CPEN 400Q Lecture 22
Fault-tolerant quantum computing

Monday 31 March 2025

Announcements

- Presentations for next two classes + two tutorials (attendance expected - come support your classmates!)
- Quiz 10 *tomorrow* before presentation
- Project rubric available on PrairieLearn
- Book final exam slot if you haven't already
- Please fill out student experience survey on Canvas

Last time

We introduced the idea of *stabilizer codes*.

Let S be a subgroup of $\mathcal{P}_n$,

$$\mathcal{P}_n = \{I, X, Y, Z\}^{\otimes n} \times \{1, -1, i, -i\}$$

Let V_S be a set of states that are $+1$ eigenstates for all $P \in S$.

Then, S is the **stabilizer** of V_S, and V_S is stabilized by S.

Last time

We defined error correcting codes in terms of the stabilizer generators of their logical states.

Bit flip code:

$|000\rangle$
$|111\rangle$ $\longrightarrow$ $\underbrace{ZZI \quad ZIZ \quad IZZ}_{\langle ZZI,\ IZZ \rangle}$

Phase flip code:

$|+++\rangle$
$|---\rangle$ $\longrightarrow \langle XXI,\ IXX \rangle$

Last time

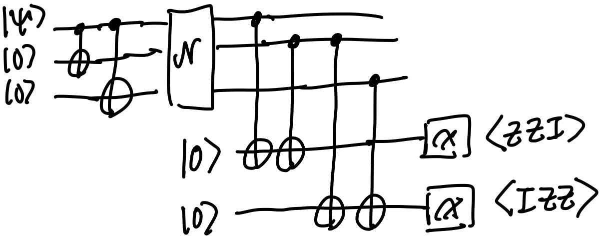
Shor code:

Name	Operator
g_1	$Z\,Z\,I\,I\,I\,I\,I\,I\,I$
g_2	$I\,Z\,Z\,I\,I\,I\,I\,I\,I$
g_3	$I\,I\,I\,Z\,Z\,I\,I\,I\,I$
g_4	$I\,I\,I\,I\,Z\,Z\,I\,I\,I$
g_5	$I\,I\,I\,I\,I\,I\,Z\,Z\,I$
g_6	$I\,I\,I\,I\,I\,I\,I\,Z\,Z$
g_7	$X\,X\,X\,X\,X\,X\,I\,I\,I$
g_8	$I\,I\,I\,X\,X\,X\,X\,X\,X$
$\bar{Z}$	$X\,X\,X\,X\,X\,X\,X\,X\,X$
$\bar{X}$	$Z\,Z\,Z\,Z\,Z\,Z\,Z\,Z\,Z$

Screenshot: Nielsen & Chuang, chapter 10.5.6.

Last time

Error detection and recovery is performed by repeatedly measuring the stabilizers.



Syndrome

No error: $+1$ $+1$

Bit-flip XII: -1 $+1$

IXI: -1 -1

IIX: $+1$ -1

Learning outcomes

Today:

1. Derive parameters for the smallest code that corrects arbitrary single-qubit errors (and express it in the stabilizer formalism)
2. State the threshold theorem, and explain at a high level why error correction works even with faulty components

Properties of stabilizer codes

distance 5 ↕ 00000 / 11111 ⇒ 2 errors

physical q logical qubits distance

Stabilizer code usually described by notation $[[n, k, d]]$:

- code has $\cancel{4}^{n-k}$ stabilizer generators
- d = distance (minimum weight of Paulis that commute with everything in S but aren't in S)
- a distance d code can correct $(d-1)/2$ errors

$\frac{2^n}{2^k}$ phys. space / logical space

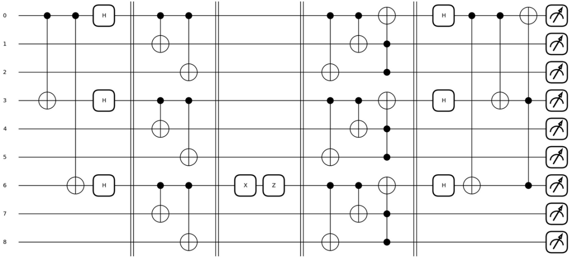
000	001
010	011
100	101
110	111

$\boxed{ZZI}$

$\boxed{IZZ}$

Shor code

The [[9, 1, 3]] code can correct arbitrary single-qubit errors, but it uses 9 qubits. Can we do better?

