Title: Towards local testability for quantum coding

Speakers: Anthony Leverrier

Collection: Symmetry, Phases of Matter, and Resources in Quantum Computing

Date: November 27, 2019 - 4:00 PM

URL: http://pirsa.org/19110133

Abstract: We introduce the hemicubic codes, a family of quantum codes obtained by associating qubits with the
p-faces of the n-cube (for n>p) and stabilizer constraints with faces of dimension (pÂ±1). The quantum code obtained by identifying antipodal faces of the resulting complex encodes one logical qubit into N=2nâˆ’pâˆ’1(np) physical qubits and displays local testability with a soundness of Î©(logâˆ’2(N)) beating the current state-of-the-art of logâˆ’3(N) due to Hastings. We exploit this local testability to devise an efficient decoding algorithm that corrects arbitrary errors of size less than the minimum distance, up to polylog factors.
We then extend this code family by considering the quotient of the n-cube by arbitrary linear classical codes of length n. We establish the parameters of these generalized hemicubic codes. Interestingly, if the soundness of the hemicubic code could be shown to be 1/log(N), similarly to the ordinary n-cube, then the generalized hemicubic codes could yield quantum locally testable codes of length not exceeding an exponential or even polynomial function of the code dimension. (joint work with Vivien Londe and Gilles ZÃ©mor)

Quantum local testability

*arXiv:*1911.03069

Anthony Leverrier, Inria

(with Vivien Londe and Gilles Zémor)

27 nov 2019

Symmetry, Phases of Matter, and Resources in Quantum Computing

We want:

a local Hamiltonian such that

- with degenerate ground space (quantum code)
- the energy of an error scales linearly with the size of the error

The current research on quantum error correction

mostly concerned with the goal of building a (large) quantum computer

desire for realistic constructions

- LDPC codes: the generators of the stabilizer group act on a small number of qubits
- spatial/geometrical locality: qubits on a 2D/3D lattice
- main contenders: surface codes, or 3D variants

A fairly reasonable and promising approach

- good performance for topological codes: efficient decoders, high threshold
- overhead still quite large for fault-tolerance (magic state distillation) but the numbers are improving regularly

Is this it?

Better quantum LDPC codes?

from a math/coding point of view, topological codes in 2D-3D are not that good

- 2D toric code $[\![n, k = O(1), d = O(\sqrt{n})]\!]$
- topological codes on 2D Euclidean manifold (Bravyi, Poulin, Terhal 2010)

$$kd^2 \leq cn$$

- topological codes on 2D hyperbolic manifold (Delfosse 2014)

$$kd^2 \leq c(\log k)^2 n$$

- things are better in 4D hyp. space: Guth-Lubotzky 2014 (also Londe-Leverrier 2018)

$$[\![n, k = \Theta(n), d = n^{\alpha}]\!], \quad \text{for} \quad \alpha \in [0.2, 0.3]$$

what can we get by relaxing geometric locality in 3D?

- we still want an LDPC construction, but allow for non local generators
- a nice mathematical topic with many frustrating open questions!

Classical LDPC codes are well understood

sparse parity-check matrix $\mathrm{H} \in \mathbb{F}_2^{\mathrm{m}\times\mathrm{n}}$:

$$\mathcal{C} = \ker \mathrm{H}$$

- good codes with $\mathrm{k} = \Theta(\mathrm{n}), \mathrm{d} = \Theta(\mathrm{n})$ can be found by picking H at random
- efficient decoding with belief propagation

quantum LDPC codes remain poorly understood

stabilizer group $\mathcal{S} = \langle g_1, \ldots, g_m \rangle$ with $g_i \in \mathcal{P}_n$ (n-qubit Pauli group) such that $[g_i, g_j] = 0$

LDPC:

- $|g_i|$ small (constant or log)
- $\forall \ell \in [n], \quad \sharp\{i : \ell \in \mathbf{supp}(g_i)\}$ small

$$\mathcal{C} = \{|\psi\rangle \in (\mathbb{C}^2)^{\otimes n} : g_i|\psi\rangle = |\psi\rangle, \forall i \in [m]\}$$

The big questions (for me!)

- what kind of parameters are possible for qLDPC?
- efficient decoding??
- links with Hamiltonian complexity

quantum LDPC codes with large minimum distance

Beating the $\sqrt{n}$ of the toric code is very hard!

