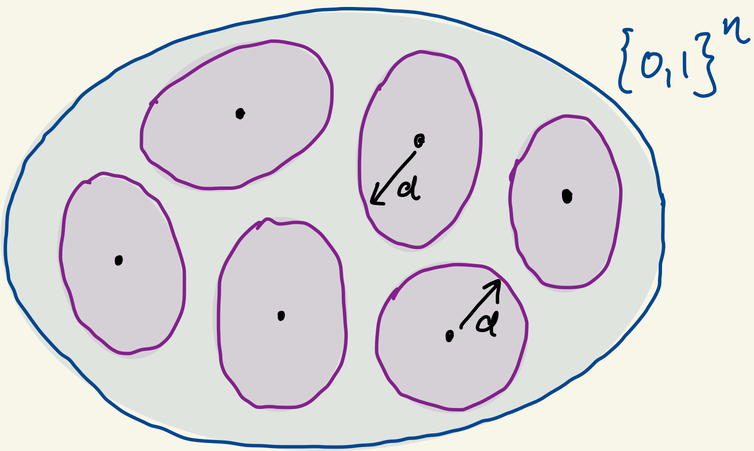
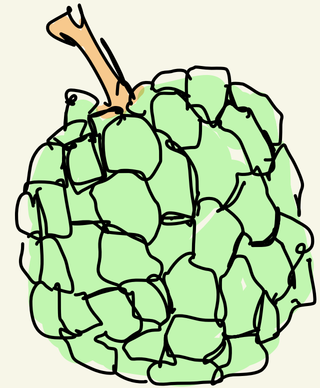
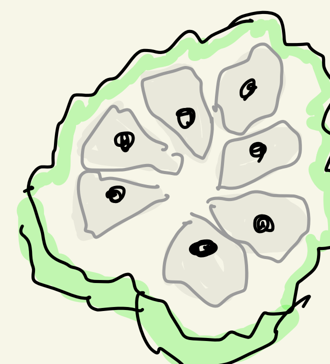
Quantum Codes In Quantum Complexity

Chinmay Nirkhe
IBM

Classical codes have a cartoon that looks like a custard apple



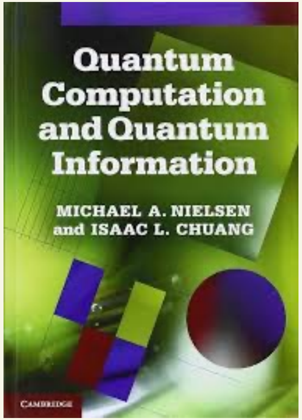




What fruit/object naturally captures the picture of quantum error-correction?

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

Nielsen & Chuang



And this is what I found:

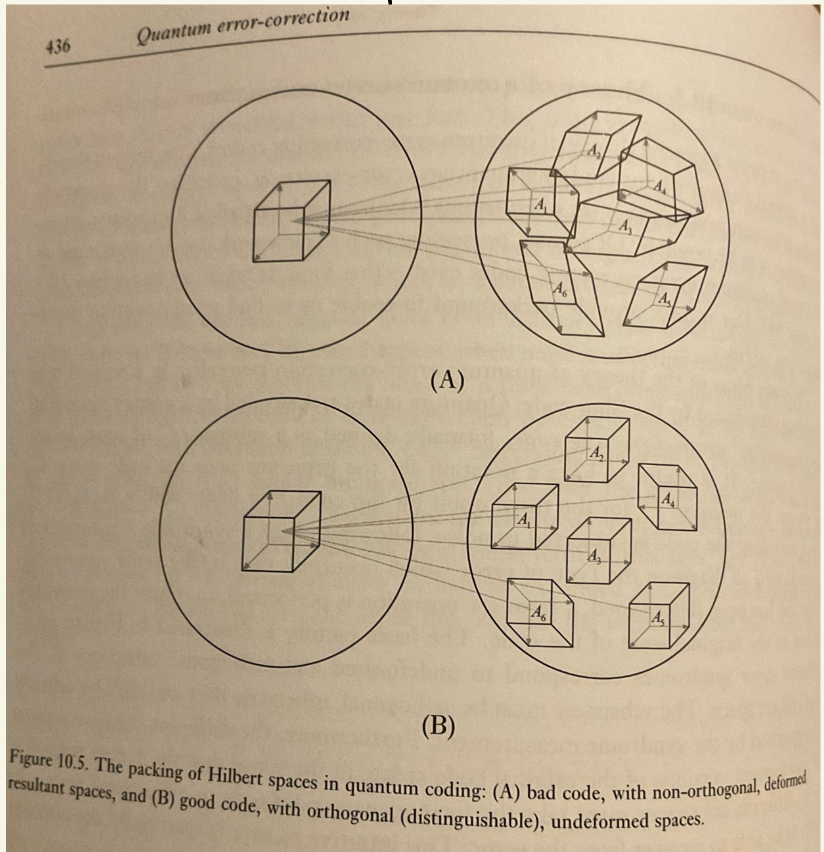


Figure 10.5. The packing of Hilbert spaces in quantum coding: (A) bad code, with non-orthogonal, deformed resultant spaces, and (B) good code, with orthogonal (distinguishable), undeformed spaces.

Outline

An information-theoretic perspective on coding

explain the Nielsen & Chuang diagram

The Knill-Laflamme conditions

The complexity of codestates (quantum)

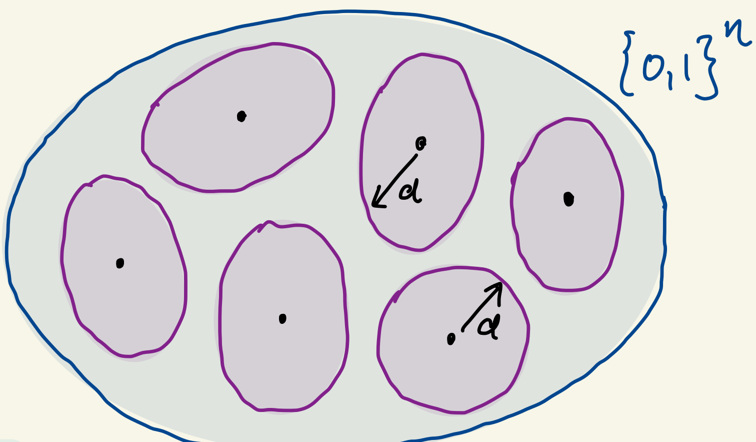
dists. over codewords (classical)

The challenge of constructing qLTCs

An information-theoretic perspective on coding

Classical codes:

2^k disjoint Hamming balls of radius d on n-bool. cube.



No assumption about structure of balls

↳ not necessarily efficiently decodable

Encoding map = bijection from k-bit strings to centers of the balls.

An error e s.t. $|e| \leq d$ on $\mathrm{enc}(\cdot)$ 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!

