QUANTUM ERROR CORRECTION & FAULT TOLERANCE

0- motivation : NISQ is not enough
Noisy intermediate-scale Q computers

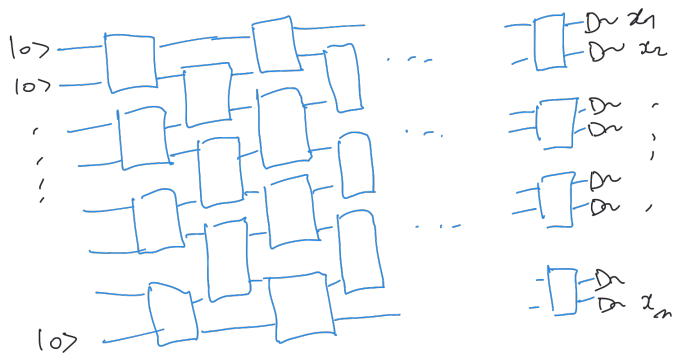
1- Fault tolerance : classical case & main ideas

2- Q error correcting codes : stabilizer codes

resources

- Daniel Gottesman arxiv : 0904.2557
- John Preskill : lecture notes (caltech)
- Dan Browne : Topological codes & computation (UCL)

Motivation



C

in reality

- q-bits are noisy
- gates ——
- measurements ——

} gates : fidelity 99.9% → error rate $p = 0.001$

⇒ largest computation : $O(1/p)$ gates at max

useful algo
- Shor
- q chemistry

} need $10^{12} - 10^{15}$ gates

→ hardware improvement won't be enough

→ turn to software

① Fault tolerance :

replace the ideal circuit C

by a larger circuit C' with noisy gates

s.t. C & C' give the same result

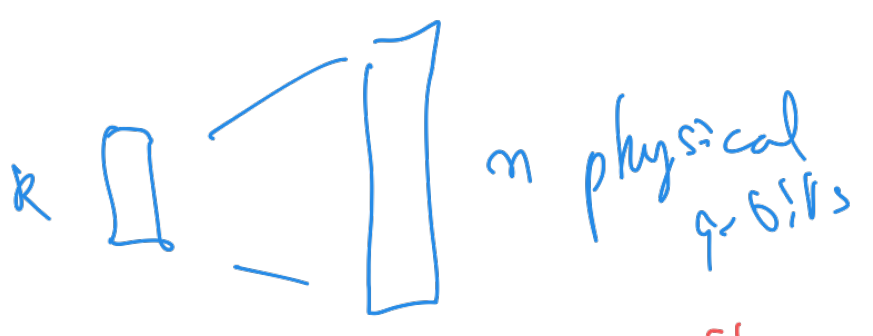
↳ Aharonov - Ben-Or 97 / Shor 96

② Quantum error correcting codes

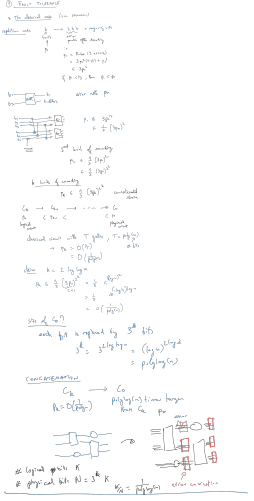
k ideal / logical q-bits are encoded

into n physical / noisy q-bits

$n > k$



Shor 95



The Q case

* no repetition code : $|\psi\rangle \not\to |\psi\rangle|\psi\rangle|\psi\rangle$ (No cloning)

* errors in the classical case : bit flips
  continuum of errors : arbitrarily "small" errors
  $p \mapsto \mathcal{N}(p)$ a channel $\mathcal{N}$
  $\mathcal{N}(\rho) = \sum_k E_k \rho E_k^\dagger$ Kraus operators
  s.t. $\sum_k E_k^\dagger E_k = \mathbb{1}$

* measuring a state perturbs it.