- Freedman, Meyer, Luo (2002): construction based on $S^1 \times S^2$

$$d \propto n^{1/2} \log^{1/4} n$$

- Kaufman, Kazhdan, Lubotzky (2016): construction based on Ramanujan complexes

$$d_X \propto n, \quad d_Z \propto \log n$$

+ balancing technique (Hastings 2017)

$$\Longrightarrow \; d \propto n^{1/2} \log^{1/2} n$$

- construction by Hastings (2017) he conjectures could yield $d \propto n^{1-\varepsilon}$

quantum LDPC codes with large minimum distance

best minimum distance when asking for constant rate

hypergraph product codes (Tillich, Zémor 2009) of two good classical LDPC codes

$$[\![n, \Theta(n), \Theta(\sqrt{n})]\!]$$

- note 1: generalization of the toric code (product of 2 repetition codes)
- note 2: existence of codes with $d \propto n$ by relaxing the LDPC condition to $\sqrt{n}$-local generators (Bravyi, Hastings 2014)

Do good qLDPC codes exist?

Decoding quantum LDPC codes

- essentially solved for topological codes!

What about general codes?

- *belief propagation*: several issues (Poulin, Chung 2008)
  - lots of small cycles
  - many symmetric patterns (half generators) where the decoder gets stuck
  - how to deal with degenerescence??
- *greedy decoding in local balls*
  - for 4D hyperbolic codes (Hastings 2014)
  - small-set-flip for quantum expander codes (Leverrier, Tillich, Zémor 2015, Fawzi, Grospellier, Leverrier 2018)

Small-set-flip for quantum expander codes

- consider a classical expander code (Sipser, Spielman 1996), i.e. such that its factor graph is an expander
- hypergraph product code $\Longrightarrow$ quantum expander code $[\![n, \Theta(n), \Theta(\sqrt{n})]\!]$

small-set-flip decoding

- for each g_i: consider all patterns of errors within g_i and apply the one that decreases the syndrome weight the most (if it exists)
- repeat while possible

- correct arbitrary errors of weight $O(\sqrt{n})$
- locality of SSF $\Longrightarrow$ distant clusters of errors are also dealt with
- cst threshold for local stochastic errors on both qubits and syndrome measurements
- *reasonable performance in practice*: threshold around 6-7 % with noiseless syndrome measurement and $\approx 3\%$ for noisy syndrome measurement for phenomenological noise model (Grospellier, Krishna 2018, Grospellier, Grouès, Krishna, Leverrier 2019)

Soundness and local testability

The analysis of the bit-flip decoder for classical expander codes and SSF for quantum expander codes relies on the soundness of the codes:

soundness of quantum expander codes

for any error e such that $|e| := d(e, \mathcal{C}) \leq c\sqrt{n}$,

$$|s(e)| \geq \eta |e|$$

for $\eta = \text{cst}$, and $s(e)$ the syndrome

If true for any e, then *locally testable code*

$\Longrightarrow$ easy to distinguish between codewords and words far from the code, making a constant number of queries to the word.

Many applications in the classical setting, mostly in theoretical CS, e.g. for PCP theorem review paper by Goldreich (2006)

Quantum locally testable codes

- notion introduced by Aharonov, Eldar (2015)
- applications remain a bit unclear at the moment, essentially in Hamitlonian complexity
  - qLTC with linear minimum distance would establish the NLTS conjecture (Eldar, Harrow 2017)
  - existing qLTC (this talk) allows to prove an average-case version of NLTS (Eldar 2019)
  - strong form of confinement of errors (Stephen's talk yesterday)
  - link with *single-shot decoding* (Campbell 2018)
- definition requires to quantize notions of *distance to code* and *weight of the syndrome*

qLTC with soundness η

- q-local quantum code $\mathcal{C} \implies$ *Hamiltonian* $H_{\mathcal{C}} = \frac{1}{qm}\sum_{i=1}^{m}\frac{1}{2}(\mathbb{1} - g_i)$
- projector $\Pi_{\mathcal{C}_t}$ on t-*fattening of the code*

$$\mathcal{C}_t := \mathrm{Span}\{(A_1 \otimes \cdots \otimes A_n)|\psi\rangle \,:\, |\psi\rangle \in \mathcal{C}, |\{i \,:\, A_i \neq \mathbb{1}\}| \leq t\}$$

$$D_{\mathcal{C}} = \sum_t t(\Pi_{\mathcal{C}_t} - \Pi_{\mathcal{C}_{t-1}})$$

A quantum code is locally testable with soundness η if

$$H_{\mathcal{C}} \succeq \frac{\eta}{N} D_{\mathcal{C}} \quad \text{(energy} \geq \eta \times \text{distance)}$$

2 known constructions

- Hastings (2017): $\eta = \frac{1}{\log^3 n}, k = 2$
- this work: $\eta = \frac{1}{\log^2 n}, k = 1$, possibly also for $k = \omega(1)$?