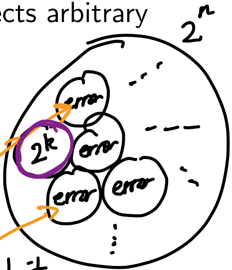


Name	Operator
g_1	$Z\,Z\,I\,I\,I\,I\,I\,I\,I$
g_2	$I\,Z\,Z\,I\,I\,I\,I\,I\,I$
g_3	$I\,I\,I\,Z\,Z\,I\,I\,I\,I$
g_4	$I\,I\,I\,I\,Z\,Z\,I\,I\,I$
g_5	$I\,I\,I\,I\,I\,I\,Z\,Z\,I$
g_6	$I\,I\,I\,I\,I\,I\,I\,Z\,Z$
g_7	$X\,X\,X\,X\,X\,X\,I\,I\,I$
g_8	$I\,I\,I\,X\,X\,X\,X\,X\,X$
$\bar{Z}$	$X\,X\,X\,X\,X\,X\,X\,X\,X$
$\bar{X}$	$Z\,Z\,Z\,Z\,Z\,Z\,Z\,Z\,Z$

Screenshot: Nielsen & Chuang, chapter 10.5.6.

The Hamming bound

What is the smallest number of physical qubits we need for a logical qubit in a (non-degenerate) code that corrects arbitrary single-qubit errors?



General bound:

- n physical qubits $\rightarrow$ space size 2^n
- k logical qubits $\rightarrow$ space size 2^k
- up to t errors

$\downarrow$

X, Y, Z individually on each qubit

j errors: 3^j

ways: $\binom{n}{j}$

$$\rightarrow \left[\sum_{j=0}^{t} \binom{n}{j} \cdot 3^j\right] \cdot 2^k \leq 2^n$$

$k=1$, $t=1$ error

$$\boxed{\binom{n}{0} \cdot 3^0} + \binom{n}{1} \cdot 3 = 1 + 3n$$

$$\Rightarrow (1+3n) \cdot 2 \leq 2^n$$

$$\Rightarrow n \geq 5$$

The smallest code: [[5, 1, 3]]

$$
\begin{aligned}
|0_L\rangle = \frac{1}{4}\Big[&|00000\rangle + |10010\rangle + |01001\rangle + |10100\rangle \\
&+|01010\rangle - |11011\rangle - |00110\rangle - |11000\rangle \\
&-|11101\rangle - |00011\rangle - |11110\rangle - |01111\rangle \\
&-|10001\rangle - |01100\rangle - |10111\rangle + |00101\rangle\Big] \\
|1_L\rangle = \frac{1}{4}\Big[&|11111\rangle + |01101\rangle + |10110\rangle + |01011\rangle \\
&+|10101\rangle - |00100\rangle - |11001\rangle - |00111\rangle \\
&-|00010\rangle - |11100\rangle - |00001\rangle - |10000\rangle \\
&-|01110\rangle - |10011\rangle - |01000\rangle + |11010\rangle\Big]
\end{aligned}
$$

Name	Operator
g_1	$XZZXI$
g_2	$IXZZX$
g_3	$XIXZZ$
g_4	$ZXIXZ$
$\bar{Z}$	$ZZZZZ$
$\bar{X}$	$XXXXX$

Screenshot: Nielsen & Chuang, chapter 10.5.6.

