Quantum LDPC codes.

Gilles Zémor

Bordeaux Mathematics Institute

November 2017, IQFA meeting, Nice

Classical erasures and errors

Transmission: n bit vector

0 1 1 0 1 0 - - - - - - - - - - - - - - - 1 1

Channel

Classical erasures and errors

Transmission: n bit vector

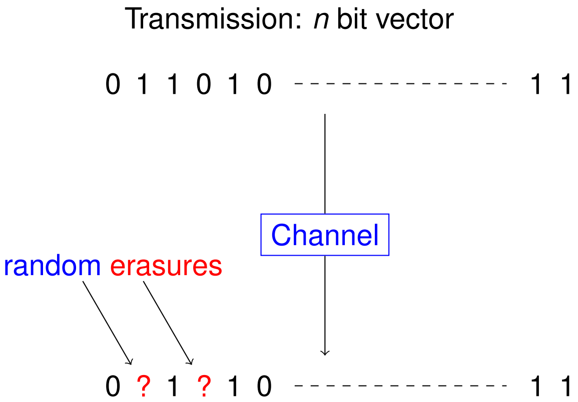
0 1 1 0 1 0 - - - - - - - - - - - - - - - - 1 1

$\boxed{\text{Channel}}$

random errors

0 0 1 1 1 0 - - - - - - - - - - - - - - - - 1 1

Classical erasures and errors



Classical coding theory

Message space $\mathcal{M} = \{0,1\}^k$.

Transform message $\mathbf{m} = [m_1, \ldots, m_k]$ into codeword

$$m_1[\mathbf{g}_1] + \cdots + m_k[\mathbf{g}_k].$$

$[\mathbf{g}_j] \in \{0,1\}^n$, $n > k$, generate a Linear code C.

Simplest linear map $\{0,1\} \to \{0,1\}^3$:

$$0 \mapsto 000$$
$$1 \mapsto 111$$

Alternatively, vector space C is defined as the set of binary vectors $\mathbf{x}$ satisfying (parity-check) equations,

$$\begin{aligned} x_3 + x_5 + x_8 &= 0 \\ x_2 + x_4 + x_5 + x_8 &= 0 \\ &\vdots \end{aligned}$$

Syndrome

Receive corrupted codeword $\mathbf{y} = \mathbf{x} + \mathbf{e}$. Compute

$$\begin{aligned}\sigma_1 &= y_3 + y_5 + y_8 \\ \sigma_2 &= y_2 + y_4 + y_5 + y_8 \\ &\vdots\end{aligned}$$

They make up the coordinates of the **syndrome** vector
$\sigma(\mathbf{y}) = \mathbf{H}^t\mathbf{y}$.
The set of parity-check equations make up the *parity-check matrix* $\mathbf{H}$.

$$C = \{\mathbf{x} \in \{0,1\}^n, \mathbf{H}^t\mathbf{x} = 0\}$$

$$\begin{bmatrix} & & \\ & \mathbf{H} & \\ & & \end{bmatrix}$$

Decoding problem

Decoding problem: given syndrome $\sigma(\mathbf{y}) = \sigma(\mathbf{x} + \mathbf{e}) = \sigma(\mathbf{e})$, find **e**.

codewords should be far away from each other: large *Hamming distance*. Code parameters: $[n, k, d]$.

Decoding is NP-complete. But...

Classical LDPC codes

Code C defined by parity-check matrix $\mathbf{H}$ of *low density*, rows and columns of constant (low) weight.

$$x_3 + x_7 + x_{23} = 0$$

Suppose syndrome computation gives us

$$y_3 + y_7 + y_{23} = 1$$
$$y_3 + y_5 + y_{11} = 1$$

Then we flip the value of y_3. Bit flipping algorithm: if flipping the value of a bit decreases the syndrome weight, then flip its value. Repeat.

Simplest of extremely efficient, suboptimal (but almost optimal when used cleverly) decoding algorithms.

Gallager 1963... Extremely active field since 1990s.

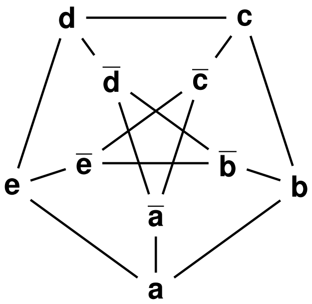
Cycle codes of graphs

Particular instance. The case when columns of **H** have exactly two '1's per column. Then **H** is incidence matrix of graph.

$$\begin{array}{cc} \text{vertices} & \begin{bmatrix} & & \\ & \mathbf{H} & \\ & & \end{bmatrix} \\ & \text{edges} \end{array}$$