Examples of codes which are NOT locally testables

- 2D toric code: errors of weight $\Omega(\sqrt{n})$ and constant energy
- D-dimensional toric code
- quantum expander codes: errors of weight $\Omega(\sqrt{n})$ and constant energy

The hemicubic code construction

alternative name: the projective code (QIP'19)

Main properties of the hemicubic codes

almost LDPC: log-local

The simplest version: 1 logical qubit

$$[\![N, 1, d \geq \sqrt{N}/1.62]\!]$$

- locally testable with $\eta = \Omega\left(\frac{1}{\log^2 N}\right)$, open whether $\eta = \Theta\left(\frac{1}{\log N}\right)$?
- efficient decoder for adversarial errors of size $\frac{d}{\text{polylog}(N)}$

The general case: $k = N^{\alpha}$

explicit parameters of the form: $[\![N, \text{poly}(N), \text{poly}(N)]\!]$

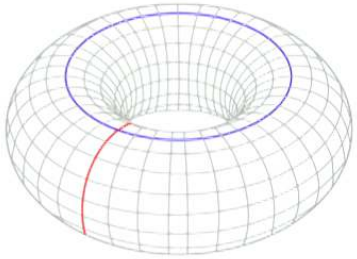
- conjectured local testability

Idea behind the construction: homological codes with large min distance?

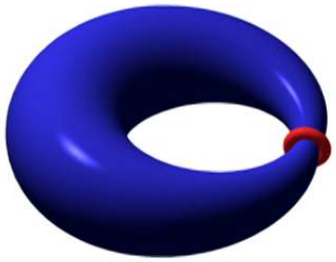
Geometric interpretation of N and d for surfaces:

- N $\approx$ area of the surface

- d = *systole* of the surface, length of the shortest loop which is not the boundary of a 2D subregion of the surface



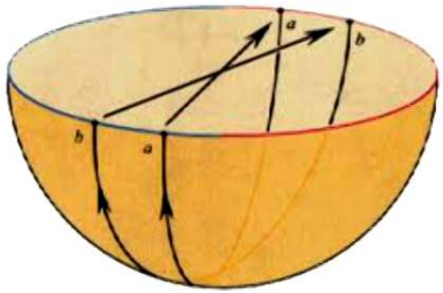
- idea: minimize N at fixed d



- work on surface with positive curvature $\Longrightarrow$ sphere (requires some identification to get a logical qubit)

The real projective plane

- identify antipodal points $\Longrightarrow$ some loops are not boundaries: homology
- 1 logical qubit
  - systole $= \pi$
  - area $= 2\pi \implies$ systole $> \sqrt{\text{area}}$
  - $\overset{?}{\Longrightarrow}$ $D > \sqrt{N}$

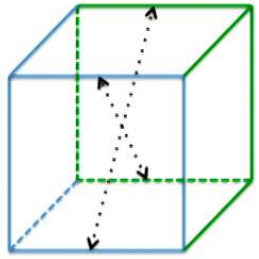


Not an infinite family of quantum codes...

Solution: increase the ambient dimension (similar to Hastings 2016)

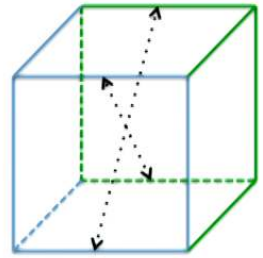
A discrete real projective plane

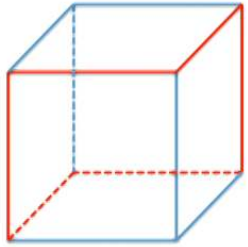
- identify pairs of antipodal faces of the cube
- $N = 6$ (qubits on edges)
- $D_X = 3$ (smallest non trivial cycle)
- $D_Z = 2$ (smallest non trivial cocycle)
- $D = \min(D_X, D_Z) = 2$
- $N = D_X D_Z$



A discrete real projective plane

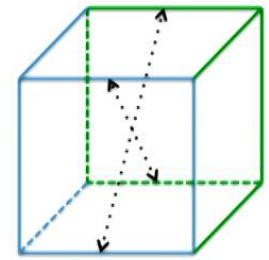
- identify pairs of antipodal faces of the cube
- $N = 6$ (qubits on edges)
- $D_X = 3$ (smallest non trivial cycle)
- $D_Z = 2$ (smallest non trivial cocycle)
- $D = \min(D_X, D_Z) = 2$
- $N = D_X D_Z$