The Steane code: [[7, 1, 3]]

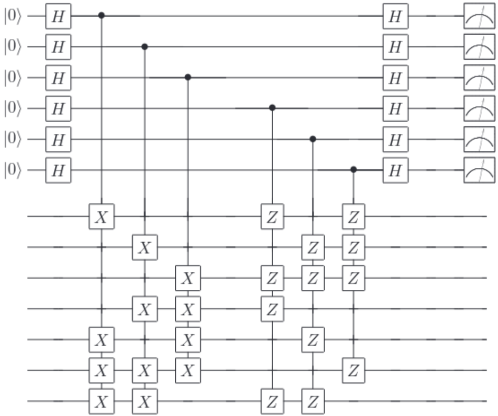
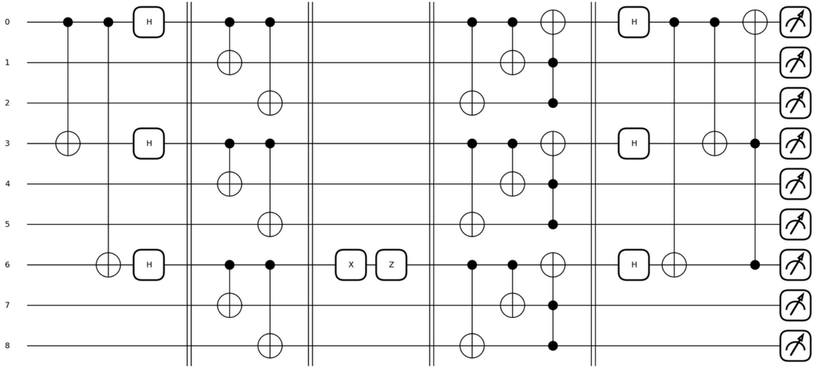


Figure 10.16. Quantum circuit for measuring the generators of the Steane code, to give the error syndrome. The top six qubits are the ancilla used for the measurement, and the bottom seven are the code qubits.

Screenshot: Nielsen & Chuang, chapter 10.5.8.

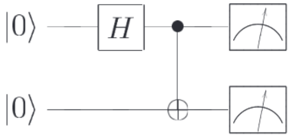
Fault-tolerant quantum computing

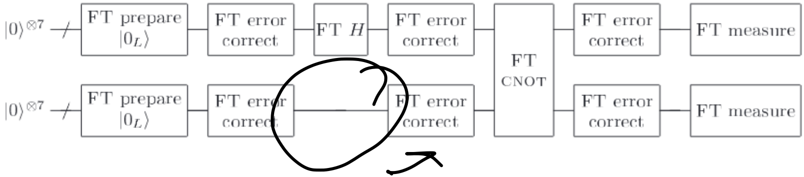
How can it be that doing all these extra operations is *better*, when in reality, all the operations are noisy?



Fault-tolerant quantum computing

Must implement all operations in a fault-tolerant manner:

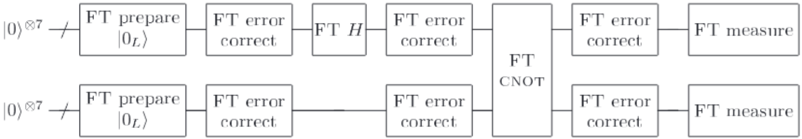




Screenshot: Nielsen & Chuang, chapter 10.6.1 (Figs. 10.18, 10.19)

Fault-tolerant quantum computing

Definition (adapted from Nielsen & Chuang): a procedure is *fault-tolerant* if the failure of a single component leads to *at most* one error per encoded block of qubits in the output.



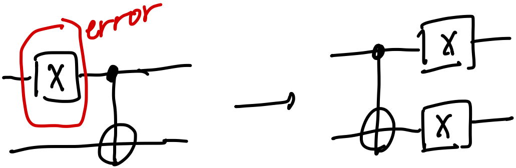
If probability of error in any component is p, what is the probability of an error in the output? (and how do we ensure it's smaller?)

Fault-tolerant quantum computing

Need to define a noise model and consider how errors *propagate* through a circuit.

