Quantum Expander Codes

Anthony Leverrier[1], Jean-Pierre Tillich[1], **Gilles Zémor**[2]

[1]INRIA, [2]Bordeaux Mathematics Institute

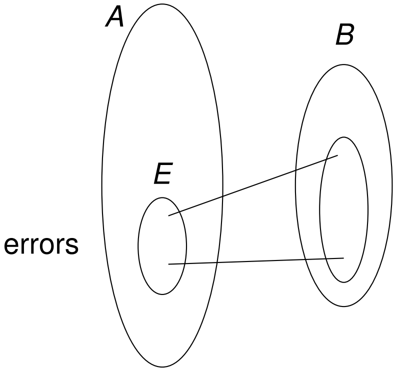
January 2016, Banff

Context

- Search for quantum codes with fast decoding (linear-time in $\#$qbits n.
- Codes with local structure (LDPC): low-weight generators.
- Deal with degeneracy: decoder has several choices for error output.
- Constructions of quantum LDPC codes are difficult to find. Random choice does not work well either. Can one find quantum LDPC codes with minimum distance $> \sqrt{n}$?
- *This contribution: decode in linear-time arbitrary (adversarial) patterns of weight $\leq$ (constant)$\sqrt{n}$ for codes with non-zero rate*.
- *Export expander code techniques.*

Classical Expander Codes (Sipser-Spielman 1996)

Code: set of binary vectors $(x_1, \ldots, x_n,)$ satisfying set of linear equations. Can be represented by a *factor* (Tanner) graph relating $A = \{1, \ldots n\}$ to the set of equations B. vertex $a \in A$ is incident to b if x_a is involved in equation $(b)\ x_a + x_i + x_j = 0$.

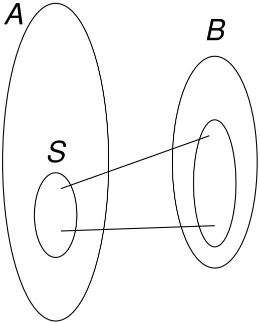


$$\begin{bmatrix} 0 \\ 0 \\ \vdots \\ 1 \\ \vdots \\ 1 \end{bmatrix}$$

Expansion

Bipartite graph (A, B) of left degree Δ is (γ, δ) (left)–expanding if for all $S \subset A$, $|S| \leq \gamma|A|$, we have

$$\#\text{neighbours}(S) \geq (1 - \delta)\Delta|S|.$$



If expansion large enough, many neighbours of S have degree 1 (*unique neighbours*). If S is set of errors, this means many equations contain exactly one symbol in error.

Expander decoding

Therefore there should exist a critical symbol such that flipping its value decreases the syndrome weight (number of unsatisfied equations).

Hence decoding algorithm: flip a symbol if it decreases the syndrome weight: repeat until syndrome =0.

Algorithm may sporadically introduce new errors, but can't happen too often because syndrome weight is decreasing all the time and

$$\text{syndrome weight} \geq (1-2\delta)\Delta \#\text{errors}$$

(expansion).
Argument works when $\delta < 1/4$ (i.e. expansion coefficient is $> 3/4$ of maximum. Guarantees correction of arbitrary pattern of $< \frac{1}{2}\gamma n$ errors.

CSS quantum codes

Two types of errors, X-errors and Z-errors. Can be modelled as two binary error vectors e_X and e_Z occurring simultaneously.

The CSS (Calderbank Shor Steane) stabilizer code structure:

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

So can be thought of as two classical codes, but
Important technicality 1: row space V_X of $\mathbf{H}_X$ and row space V_Z of $\mathbf{H}_Z$ must be orthogonal.

It is possible to compute (measure) syndrome $\sigma_X(e_X)$ and syndrome $\sigma_Z(e_Z)$.

Quantum LDPC codes

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

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.

Decoding problem is purely classical: find most plausible e_X and e_Z from syndromes.

Why not decode both codes separately, from syndromes $\sigma_X(e_X)$ and $\sigma_Z(e_Z)$, with each code ignoring the other one ? In particular why not use classical expander decoding on the two factor graphs of $\mathbf{H}_X$ and $\mathbf{H}_Z$?

Quantum expander decoding ?

Answer: because expansion is incompatible with existence of the other code.

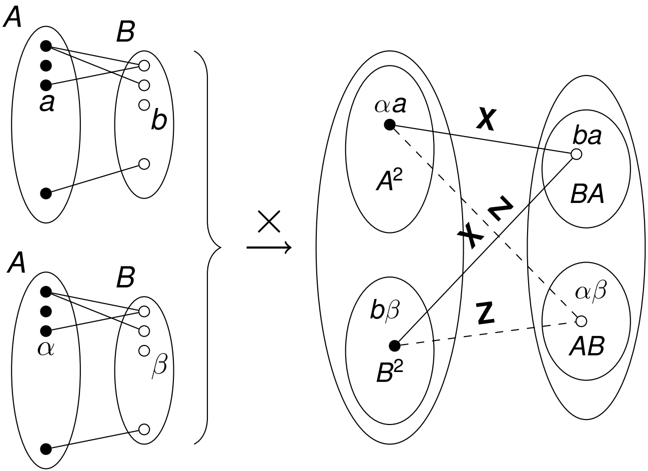
Each of the two classical codes defined by the parity-check matrices $\mathbf{H}_X$ and $\mathbf{H}_Z$ have *constant* minimum distances, when they are LDPC. (Can individually correct only a constant number of classical errors).

