitaev's toric code [Kit97].

Kitaev's toric code

- Embed an $m \times m$ grid on a torus.

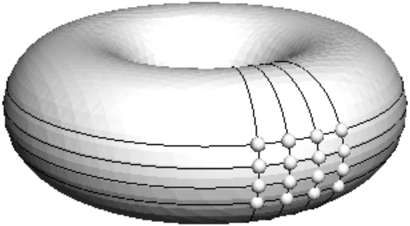
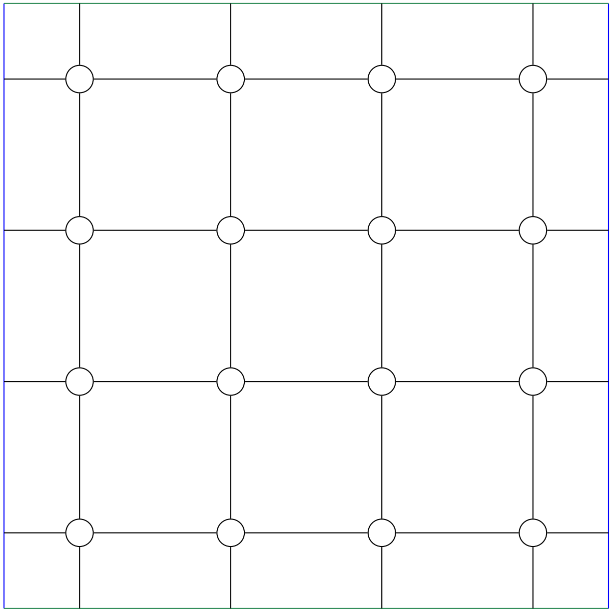


Figure 2 : An example with $m = 4$.

An $m \times m$ grid on a torus



Constructing the toric code

- Consider cellular $\mathbb{F}_2$-homology of this embedded graph. This gives us a chain complex

$$\mathcal{F} \xrightarrow{\partial_2} \mathcal{E} \xrightarrow{\partial_1} \mathcal{V}.$$

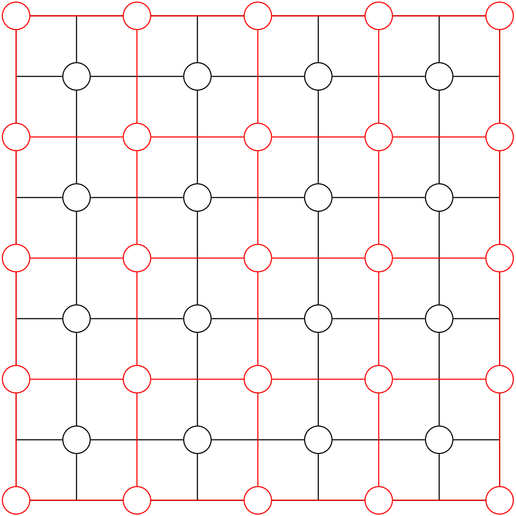
- Take $H_X = [\partial_1]$ and $H_Z = [\partial_2]^T$. Then $H_X H_Z^T = 0$.
- The number of edges is $n = 2m^2$.
- The first homology group is

$$H_1 = \ker \partial_1 / \operatorname{im} \partial_2 \cong C_X / C_Z^{\perp}.$$

- Thus $k = n - \dim C_X^{\perp} - \dim C_Z^{\perp} = \dim(C_X / C_Z^{\perp}) = 2$.

The dual of an $m \times m$ grid on a torus

- The first cohomology group is $H^1 \cong C_Z / C_X^\perp$, which is also the homology of the Poincare dual graph, pictured below for $m = 4$.

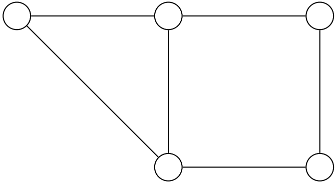


Finding the minimum distance

- The minimum distance d is the minimum length of a non-boundary cycle in the graph and its dual graph. So $d = m$.
- So we have an $[n, k, d]$ code with $n = 2m^2$, $k = 2$ and $d = m$.
- In particular, $d = \sqrt{n/2}$.