Example: the Petersen code

$$\mathbf{H} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \end{bmatrix}$$

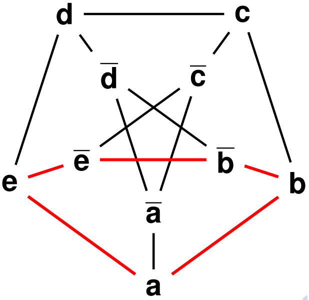


Example: the Petersen code

$$\mathbf{H} = \begin{bmatrix} 1&0&0&0&1&1&0&0&0&0&0&0&0&0&0 \\ 1&1&0&0&0&0&1&0&0&0&0&0&0&0&0 \\ 0&1&1&0&0&0&0&1&0&0&0&0&0&0&0 \\ 0&0&1&1&0&0&0&0&1&0&0&0&0&0&0 \\ 0&0&0&1&1&0&0&0&0&1&0&0&0&0&0 \\ 0&0&0&0&0&1&0&0&0&0&1&0&0&0&1 \\ 0&0&0&0&0&0&1&0&0&0&0&0&1&1&0 \\ 0&0&0&0&0&0&0&1&0&0&1&1&0&0&0 \\ 0&0&0&0&0&0&0&0&1&0&0&0&0&1&1 \\ 0&0&0&0&0&0&0&0&0&1&0&1&1&0&0 \end{bmatrix}$$

$$\mathbf{c} = \begin{bmatrix} 1&0&0&0&1&0&1&0&0&1&0&0&1&0&0 \end{bmatrix}$$

Codewords are cycles



Cycle codes: parameters

$[n, k, d]$ code in $\{0, 1\}^n = \{0, 1\}^{\mathcal{E}}$

$$\text{Vectors of } \{0, 1\}^n \leftrightarrow \text{Subsets of edges}$$

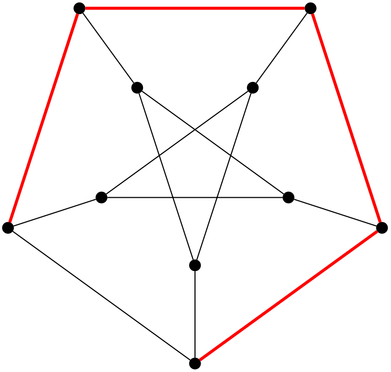
Cycle codes have length n, dimension

$$k = \#\text{Edges} - \#Vertices + 1$$

and the minimum distance is the size of the smallest cycle (girth of the graph).

Petersen: $[15, 6, 5]$.

Erasure Correction



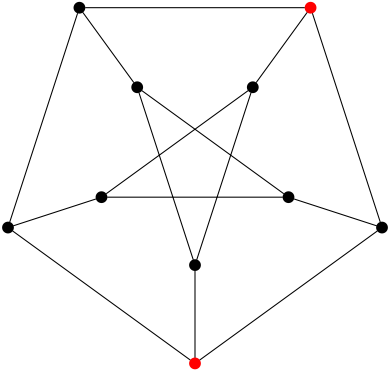
Look at erased connected components, correct hanging edges, repeat.
Terminates properly if the set of erased edges does not cover a cycle. One can *always* correct $d-1$ erasures.

Error Correction

In principle we can always correct $e < d/2$ errors. Practically ?

Error Correction

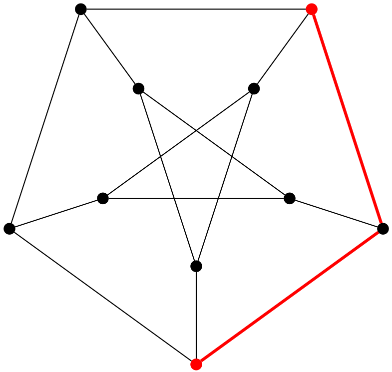
In principle we can always correct $e < d/2$ errors. Practically ?



Identify vertices incident to an odd number of 1s.
Then connect them with as few edges as possible. Those are the bits in error.

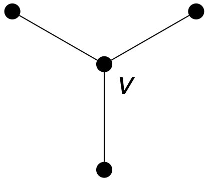
Error Correction

In principle we can always correct $e < d/2$ errors. Practically ?



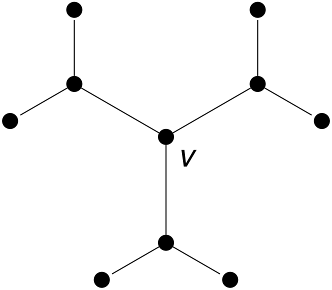
Identify vertices incident to an odd number of 1s.
Then connect them with as few edges as possible. Those are the bits in error.
Polynomial time ! Non-trivial: Edmunds' Blossom algorithm.