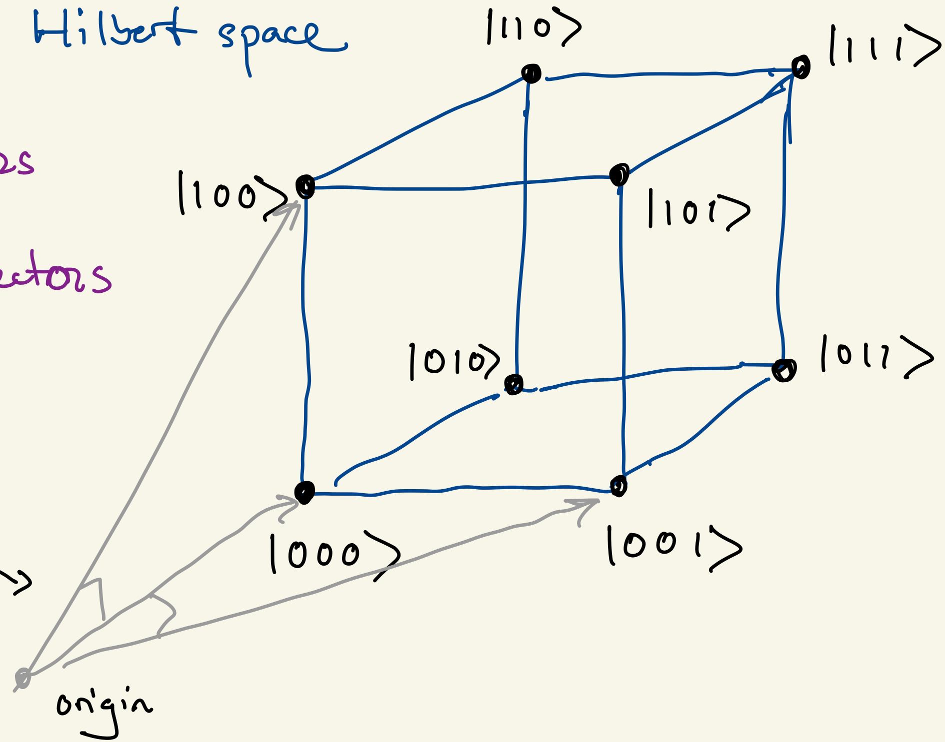
How do we draw such a cartoon explaining quantum error-correction if there are an infinite set of errors?

But first, how to read my drawings of high-dimensional spaces

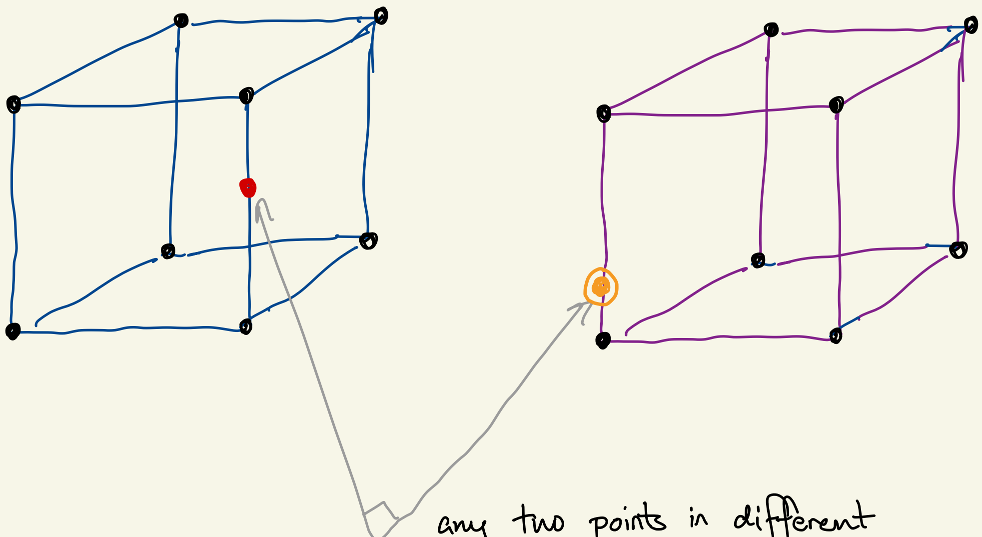
3 - qubit = 2^3 dim Hilbert space

In my drawings, corners represent orthogonal vectors

denoting that both 90° angles



Direct sum of Hilbert spaces

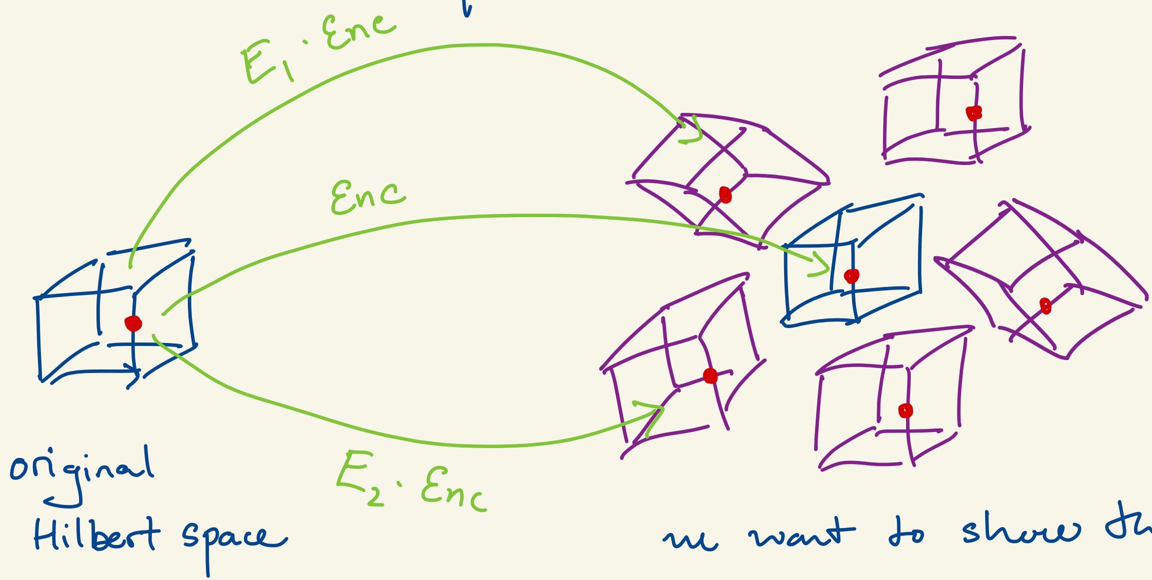


any two points in different shapes are orthogonal.

Ok, now to correcting errors

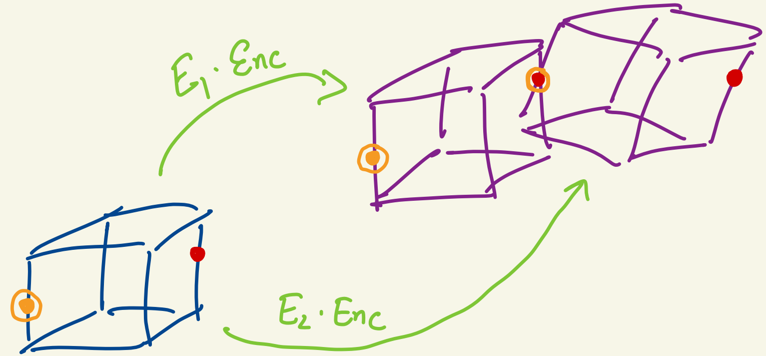
The packing of Hilbert spaces perspective

goal: correct against unitary errors $E_1, E_2, \ldots, E_J$ (for now)



we want to show that $\exists$ orthogonal spaces per error.