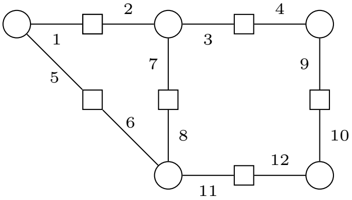
Hypergraphs

- A hypergraph is a generalization of a graph where an edge can be connected to more than 2 vertices.
- A graph:



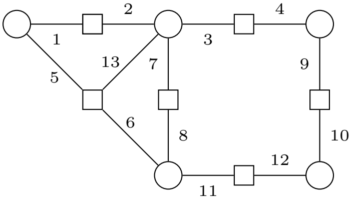
Hypergraphs

- A hypergraph is a generalization of a graph where an edge can be connected to more than 2 vertices.
- The hypergraph version of the graph:



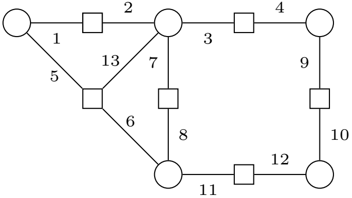
Hypergraphs

- A hypergraph is a generalization of a graph where an edge can be connected to more than 2 vertices.
- A hypergraph that is not a graph:



Hypergraphs

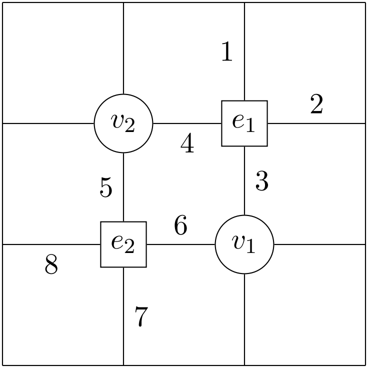
- A hypergraph is a generalization of a graph where an edge can be connected to more than 2 vertices.
- A hypergraph that is not a graph:



- Combinatorially we think of a hypergraph as a pair of partitions V and E of $\{1, \ldots, n\}$ where the numbers 1 to n label half-edges we call darts.

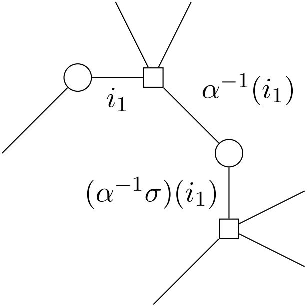
Hypermaps

- A hypermap is an embedding of the bipartite graph representation of a hypergraph into a surface. We write the dart's label counterclockwise of the dart with respect to rotation about edges.
- The picture below is a hypergraph embedded on a torus.

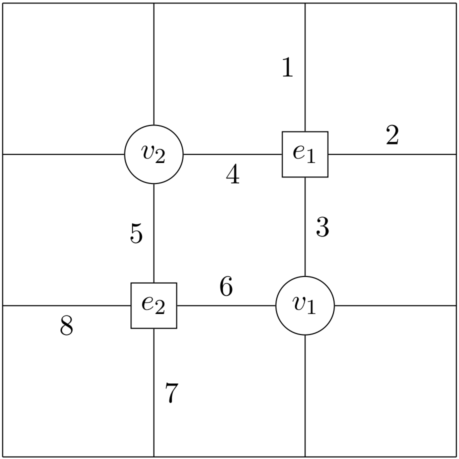


Combinatorial Hypermaps

- A combinatorial hypermap is a pair of permutations $\sigma, \alpha \in S_n$ such that $\langle \sigma, \alpha \rangle$ is transitive. For a survey of hypermaps from this point of view see [CM92].
- From a topological hypermap define σ to rotate darts counterclockwise around vertices and α to rotate darts clockwise around edges. Then $\alpha^{-1}\sigma$ rotates darts clockwise around faces.



- The next slide shows the combinatorial hypermap corresponding to the example we saw earlier.