Solutions

- no need to copy the state $\{0,1\} \to \{0,1\}^3$, $0 \mapsto 000$, $1 \mapsto 111$

$C^n \otimes |\psi\rangle$ — U — $|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$

- linearity of QM
  $\mathcal{N}(\rho) = \sum_k E_k \rho E_k^\dagger$ $E_k = \sum$ Pauli matrices.
  single q-bit $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \alpha \mathbb{1} + \beta \sigma_x + \gamma \sigma_z + \delta \sigma_z$ (Pauli projectors)

$\Rightarrow$ it is sufficient to correct Pauli errors.

Lemma : If a code can correct an arbitrary single-q-bit Pauli error (in fact X, Z errors)
then it will correct an arbitrary single-q-bit error.

$\sigma_Y = i \sigma_x \sigma_z$

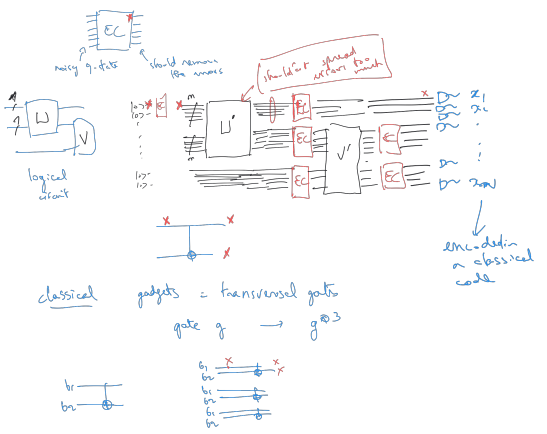
only 2 types of errors

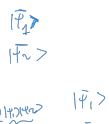
X errors : bit flip $|0\rangle \leftrightarrow |1\rangle$ } like classical

Z errors : phase-flip $|0\rangle \leftrightarrow |1\rangle$, $|1\rangle \mapsto -|1\rangle$ }

Q fault tolerance

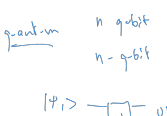
error correcting modules





classical gadgets = transversal gates

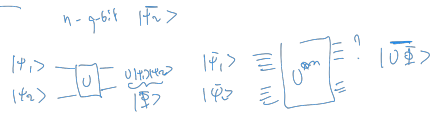
gate $g \longrightarrow g^{\otimes 3}$



quantum

n qubit $|\bar{\psi}_1\rangle$

n-qubit $|\bar{\psi}_2\rangle$

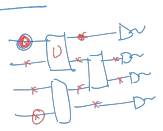


No go theorem

$\#$ QECC st you can apply gates transversally for a universal gate set.

for CSS codes, you can do all Clifford transversally

Noise model



noise can occur on all the physical locations

errors : finite or arbitrary

* correlated or uncorrelated

local stochastic error model

for any set L of l locations
$P(L \subseteq \text{error}) \leq p^l$

Threshold theorem (Aharonov, Ben-Or 97)

Provided that the error rate $p \leq p_0$ (cst),
then you can replace a logical circuit C with T gates by a phys. circuit C' with T' gates (noisy)
st C and C' return the same result

$T' = T\, O(\text{polylog}(T))$

what is the value of p_0?

$p_0 > 0.001$ (analytical proofs)
$p_0 \sim$ a few % (numerical)

unitary error

$U = e^{i\varepsilon X}$

n q-bits $U^{\otimes n} = e^{i\varepsilon(X_1 + X_2 + \dots X_n)}$

$\simeq \underbrace{\mathbb{1}}_{\text{0 error}} + \underbrace{i\varepsilon(X_1 + \dots X_n)}_{\text{1 error}} - \underbrace{\varepsilon^2(X_1 X_2 + \dots)}_{\text{2 errors}}$

$+ \underbrace{\varepsilon^t(X_1 X_2 \dots X_t + \dots)}_{\text{t errors}}$

Shor 3-qubit $S = \langle Z_1Z_2, Z_2Z_3 \rangle$

Shor 9-qubit $S = \langle Z_1Z_2, Z_2Z_3, Z_4Z_5, Z_5Z_6, Z_7Z_8, Z_8Z_9, X_1X_2X_3X_4X_5X_6, X_4X_5X_6X_7X_8X_9 \rangle$

---

quantum LDPC codes
↳ low-density parity-check matrix

- classical LDPC code : $C = \ker H$ st H is sparse
- q LDPC code : - $|g_i| = O(1)$
  $g_i = Z_1 \mathbb{1}_2 \mathbb{1}_3 X_4 I \cdots$
  - each q-bit is acted upon nontrivially by $O(1)$ generators.