Simple example of a non-code

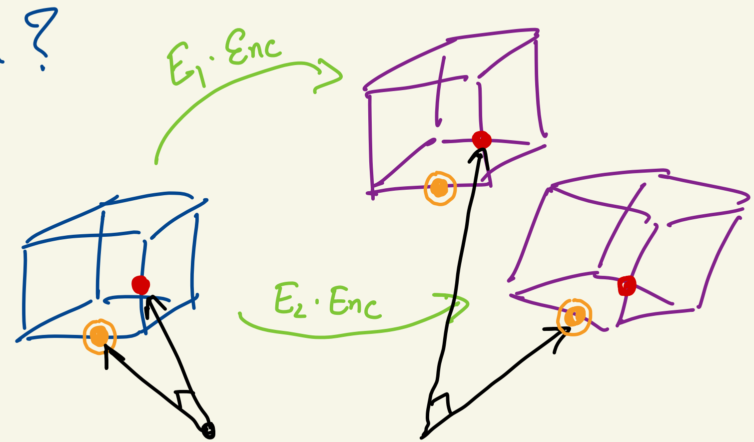


i.e. $E_1 \cdot Enc(|\bullet\rangle) = E_2 \cdot Enc(|\odot\rangle)$

$\Rightarrow$ cannot distinguish these errors.

Actually, stronger statement: If $|\bullet\rangle \perp |\odot\rangle$, then these states should be orthogonal.

Why orthogonal?



Fact: 2 states $|a\rangle$ and $|b\rangle$ are perfectly distinguishable

iff $|a\rangle \perp |b\rangle$ (orthogonal vectors)

Notice: only correcting E_1 & E_2 if we can distinguish

$E_1 \cdot \mathrm{Enc}(|\bullet\rangle)$ and $E_2 \cdot \mathrm{Enc}(|\odot\rangle)$

$\Rightarrow$ These vectors are orthogonal.

It would be too much to ask that

$$E_1 \cdot \mathrm{Enc}(|\bullet\rangle) \quad \text{and} \quad E_2 \cdot \mathrm{Enc}(|\bullet\rangle)$$

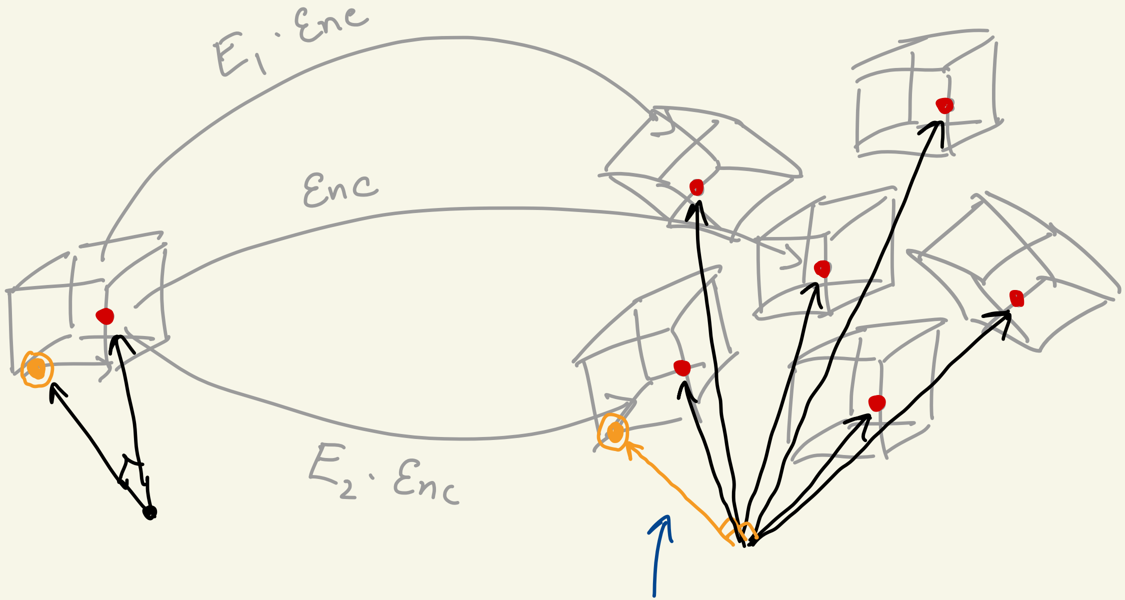
<u>Pf</u>: consider $E_1 \approx_\epsilon E_2$.

By linearity, these states must be close. $\square$

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:



$E_2 \cdot Enc(|\odot\rangle)$ is orthogonal to every

$E_j \cdot Enc(|\bullet\rangle)$

If $|\bullet\rangle \perp |\odot\rangle$, then

$$\Rightarrow \operatorname{span}_{j_1}\left\{ E_{j_1} \cdot \mathrm{Enc}(|\bullet\rangle) \right\} \perp \operatorname{span}_{j_2}\left\{ E_{j_2} \cdot \mathrm{Enc}(|\odot\rangle) \right\}$$

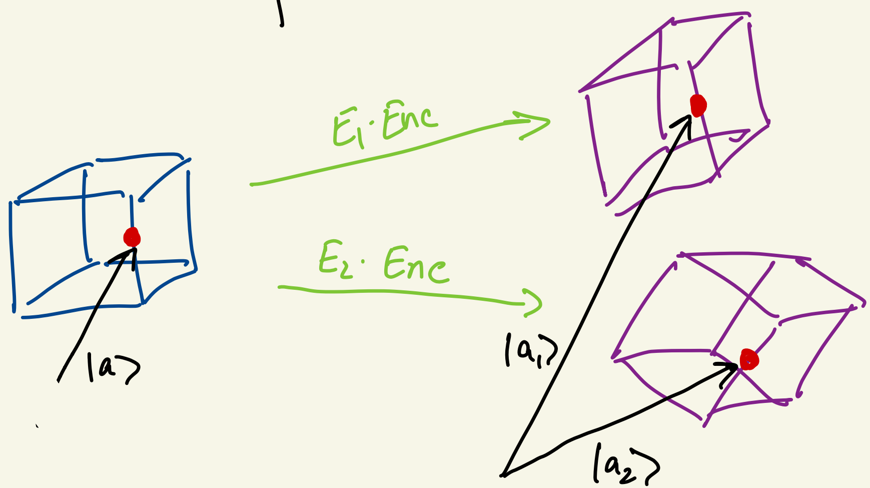
$\Rightarrow$ correcting against errors $E_1, \dots, E_J$ implies correcting against unitary errors in their span.

$\therefore$ 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 $E \in \mathcal{E}$, consider a basis s.t.

$$\operatorname*{span}_{E \in \mathcal{E}} \left\{ E \cdot \mathrm{Enc}|a\rangle \right\} = \operatorname*{span}_{E_1, \dots, E_J} \left\{ E_i \, \mathrm{Enc}|a\rangle \right\}.$$

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

$$\operatorname*{span}_{E \in \mathcal{E}} \left\{ E \cdot \mathrm{Enc}|b\rangle \right\} = \operatorname*{span}_{E_1, \dots, E_J} \left\{ E_i \, \mathrm{Enc}|b\rangle \right\}.$$

$\Rightarrow$ gives natural notion of a basis $E_1 \dots E_J$ for $\mathcal{E}$.