We have

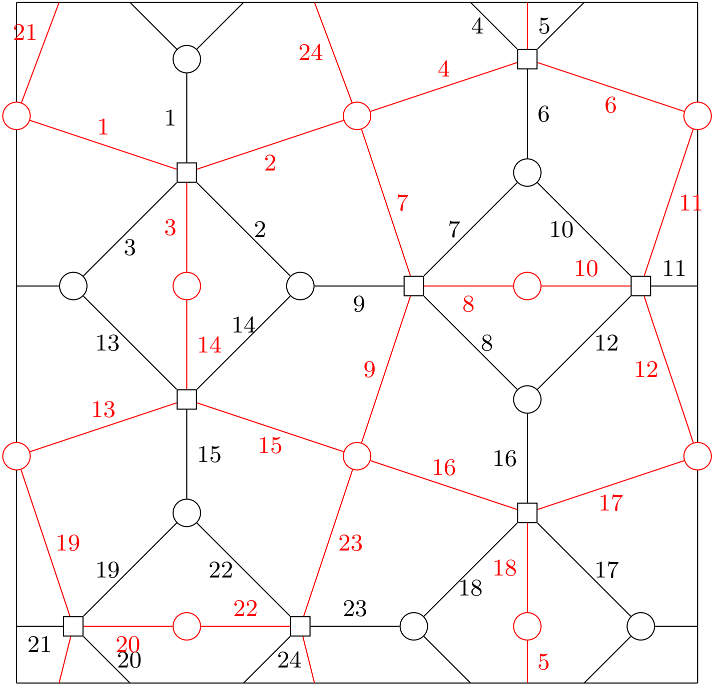
$$\sigma = (1\ 8\ 3\ 6)(2\ 5\ 4\ 7), \qquad \alpha = (1\ 2\ 3\ 4)(5\ 6\ 7\ 8)$$

and from this we can calculate

$$\alpha^{-1}\sigma = (1\ 7)(2\ 8)(3\ 5)(4\ 6).$$

The dual hypermap

- Combinatorially, the dual of the hypermap (σ, α) is $(\sigma', \alpha') = (\alpha^{-1}\sigma, \alpha^{-1})$.
- Topologically, to create the dual hypermap H^* of H:
  1. put a vertex of H^* inside each face of H,
  2. draw a dart of H^* going from each vertex of H^* to edges around the corresponding face of H,
  3. move labels from H to H^* without crossing darts in either hypermap,
  4. give the surface the opposite orientation.
- The next slide shows an example of a hypermap in black with its dual hypermap in red.



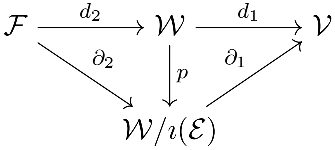
21
24
4
5
4
6
1
1
2
6
7
3
2
7
10
11
3
10
11
9
8
13
14
14
8
12
9
12
13
15
15
16
16
17
19
23
18
19
22
17
18
22
23
21
20
20
24
5

Hypermap homology

- Denote the darts labeled $1, \dots, n$ by $w_1, \dots, w_n$ and define an $\mathbb{F}_2$-chain complex

$$\mathcal{F} \xrightarrow{d_2} \mathcal{W} \xrightarrow{d_1} \mathcal{V}$$

  by $d_2(f) = \sum_{i \in f} w_i$ and $d_1(w_i) = v_{\ni i} + v_{\ni \alpha^{-1}(i)}$.
- Also define $\imath\colon \mathcal{E} \to \mathcal{W}$ by $\imath(e) = \sum_{i \in e} w_i$ extended linearly.
- Notice that d_2 and $\imath$ are injective, $d_1 \circ d_2 = 0$ and $d_1 \circ \imath = 0$.
- So we have a commutative diagram



  and it is the ∂_i boundary operators that we use to define hypermap-homology.