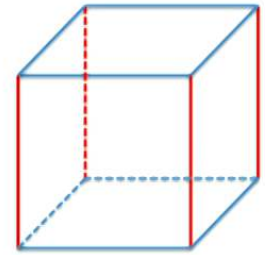




A discrete real projective plane

- identify pairs of antipodal faces of the cube
- $N = 6$ (qubits on edges)
- $D_X = 3$ (smallest non trivial cycle)
- $D_Z = 2$ (smallest non trivial cocycle)
- $D = \min(D_X, D_Z) = 2$
- $N = D_X D_Z$





The hemicubic code: a discrete real projective n-space

- n-hemicube: antipodal quotient of the n-hypercube
- qubits on p-faces ($1 \leq p \leq n-1$), generators on $(p \pm 1)$-faces
- $N = \binom{n}{p} 2^{n-p-1}, \quad K = 1$
- $D_X = \binom{n}{p}$ (minimal nontrivial cycle has a p-face in every direction)
- $D_Z = 2^{n-p-1}$ (minimal nontrivial cocycle consists of all p-faces in a given direction)
- $N = D_X D_Z$
- $D_X \approx D_Z \approx \sqrt{N}$ for $p = \alpha n$ with $\alpha \approx 0.227$.

This code has already appeared in the literature in a completely different form relying on Khovanov homology (Audoux 2013).

Local testabilty of the hemicubic code

Recall that we want to prove that a lower bound on the syndrome weight:

$$\frac{1}{qm}|s(e)| \geq \frac{\eta}{N} d(e, \mathcal{C}), \quad \forall e \in \mathcal{P}_N$$

Hemicubic code: $m = \Theta(N)$, $q = \Theta(\log N)$

We will prove $|s(e)| = \Omega\left(\frac{d(e,\mathcal{C})}{\log N}\right)$, which implies $\eta = \Omega\left(\frac{1}{\log^2 N}\right)$.

Geometric interpretation

for a homological code, $|s(e)|$ is the weight of a boundary and $d(e, \mathcal{C})$ is the minimal weight of its filling.

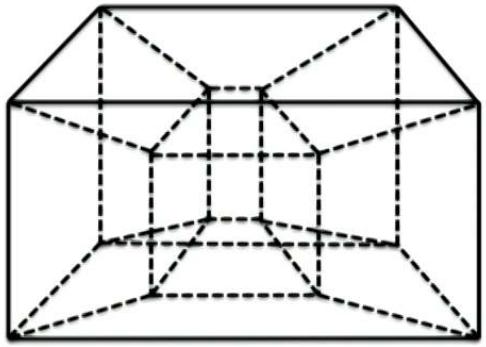
We are looking for filling inequalities.

A filling inequality for the n-hypercube

The syndrome is a boundary B. We are looking for a filling F of it of low weight.

Filling inequality by Dotterrer (2012)

- qubits on 2-faces, checks on edges
- send the syndrome to the left by filling with horizontal squares
- iterate
- choose the order of directions carefully



Dotterrer's bound

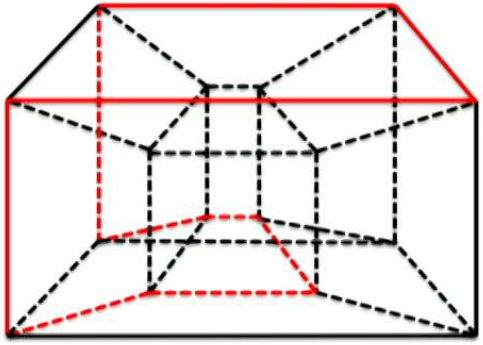
- Dotterrer's algorithm yields: $|B| \geq \mathrm{cst}\,|F| \quad \Longrightarrow \quad |S(e)| \geq \mathrm{cst}\,d(e, \mathcal{C})$
- here: no homology, but a similar approach works for the hemicube
- our current analysis loses a log factor compared to Dotterrer

A filling inequality for the n-hypercube

The syndrome is a boundary B. We are looking for a filling F of it of low weight.