Assume noise consists of single-qubit Pauli errors with some associated probabilities (some correlation allowed).

Example:



$|00\rangle \to |00\rangle$ $\qquad$ $|10\rangle \to |11\rangle$

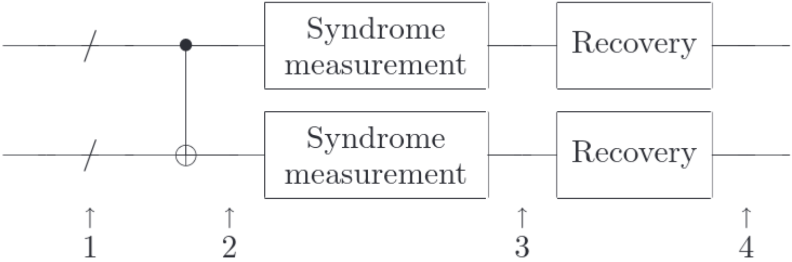
$|01\rangle \to |01\rangle$ $\qquad$ $|11\rangle \to |10\rangle$

$|10\rangle \to |11\rangle$ $\qquad$ $|00\rangle \to |00\rangle$

$|11\rangle \to |10\rangle$ $\qquad$ $|01\rangle \to |01\rangle$

Example: fault-tolerant CNOT

If one error occurs before/within this circuit, how many different ways can we experience *two or more* errors in the encoded first qubit at the output?



Screenshot: Nielsen & Chuang, chapter 10.6.1 (Fig. 10.21)

Example: fault-tolerant CNOT

We will use the Steane code as an example:

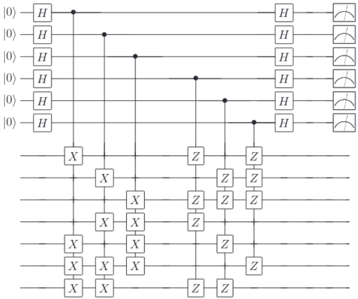


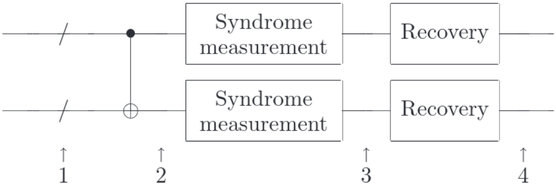
Figure 10.16. Quantum circuit for measuring the generators of the Steane code, to give the error syndrome. The top six qubits are the ancilla used for the measurement, and the bottom seven are the code qubits.

- 6 syndrome measurements (6 gates, measurement, recovery)
- logical CNOT is transversal (CNOT between all pairs); 7 points of failure that can propagate

Screenshot: Nielsen & Chuang, chapter 10.5.8.

Example: fault-tolerant CNOT

Example error mechanisms:



1. pre-existing error at step 1 on one qubit ($c_0 p$) or both qubits $c_0^2 p^2$, where $c_0 \approx 70$
2. two failures during the syndrome measurement $c_4 p^2$, where $c_4 \approx 70^2 \approx 5 \cdot 10^3$

Screenshot: Nielsen & Chuang, chapter 10.6.1 (Fig. 10.21)

Example: fault-tolerant CNOT

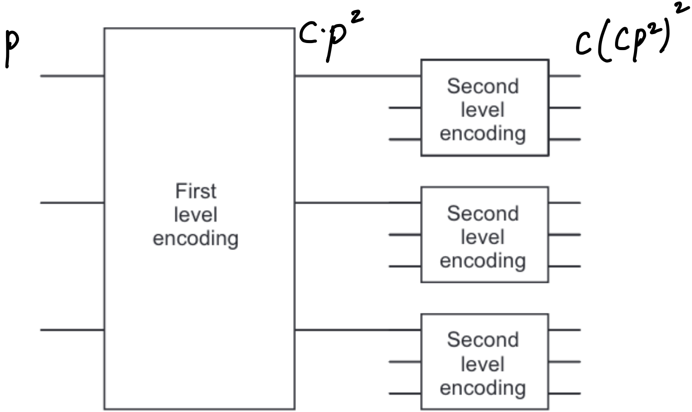
Can work through example of Nielsen & Chuang; key point is that probability of two or more errors in first encoded block is

$$\approx 10^4 p^2$$

As long as $p < 10^{-4}$, this is less than original error probability (more robust estimates closer to $10^{-5} - 10^{-6}$)

The threshold theorem

What if our p is too large? Concatenate codes...