Hypermap homology group

- Define the first homology of the hypermap to be $H_1 = \ker \partial_1 / \operatorname{im} \partial_2$.
- By counting dimensions we can show that $\dim H_1 = 2g$ where g is the genus of the hypermap.
- Considering the ‘non-hypermap’ homology of the embedded bipartite graph representation of the hypermap we have the commutative diagram

$$\begin{array}{ccccc}
\mathcal{F} & \xrightarrow{\partial_2} & \mathcal{W}/\imath(\mathcal{E}) & \xrightarrow{\partial_1} & \mathcal{V} \\
\downarrow{\scriptstyle id} & & \downarrow{\scriptstyle \mu} & & \downarrow{\scriptstyle i_{\mathcal{V}}} \\
\mathcal{F} & \xrightarrow{\bar{d}_2} & \mathcal{W} & \xrightarrow{\bar{d}_1} & \mathcal{V} \oplus \mathcal{E}
\end{array}$$

  where $\mu(w_i + \imath(\mathcal{E})) = w_i + w_{\alpha^{-1}(i)}$.
- We can show $\mu_* \colon \ker \partial_1 / \operatorname{im} \partial_2 \to \ker \bar{d}_1 / \operatorname{im} \bar{d}_2$ is an isomorphism.

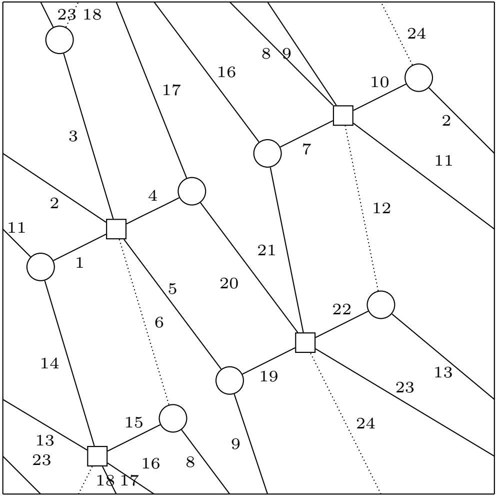
Hypermap homology codes

- To create a CSS code from hypermap-homology we need to choose a basis for $\mathcal{W}/\imath(\mathcal{E})$.
- From now on we choose a basis given by all darts except one for each edge. (I'll call this a *special basis*). We will draw darts in the basis with solid lines and darts not in the basis with dotted lines.
- Having chosen a basis for $\mathcal{W}/\imath(\mathcal{E})$ and using the distinguished bases for $\mathcal{F}$ and $\mathcal{V}$ we form matrices $H_X = [\partial_1]$ and $H_Z = [\partial_2]^T$.
- Since $H_X H_Z^T = 0$ this gives us a CSS code.
- Then $n = |W| - |E|$, $k = 2g$ and

$$d = \min\{\mathrm{wt}(c) \colon c \in (C_X \setminus C_Z^{\perp}) \cup (C_Z \setminus C_X^{\perp})\}.$$

An example

- The following hypermap based on a graph from [GKN03] gives rise to a $[20, 2, 3]$ code. (The minimum distance was found by computer).



Finding minimum distance

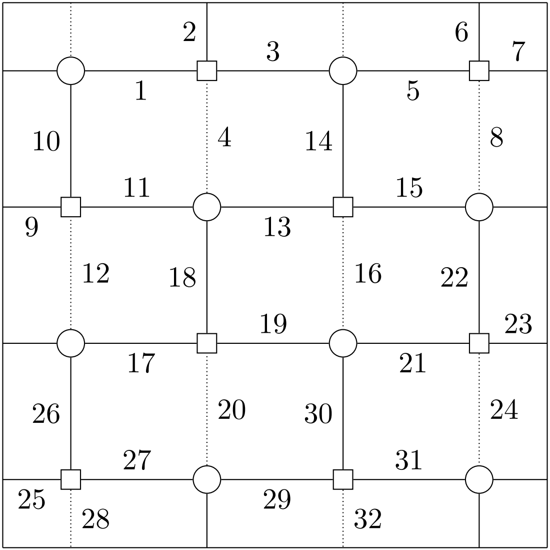
- We can show $\mu\colon \ker \partial_1 \setminus \operatorname{im} \partial_2 \to \ker \overline{d}_1 \setminus \operatorname{im} \overline{d}_2$ is a bijection and thus

$$\operatorname{minwt}(C_X \setminus C_Z^{\perp}) = \operatorname{minwt}\{\mu^{-1}(x)\colon x \in \ker \overline{d}_1 \setminus \operatorname{im} \overline{d}_2\}.$$

- For $C_Z \setminus C_X^{\perp}$, we consider the dual hypermap. We can show that $\operatorname{minwt}(C_Z \setminus C_X^{\perp})$ is given by the minimum weight of non-boundary cycles in weighted classical homology on the dual hypermap where darts in the chosen basis for $\mathcal{W}/\imath(\mathcal{E})$ have weight 1 and darts not in the basis have weight 0.

