Quantum Codes In Quantum Complexity

Chinmay Nirkhe
IBM
Classical codes have a cartoon that looks like a custard apple.
What fruit/object naturally captures the picture of quantum error-correction?

So I turned to the "Bible" of quantum computing:

Nielsen & Chuang
And this is what I find:

Figure 10.5. The packing of Hilbert spaces in quantum coding: (A) bad code, with non-orthogonal, deformed resultant spaces, and (B) good code, with orthogonal (distinguishable), undeformed spaces.
Outline

An information-theoretic perspective on coding
explain the Nielsen & Chung diagram

The Knill–Laflamme conditions

The complexity of code states (quantum)
dists. over codewords (classical)

The challenge of constructing qLTCs
An information-theoretic perspective on coding

Classical codes:

$2^k$ disjoint Hamming balls of radius $d$ on $\{0,1\}^n$. Cube.

$[0,1]^n$ | No assumption about structure of balls
\| $\subseteq$ not necessarily efficiently decodable
Encoding map = bijective from k-bit strings to centers of the balls.

An error \( e \) s.t. \( |e| \leq d \) on \( \text{enc}(\cdot) \) doesn't leave the Ball. So decodability is possible!

What is the quantum analog of this info. - theoretic perspective?
Issue: While classical errors are discrete, quantum errors are continuous!

How do we draw such a cartoon explaining quantum error-correction if there are an infinite set of errors?
But first, how to read my drawings of high-dimensional spaces.

3-qubit = $2^3$ dim Hilbert space

In my drawings, corners represent orthogonal vectors denoting that both 90° angles
Direct sum of Hilbert spaces

any two points in different shapes are orthogonal.

Ok, now to correcting errors
The packing of Hilbert spaces perspective

Goal: correct against unitary errors $E_1, E_2, \ldots, E_j$ (for now)

\[ \text{original Hilbert space} \]

\[ E_1 \cdot \text{Enc} \]

\[ E_2 \cdot \text{Enc} \]

\[ \text{Enc} \]

\[ \text{Enc} \]

We want to show that $3$ orthogonal spaces per error.
Simple example of a non-code

1.e. $E_1 \cdot \text{Enc}(1 \cdot >) = E_2 \cdot \text{Enc}(1 \ circ >)$

$\Rightarrow$ cannot distinguish these errors.

Actually, stronger statement: if $1 \ circ > \perp 1 \ circ >$, then these states should be orthogonal.
Why orthogonal?

Fact 2 states \( |a\rangle \) and \( |b\rangle \) are perfectly distinguishable if \( |a\rangle \perp |b\rangle \) (orthogonal vectors).

Notice: only connecting \( E_1 \) \& \( E_2 \) if we can distinguish 
\[ E_1 \cdot \text{Enc}(|1\cdot\rangle) \] and 
\[ E_2 \cdot \text{Enc}(|10\rangle) \]

\( \Rightarrow \) These vectors are orthogonal.
It would be too much to ask that

\[ E_1 \cdot \text{Enc}(1 \cdot >) \text{ and } E_2 \cdot \text{Enc}(1 \cdot >) \]

\[ \text{Pf: consider } E_1 \approx_c E_2. \]

By linearity, these states must be close. \( \Box \)

But for some errors \( E_1, E_2 \), they will be orthogonal.

Morally, these errors will form a "basis" for the set of errors we can correct.
The benefit of orthogonality:

\[ E_1 \cdot \text{Enc} \]

\[ E_2 \cdot \text{Enc} \]

\[ E_2 \cdot \text{Enc}(1 \odot >) \text{ is orthogonal to every } E_j \cdot \text{Enc}(1 \odot >) \]
If $|\cdot\rangle \perp |\circ\rangle$, then

$$\Rightarrow \text{span} \left\{ E_{d_1} \cdot \text{Enc}(|\cdot\rangle) \right\} \perp \text{span} \left\{ E_{d_2} \cdot \text{Enc}(|\circ\rangle) \right\}$$

$$\Rightarrow$$ correcting against errors $E_{d_1}, \ldots, E_{d_j}$ implies correcting against unitary errors in their span.

\[ \therefore \text{Suffices to prove my error-correction properties for a "basis" of the errors. Rest follows directly necessarily.} \]

Why prev. talks only discussed correcting bit-flip ($X$) and phase-flip ($Z$) errors.
A basis for the set of errors.

Exercise:

Show that \( \langle a_1 | a_2 \rangle = \eta_{12} \), an invariant that only depends on \( E_1, E_2 \) and not the state \( |a\rangle \).