Girth, minimum distance, upper bounds



As long as no cycles are formed, neighbourhood of v in regular graph G grows exponentially.
Hence $\exp(d) \leq |G|$ and $d \leq \log n$.

Girth, minimum distance, upper bounds



As long as no cycles are formed, neighbourhood of v in regular graph G grows exponentially.
Hence $\exp(d) \leq |G|$ and $d \leq \log n$.

Girth, minimum distance, lower bounds

Can $d \geq \log n$ be achieved for regular graphs (fixed positive rate) ?

Girth, minimum distance, lower bounds

Can $d \geq \log n$ be achieved for regular graphs (fixed positive rate) ?

Yes.

Girth, minimum distance, lower bounds

Can $d \geq \log n$ be achieved for regular graphs (fixed positive rate) ?

Yes.

- Random methods (Erdös Sachs, also Gallager)

Girth, minimum distance, lower bounds

Can $d \geq \log n$ be achieved for regular graphs (fixed positive rate) ?

Yes.

- Random methods (Erdös Sachs, also Gallager)
- Margulis' algebraic method.

Margulis' approach

Construct Cayley graphs $\mathcal{G} = \mathcal{C}(G, S)$.

$$\mathbf{g} \text{ ---- } \mathbf{gs}$$

Obtain $\mathcal{G}$ as finite quotient of infinite regular tree, by choosing for G quotient of free group Γ on generator set S.

Concrete example: Γ free group generated by

$$A = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \quad A^{-1} = \begin{bmatrix} 1 & -2 \\ 0 & 1 \end{bmatrix} \quad B = \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix} \quad B^{-1} = \begin{bmatrix} 1 & 0 \\ -2 & 1 \end{bmatrix}.$$

in $\mathrm{SL}_2(\mathbb{Z})$. Take quotient by choosing $G = \mathrm{SL}_2(\mathbb{F}_\mathrm{p})$ for same generator set S.

Girth argument: as long as matrix elements stay smaller than p, local one-to-one correspondence between products of elements of G and Γ, i.e. between neighbourhoods of infinite tree and finite graph, hence $d \geq \log n$.

Cycle codes and erasure channel

Behaviour of cycle code on the erasure channel ?

Standard LDPC approach. Erasure channel is simpler than BSC (Binary Symmetric), figure out resistance to erasures first.

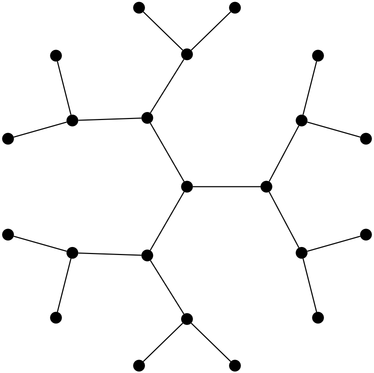
Each coordinate is erased with independent probability p. Yields erasure vector in $\{0,1\}^n$. Decodable iff erasure vector does not cover a codeword.

In other words, what is the probability that a random set of edges contains a cycle (non decodable event) ?

For a regular graph of degree Δ, relate to percolation on infinite Δ-regular tree.

Percolation on trees

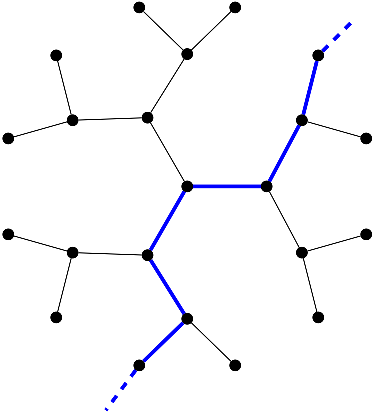
Infinite tree. Choose every edge with probability p. Probability that the chosen subgraph contains an infinite path (percolation) ?



Answer: zero if $p < 1/(\Delta - 1)$,   one if $p > 1/(\Delta - 1)$.

Percolation on trees

Infinite tree. Choose every edge with probability p. Probability that the chosen subgraph contains an infinite path (percolation) ?



Answer: zero if $p < 1/(\Delta - 1)$, one if $p > 1/(\Delta - 1)$.

Critical probabilities

Percolation on infinite tree implies erasure pattern covers cycles in the finite Δ-regular graph.

Example: $\Delta = 4$.

Beyond the critical probability $p > 1/3$, erasure recovery is not possible for cycle codes (Decreusefond Z. 1997)

For $p < 1/3$, it is if the graph is “good” enough: e.g. Ramanujan graphs (Tillich Z. 1997)

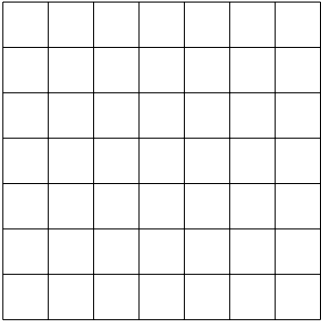
Compare with Shannon bound.

$$p_c \leq 1 - R = 1/2.$$

Digression

Percolation for other infinite Δ-regular graphs.

