Efficient decoding of random errors for quantum expander codes

Omar Fawzi, Antoine Grospellier, Anthony Leverrier

Efficient decoding of random errors for quantum expander codes

Omar Fawzi, Antoine Grospellier, Anthony Leverrier

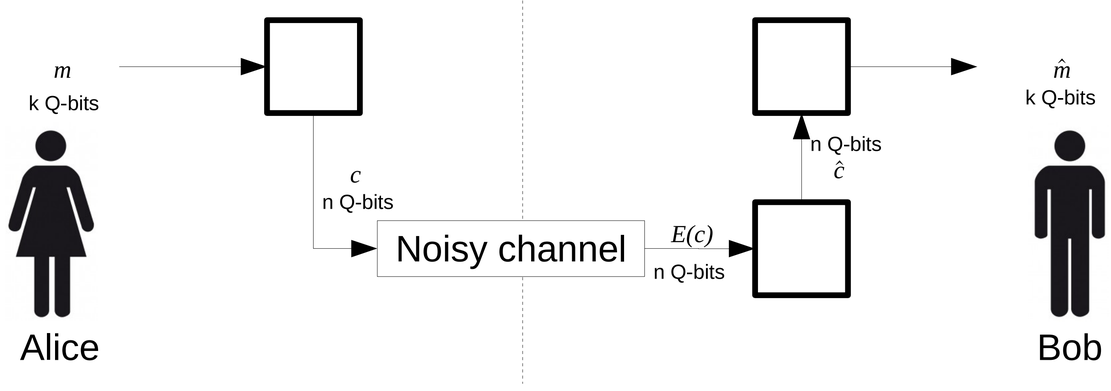
ENS Lyon, INRIA Paris

https://arxiv.org/abs/1711.08351

Abstract

We show that quantum expander codes, a constant-rate family of quantum LDPC codes, with the quasi-linear time decoding algorithm of Leverrier, Tillich and Zémor can correct a constant fraction of random errors with very high probability. This is the first construction of a constant-rate quantum LDPC code with an efficient decoding algorithm that can correct a linear number of random errors with a negligible failure probability. Finding codes with these properties is also motivated by Gottesman's construction of fault tolerant schemes with constant space overhead.

What is a quantum code?



A $[\![n, k, d]\!]$ quantum code is defined by:

- n the size of the encoded message that Alice sends through the noisy channel
- k the size of the original message that Alice wants to send to Bob
- d the minimum weight of a Pauli error that Bob cannot correct

The "Good" quantum code quest

A $[\![n, k, d]\!]$ quantum code is "good" if:

- $k = \Theta(n)$
- $d = \Theta(n)$
- This code is LDPC
- There is an efficient decoding algorithm to correct linear size errors

No such code is known

Quantum expander codes

Quantum expander codes have been introduced in [1]. They satisfy:

- $k = \Theta(n)$
- $d = \Theta(\sqrt{n})$
- This code is LDPC
- There is an efficient decoding algorithm to correct errors of size $\Theta(\sqrt{n})$

The problem we have solved

For quantum expander codes, some errors of size $\Theta(\sqrt{n})$ cannot be corrected by any decoding algorithm. Do random errors of size $\Theta(n)$ are corrected by the decoding algorithm of [1] with a good probability?

Motivation

Shor's algorithm needs $k \approx 1000$ logical qubits in order to break RSA. With the usual fault tolerant techniques, this means $n \approx 10^6 - 10^9$ physical qubits. In [2], Gottesman gives a way to drastically reduce this overhead, but he assumes that some quantum codes with nice properties exist. For the moment, no existing code is totally satisfying and quantum expander codes are natural candidates. Our goal is to prove that quantum expander codes have the required properties to be plugged into the construction of Gottesman.

Our main theorem

There exists a constant $p_0 > 0$ such that if the noise parameter p satisfies $p < p_0$, then the decoding algorithm of [1] corrects a random error with probability at least $1 - e^{\Theta(\sqrt{n})}$.

