An efficient decoding of random errors for quantum expander codes

*arXiv:*1711.08351

joint work with O. Fawzi and A. Grospellier

Anthony Leverrier
(Inria Paris)

Conference on "Quantum Information Theory"

Outline of the talk

- quantum error correcting codes
- quantum expander codes
- quantum fault-tolerance with constant overhead (Gottesman'13)
- analysis of decoding algorithm for quantum expander codes

Outline of the talk

- quantum error correcting codes
- quantum expander codes
- quantum fault-tolerance with constant overhead (Gottesman'13)
- analysis of decoding algorithm for quantum expander codes

Quantum error correcting codes

goal: protect quantum information for communication or computation

- encode k logical qubits into n physical qubits
- natural setting for communication: *constant rate* code, i.e. $\frac{k}{n} = \mathbf{cst}$

For computation: threshold theorem (Aharonov, Ben-Or'97)

Theory: A logical circuit using m qubits and containing T gates is replaced by a fault-tolerant circuit using $O(m\,\mathbf{polylog}(mT))$ qubits.

Practice: break RSA with 4000 logical qubits, but $10^6 - 10^9$ physical qubits ...

Gottesman's breakthrough ('13):
using the right family of constant rate LDPC codes, the overhead (ratio physical/logical) for FT can be made *constant!*

Quantum codes

- subspace of dimension 2^k of $(\mathbb{C}^2)^{\otimes n}$
- given a set of commuting generators $g_1, \cdots, g_{n-k}$ acting on n qubits,

$$\mathcal{Q} = \{|\psi\rangle \in (\mathbb{C}^2)^{\otimes n} \,:\, g_i|\psi\rangle = |\psi\rangle \quad \forall g_i\}$$

- *syndrome:* which constraints are satisfied or violated

LDPC codes (low-density parity-check matrix)

- g_i acts non trivially on *constant* nb of qubits
- each qubit acted upon by *constant* nb of generators

$\Longrightarrow$ $\mathcal{Q}$ is the degenerate groundspace of the *local Hamiltonian* $H = -\sum_i g_i$

Minimum distance $d_{\min}$

- size of support of a minimal Pauli error that maps a codeword to an orthogonal one
- record for LDPC codes $d_{\min} = \Theta(n^{1/2} \log^{1/4} n)$ (Freedman, Luo, Meyer'02)

Topological codes

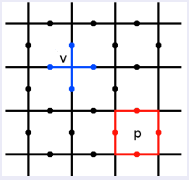
CSS codes: generators g_i either product of σ_X or product of σ_Z

$\Longrightarrow$ only need to enforce that X-type generators commute with Z-type generators

Surface codes (Kitaev'97)

Consider a closed surface $\mathcal{S}$ with a tiling:

- qubits on edges
- X-type generators associated with vertices
- Z-type generators associated with plaquettes



parameters of the code given
by properties of the surface:

[[n, k, d_{min}]] $\approx$ [[size of $\mathcal{S}$, *genus (# holes)*, systole (size of min noncontractible loop)]]

- toric code: $[[n, k, d_{min}]] = [[n, 2, \sqrt{n/2}]]$
- with constant rate: $[[n, k, d_{min}]] = [[n, \Theta(n), \Theta(\log n)]]$

optimal for 2d *hyperbolic codes* (Delfosse'13 using Gromov's systolic inequality)

Generalization to higher dimensional manifolds

similar construction with arbitrary compact manifolds:
even dimensions are nice:

- qubits on $\frac{d}{2}$-cells
- X-generators and Z-generators play the same role by Poincaré duality

4D hyperbolic codes (Guth-Lubotzky'13)

cellulation of a 4D compact manifold

- beat Delfosse's bound: $[[n, k, d_{min}]] = [[n, \Theta(n), \Theta(n^c)]]$ for $0.2 \leq c \leq 0.3$
- efficient decoding algorithm for errors of weight $O(\log n)$ (Hastings'13)

soon on the arXiv (V. Londe, AL):

- 4D hyperbolic codes with regular cellulation with hypercubes
- possibility to exploit the local structure to design better decoding algorithms

