Portland State University

05/29/2020

# S'20 CS410/510
# Intro to quantum computing

Fang Song

## Week 9

- Quantum error correction
- Quantum fault-tolerance

Credit: based on slides by Richard Cleve

# Exercise

**2.** Let $|A\rangle, |B\rangle$ be as defined below. Show that $I = a|A\rangle\langle A| + b|B\rangle\langle B|$

- $A \subseteq \{0,1\}^n, B = \{0,1\}^n \backslash A$
- $|A\rangle := \frac{1}{\sqrt{a}} \sum_{x \in A} |x\rangle, \ |B\rangle := \frac{1}{\sqrt{b}} \sum_{x \in B} |x\rangle$

$\langle A|B\rangle = 0$

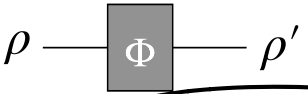
$\langle A|A\rangle = 1$

$|A\rangle\langle A|$

$(a|A\rangle\langle A| + b|B\rangle\langle B|)|A\rangle$

$= a|A\rangle$

# Recall: quantum channels




Let $A_1, A_2, \ldots, A_m$ be matrices satisfying $\sum_{j=1}^{m} A_j^\dagger A_j = I$.

Then the mapping $\rho \mapsto \sum_{j=1}^{m} A_j \rho A_j^\dagger$ is a general quantum operator.

- N.B. $A_i$ need NOT be square matrices
- Also known as quantum channels

# Examples of quantum channels

3. **Partial trace** $A_0 = I \otimes \langle 0| = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}, A_1 = I \otimes \langle 1| = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$

- Check validity: $A_0^\dagger A_0 + A_1^\dagger A_1 = \mathbb{1} \rightarrow \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes (1 \; 0)$

- Apply to $|0\rangle\langle 0| \otimes |+\rangle\langle +|$

$\sum A_i \rho A_i^\dagger = |0\rangle\langle 0|$

$A_0 (|0\rangle\langle 0| \otimes |+\rangle\langle +|) A_0^\dagger$

$= I \otimes \langle 0| (|0\rangle\langle 0| \otimes |+\rangle\langle +|) I \otimes |0\rangle$

$= |0\rangle\langle 0| \otimes \langle 0|+\rangle\langle +| \; I \otimes |0\rangle$

$= |0\rangle\langle 0| \otimes \langle 0|+\rangle\langle +|0\rangle = \frac{1}{2}|0\rangle\langle 0|$

$A_1 (|0\rangle\langle 0| \otimes |+\rangle\langle +|) A_1^\dagger$

$= |0\rangle\langle 0| \otimes \langle 1|+\rangle\langle 1|+\rangle = \frac{1}{2}|0\rangle\langle 0|$

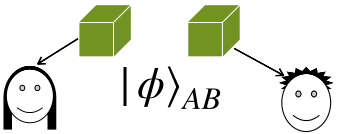
- Apply to $|\phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

$(A \otimes B)(C \otimes D) = AC \otimes BD$

$A_0 = I \otimes \langle 0|$

$A_1 = I \otimes \langle 1|$

# Exercise




1. let $Tr_B$ denote partial trace of subsystem $B$. Suppose Alice and Bob shares two qubits in state $|\phi\rangle_{AB}$.

- Apply $Tr_B$ to $|\phi\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

$\rho_{AB} = \frac{1}{2}(|00\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 00| + |11\rangle\langle 11|)$

$\{(\frac{1}{2}, |0\rangle), (\frac{1}{2}, |1\rangle)\}$ $\quad \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| = I_A$

$A_0 \rho_{AB} A_0^\dagger = \frac{1}{2}|0\rangle\langle 0|$ +

$A_1 \rho_{AB} A_1^\dagger = \frac{1}{2}|1\rangle\langle 1|$

- Apply $Tr_B$ to $|\phi\rangle_{AB} = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$

$Tr_B(|\phi\rangle\langle\phi|_{AB}) = I_A$

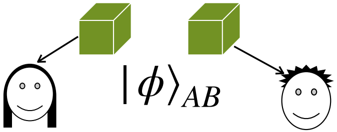
$\rho_{AB} = \frac{1}{2}(|01\rangle\langle 01| + |01\rangle\langle 10| + |10\rangle\langle 01| + |10\rangle\langle 10|)$

$A_0 \rho A_0^\dagger = \frac{1}{2}|1\rangle\langle 1|$ +

$A_1 \rho A_1^\dagger = \frac{1}{2}|0\rangle\langle 0|$

- Is Alice able to tell the two cases on her side?