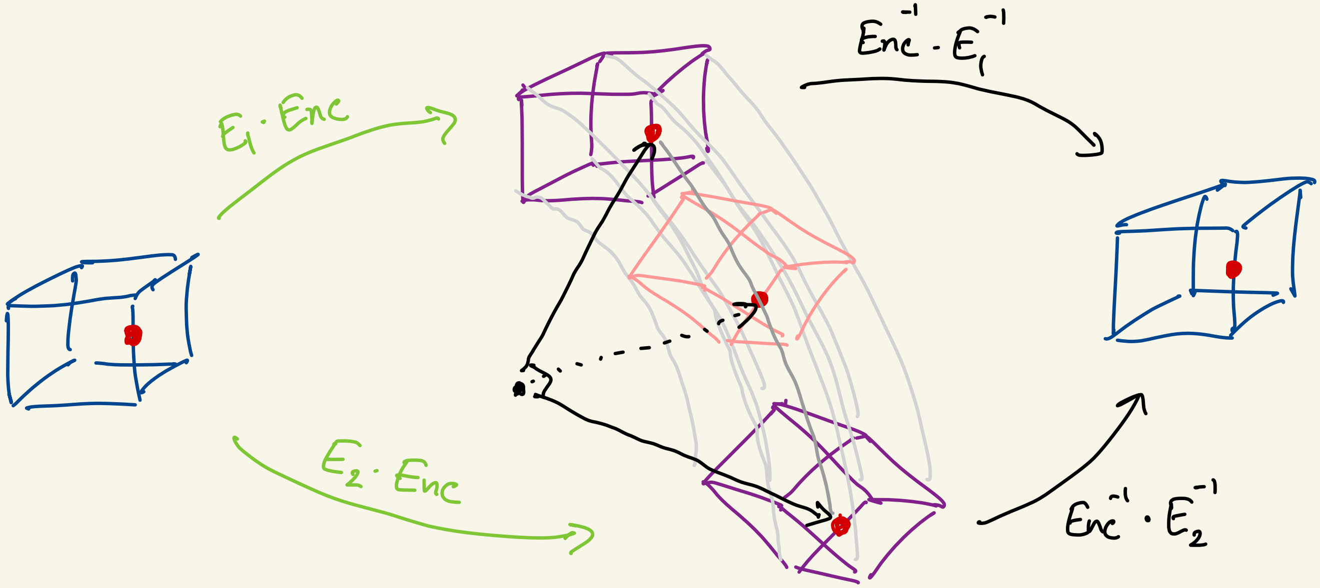
Equiv., can define an inner product on correctable errors

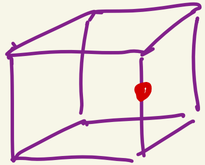
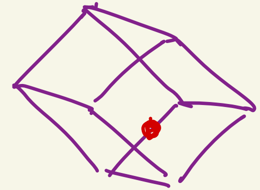
$$\langle E_i, E_j \rangle \overset{\text{def}}{=} \eta_{ij}$$

$$\overset{\text{def}}{=} \langle a | Enc^\dagger E_i^\dagger E_j \, Enc | a \rangle \quad \text{for any } |a\rangle.$$

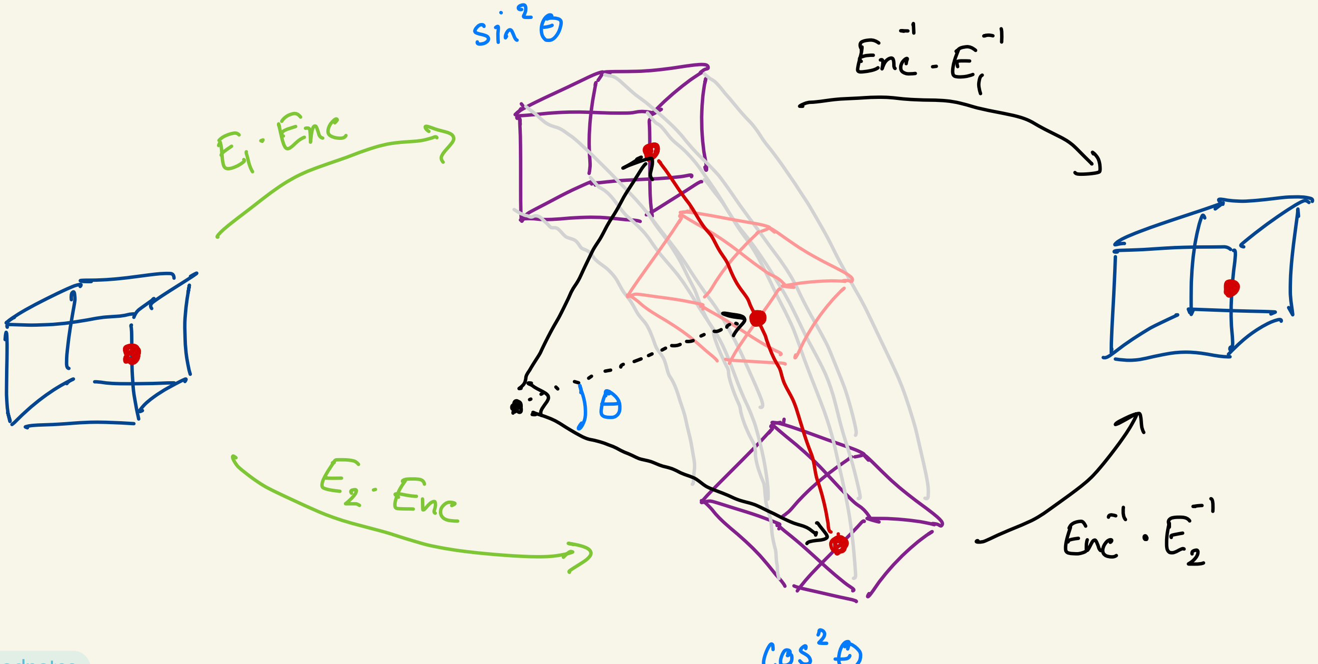
The basis we found is a basis with respect to this inner product.

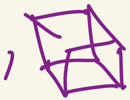
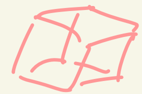
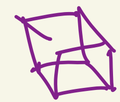
Ok, but does the decoding channel/algorithm look like for the set of continuous errors?



Note that  and  are orthogonal

(assumption that they are a basis for errors)



$\exists$ a measurement perfectly distinguishing the ,  errors. If we measure  error using this, it collapses to either  or . Plus, we know which one!

$\sin^2\theta$ $\cos^2\theta$

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.