Outline of the talk

- quantum error correcting codes
- quantum expander codes
- quantum fault-tolerance with constant overhead (Gottesman'13)
- analysis of decoding algorithm for quantum expander codes

Hypergraph product codes (Tillich - Zémor'09)

inspired by the toric code, interpreted as a product of 2 cycles (= 2 repetition codes)
more generally, consider two classical codes

$$\mathcal{C}_1 = \ker \mathrm{H}_1, \quad \mathcal{C}_2 = \ker \mathrm{H}_2$$

Tillich-Zémor construction

CSS code corresponding to the "tensor product" of the chain complexes of length 2 corresponding to H_1 and $\mathrm{H}_2^{\mathrm{T}}$:

$$[\mathrm{n}_1, \mathrm{k}_1, \mathrm{d}_1] \otimes [\mathrm{n}_2, \mathrm{k}_2, \mathrm{d}_2] \to [[\mathrm{N}, \mathrm{K}, \mathrm{D}_{\min}]]$$

If $\mathcal{C}_1 = \mathcal{C}_2$ is a good LDPC code, then the hypergraph product code is a *constant rate LDPC code* with

$$\mathrm{D}_{\min} = \Theta(\sqrt{\mathrm{N}}).$$

$\Longrightarrow$ best known construction for quantum LDPC codes

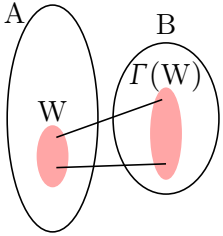
but no known efficient decoding algorithm

Quantum expander codes (AL - Tillich - Zémor'15)

hypergraph product of codes with *expanding factor graphs*

- factor graph associated with H: bipartite graph $(A \cup B, \mathcal{E})$ where $a \sim b \iff H_{a,b} = 1$
- bipartite graph (A, B) of left degree d_A is (γ, δ)-expanding if for all $W \subset A$ s.t. $|W| \leq \gamma |A|$, we have

$$|\Gamma(W)| \geq (1-\delta) d_A |W| \qquad (\delta - \text{close to maximum})$$



- we require that the factor graph is both left and right expanding, with $\delta < \frac{1}{6}$
- such graphs can be found with high probability in a randomized fashion

Efficient decoding algorithm for quantum expander codes

- inspired by the Sipser-Spielman decoding algorithm for *classical* expander codes ('96):
  - flip a bit if it decreases the syndrome weight
  - for $\delta < \frac{1}{4}$, corrects all errors of weight $< \frac{\gamma}{2} n$

Quantum case (AL - Tillich - Zémor'15)

- decode X errors and Z errors independently
- look at a generator, and *flip a subset of qubits* if it decreases the syndrome weight (local Hamiltonian picture, flip small sets of qubits that decrease the energy)
- for $\delta < \frac{1}{6}$, corrects all errors of weight $O(\sqrt{n})$
- optimal for adversarial errors

- (quasi)-linear time decoding algorithm *(new result: can be parallelized to $O(\log n)$ time)*
- what about *random errors of linear weight*?

YES! *arXiv:1711.08351*

Efficient decoding algorithm for quantum expander codes

- inspired by the Sipser-Spielman decoding algorithm for *classical* expander codes ('96):
  - flip a bit if it decreases the syndrome weight
  - for $\delta < \frac{1}{4}$, corrects all errors of weight $< \frac{\gamma}{2} n$

Quantum case (AL - Tillich - Zémor'15)

- decode X errors and Z errors independently
- look at a generator, and *flip a subset of qubits* if it decreases the syndrome weight (local Hamiltonian picture, flip small sets of qubits that decrease the energy)
- for $\delta < \frac{1}{6}$, corrects all errors of weight $O(\sqrt{n})$
- optimal for adversarial errors

- (quasi)-linear time decoding algorithm *(new result: can be parallelized to $O(\log n)$ time)*
- what about *random errors of linear weight*?