# Exercise




**2. let $Tr_B$ denote partial trace of subsystem $B$. Suppose Alice and Bob shares two qubits in state $|\phi\rangle_{AB}$.**

- Apply $Tr_B$ to $|\phi\rangle_{AB} = \frac{3}{5}|00\rangle + \frac{4}{5}|11\rangle$

- Apply $Tr_B$ to $|\phi\rangle_{AB} = \frac{4}{5}|00\rangle - \frac{3}{5}|11\rangle$

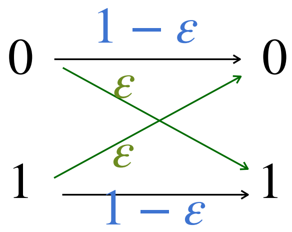
- Is Alice able to tell the two cases on her side?

# Error correction codes

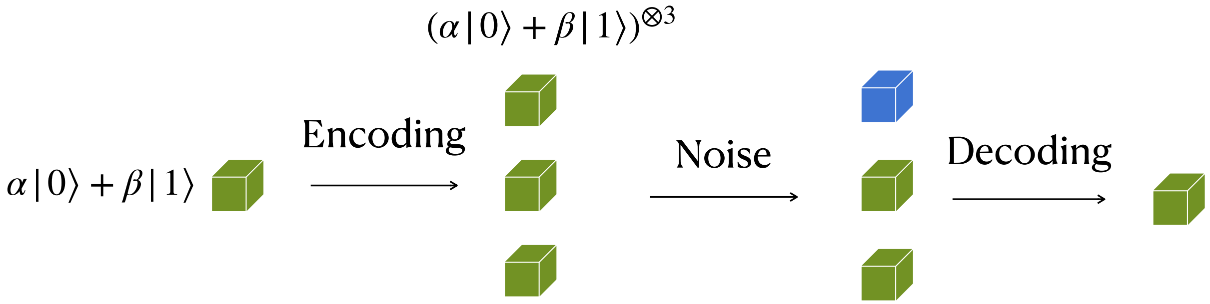
# Classical error correcting codes (ECC)

- Protecting data against noises during transmitting or storing


- Binary symmetric channel: each bit flips w. probability $\varepsilon$ independently
  - A simple noise model, reality may be more complex and unpredictable



# Quantum repetition code?




**:( This would violate no-cloning ...**

# 3-bit repetition code

- **Redundancy is our friend**
  - $E : b \mapsto bbb$; repete to encode
  - $D : b_1b_2b_3 \mapsto maj(b_1, b_2, b_3)$; take majority to decode
- **Effective error probability reduces from $\varepsilon$ to $3\varepsilon^2 - 2\varepsilon^3$**

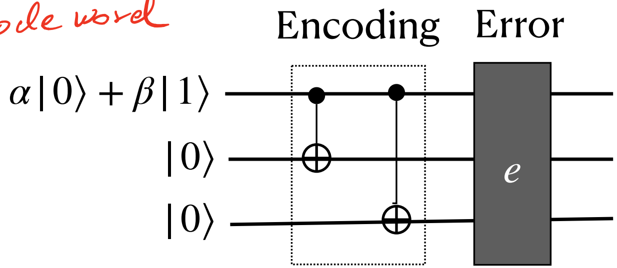
| $\varepsilon$ | $3\varepsilon^2 - 2\varepsilon^3$ | **Error reduced by a factor of** |
|---|---|---|
| 0.1 | 0.009 | 11 |
| 0.01 | 0.0001 | 100 |
| 0.001 | 0.0000001 | 1000 |

# 3-qubit code for one $X$-error

- Encoding $E$ logical $|0\rangle$ logical $|1\rangle$
  - $|0\rangle \mapsto |0_L\rangle := |000\rangle, |1\rangle \mapsto |1_L\rangle := |111\rangle$
  - $\alpha|0\rangle + \beta|1\rangle \mapsto \alpha|000\rangle + \beta|111\rangle$ ← code word