Most classical case and most studied: $\mathbb{Z}^2$, infinite grid.

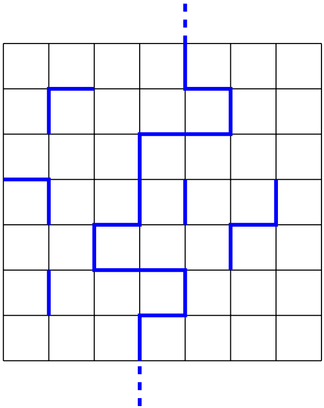


Critical probability: $p_c = 1/2$.

Digression

Percolation for other infinite Δ-regular graphs.

Most classical case and most studied: $\mathbb{Z}^2$, infinite grid.

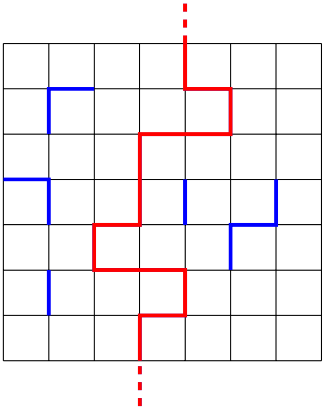


Critical probability: $p_c = 1/2$.

Digression

Percolation for other infinite Δ-regular graphs.

Most classical case and most studied: $\mathbb{Z}^2$, infinite grid.



Critical probability: $p_c = 1/2$.

Classical LDPC coding, summary

- defined by sparse parity-check matrix.
- super simple decoding (e.g. bit-flipping)
- cycle codes of graphs: simplest non-trivial instances of LDPC codes
- bit-flipping doesn't work for cycle codes, but effecient decoding anyway
- can be constructed randomly or by algebraic (arithmetic) methods
- erasure decoding collapses when you have percolation

Quantum errors

qubit:

$$|\phi\rangle = \alpha|0\rangle + \beta|1\rangle.$$

X error:

$$X|\phi\rangle = \alpha|1\rangle + \beta|0\rangle.$$

Z error:

$$Z|\phi\rangle = \alpha|0\rangle - \beta|1\rangle.$$

Both at the same time: XZ.

Or any complex linear combination of I, X, Z, XZ.

Protecting $|\phi\rangle$

Take $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$ to

$$\alpha \sum_{M \in S} M|0000000\rangle + \beta \sum_{M \in S} M|1111111\rangle$$

where S is abelian group of error patterns generated by

$$\begin{matrix} IXXXXII \\ XIXXIXI \\ XXIXIIX \end{matrix} \qquad \text{and} \qquad \begin{matrix} IZZZZII \\ ZIZZIZI \\ ZZIZIIZ \end{matrix}$$

that come from the binary matrix

$$\mathbf{H} = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

Syndrome computation

Suppose $|\psi\rangle$ is corrupted to $E|\psi\rangle$

$$E = IIIIXII \quad \text{(say)}$$

and suppose we can somehow compute classical syndrome of corresponding binary vector e

$$\sigma(e) = \mathbf{H}^t e$$

then classical decoding recovers e and E, and we apply the unitary E^{-1} to the corrupted quantum state to recover $|\psi\rangle$.

Is this possible ? Yes !

Syndrome computation

For any value $s = (s_X, s_Z)$ (X-syndrome and Z-syndrome) the set of states

$$E_s|\psi\rangle,$$

for E_s a Pauli error of syndrome s and $|\psi\rangle$ an encoded quantum state, generates a subspace $C(s)$ such that

$$\mathcal{H} = \bigoplus_s^{\perp} C(s).$$

Meaning we can measure the syndrome.

Furthermore, measuring “forces” the error to be a Pauli error.

CSS quantum codes

The CSS (Calderbank Shor Steane) stabilizer code structure:

$$\mathbf{H} = \begin{bmatrix} \mathbf{H}_X \\ \mathbf{H}_Z \end{bmatrix}$$

Important technicality 1: row space V_X of $\mathbf{H}_X$ and row space V_Z of $\mathbf{H}_Z$ must be orthogonal.

Important technicality 2: error vectors E_X in V_X have zero s_Z syndrome, but they don't count: $E_X|\psi\rangle = |\psi\rangle$.

Problematic errors. Errors of zero syndrome not in V_X or V_Z.

CSS codes, parameters

Dimension of quantum code is $n - \dim V_X - \dim V_Z$.

Minimum distance d is minimum weight of vector orthogonal to V_X *but not in* V_Z *or* orthogonal to V_Z *but not in* V_X.