YES! *arXiv:1711.08351*

Outline of the talk

- quantum error correcting codes
- quantum expander codes
- quantum fault-tolerance with constant overhead (Gottesman'13)
- analysis of decoding algorithm for quantum expander codes

Gottesman's desiderata for the code family

constant overhead fault-tolerance if ∃ family of quantum LDPC codes with:

- constant rate
- $d_{\min} = \Omega(n^{\varepsilon})$ for $\varepsilon > 0$
- efficient decoding algorithm, that suppresses errors exponentially
- deals with *local stochastic* qubit errors and measurement errors

local stochastic noise

V = set of qubits; an error of parameter p is a random set $W \subseteq V$ such that for all $F \subseteq V$,

$$\mathbb{P}(F \subseteq W) \leq p^{|F|}$$

$\Longrightarrow$ location of error is arbitrary, but prob decays exponentially with weight

Gottesman's desiderata for the code family

constant overhead fault-tolerance if ∃ family of quantum LDPC codes with:

- constant rate
- $d_{\min} = \Omega(n^{\varepsilon})$ for $\varepsilon > 0$
- efficient decoding algorithm, that suppresses errors exponentially
- deals with *local stochastic* qubit errors and measurement errors

local stochastic noise

V = set of qubits; an error of parameter p is a random set $W \subseteq V$ such that for all $F \subseteq V$,

$$\mathbb{P}(F \subseteq W) \leq p^{|F|}$$

$\Longrightarrow$ location of error is arbitrary, but prob decays exponentially with weight

Decoding cst rate LDPC codes against random errors

Family	d_{min}	Error suppression
surface codes	$O(\log n)$	polynomial Edmond's matching algo
4D hyperbolic codes (Guth-Lubotzky'13)	$\in [n^{0.2}, n^{0.3}]$	polynomial (Hastings'13)
hypergraph product codes (Tillich-Zémor'09)	$\Theta(n^{1/2})$	no efficient decoding algo known in general
quantum expander codes (AL-Tillich-Zémor'15)	$\Theta(n^{1/2})$	exponential *(this work)*

Decoding cst rate LDPC codes against random errors

Family	d_{min}	Error suppression
surface codes	$O(\log n)$	polynomial Edmond's matching algo
4D hyperbolic codes (Guth-Lubotzky'13)	$\in [n^{0.2}, n^{0.3}]$	polynomial (Hastings'13)
hypergraph product codes (Tillich-Zémor'09)	$\Theta(n^{1/2})$	no efficient decoding algo known in general
quantum expander codes (AL-Tillich-Zémor'15)	$\Theta(n^{1/2})$	exponential *(this work)*

Decoding cst rate LDPC codes against random errors

Family	d_{min}	Error suppression
surface codes	$O(\log n)$	polynomial Edmond's matching algo
4D hyperbolic codes (Guth-Lubotzky'13)	$\in [n^{0.2}, n^{0.3}]$	polynomial (Hastings'13)
hypergraph product codes (Tillich-Zémor'09)	$\Theta(n^{1/2})$	no efficient decoding algo known in general
quantum expander codes (AL-Tillich-Zémor'15)	$\Theta(n^{1/2})$	exponential *(this work)*

Decoding cst rate LDPC codes against random errors

Family	d_{min}	Error suppression
surface codes	$O(\log n)$	polynomial Edmond's matching algo
4D hyperbolic codes (Guth-Lubotzky'13)	$\in [n^{0.2}, n^{0.3}]$	polynomial (Hastings'13)
hypergraph product codes (Tillich-Zémor'09)	$\Theta(n^{1/2})$	no efficient decoding algo known in general
quantum expander codes (AL-Tillich-Zémor'15)	$\Theta(n^{1/2})$	exponential *(this work)*

Outline of the talk

- quantum error correcting codes
- quantum expander codes
- quantum fault-tolerance with constant overhead (Gottesman'13)
- analysis of decoding algorithm for quantum expander codes

Our result on quantum expander codes

*Our result arXiv:*1711.08351 *(O. Fawzi, A. Grospellier, AL)*

there exists $p_{\text{th}} > 0$ such that the decoding algorithm corrects random errors (i.i.d. and local stochastic) with probability $1 - O(\exp(-c\sqrt{n}))$ for $p \leq p_{\text{th}}$

- our bound of p_{th} is very small ($\approx 10^{-16}$)
- (since yesterday!) the algorithm can also deal with errors on the syndrome (with better expansion $\delta < \frac{1}{24}$)
- *satisfies all the desiderata for Gottesman constant overhead FT scheme*
- but quite impractical . . . next step: numerical simulations

What is there to prove?