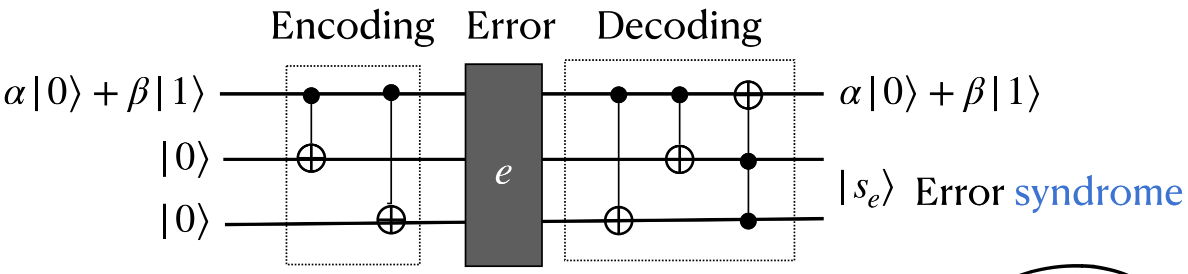
$X \otimes I \otimes I(\alpha|000\rangle + \beta|111\rangle)$

$= \alpha|100\rangle + \beta|011\rangle$




- What if a quantum bit-flip error?
  - $I \otimes I \otimes I \quad X \otimes I \otimes I \quad I \otimes X \otimes I \quad I \otimes I \otimes X$

# 3-qubit code for one $X$-error




| | | | | |
|---|---|---|---|---|
| Error | $I \otimes I \otimes I$ | $X \otimes I \otimes I$ | $I \otimes X \otimes I$ | $I \otimes I \otimes X$ |
| Error syndrome | $\|00\rangle$ | $\|11\rangle$ | $\|10\rangle$ | $\|01\rangle$ |

$\alpha|100\rangle + \beta|011\rangle$

$\xrightarrow{CNOT_{1\to3}} \alpha|101\rangle + \beta|011\rangle$

$\xrightarrow{CNOT_{1\to2}} \alpha|111\rangle + \beta|011\rangle = (\alpha|1\rangle + \beta|0\rangle)|11\rangle$

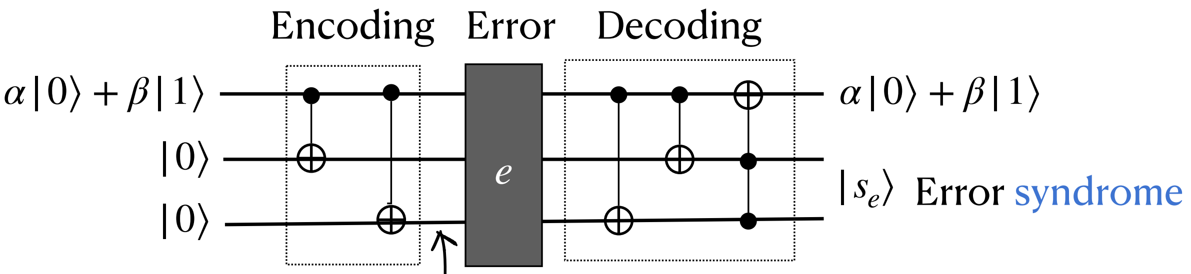
$\xrightarrow{X\oplus} \alpha|0\rangle + \beta|1\rangle$

$\alpha|001\rangle + \beta|110\rangle$

$\xrightarrow{CNOT_{1\to3}} \alpha|001\rangle + \beta|111\rangle$

$\xrightarrow{CNOT_{1\to2}} \alpha|001\rangle + \beta|101\rangle = (\alpha|0\rangle + \beta|1\rangle)|01\rangle$