Filling inequality by Dotterrer (2012)

- qubits on 2-faces, checks on edges
- send the syndrome to the left by filling with horizontal squares
- iterate
- choose the order of directions carefully



Dotterrer's bound

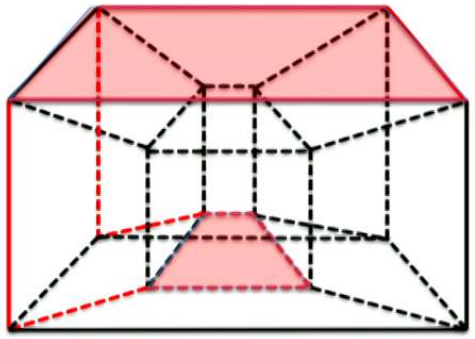
- Dotterrer's algorithm yields: $|B| \geq \mathrm{cst}\,|F| \quad \Longrightarrow \quad |S(e)| \geq \mathrm{cst}\,d(e, \mathcal{C})$
- here: no homology, but a similar approach works for the hemicube
- our current analysis loses a log factor compared to Dotterrer

A filling inequality for the n-hypercube

The syndrome is a boundary B. We are looking for a filling F of it of low weight.

Filling inequality by Dotterrer (2012)

- qubits on 2-faces, checks on edges
- send the syndrome to the left by filling with horizontal squares
- iterate
- choose the order of directions carefully



Dotterrer's bound

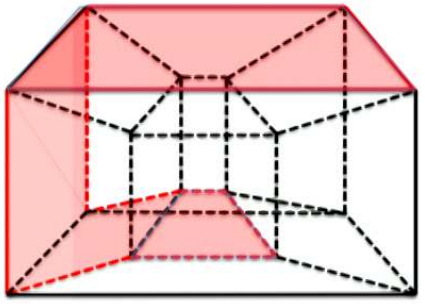
- Dotterrer's algorithm yields: $|B| \geq \mathrm{cst}\,|F| \quad \Longrightarrow \quad |S(e)| \geq \mathrm{cst}\,d(e, \mathcal{C})$
- here: no homology, but a similar approach works for the hemicube
- our current analysis loses a log factor compared to Dotterrer

A filling inequality for the n-hypercube

The syndrome is a boundary B. We are looking for a filling F of it of low weight.

Filling inequality by Dotterrer (2012)

- qubits on 2-faces, checks on edges
- send the syndrome to the left by filling with horizontal squares
- iterate
- choose the order of directions carefully



Dotterrer's bound

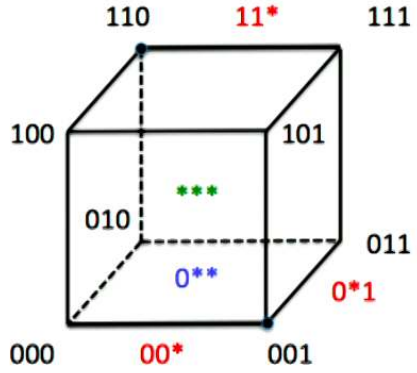
- Dotterrer's algorithm yields: $|\mathrm{B}| \geq \mathrm{cst}\,|\mathrm{F}| \quad \Longrightarrow \quad |\mathrm{S}(\mathrm{e})| \geq \mathrm{cst}\,\mathrm{d}(\mathrm{e}, \mathcal{C})$
- here: no homology, but a similar approach works for the hemicube
- our current analysis loses a log factor compared to Dotterrer

antipodal map = translation by the classical repetition code

codewords of the repetition code: $\{000,111\}$

$\tau_{111}(001) = 001 + 111 = 110$
$\tau_{111}(00*) = 00* + 111 = 11*$

τ_{111} is the antipodal map.



Generalization

Quotient of the n-cube by arbitrary linear codes?

The general construction

The simple construction identifies some cell x of the n-cube with $x + 111\cdots1$.

In other words, the faces are identified if they differ by an element of the repetition code.

- choose a classical linear code $\mathcal{C} = [n, k, d]$
- associate qubits with p-faces of the n-cube, where we identify elements of a given coset of $\mathcal{C}$:

$$x \sim y \quad \Longleftrightarrow \quad x + y \in \mathcal{C}$$

- many more logical qubits: $k = \binom{p+k-1}{p}$
- surprisingly, dimension and minimum distance only depend on the k and d from $\mathcal{C}$, not on H

Perspectives

hemicubic code

- simplest version: n-cube with identified antipodal faces
  - $d = \sqrt{N}$
  - locally testable
- general version
  - n-cube with identification of cosets of a linear code
  - explicit dimension and minimum distance
  - conjectured to be locally testable?

main open question

- what kind of length is possible for quantum LTC? exponential in k, polynomial?

Thanks!