Hint: Use the property that errors \( E_1, E_2 \) are unitary.
Why does this yield a notion of a basis for the space of errors?

If we can correct all errors $E \in E$, consider a basis $s.t.$

$$\text{span} \left\{ E \cdot \text{Enc} |a\rangle \right\}_{E \in E} = \text{span} \left\{ E_i \cdot \text{Enc} |a\rangle \right\}_{E_{11 \ldots 1} E_j}.$$

By exercise, for any other state $|b\rangle$,

$$\text{span} \left\{ E \cdot \text{Enc} |b\rangle \right\}_{E \in E} = \text{span} \left\{ E_i \cdot \text{Enc} |b\rangle \right\}_{E_{11 \ldots 1} E_j}.$$

$\Rightarrow$ gives natural notion of a basis $E_{1 \ldots E_j}$ for $E$. 
Equiv., can define an inner product on correctable errors 

\[ \langle E_i, E_j \rangle \overset{\text{def}}{=} \eta_{ij} \]

\[ \overset{\text{def}}{=} \langle a | \text{Enc}^+ E_i^+ E_j \text{Enc} | a \rangle \text{ for any } |a\rangle. \]

The basis we found is a basis with respect to this inner product.
Ok, but does the decoding channel/algorithm look like for the set of continuous errors?
Note that $E_1 \cdot \text{Enc}$ and $E_2 \cdot \text{Enc}$ are orthogonal (assumption that they are a basis for errors).
If a measurement perfectly distinguishing the $\square$, $\circ$ errors. If we measure $\square$ error using this, it collapses to either $\square$ or $\circ$. Plus, we know which one!

\[ \sin^2 \theta \quad \cos^2 \theta \]

Gives decoding procedure for a continuous space of errors from a decoding procedure for discrete set.
Generalized error correction procedure:

1. Measure syndrome, i.e. collapse cont. error to a basis error. Syndrome = name of basis error.

2. Correct error based on syndrome.

Step 1 is non-unitary and Step 2 is unitary.

“destructive”

“information preserving”

Error-correction is a controlled destructive process.
Decomposition of space into direct sum from error basis.

Can also correct error channels where elements $\in \mathcal{E}$. 

original Hilbert space

$E_1 \cdot \text{Enc}$

$E_2 \cdot \text{Enc}$
Classical picture

all words that correct to $a$

Quantum picture

subspace of states that correct to $|a\rangle$
The Knill-LaFlamme conditions

Mathematically capture all the orthogonality conditions we drew in the cartoons.

Let $C$ be a quantum code, i.e. $C = \text{image of encoding map}$.
Let $\Pi$ be the projector onto subspace $C$.

Then, $C$ corrects $\{E_i\}$ if

\[
\Pi E_i^\dagger E_j \Pi = \eta_{ij} \Pi 
\]

(coefficients s.t. $\eta_{ij} = (\eta_{ji})^\dagger$.
(the inner product between the error spaces)
Not hard to show this is equivalent to \( \forall |a\>, |b\>, i, j, \langle a | \text{Enc}^\dagger E_i^\dagger E_j \text{Enc} | b \rangle = \langle a | b \rangle \cdot \langle E_i | E_j \rangle \) \( \eta_{ij} \) prev. defined.

Read Nielsen & Chuang Thm 10.1 for formal pf and explicit construction of the recovery channel.

But morally, its the same as the pictoral argument we've drawn so far.
Correcting errors of size $d$.

Error of size $d$: $E$ can be written as $E' \otimes \frac{1}{a} \otimes \frac{1}{n-a}$ qubits.

Correcting all errors of size $d$ equiv. to

Correcting all Pauli ($X-, Y-, Z-$ type) errors of size $d$. equiv. to. correcting all erasure error of size $d$. 
Information destroying channel:

Apply a uniformly random Pauli: \( E(\cdot) = \frac{1}{4\lambda} \sum_{\mathbf{p}} P(\cdot) P^\dagger \).

Can correct information destroying channel if you can correct the Pauli errors.

Correcting d sized errors \( \iff \) correcting d qubit erasures
Thus, quantum codes don’t contain information locally.

The reduced density matrix for any $d$-qubit region of a quantum code is the same no matter what state is encoded.