# Does it help with Z-error? phase flip




- **Example.** $e = Z \otimes I \otimes I$

$\alpha|000\rangle + \beta|111\rangle$

$\xrightarrow{Z\otimes I\otimes I}$ $\alpha|000\rangle - \beta|111\rangle$

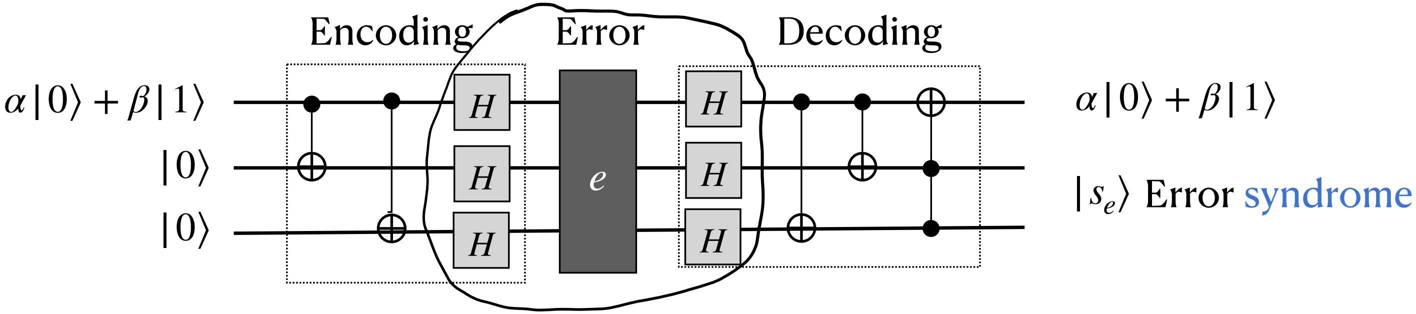
$\xrightarrow{CNOT_{1-3}}$ $\alpha|000\rangle - \beta|110\rangle$

$\xrightarrow{CNOT_{1-2}}$ $\alpha|000\rangle - \beta|100\rangle = (\alpha|0\rangle - \beta|1\rangle)|00\rangle$

$Z(\alpha|0\rangle + \beta|1\rangle)$

# 3-qubit code for one $Z$-error

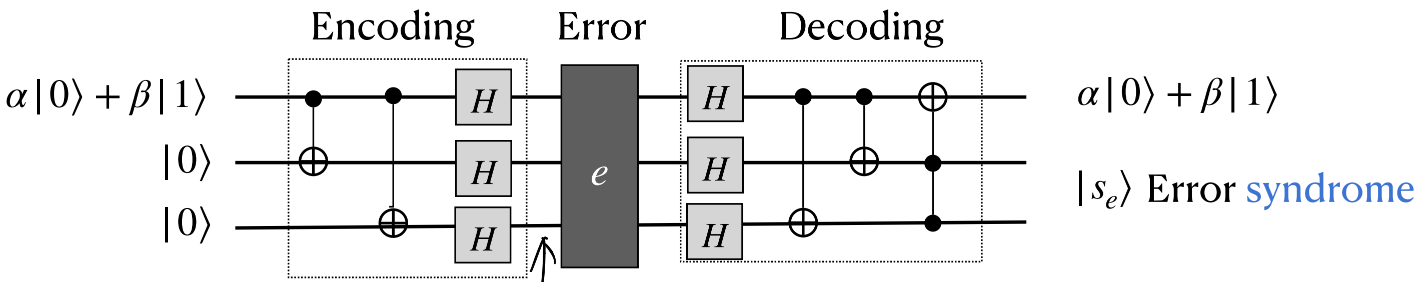
- **Observation.** $HZH = X$. Reducing $Z$-erro to $X$-error




- **Encoding** $E$. $|0\rangle \mapsto |0_L\rangle := |+++\rangle, |1\rangle \mapsto |1_L\rangle := |---\rangle$

| | | | | |
|---|---|---|---|---|
| Error | $I \otimes I \otimes I$ | $X \otimes I \otimes I$ | $I \otimes X \otimes I$ | $I \otimes I \otimes X$ |
| Error syndrome | $\|00\rangle$ | $\|11\rangle$ | $\|10\rangle$ | $\|01\rangle$ |

# Does it help with $X$-error?




- **Example.** $e = X \otimes I \otimes I$

$|0_L\rangle = |{+}{+}{+}\rangle$

$|1_L\rangle = |{-}{-}{-}\rangle$

$\alpha|0\rangle + \beta|1\rangle = \alpha|{+}{+}{+}\rangle + \beta|{-}{-}{-}\rangle$

$\xrightarrow{X \otimes I \otimes I} \alpha|{+}{+}{+}\rangle - \beta|{-}{-}{-}\rangle$