Objective: study quantum CSS codes. $\mathbf{H}_X$ and $\mathbf{H}_Z$ both low-density.

Motivation: as before, efficient decoding. Decoding: find E_X and E_Z from syndromes s_X and s_Z. Totally classical computation.

Additional motivation: use degeneracy, meaning same syndrome can correct many different errors.

Asymptotic constructions of quantum LDPC codes

Challenge: construct quantum LDPC code with non-trivial (growing) minimum distance.

- Many constructions give *constant* minimum distance.

Asymptotic constructions of quantum LDPC codes

Challenge: construct quantum LDPC code with non-trivial (growing) minimum distance.

- Many constructions give *constant* minimum distance.
- Random methods don't work. Choose low density $\mathbf{H}_X$ at random. Then $V_X^\perp$ has minimum distance linear in n. No codewords of low weight means there is nothing to put in $\mathbf{H}_Z$.

Asymptotic constructions of quantum LDPC codes

Challenge: construct quantum LDPC code with non-trivial (growing) minimum distance.

- Many constructions give *constant* minimum distance.
- Random methods don't work. Choose low density $\mathbf{H}_X$ at random. Then $V_X^\perp$ has minimum distance linear in n. No codewords of low weight means there is nothing to put in $\mathbf{H}_Z$.
- Best known lower bound on d for a quantum CSS code of dimension 1: $\sqrt{n}\log n$ (!)

Asymptotic constructions of quantum LDPC codes

Challenge: construct quantum LDPC code with non-trivial (growing) minimum distance.

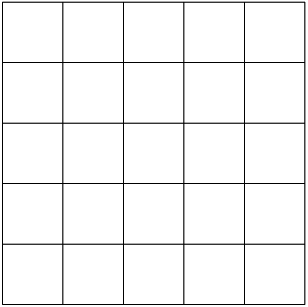
- Many constructions give *constant* minimum distance.
- Random methods don't work. Choose low density $\mathbf{H}_X$ at random. Then $V_X^\perp$ has minimum distance linear in n. No codewords of low weight means there is nothing to put in $\mathbf{H}_Z$.
- Best known lower bound on d for a quantum CSS code of dimension 1: $\sqrt{n}\log n$ (!)
- How does one construct CSS codes of constant rate and *growing* minimum distance ?

Asymptotic constructions of quantum LDPC codes

Challenge: construct quantum LDPC code with non-trivial (growing) minimum distance.

- Many constructions give *constant* minimum distance.
- Random methods don't work. Choose low density $\mathbf{H}_X$ at random. Then $V_X^\perp$ has minimum distance linear in n. No codewords of low weight means there is nothing to put in $\mathbf{H}_Z$.
- Best known lower bound on d for a quantum CSS code of dimension 1: $\sqrt{n}\log n$ (!)
- How does one construct CSS codes of constant rate and *growing* minimum distance ?
- What is the quantum counterpart of cycle codes of graphs ?

The basic construction: Kitaev's toric code



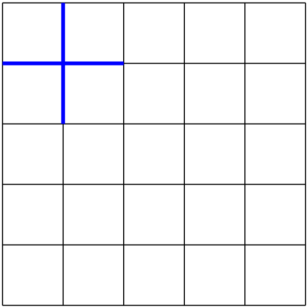
$$\mathbf{H}_X = \begin{bmatrix} \quad \end{bmatrix}$$

$$\mathbf{H}_Z = \begin{bmatrix} \quad \end{bmatrix}$$

$\mathbf{H}_X$ parity-check matrix of cycle code of graph.

$\mathbf{H}_Z$: rows consist of elementary cycles (faces).

The basic construction: Kitaev's toric code



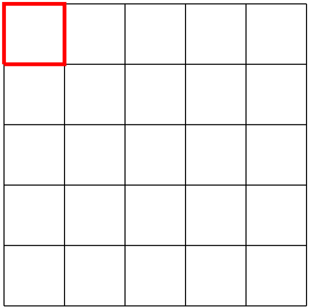
$$\mathbf{H}_X = \begin{bmatrix} 111100 \;\cdots & & \\ & & \\ & & \end{bmatrix}$$

$$\mathbf{H}_Z = \begin{bmatrix} & & \\ & & \\ & & \end{bmatrix}$$

$\mathbf{H}_X$ parity-check matrix of cycle code of graph.

$\mathbf{H}_Z$: rows consist of elementary cycles (faces).