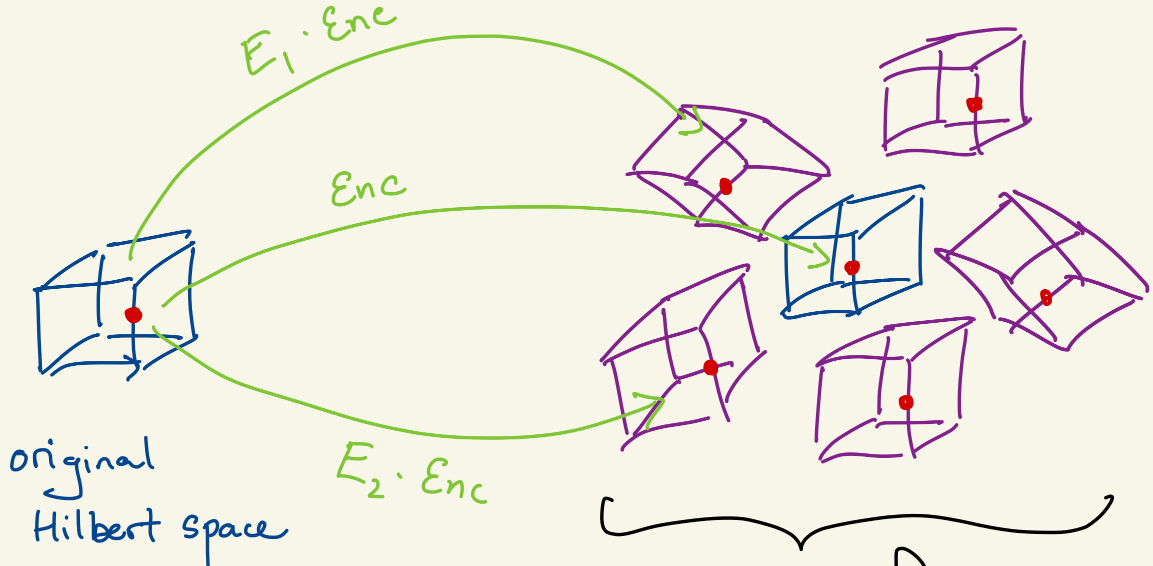
syndrome = name of basis error.

② correct error based on syndrome.

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

"destructive" "information preserving"

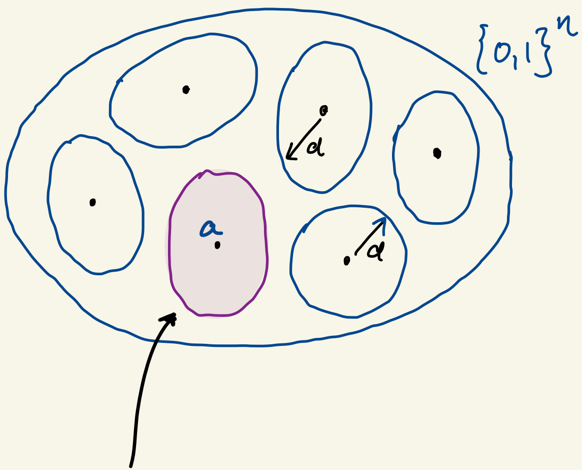
error-correction is a controlled destructive process.



Decomposition of space into direct sum from error basis.

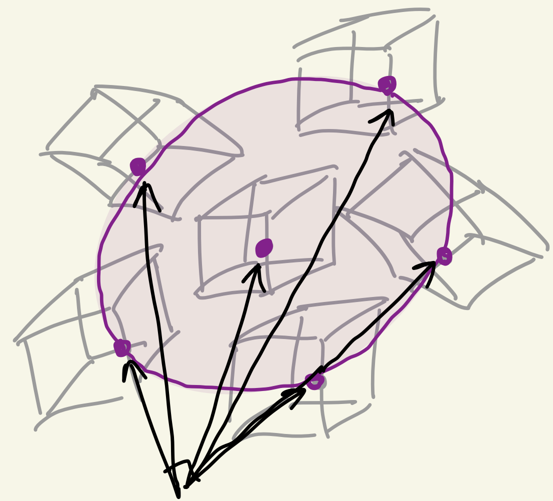
Can also correct error channels whose elements $\in \mathcal{E}$.

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 = image of encoding map.

Let Π be the projector onto subspace C.

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

$$\boxed{\Pi E_i^\dagger E_j \Pi = \eta_{ij} \Pi}$$

coefficients s.t. $\eta_{ij} = \eta_{ji}^\dagger$.

(the inner product between the error spaces)

Not hard to show this is equivalent to $\forall\ |a\rangle, |b\rangle, i, j,$

$$\langle a | \mathrm{Enc}^\dagger E_i^\dagger E_j \,\mathrm{Enc} | b \rangle = \langle a | b \rangle \cdot \underbrace{\langle E_i, E_j \rangle}_{\eta_{ij} \text{ prev. defined.}}$$

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 $\underbrace{E'}_{d} \otimes \underbrace{\mathbb{1}}_{n-d \text{ qubits}}$

Correcting all errors of size d equiv. to

Correcting all Pauli (X-, Y-, Z-type) errors of size d.

equiv to. correcting all erasure errors of size d.

Information destroying channel.

Apply a uniformly random Pauli. $\mathcal{E}(\cdot) = \frac{1}{4^d} \sum_P \underbrace{P(\cdot)P^\dagger}_{\text{contained in span of Paulis.}}$

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

$$\boxed{\text{Correcting } d \text{ sized errors} \iff \text{correcting } d \text{ qubit erasures}}$$

Thm. 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 $|\psi_1\rangle = Enc(|x_1\rangle)$ and $|\psi_2\rangle = Enc(|x_2\rangle)$ 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,
$$\langle \psi_i | E | \psi_i \rangle = \langle \psi_i | \Pi E \Pi | \psi_i \rangle$$

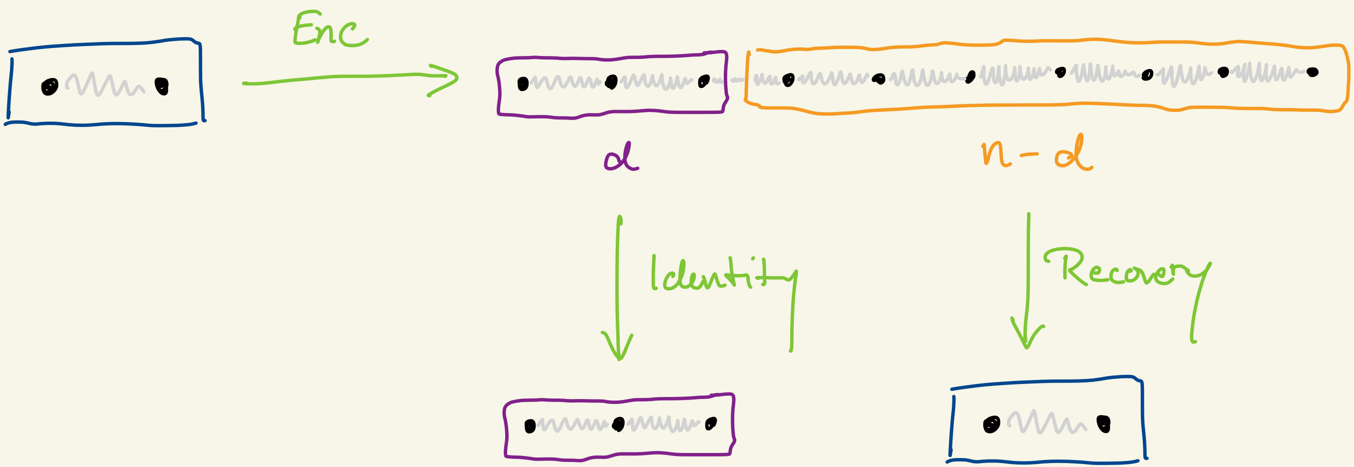
Knill-Laflamme condition

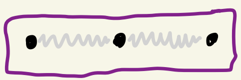
$$= \langle \psi_i | \eta_E \Pi | \psi_i \rangle$$

$$= \eta_E .$$

<u>Pf (v2)</u> If reduced density matrices for d-sized region varied dependent on encoded state,

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.

$$\boxed{\text{"local indistinguishability"}}$$

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.

$$x \in \{0,1\}^k \longmapsto \{ b \cdot x \in \{0,1\} \}_{b \in \{0,1\}^k}$$

$$a \cdot x = (b \cdot x) + ((a+b) \cdot x) \qquad \forall\, b.$$

- 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 statisical 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 reversability.