Challenge

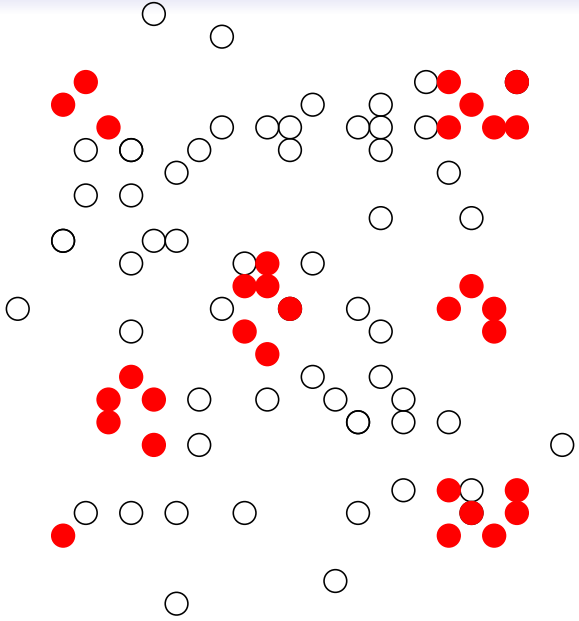
- we know that the algorithm corrects *arbitrary* errors of size $O(\sqrt{n})$
- we want to correct *random* errors of weight $\Theta(n)$
- is it possible?
- intuition: yes! because problematic errors of size $O(\sqrt{n})$ are very rare

  $\Longrightarrow$ will not typically occur (Kovalev, Pryadko'12)

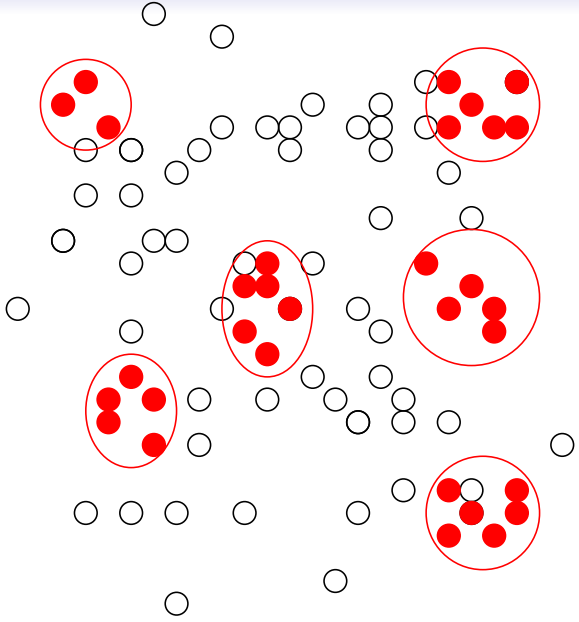
percolation theory: with high probability, the error will consist of small clusters (connected components) each of size $O(\log n)$

$\Longrightarrow$ the decoding algorithm should be able to deal with each of this cluster