Tools

- Factor graph and adjacency graph of a code
- Expander graphs
- Percolation theory

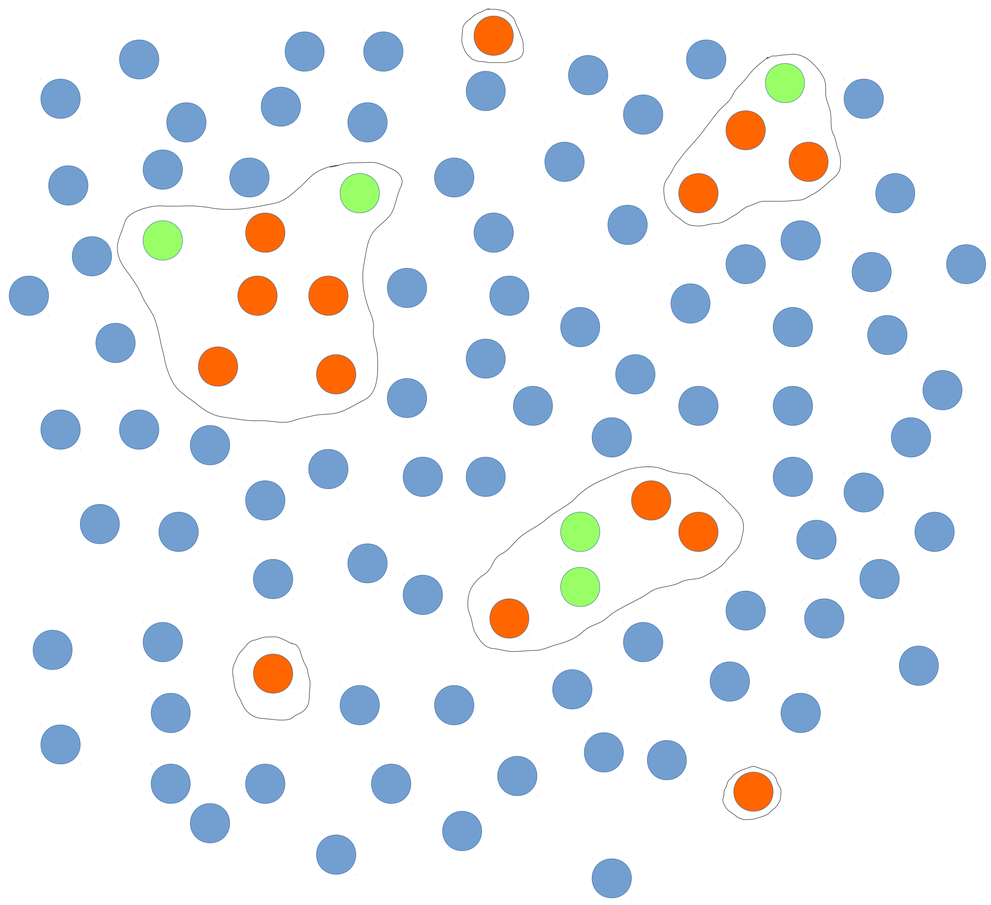
Usual percolation theorem

Let $\mathcal{G}$ be a graph of degree bounded by d and W a set of vertices where each vertex has been chosen independently with probability p. For all $p < \frac{1}{d-1}$, with high probability: if X is a connected set of $\mathcal{G}$ then $X \subseteq W \Rightarrow |X| < cst. \log(n)$.

Main idea to prove our theorem: represent qubits by vertices on a bounded degree graph and represent random errors on qubits by a percolation process. The error is thus composed of small clusters which can be corrected independently.
Main issue: the clusters can merge during the decoding algorithm and so we can get clusters which are too big to be corrected.

Generalised percolation theorem

Let $\mathcal{G}$ be a graph of degree bounded by d and W a set of vertices where each vertex has been chosen independently with probability p. For all $\alpha > 0$ and $p < cst(\alpha, d)$, with high probability: if X is a connected set of $\mathcal{G}$ with $|X \cap W| \geq \alpha |X|$ then $|X| < cst. \log(n)$.



The dots represent qubits:

- Red dots are qubits initially in error
- Green dots are qubits in error during some step of the decoding algorithm

Our proof

Take X a connected component composed of red dots and green dots. Then $|\{\text{red dots in } X\}| \geq \alpha |X|$. We apply the percolation theorem:

- $|X| < cst. \log(n)$
- Since the decoding algorithm corrects any adversarial error of size $\Theta(\sqrt{n})$, it corrects the error contained in X
- Since each connected component of the error is corrected, the entire error is corrected

Future work

- Run simulations: our theoretical threshold is $p_0 = 3.10^{-16}$ but in practice it should be better
- Apply our work to fault tolerant quantum computation: [2]

References

[1] Anthony Leverrier, Jean-Pierre Tillich, and Gilles Zémor.
Quantum expander codes.
In *Foundations of Computer Science (FOCS), 2015 IEEE 56th Annual Symposium on*, pages 810–824. IEEE, 2015.

[2] Daniel Gottesman.
Fault-tolerant quantum computation with constant overhead.
arXiv preprint arXiv:1310.2984, 2013.

inventeurs du monde numérique
1967 › 2017 » 2067
Imaginons notre futur

ENS DE LYON