⇒ LDPC is very important for implementations.

open questions
- what kind of distance is possible?
- can we get good distance & good rate k/n?

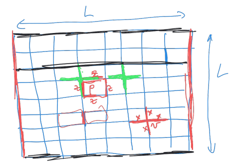
(classical case : take H sparse at random)
$C = \ker H$
→ whp $k/n = \Theta(1)$
$d/n = \Theta(1)$
+ efficient decoding algo

Q case : taking g_i's at random won't work.
because of commutation.

$g_1 = X_1 \quad X_4 \quad Z_6 \quad X_{10}$
$g_2 = \quad X_2 \quad Z_4 \quad Z_7 \quad Z_{10}$
$g_3 = Z_1 Z_2 X_3 \quad X_7 \quad Z_{10}$

CSS trick : pick g_i's in two families
$g_i^X = X_1 \; X_3 \; X_7$ (product of I and X)
$g_j^Z = Z_7 \; Z_8 \cdots$ (product of I and Z)

KITAEV : toric code 97



q-bits on the edges : $n = 2L^2$

for all plaquettes (L^2)
$g_p^Z = \bigotimes_{e \in \partial p} Z_e$

for all vertices : $g_v^X = \bigotimes_{e \ni v} X_e$

generators share 0 or 2 edges
⇒ they all commute

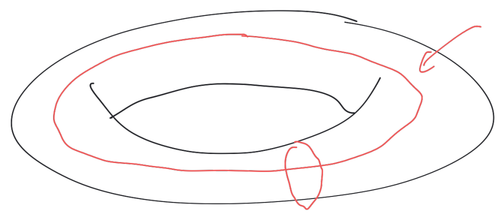
$n = 2L^2$ physical q-bits
constraints $= L^2 + L^2 = 2L^2$ generators
↳ not all independent

$\prod_p g_Z = \mathbb{1}$
$\prod_v g_v^X = \mathbb{1}$
} only $2L^2 - 2$ indep generators.

⇒ $k = 2$ 2 logical q-bits

$[\![n, k, d]\!] = [\![2L^2, 2, L]\!]$

$k = 2$
$d = O(\sqrt{n})$

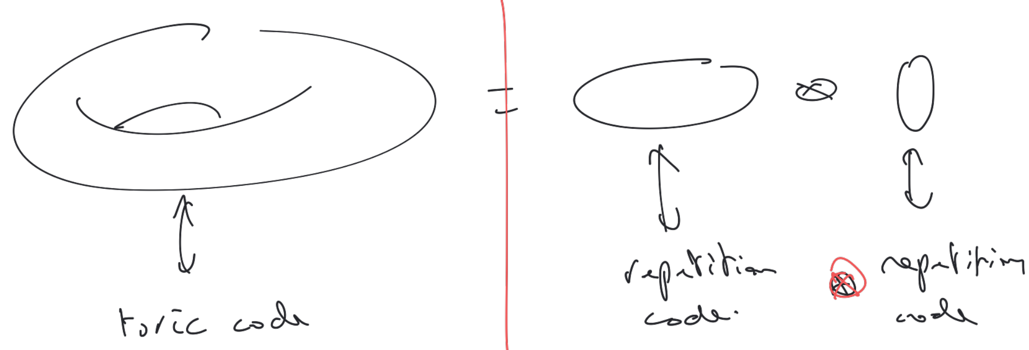

logical operators

but min distance (LDPC codes)
- before 2020 : $\sqrt{n} \log^{1/4} n$
- Hastings Haah O'Donnell $d = n^{0.6}$ → derandomization by Breuckmann
- Panteleev, Kalachev $d = \frac{n}{\log n}$

$$k d^2 = O(n^2)$$ for all known constructions.

take $k = \Theta(n) \rightarrow d = O(\sqrt{n})$

Tillich, Zémor



↳ product of 2 classical LDPC codes = hypergraph product codes.

⇒ Q LDPC code