Classical intuition: Noise sensitivity.

For AC^0 circuit $F : \{0,1\}^{kn} \longrightarrow \{0,1\}$

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

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 <u>any</u> encoded state $\mathrm{Enc}(|a\rangle)$ has depth t, then we can distinguish $\mathrm{Enc}(|a\rangle)$ and $\mathrm{Enc}(|b\rangle)$ in depth $t+1$ for $|a\rangle \perp |b\rangle$.

Pf. Run circuit in reverse.

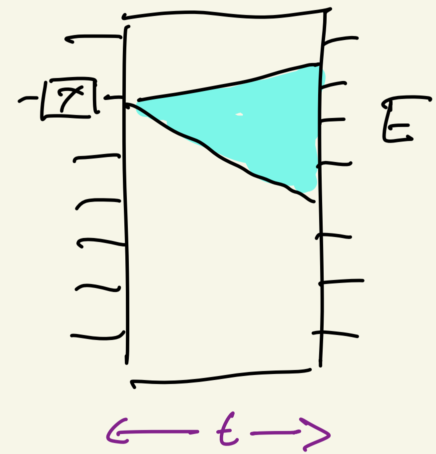
$$\mathrm{Enc}^{-1} \cdot \mathrm{Enc}(|a\rangle)$$

$$= |0,0,\dots,0\rangle \quad \perp \quad \mathrm{Enc}^{-1} \cdot \mathrm{Enc}(|b\rangle)$$

Some qubit can be measured to distinguish. $\square$

Suffices to show that encoded state cannot be distinguished by $\Omega(\log d)$ 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 codestates

- Prev statements were about exact codewords
- Do not assume any structure other that 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, Nirkhe '22)

For "good" codes, all states of energy $\leq \epsilon_0 n$ 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.

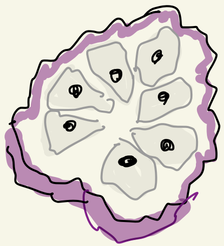
A fruity perspective on CSS codes

Calderbank, Shor, Steane

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

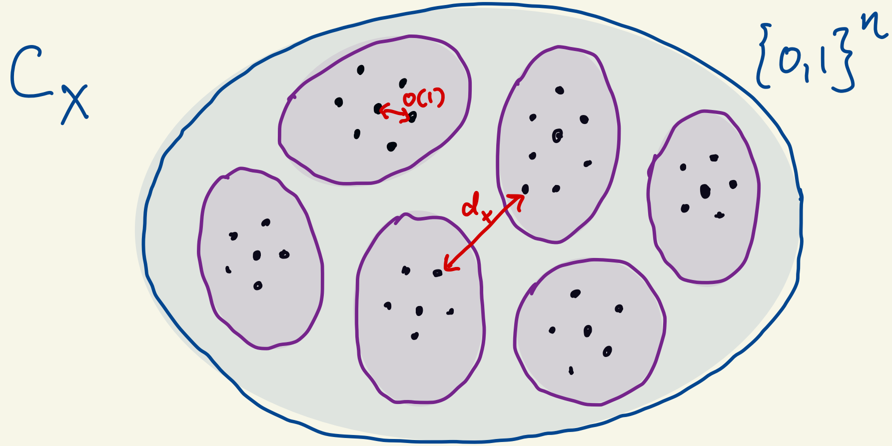


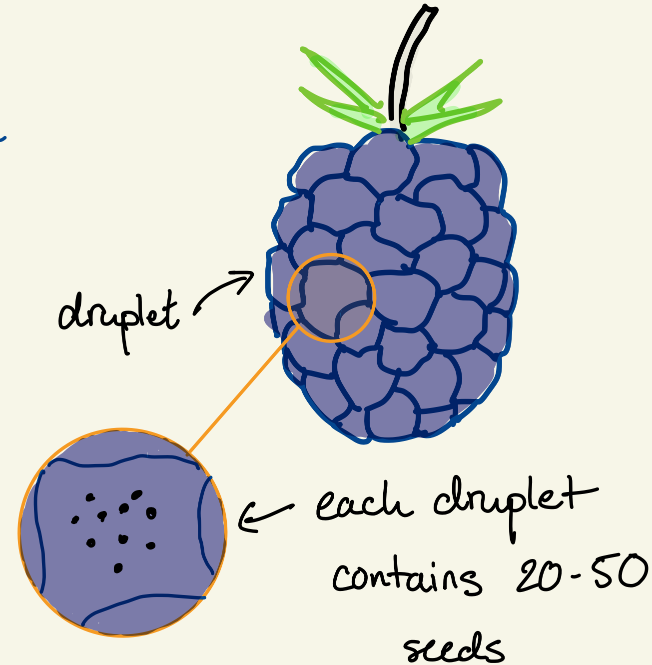
C_X

and

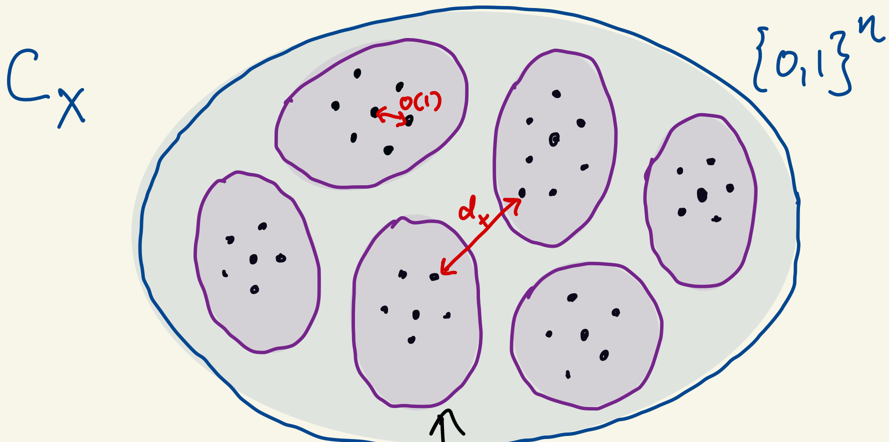
C_Z

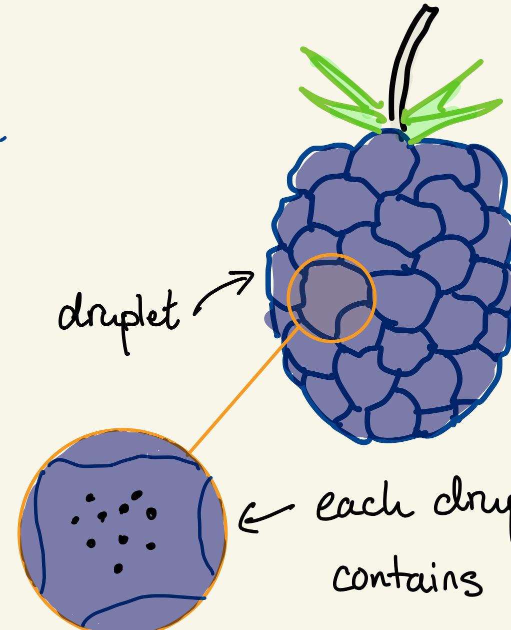
But the more accurate picture is two blackberries