Worse: error vectors e_X and e_Z are really defined modulo row-spaces V_Z and V_X of $\mathbf{H}_Z$ and $\mathbf{H}_X$. The value of an individual bit is meaningless.

Must rely on expansion of some other object.

Quantum "product" codes (Tillich-Z 2009)

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



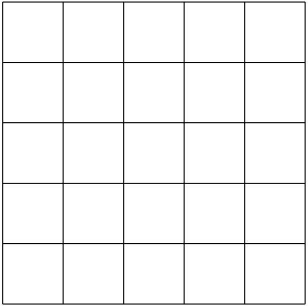
Quantum Parameters

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.

Potential therefore for correcting $\Omega(\sqrt{n})$ adversary errors.

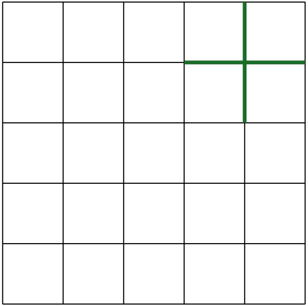
Particular instance: the Kitaev code



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

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

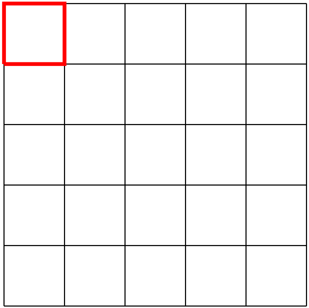
Particular instance: the Kitaev code



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

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

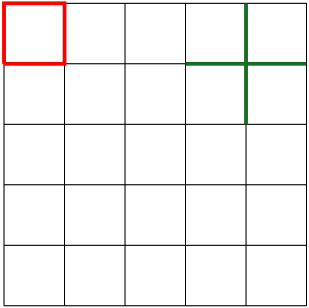
Particular instance: the Kitaev code



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

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

Particular instance: the Kitaev code



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

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

Dimension 2, minimum distance scales as $\sqrt{n}$.

Original graph $A \leftrightarrow B$ is just simple cycle. No expansion.

Decoding idea

Decode locally, but not individual bits.

Decode individual *generators*.

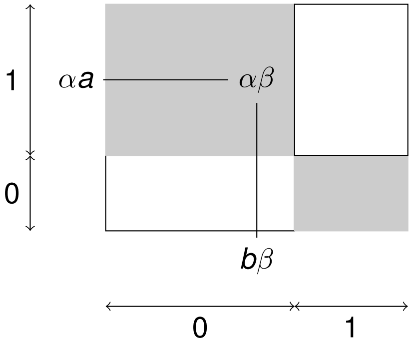
Find a pattern inside a generator that decreases the syndrome weight.

Repeat until syndrome is zero.

Remark: we are not modifying the "received vector". There is no received vector, just the syndrome. We are constructing a low-weight error pattern that has the given syndrome.

Details of a generator

Generator g_{ba}. Set of coordinate positions. Consists of αa A^2, $b\beta \in B^2$ for a, b fixed, α neighbour of b, β neighbour of a.

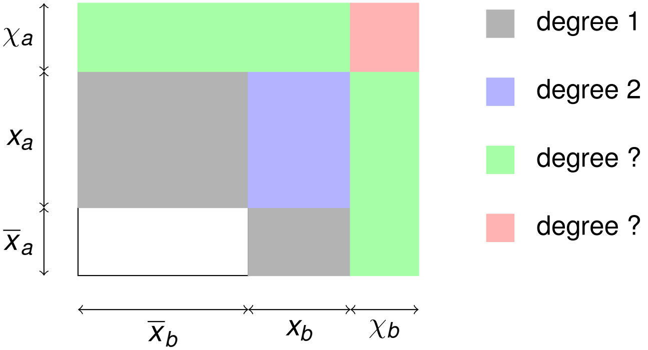


Inside of rectangle consists of all $\alpha\beta$: syndrome coordinates.
Shaded area: syndrome coordinates that are at “1”.

Critical generators

Classical expander codes: decoding relies on existence of bit node with many unique neighbours.

Quantum case: rely on the existence of *critical generator*.



When “flipping” error positions x_a and x_b , only syndrome coordinates can transition $0 \to 1$. Weight always decreases if small enough.

Critical generators and expansion

Weight decreases if $\chi_a \leq \frac{1}{3}\Delta_B$ and $\chi_b \leq \frac{1}{3}\Delta_A$.

Existence of a critical generator guaranteed if expansion *of component graphs $A \leftrightarrow B$ and $B \leftrightarrow A$ is large enough.* We need expansion of $5/6$ of graph degree. Compare with $3/4$ in classical LDPC case.

Key: Consider projection of error set on first and second coordinates.

Theorem: If expansion of $5/6$degree in $A \leftrightarrow B$ and $B \leftrightarrow A$ guaranteed for subsets of vertices less than $\gamma_A|A|$ and $\gamma_B|B|$, then algorithm corrects every pattern of weight less than

$$\frac{1}{1+3\Delta_B}\min(\gamma_A|A| + \gamma_B|B|).$$

Questions

- Construct (rather than randomly choose) bipartite graphs $A \leftrightarrow B$ that have strong expansion from both sides ?
- Behaviour of algorithm for typical errors (rather than adversarial): deal with $\#$errors linear in n ?
- Better codes ? Minimum distance linear in n ?