The basic construction: Kitaev's toric code



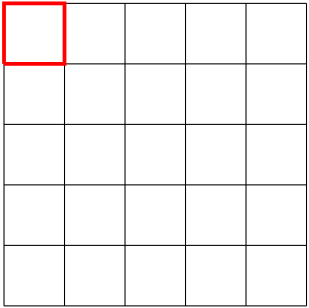
$$\mathbf{H}_X = \begin{bmatrix} 111100 \quad \cdots & & \\ & & \\ & & \end{bmatrix}$$

$$\mathbf{H}_Z = \begin{bmatrix} 001111 \quad \cdots & & \\ & & \\ & & \end{bmatrix}$$

$\mathbf{H}_X$ parity-check matrix of cycle code of graph.

$\mathbf{H}_Z$: rows consist of elementary cycles (faces).

The basic construction: Kitaev's toric code



$$\mathbf{H}_X = \begin{bmatrix} 111100 \quad \cdots & \\ & \\ & \\ \end{bmatrix}$$

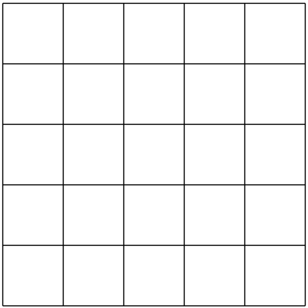
$$\mathbf{H}_Z = \begin{bmatrix} 001111 \quad \cdots & \\ & \\ & \\ \end{bmatrix}$$

$\mathbf{H}_X$ parity-check matrix of cycle code of graph.

$\mathbf{H}_Z$: rows consist of elementary cycles (faces).

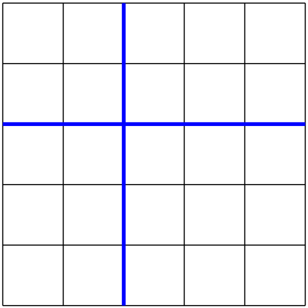
Dimension:
$k = n - \dim V_X - \dim V_Z = \dim V_X^{\perp}/V_Z = \dim V_Z^{\perp}/V_X = 2.$

Kitaev's toric code, minimum distance



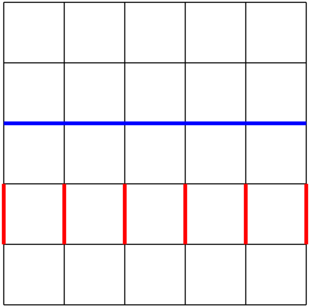
Cycles that are not sums of faces. In $V_X^\perp$ but not in V_Z.

Kitaev's toric code, minimum distance



Cycles that are not sums of faces. In $V_X^{\perp}$ but not in V_Z.

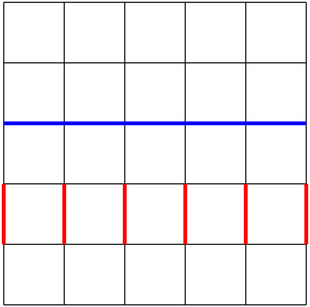
Kitaev's toric code, minimum distance



Cycles that are not sums of faces. In $V_X^\perp$ but not in V_Z.

Vector of $V_Z^\perp$ not in V_X.

Kitaev's toric code, minimum distance



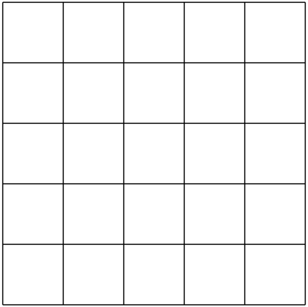
Cycles that are not sums of faces. In $V_X^\perp$ but not in V_Z.

Vector of $V_Z^\perp$ not in V_X.

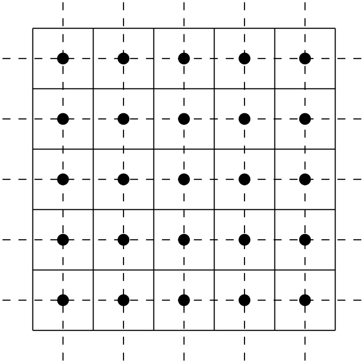
We obtain the quantum code's parameters

$$[[2m^2, 2, m]] \qquad d = \sqrt{n/2}.$$

Graph duality

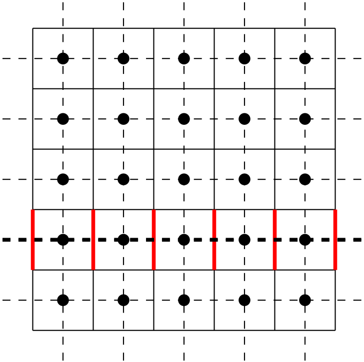


Graph duality



Dual graph G^* of G.

Graph duality



Dual graph G^* of G.

Vector of $V_Z^\perp$ not in V_X is cycle of dual graph.

Quantum erasure channel

Non erased positions are not in error.