But the more accurate picture is two blackberries





each droplet contains 20-50 seeds

each droplet is related by adding $C_Z^{\perp}$

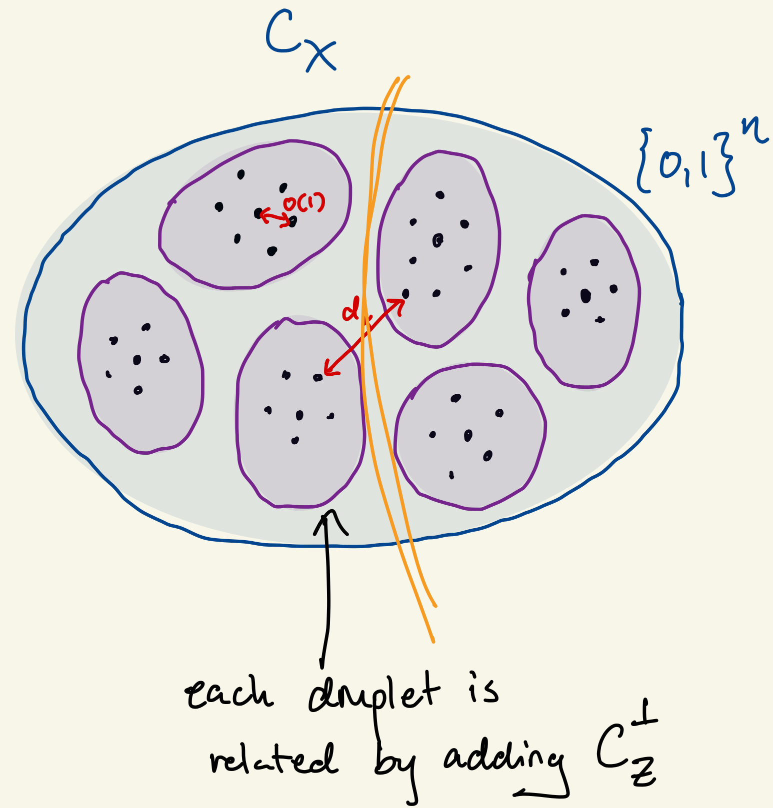
since $H_X H_Z^{\perp} = 0$ for CSS.

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.

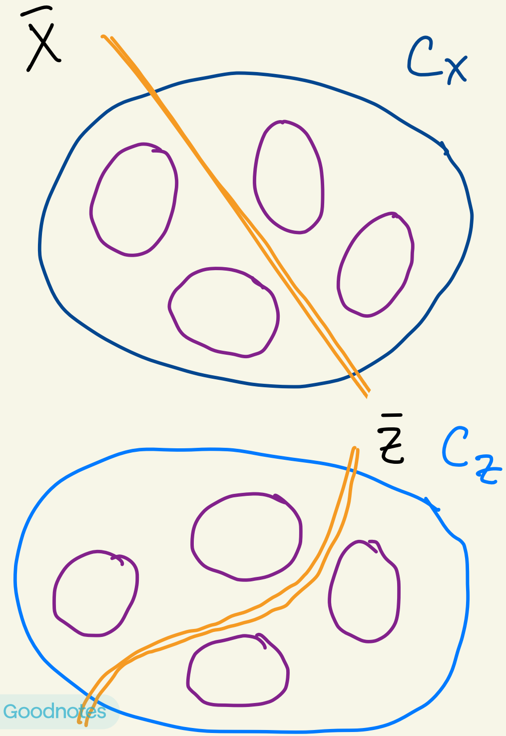
Same follows for C_Z.

Second, logical bit measurements are seperating hyperplanes between the droplets of C_X.



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



__Fact__ Var $\bar{X}$ measurement + Var $\bar{Z}$ measurement

is at least 1.

0/1 R.V.s

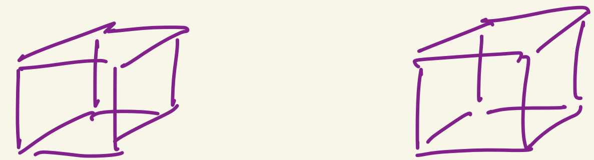
__Corollary__ Measuring a code state generates some uncertainty in one of the two basis measurements.

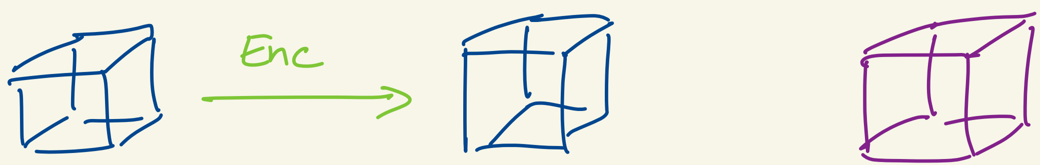
__Cor__ Can be used to prove __robust__ state complexity (NLTS).

Quantum locally testable codes and why they still elude construction

First, we have to define a "syndrome" for quantum error correction.

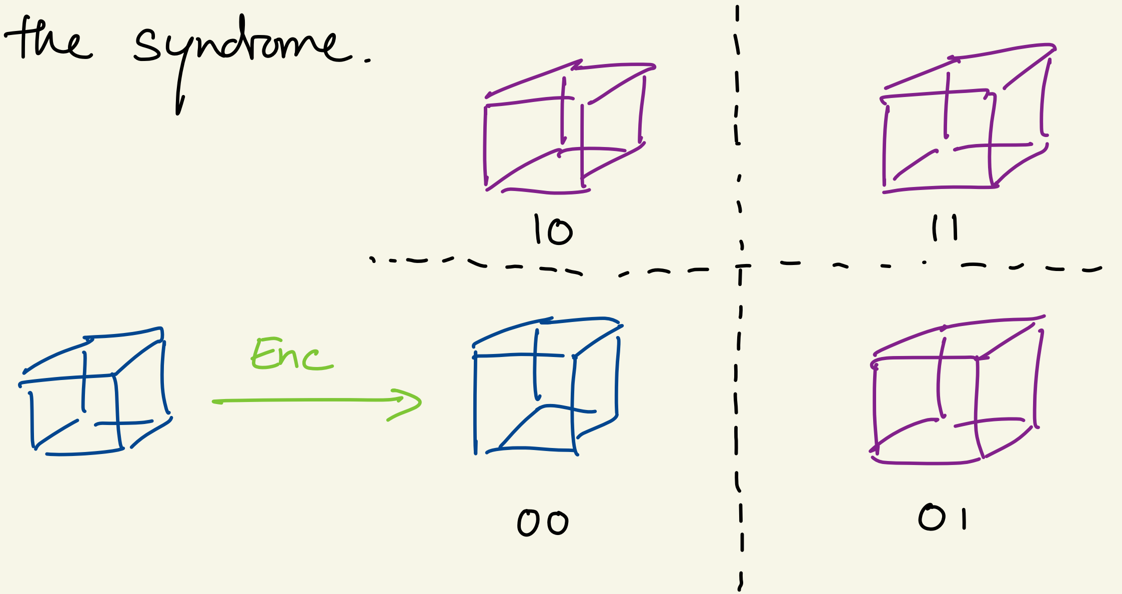
Consider a basis for the set of correctable errors.