Screenshot: Nielsen & Chuang, chapter 10.6.1 (Fig. 10.22)

The threshold theorem

Q: if you concatenate k times, what is the failure probability at the k'th level?

$$\frac{(cp)^{2^k}}{c}$$

Q: suppose g is the maximum number of operations in a fault-tolerant procedure. What is the simulation overhead?

$$g^k$$

Q: given a circuit with polynomial $p(n)$ gates, how many times do we need to concatenate to get total accuracy ϵ?

$$\frac{(cp)^{2^k}}{c} \leq \frac{\varepsilon}{p(n)}$$

The threshold theorem

$$\frac{(cp)^{2^k}}{c} \leq \frac{\varepsilon}{p(n)}$$

Can find k as long as $p < p_{th} = 1/c$ (*threshold condition*).

The size of the simulation circuit then becomes

$$O(\mathrm{poly}(\log(p(n)/\varepsilon))\, p(n))$$

Surface codes

Promising code, used in many recent demonstrations of fault-tolerance:

- threshold estimated at $\approx 1\%$
- logical error rate

$$\epsilon_d \propto \left(\frac{p}{p_{thr}}\right)^{\frac{d+1}{2}}$$

- suitable for nearest neighbour connectivity
- high qubit cost $(2d^2 - 1)$
- decoding is challenging

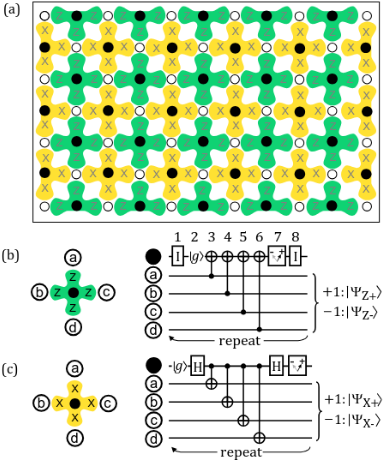


Image: Fowler et al. (2012) Surface codes: Towards practical large-scale quantum computation. PRA 86, 032324

Surface codes

In L01 I showed this plot of Google's *Willow* processor results.
Now you can interpret it!

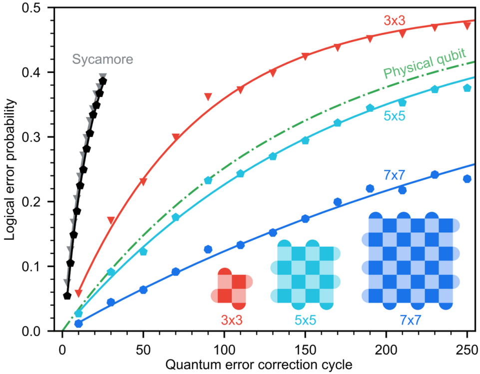


Image: https://research.google/blog/making-quantum-error-correction-work/

Open challenges in error correction

Very hot area, lots of open questions, and lots to do...

- find codes with better properties (fewer qubits, less connectivity limitations)
- improve performance of decoders
- develop the software stack (many compilation challenges!)
- continue to improve the hardware (better physical qubits means lower overhead)

Next time

Next class (tutorial tomorrow):

- Quiz 10
- Project presentation
- Summary and final “survey” question

Action items:

1. Work on project
2. Book final exam time slot on Canvas

Recommended reading:

- For this class: Codebook EC; N&C 10.6