**Pf.** If the first $d$ qubits of $|\psi_1\rangle = \text{Enc}(|x_1\rangle)$ and $|\psi_2\rangle = \text{Enc}(|x_1\rangle)$ are distinguishable, then $\exists$ unitary $E = E' \otimes \mathbb{1}_{n-d}$ s.t. $\langle \psi_1 | E | \psi_1 \rangle \neq \langle \psi_2 | E | \psi_2 \rangle$. 
But,

\[ \langle \psi_i | E | \psi_i \rangle = \langle \psi_i | \Pi E \Pi | \psi_i \rangle \]

\[ = \langle \psi_i | \eta E \Pi | \psi_i \rangle \]

\[ = \eta E. \]

PF (v2) If reduced density matrices for d-sized regions varied dependent on encoded states,

this violates the no cloning theorem.
If varied depending on original state, then the total transformation is non-linear and violates the no-cloning theorem.

"local indistinguishability"
Quantum codes are not locally decodable
- because local views have no info. on the encoded state!
- contrast to Hadamard code (classically), where any bit of info can be extracted from 2 bits of encoded word.

\[ x \in \{0,1\}^k \rightarrow \{ b \cdot x \in \{0,1\} \}_{b \in \{0,1\}^k} \]

\[ a \cdot x = (b \cdot x) + ((a + b) \cdot x) \quad \forall \ b. \]

- info. is held globally in quantum codes
Applications of quantum codes past correcting errors

- Cryptography: Secret sharing
  Encode state into $n$ qubits via code and divide into $m$ pieces. Require $\frac{d \cdot m}{n}$ pieces to recover state

- Entanglement Complexity
  Prove there exist states which require $\Omega(\log n)$ circuit depth to generate.
Classical analog (Lovett & Viola '12):

Image distributions of $AC^0$ circuits and uniform distribution over a "good" classical far, are statistical distance

$$\geq 1 - n^{-\Omega(1)}$$

apart.

Quantum: Every code state $Enc(\cdot)$ requires depth at least $\Omega(\log d)$ to generate.

Key diff: Classically, we can talk about unbounded
fan-in circuits ($AC^0$). Quantumly, fan-in = fan-out by reversibility.

Classical intuition: Noise sensitivity.

For $AC^0$ circuit $F : \{0,1\}^n \rightarrow \{0,1\}$

$$\Pr_{x,e \sim \text{noise}} \left[ F(x) \neq F(x+e) \right] \leq O(p \log n).$$

Whereas, encoding maps of codes are very noise sensitive as $F(x)$ and $F(x+e)$ differ in $\geq d$ bits.
Quantum intuition/proof:
If any encoded state $\text{Enc}(1a>)$ has depth $t$, then we can distinguish $\text{Enc}(1a>)$ and $\text{Enc}(1b>)$ in depth $t+1$ for $1a> \perp 1b>$.

Pr. Run circuit in reverse.

$$\text{Enc}^{-1} \cdot \text{Enc}(1a>)$$

$$= |0,0,\ldots,0> \perp \text{Enc}^{-1} \cdot \text{Enc}(1b>)$$

Some qubit can be measured to distinguish. $\Box$
Suffices to show that encoded state cannot be distinguished by $2(\log d)$ depth circuits.

This follows from local indistinguishability of $d$ qubit regions as depth $t$ distinguishing circuits imply $2^t$-sized distinguishing measurements.
Understanding the complexity of approximations of codes:

- Prev statements were about exact codewords.
- Do not assume any structure other than rate ≥ 1 and distance d.
  (Don't have to be CSS, Stabilizer, etc., or have low-weight checks.)
- Assuming more parameters and structure of the code can be used to prove robust complexity lower bounds.
NLTS Theorem (Anshu, Breuckmann, Nicklhe, ’22)
For “good” codes, all states of energy \( \leq \epsilon n \) w.r.t. code must require \( \Omega(\log n) \) circuit depth to generate.

This result is a necessary consequence of QPCP conjecture + QMA \( \neq \) NP.

More on this (probably) during future workshops.
A fruity perspective on CSS codes

All the prev. q. talks in this series have assumed CSS codes

CSS codes are described by two classical codes \((C_X, C_Z)\)

At first glance, you might think that the picture is two custard apples
But the more accurate picture is two blackberries

$C_X \{0,1\}^n$

droplet

each droplet contains 20-50 seeds
But the more accurate picture is two blackberries

\( C_x \) \( \{0,1\}^n \)

Each druplet is related by adding \( C^1_x \)

Since \( H_x H^1_x = 0 \) for CSS.

each druplet contains 20-50 seeds
But there is even more structure.

Measuring a codestate in $X$-basis will necessarily give you an outcome that is a codeword of $C_x$.

Same follows for $C_z$.