whp, clusters of size $O(\log n) \ll \sqrt{n}$

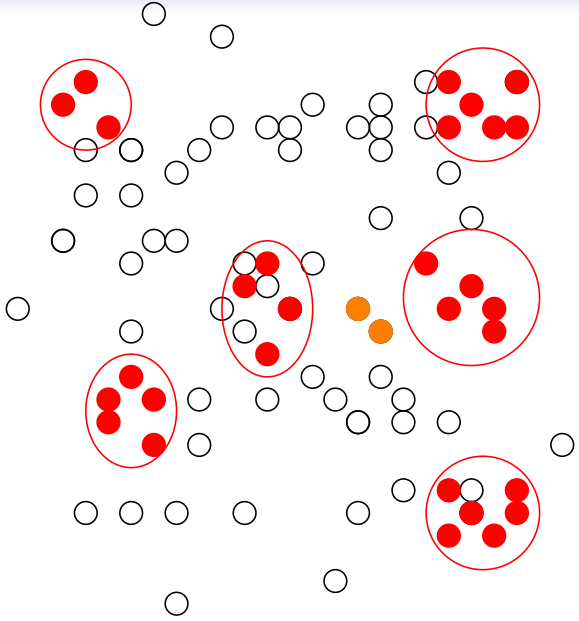


whp, clusters of size $O(\log n) \ll \sqrt{n}$



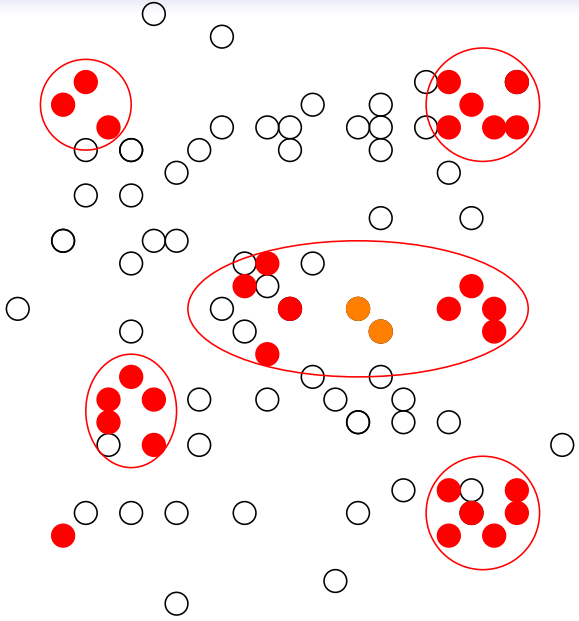
whp, clusters of size $O(\log n) \ll \sqrt{n}$

pb: the algo can sometimes introduce new errors, issue if clusters merge...



whp, clusters of size $O(\log n) \ll \sqrt{n}$

pb: the algo can sometimes introduce new errors, issue if clusters merge...



Local decoding algorithm

- we want to show that clusters cannot merge to reach size $\Omega(n^{1/2})$
- *idea 1:* the decoding algorithm is local: distant errors don't "interfere" at a given step
- *idea 2:* the number of errors (temporarily) introduced by the decoding algorithm is linear in the initial error size

α-locality

there exists $\alpha \leq 1$ such that for any execution $W_0 \xrightarrow{\mathcal{A}} W_1 \xrightarrow{\mathcal{A}} \dots \xrightarrow{\mathcal{A}} W_f$, it holds that

$$\left|\bigcup_i W_i\right| \leq \frac{1}{\alpha}|W_0|.$$

For quantum expander codes, $\alpha = f(\delta)$.

$\implies$ means that W_0 represents a fraction α of the set $\bigcup_i W_i$

problem if $|\bigcup_i W_i| = \Omega(\sqrt{n})$

The algorithm corrects α-subsets

α-subsets, $\mathrm{MaxConn}_\alpha(\mathrm{W})$

An *α-subset* X of a set $\mathrm{W} \subseteq \mathrm{V}$ is a set $\mathrm{X} \subseteq \mathrm{V}$ is that that a fraction α of X belongs to W, $\iff |\mathrm{X} \cap \mathrm{W}| \geq \alpha |\mathrm{X}|$.