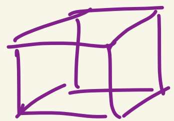
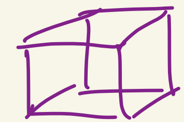


If we are encoding k qubits into n qubits, there is a basis of size 2^{n-k}. Label the different errors by bit strings of length $\geq n-k =: m$.

The label is the syndrome.



The weight of check i is the min size of distinguishable observable M_i between

$\{$  $x_1 x_2 \ldots 0\, x_{i+1} \ldots x_m \}$ and $\{$  $x_1 x_2 \ldots 1\, x_{i+1} \ldots x_m \}$

Such an observable necessarily exists by orthogonality.

Some "syndrome labelings" are better than others!

qLTC def: Code is ρ - quantum locally testable if for all codewords $|\psi\rangle$ and errors E of size $\geq \delta n$, then

$$\mathop{\mathbb{E}}_{i=1\ldots m} \Pr\left[\text{observable } M_i \text{ detects } E|\psi\rangle\right] \geq \rho\,\delta.$$

$\rho = \Omega(1)$ would be optimal.

Made with Goodnotes

Best known:

① Leverrier, Londe, Zémor '19:

soundness $\frac{1}{\log n}$, check weight $O(\log n)$,

distance $\Theta(\sqrt{n})$.

② Cross, He, Natarajan, Szegedy, Zhu '23:

soundness $\Omega(1)$, check weight $O(1)$,

distance $O(1)$.

<u>OR</u> soundness $\Omega(1)$, check weight $O(\log n)$,

distance $O(\log n)$.

Intuition for <u>why</u> qLTCs are hard to find:

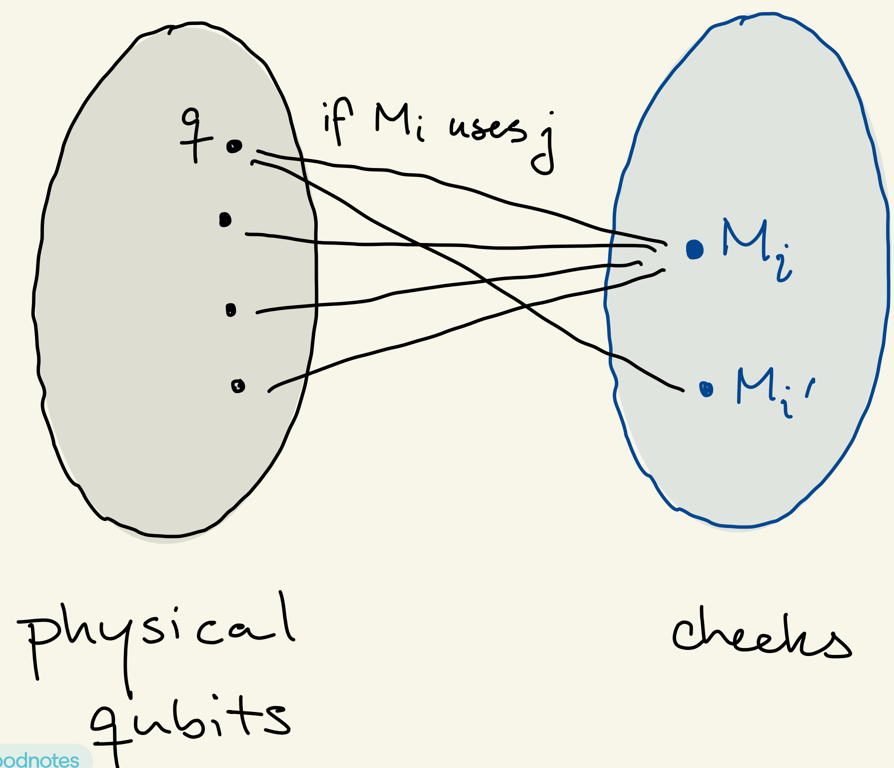
<u>Classically</u>, <u>expansion</u> is crucial for <u>constructing</u> LTCs. Examples: Expander repitition code or Hadamard code.

Quantum expansion places a limit on the qLTC soundness.

Roughly, ϵ-optimal small set expansion of checks implies $O(\epsilon)$ soundness. (Aharonov-Eldar '13)

Implies a "goldilocks" regime of expansion in order to build qLTCs of constant soundness.

Check vs qubit adjacency graph



Check weight w.

qubits participate in D checks.

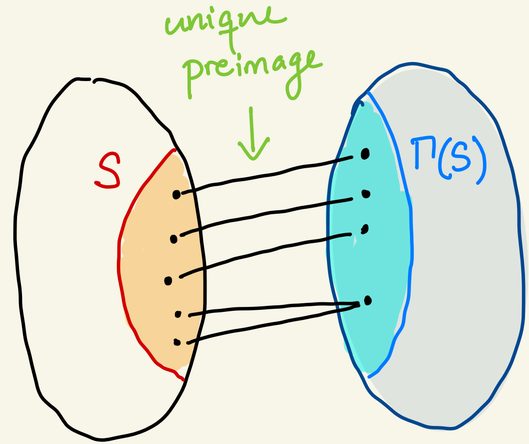
ϵ - small set expander if for all sets S of $\leq w$ qubits,

$$\underbrace{|\Gamma(S)|}_{\text{number of checks using qubits from } S} \geq \underbrace{|S| \cdot D}_{\text{optimal}} \cdot \underbrace{(1-\epsilon)}_{\text{near-optimal}}$$

<u>Fact</u> If $\epsilon < \frac{1}{2}$, then for any S,

$1 - 2\epsilon$ of checks in $\Gamma(S)$ have a <u>unique</u>

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.

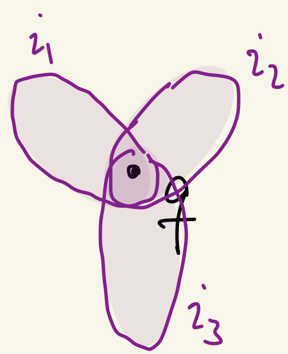
Unique preimage due to small-set expander lets us conclude that most checks only share 1 qubit.

. . . (skip steps) . . .

Construct a large error that violates few checks.

<u>Morally</u> <u>why</u>?? Since checks commute*,

if $\exists$ a qubit q s.t. all checks i <u>using</u> q <u>only</u> intersect at q, then $\exists$ a codestate which is unentangled at qubit q. ← Pf by rep. thy (Bravyi-Vyali)



$\Rightarrow$ violate the local indistinguishability of 1-qubit reduced density matrices.

Key idea: Show that if we 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.

$\Rightarrow$ 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 - 22nd.

The End. Questions?