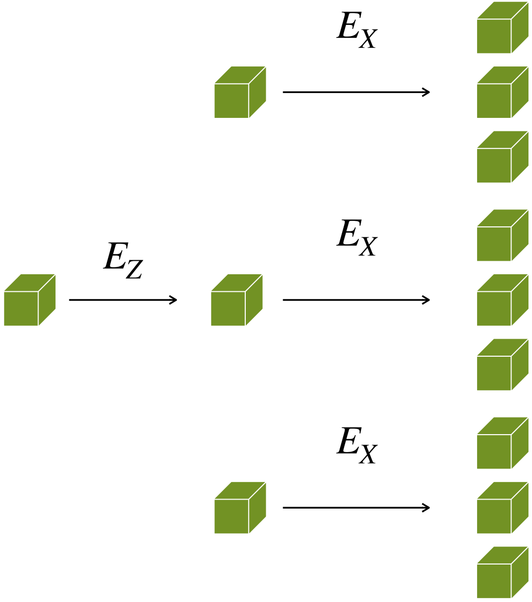
$\xrightarrow{H \otimes H \otimes H} \alpha|000\rangle - \beta|111\rangle$

$\vdots$

$\longrightarrow (\alpha|0\rangle - \beta|1\rangle)|00\rangle$

# Shor's 9-qubit code

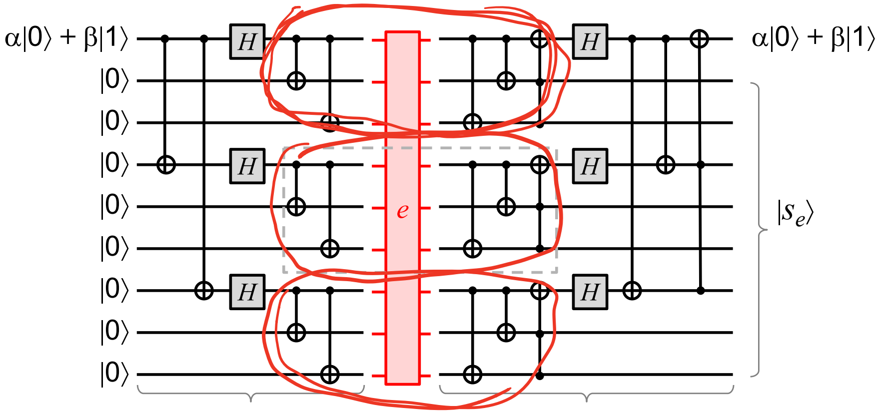
Rohs's




$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

- $|0\rangle \mapsto |+++\rangle \mapsto \left(\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)\right)^{\otimes 3} =: |0_L\rangle$
- $|1\rangle \mapsto |---\rangle \mapsto \left(\frac{1}{\sqrt{2}}(|000\rangle - |111\rangle)\right)^{\otimes 3} =: |1_L\rangle$

# Shor's 9-qubit code




- **Able to correct a single $X$ or $Z$ error**
  - "Inner " part corrects any single-quit $X$ error
  - "Inner " part corrects any single-quit $X$ error
- **Since $Y = iXZ$, single-quit $Y$-error can be corrected too**

# Arbitrary one-qubit errors

- **Observation.** Any one-qubit unitary $U$ can be written as $U = \lambda_0 I + \lambda_1 X + \lambda_2 Y + \lambda_3 Z$ for some $\lambda_i \in \mathbb{C}$.

$$\alpha|0\rangle + \beta|1\rangle \overset{E}{\mapsto} \alpha|0_L\rangle + \beta|1\rangle_L \overset{I\otimes U\otimes\ldots\otimes I}{\mapsto} |\tilde{\psi}\rangle$$

$$\overset{D}{\mapsto} (\alpha|0\rangle + \beta|1\rangle)(\lambda_0|s_I\rangle + \lambda_1|s_X\rangle + \lambda_2|S_Y\rangle + \lambda_3|S_Z\rangle)$$

- **Corollary.** Shor's 9-qubit code protects against any one-qubit unitary error. In fact the error can be any one-qubit quantum channel $\Phi$.