Second, logical bit measurements are separating hyperplanes between the droplets of $C_x$.

each droplet is related by adding $C_z^\perp$
Uncertainty principle of Q.M. applied to CSS codes

Consider the logical bit flip $\bar{X}$ and phase flip $\bar{Z}$ of the first qubit.

\[ \text{Fact: } \text{Var} \bar{X} \text{ measurement + Var} \bar{Z} \text{ measurement is at least 1.} \]

\[ 0/1 \text{ R.V.s} \]

Corollary: Measuring a code state generates some uncertainty in one of the two basis measurements.

Cor: Can be used to prove robust state complexity (NLTS).
Quantum locally testable codes and why they still elude construction

First, we have to define a “syndrome” for quantum error correction. Consider a basis for the set of correctable errors.
If we are encoding $k$ qubits into $n$ qubits, there is a basis of size $2^{n-k}$. Label the different errors by bit strings of length $\geq n-k =: m$. The label is the syndrome.
The weight of check $i$ is the min size of distinguishable observable $M_i$ between

\[
\begin{align*}
\{ \chi_1 \chi_2 \ldots 0 \chi_{i+1} \ldots \chi_m \} \\
\{ \chi_1 \chi_2 \ldots 1 \chi_{i+1} \ldots \chi_m \}
\end{align*}
\]

Such an observable necessarily exists by orthogonality.

Some "syndrome labelings" are better than others!
A QLTC code is \( \rho \)-quantum locally testable if for all codewords \( |\psi\rangle \) and errors \( E \) of size \( \geq 8m \), then

\[
\forall E \quad \Pr_{i=1\ldots m} \left[ \text{observable } M_i \text{ detects } E|\psi\rangle \right] \geq \rho \delta.
\]

\( \rho = \frac{R(1)}{2} \) would be optimal.
Best known:

1. Leverrier, Londe, Zémor ’19:
   - soundness $\frac{1}{\log n}$, check weight $O(\log n)$,
   - distance $\Theta(\sqrt{n})$.

2. Gross, He, Natrajjan, Szegedy, Zhu ’23:
   - soundness $\Omega(1)$, check weight $O(1)$,
   - distance $O(1)$. 
OR soundness \( \Omega(1) \), check weight \( O(\log n) \), distance \( O(\log n) \).

Intuition for why \( \varphi \)LTCs are hard to find:

Classically, \underline{expansion} is crucial for constructing LTCs. Examples: Expander repetition code or Hadamard code.
Quantum, expansion places a limit on the gLTC soundness.

Roughly, e-optimal small set expansion of checks implies $O(e)$ soundness. (Aharonov-Eldar '13) Implies a "goldilocks" regime of expansion in order to build gLTCs of constant soundness.
Check vs qubit adjacency graph

Check weight \(W\). Qubits participate in \(D\) checks.
$\epsilon$-small set expander if for all sets $S$ of \leq \omega$ qubits,

$$|\Omega(S)| \geq |S| \cdot \Delta \cdot (1 - \epsilon)$$

\begin{itemize}
  \item number of checks
  \item optimal
  \item near-optimal
  \item using qubits from $S$
\end{itemize}

Fact: if $\epsilon < \frac{1}{2}$, then for any $S$,

$$1 - 2\epsilon$$ of checks in $\Omega(S)$ have a unique
preimage in \( S \).

Note that the checks \( M_i \) must commute* since we can apply them in any order to get syndrome.

* technically, only need to commute on codespace.

Unique preimage due to small-set expander lets us conclude that most checks only share 1 qubit.
... (skip steps)...

Construct a large error that violates few checks.

Morally why? Since checks commute,

if \exists a qubit q s.t. all checks \ i \ using q only intersect at q, then

\exists a code state which is unentangled at qubit q.

Pf by rep. thy (Bravyi-Vyalyi)
violate the local indistinguishability of 1-qubit reduced density matrices.

Key idea: Show that if one couldn't create a large error that violates few checks, then such a "lonely" qubit must exist.

A world with qLTCs.
Clasically, LTCs were pivotal in the construction of PCPs.

Is the quantum analog also true?

Not so clear...

In some sense, PCP theorem is a elegant wrapping of a NP witness in a locally-decodable LTC.
Ex. Exponentially long PCP via Hadamard code

Issue: Quantum codes can't have good distance and be locally decodable.

⇒ Immediate construction of exponentially long qPCP doesn't follow from qLTC.

Problem is wide open!
More to come in workshop on quantum complexity: Mar 18 - 22\textsuperscript{nd}.

The End. Questions?