Efficient decoding of random errors for quantum expander codes
Omar Fawzi, Antoine Grospellier, Anthony Leverrier

To cite this version:
Omar Fawzi, Antoine Grospellier, Anthony Leverrier. Efficient decoding of random errors for quantum expander codes. 8th colloquium of the GDR IQFA - Ingénierie Quantique, des Aspects Fondamentaux aux Applications, Nov 2017, Nice, France. hal-01671496

HAL Id: hal-01671496
https://hal.science/hal-01671496v1
Submitted on 22 Dec 2017

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers. L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
Efficient decoding of random errors for quantum expander codes
Omar Fawzi, Antoine Grosspellier, 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.

Quantum expander codes have been introduced in [1]. They satisfy:
- \( k = \Theta(n) \)
- \( d = \Theta(\sqrt{n}) \)
- There is an efficient decoding algorithm to correct errors of size \( \Theta(\sqrt{n}) \)

No such code is known

Quantum expander codes have been introduced in [1]. They satisfy:
- \( k = \Theta(n) \)
- \( d = \Theta(\sqrt{n}) \)
- There is an efficient decoding algorithm to correct errors of size \( \Theta(\sqrt{n}) \)

The “Good” quantum code quest

A \([n, k, d]\) quantum code is “good” if:
- \( k = \Theta(n) \)
- \( d = \Theta(n) \)
- There is an efficient decoding algorithm to correct linear size errors

No such code is known

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 \( n \approx 10^7 \times 10^7 \) 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 \( 1 - e^{10/\sqrt{n}} \).

Tools

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

Usual percolation theorem

Let \( G \) 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 \( p < \text{cst}(\alpha, d) \), with high probability: if \( X \) is a connected set of \( G \) then \( X \subseteq W \Rightarrow \vert X \vert < \text{cst}. \log(n) \).

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.

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.