- More QECC: CSS codes & stabilizer codes
  - 5-qubit code: optimal for correcting single-qubit errors
  - Surface code: elegant theory and promising in realization

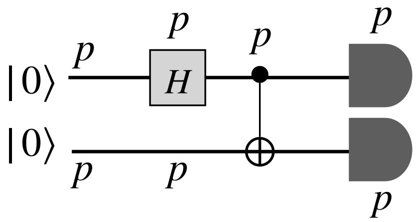
# Fault-tolerant computing

# Error is ubiquitous

**QECC solves the problem of storing and transmitting quantum information.**

**But we want to do more: computation on them**

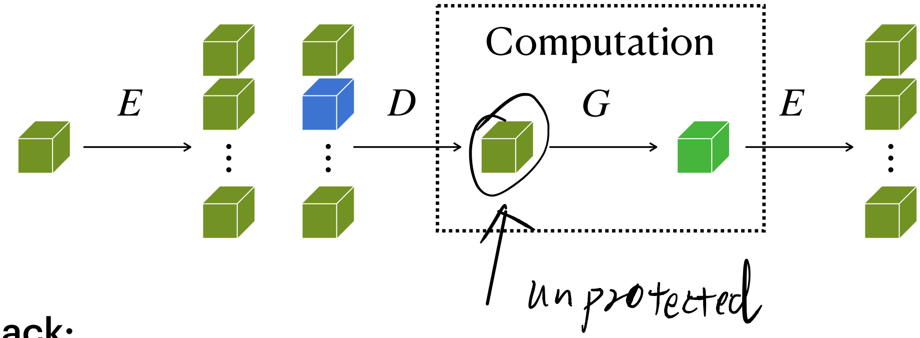
- **Observation. Any "location" can "fail".**
  - Gate, measurement, storage, prep, ...




- **Simple error model: each location fails with probability $p$**
  - **Circuit of size $\ell$.** $\Pr$[**no error**] $= (1-p)^{\ell} \approx 1 - \ell \cdot p \to 0$

# Attempt 1

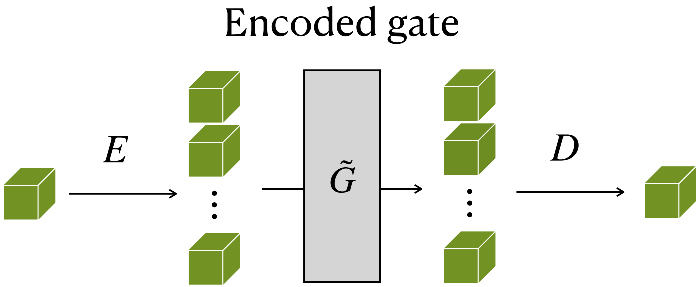
- Enc — Dec — Compute — Enc



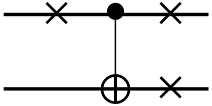

- Drawback:

# Attempt 2

- Computing on encoded data

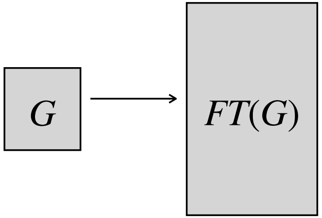



- Challenges
  - Non-perfect $\tilde{G}$: ok if not many
  - Error propagation



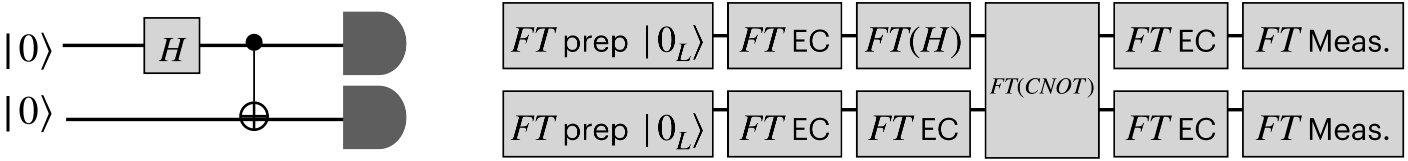
# Fault-tolerant gadget

- When designed encoded gates, make sure not to introduce too many errors
  - FT gate,
  - FT state prep
  - FT measurement




Specific to the error-correcting code used

- Putting it together: FT operations + Frequent FT error-correcting



# Threshold theorem

**Theorem**. There is a fixed constant $p_{th}$ such that a circuit of size $T$ can be translated to a circuit of size $O(T \log T)$ that is robust against the error model with error $p \leq p_{th}$.

- $p_{th}$ depends heavily on the QECC
  - Steane code: $\sim 10^{-5}$
  - Surface code: $\sim 10^{-2}$
- Another key idea: concatenation

# Quantum computational complexity

# Encounters so far

- **Computability:** can you solve it, in principle?

[Given program code, will this program terminate or loop indefinitely?]