Square grid hypermap

- Take an $m \times m$ grid hypermap ($m = 4$ in the picture).

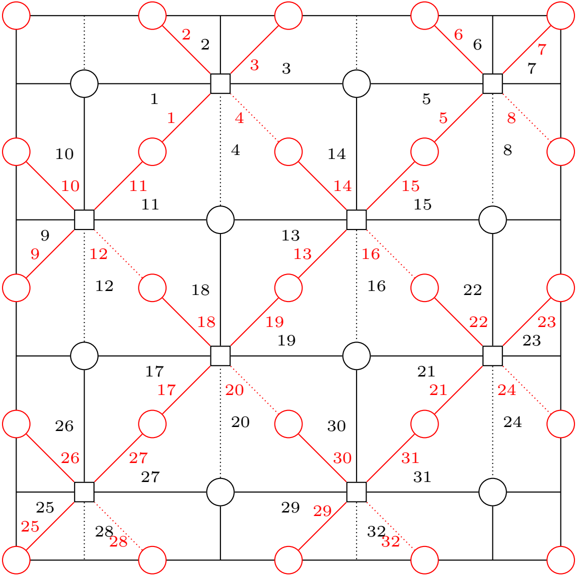


Square grid hypermap parameters

- This gives us an $[n, k, d]$ code with $n = 2m^2 - m^2/2 = (3/2)m^2$ and $k = 2$.
- A horizontal or vertical classical cycle x has $\mathrm{wt}(\mu^{-1}(x)) = m$.
- To see that this is the minimum: if $x \in \ker \overline{d}_1 \setminus \operatorname{im} \overline{d}_2$ then WLOG x has at least m horizontal darts. But μ takes a dart to one horizontal and one vertical dart so $\mathrm{wt}(\mu^{-1}(x)) \geq m$.
- Thus $\mathrm{minwt}(C_X \setminus C_Z^{\perp}) = m$.

Square grid hypermap parameters

- We can see from the dual that $\mathrm{minwt}(C_Z \setminus C_X^{\perp}) = m$.



Square grid hypermap parameters

- Thus a square grid hypermap code has parameters $[(3/2)m^2, 2, m]$.
- Comparing this to the toric code which has parameters $[2m^2, 2, m]$ we see that we can store the same amount of quantum information with the same error correcting capability using less physical qubits.

Summary

- Quantum computers need error correction.
- CSS codes can be constructed from $\mathbb{F}_2$-homology.
- We constructed hypermap-homology codes by generalizing the toric code; instead of embedding a graph we embedded a hypergraph.
- We proved results, especially in the case of a special basis, allowing us to compute the parameters $[n, k, d]$.
- For an $m \times m$ square grid the hypermap-homology code has better performance than the toric code.

Some open questions

- Can we find families of hypermaps which have better parameters than the square grid hypermap?
- Must hypermap-homology codes with the special basis we have described satisfy $kd^2 < cn$ for some constant c?
- Can we analyze hypermap-homology codes with a non-special basis?

The End

- Thankyou!
- Any questions?

References I

R. Cori and A. Machi.
Maps, hypermaps and their automorphisms: a survey i, ii, iii.
In *Exposition. Math*, volume 10, pages 403–427, 1992.

A.R. Calderbank and P.W. Shor.
Good quantum error-correcting codes exist.
Physical Review A, 54(2):1098, 1996.

A. Gagarin, W. Kocay, and D. Neilson.
Embeddings of small graphs on the torus.
Cubo. v5, pages 351–371, 2003.

Alexi Kitaev.
Quantum error correction with imperfect gates.
In *Proceeding of the Third International Conference on Quantum Communication and Measurement*, 1997.

References II

D.J.C. MacKay, G. Mitchison, and P.L. McFadden.
Sparse-graph codes for quantum error correction.
Information Theory, IEEE Transactions on,
50(10):2315–2330, 2004.