In classical case: erasure vector is not correctable is it contains (in its support) a codeword, i.e. an error pattern of syndrome 0.

In quantum case: erasure vector is not correctable if it contains (in its support) a error pattern of syndrome (either s_X or s_Z) 0 that is not in V_X or V_Z (a problematic error pattern).

For Kitaev code: non-correctable erasure pattern if erased set of edges contains cycle that is not sum of faces, either in primal or dual graph.

Quantum erasure channel

Non erased positions are not in error.

In classical case: erasure vector is not correctable is it contains (in its support) a codeword, i.e. an error pattern of syndrome 0.

In quantum case: erasure vector is not correctable if it contains (in its support) a error pattern of syndrome (either s_X or s_Z) 0 that is not in V_X or V_Z (a problematic error pattern).

For Kitaev code: non-correctable erasure pattern if erased set of edges contains cycle that is not sum of faces, either in primal or dual graph.

critical probability for this event – Percolation on $\mathbb{Z}^2$!

$$p_c = \frac{1}{2}$$

Compare with capacity of quantum erasure channel

$$R \leq 1 - 2p.$$

Decoding errors

Decode both cycle graphs separately. Use Edmonds algorithm.
Many alternatives.
Is Kitaev code optimal for errors ?

Towards non-zero rate,the homological connection

Generalize to G a 2-complex (vertices, edges, faces) that makes up a combinatorial surface: has dual 2-complex G^*, (vertices $\leftrightarrow$ faces).

Spaces V_X and V_Z defined as before, and we have:

$$V_X^\perp / V_Z = H_1(G), \qquad V_Z^\perp / V_X = H^1(G) = H_1(G^*)$$

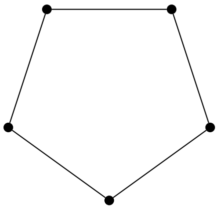
(homology and cohomology groups of G).

Minimum distance is weight of smallest cycle that is not a boundary, either in G or in G^*.

Generalizes cycle codes that are homology groups of 1-complexes (graphs).

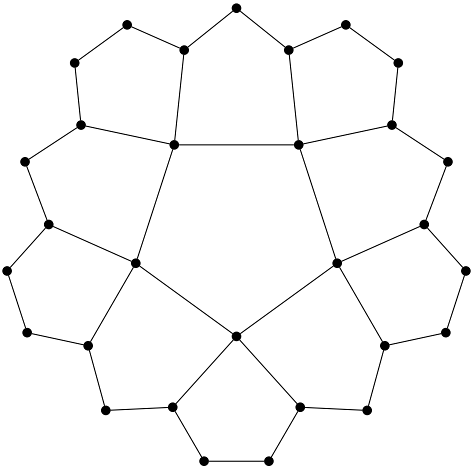
Tilings of hyperbolic plane

Look for graphs that locally look like tilings of hyperbolic plane.
E.g. graph of degree 4 and faces are pentagons.



Tilings of hyperbolic plane

Look for graphs that locally look like tilings of hyperbolic plane.
E.g. graph of degree 4 and faces are pentagons.



Quantum codes from combinatorial surfaces

If such finite graphs exist they have positive rate. For degree 4 and pentagons: $R \geq 1/10$.
How does one construct the combinatorial surface from the infinite graph ?

Quantum codes from combinatorial surfaces

If such finite graphs exist they have positive rate. For degree 4 and pentagons: $R \geq 1/10$.
How does one construct the combinatorial surface from the infinite graph ?

Random constructions ???

Quantum codes from combinatorial surfaces

If such finite graphs exist they have positive rate. For degree 4 and pentagons: $R \geq 1/10$.
How does one construct the combinatorial surface from the infinite graph ?

Random constructions ???

Algebraic constructions (Margulis) ? Yes.

Furthermore, large injectivity radius will yield growing minimum distance.

Triangular groups

Realise infinite tiling through triangular group, then take finite quotient.

Triangular group T: generators $\{a, b\}$, relations

$$a^2 = 1, b^\ell = 1, (c)^m = 1 \quad \text{for } c = ab$$

Cosets of $\langle a \rangle$: edges. Cosets of $\langle b \rangle$ vertices. Cosets of $\langle c \rangle$ faces. Two cosets incident if they have non-empty intersection.

Construction of the finite graph

Margulis type approach (Širáň 2001). Realise triangular group T as a matrix group.

B and C matrices of $\mathrm{SL}_3(\mathbb{Z}[\xi])$:

$$B = \begin{bmatrix} -1 & -P_\ell(\xi) & 0 \\ P_\ell(\xi) & P_\ell(\xi)^2 - 1 & 0 \\ P_m(\xi) & P_m(\xi)P_\ell(\xi) & 1 \end{bmatrix} \quad \text{and} \quad C = \begin{bmatrix} P_m(\xi)^2 - 1 & 0 & P_m(\xi) \\ P_\ell(\xi) & 1 & 0 \\ -P_m(\xi) & 0 & -1 \end{bmatrix}.$$

$\xi = 2\cos(\pi/m\ell)$ and P_k Chebychev polynomial.