$\mathsf{MaxConn}_\alpha(\mathrm{W})$: maximum size of a connected α-subset of W

- A 1-subset of W is a subset in the usual sense
- $\mathsf{MaxConn}_1(\mathrm{W})$ is the size of the largest connected subset of W

α-locality $\implies \bigcup_i \mathrm{W}_i$ is an α-subset of W

Theorem

The local decoding algorithm with parameter α will correct all errors $\mathrm{W} \subseteq \mathrm{V}$ satisfying

$$\mathit{MaxConn}_\alpha(\mathrm{W}) \leq \mathrm{O}(\sqrt{\mathrm{n}}) \tag{1}$$

Eqn. (1) holds with high probability for noise model with p below some threshold

α-percolation

Theorem (α-percolation)

Let $\mathcal{G} = (V, \mathcal{E})$ a graph with degree upper bounded by d. Let $\alpha \in (0, 1]$ and let $t \geq 1$ be an integer. Let

$$p_{th} = \left(\frac{2^{-h(\alpha)}}{(d-1)(1+\frac{1}{d-2})^{d-2}} \right)^{\frac{1}{\alpha}},$$

where $h(\alpha) = -\alpha \log_2 \alpha - (1-\alpha)\log_2(1-\alpha)$ is the binary entropy function.

Then, for local stochastic error W with parameter $p < p_{th}$, we have

$$\mathbb{P}[\mathit{MaxConn}_\alpha(W) \geq t] \leq C|V| \left(\frac{p}{p_{th}} \right)^{\alpha t}.$$

idea: the number of connected components containing a set W (or an α-subset of W) is relatively small on a constant degree graph

Noisy syndrome

to apply Gottesman's result, the decoding algorithm must tolerate noise on the syndrome

Theorem (New result, not in the arXiv paper)

- even if the syndrome is noisy, there exists a generator and a set of qubits within that generator that can be flipped to decrease the syndrome weight
- sufficient for the quantum fault-tolerance scheme

Related result

if the syndrome is noiseless, then there are many sets of qubits that decrease the syndrome weight:

$\Longrightarrow$ *the decoding algorithm can be parallelized: time complexity* $= \mathrm{O}(\log |\mathrm{W}|)$

Conclusion

Quantum expander codes (= constant rate LDPC codes)

- efficient decoding algorithm that corrects
  - arbitrary errors of weight $O(\sqrt{n})$
  - random errors (locally stochastic or i.i.d.) with prob $1 - cn \left(\frac{p}{p_{th}}\right)^{C\sqrt{n}}$
- also tolerates (low) locally stochastic noise on the syndrome

$\Longrightarrow$ *satisfies Gottesman's desiderata for constant overhead quantum fault-tolerance*

Proof-of-principle result, but pretty bad bounds

- requires high expansion $\Longrightarrow$ factor graph with degree ≥ 25
- $p_{th} \approx 10^{-16}$ for qubits, even worse for syndrome

$\Longrightarrow$ perform numerical simulation

Thanks!

Conclusion

Quantum expander codes (= constant rate LDPC codes)

- efficient decoding algorithm that corrects
  - arbitrary errors of weight $\mathrm{O}(\sqrt{\mathrm{n}})$
  - random errors (locally stochastic or i.i.d.) with prob $1 - \mathrm{cn}\left(\frac{\mathrm{p}}{\mathrm{p_{th}}}\right)^{\mathrm{C}\sqrt{\mathrm{n}}}$
- also tolerates (low) locally stochastic noise on the syndrome

$\Longrightarrow$ *satisfies Gottesman's desiderata for constant overhead quantum fault-tolerance*

Proof-of-principle result, but pretty bad bounds

- requires high expansion $\Longrightarrow$ factor graph with degree ≥ 25
- $\mathrm{p_{th}} \approx 10^{-16}$ for qubits, even worse for syndrome

$\Longrightarrow$ perform numerical simulation

Thanks!

Conclusion

Quantum expander codes (= constant rate LDPC codes)

- efficient decoding algorithm that corrects
  - arbitrary errors of weight $O(\sqrt{n})$
  - random errors (locally stochastic or i.i.d.) with prob $1 - cn \left(\frac{p}{p_{th}}\right)^{C\sqrt{n}}$
- also tolerates (low) locally stochastic noise on the syndrome

$\Longrightarrow$ *satisfies Gottesman's desiderata for constant overhead quantum fault-tolerance*

Proof-of-principle result, but pretty bad bounds

- requires high expansion $\Longrightarrow$ factor graph with degree ≥ 25
- $p_{th} \approx 10^{-16}$ for qubits, even worse for syndrome

$\Longrightarrow$ perform numerical simulation

Thanks!