Uncomputable!

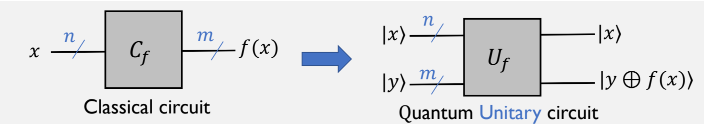
> **Church-Turing Thesis.** A problem can be computed in any ***reasonable*** model of computation iff. it is computable by a **Boolean circuit**.

- **Complexity:** can you solve it, under resource constraints?

[Can you factor a 1024-bit integer in 3 seconds?]

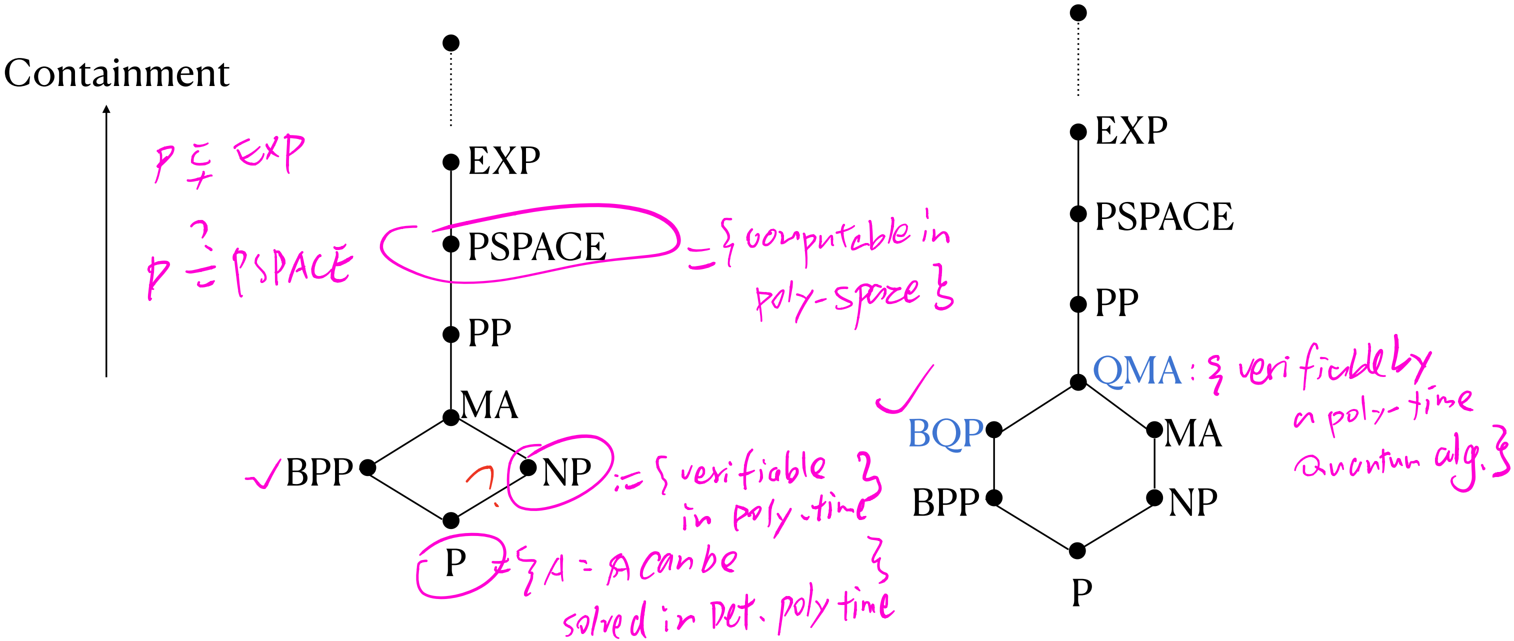
> **Extended Church-Turing Thesis.** A function can be computed efficiently in any *reasonable* model of computation iff. it is efficiently computable by a **Boolean circuit**.

✓ ← Quantum computer → Disprove ECTT?




**Corollary.** BPP⊆BQP [More to come in future]

# Landscape of complexity classes



# Discussion: quantum party is on!?

- What do you think about its description of quantum computing?

- Think of a few local companies. Can you identify where quantum computers might help them?

# Looking forward to your presentations!

Scratch