Generators $a = CB$ and $b = B$ generate subgroup of $\mathrm{SL}_3(\mathbb{Z}[\xi])$ with exactly the presentation $a^2 = 1$, $b^\ell = 1$ and $(ab)^m = 1$.

Reduce coefficients modulo p to get desired finite group.

Minimum distance

In infinite graph.
r-neighbourhood of a vertex is planar, so every cycle is sum of faces. Same for dual graph.

In finite graph.
As long as r-neighbourhood of finite graph is isomorphic to r-neighbourhood of infinite tiling then cycle of length $< 2r$ (included in r-neighbourhood) is sum of faces.

We have local isomorphism for $r \geq \log n$ (Širáň, à la Margulis). Hence

$$d \geq \log n.$$

Best one can do for quantum codes from tilings of surfaces (Delfosse 2013).

Behaviour on erasure channel

Upper bound on critical probability for erasure correction given by:

Critical probability for percolation on infinite tiling.

Behaviour on erasure channel

Upper bound on critical probability for erasure correction given by:

Critical probability for percolation on infinite tiling.

Non-trivial computation. Recent progress (Delfosse Z. 2016).

Cannot achieve capacity of quantum erasure channel.

Towards better quantum LDPC codes

Construction (Tillich, Z 2009) gives quantum LDPC codes with constant positive rate and minimum distance $O(\sqrt{n})$.

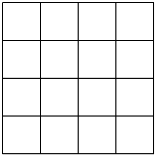
Towards better quantum LDPC codes

Construction (Tillich, Z 2009) gives quantum LDPC codes with constant positive rate and minimum distance $O(\sqrt{n})$.

Ideas: consider product graph construction: two graphs G and G' give product graph $G \cdot G'$ where $(x, x') —— (y, y')$ if

- either $x = y$ and $x' —— y'$
- or $x —— x'$ and $x' = y'$.

Remark: 2-dimensional torus

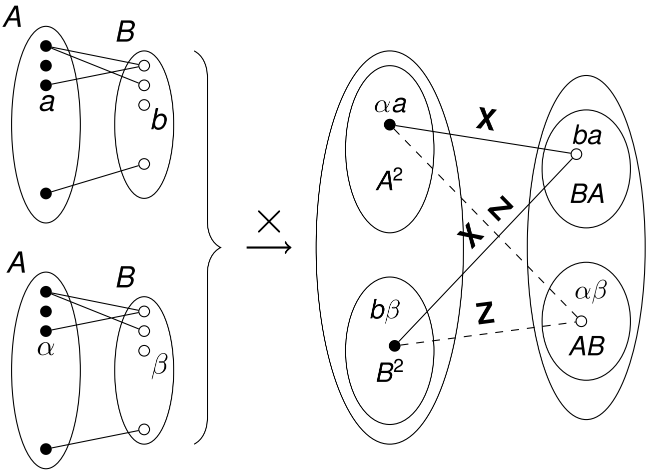


is product of two cycles, with a face being determined by edge $\{a, b\}$ of G and $\{x, y\}$ of G'.

$$
\begin{tikzcd}
(a, y) \arrow[r, dash] \arrow[d, dash] & (b, y) \arrow[d, dash] \\
(a, x) \arrow[r, dash] & (b, x)
\end{tikzcd}
$$

Quantum “product” codes (Tillich-Z 2009)

Code can be described by two factor graphs. Start with ordinary bipartite graph $A \leftrightarrow B$ and create:



Quantum Parameters

Length: $n = |A|^2 + |B|^2$.
Dimension: $k \geq (|A| - |B|)^2$
Minimum distance: equal to $\min(d, d^T)$

where d is minimum distance of "original" classical LDPC code defined by factor graph $A \leftrightarrow B$, and d^T is the minimum distance of the *transpose code* i.e. the code defined by the factor graph $B \leftrightarrow A$. Typically minimum distance is exactly d.

Can be decoded in quasi-linear time from any pattern of $O(\sqrt{n})$ errors (Leverrier, Tillich, Z. 2015).

Conclusion and open problems

- Quantum codes associated to 2-complexes are the quantum counterpart of cycle codes of graphs.
- Strong topological connection.
- Do asymptotically good quantum LDPC stabilizer (CSS) codes exist ?
- Do quantum LDPC codes exist with $d = O(n)$ (even with dimension 1) ?
- Really efficient decoding ?