- Day 4 Recap:
  - ADAPT-QAOA (2103.17047)
  - Feedback-based ALgorithm Quantum Optimization (FALQON, 2103.08619)
  - Data re-uploading for a universal quantum classifier (1907.02085)

- Day 5 Plan:
  - Quantum Fourier Transformation and Phase estimation
  - Error correction

  - Bernstein-Vazirani Algorithm and Simon’s algorithm
  - Shor’s algorithm, Grover’s algorithm

Discrete Fourier Transformation

- Simon's algorithm $\longrightarrow$ Shor's algorithm (factoring numbers) makes use of QFT.
- Discrete Fourier Transformation (DFT): signal processing, quantum theory (position $\leftrightarrow$ momentum).
- Assume a vector f of N complex numbers: $f_k\,,\; k = 0,1,\cdots,N-1$
- DFT is a mapping from N complex # to N complex #.

$$\text{DFT}:\; f_k \;\longrightarrow\; \tilde{f}_j = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} w^{-jk} f_k \qquad\qquad w = \exp\left(\frac{2\pi i}{N}\right)$$

$$\text{Inverse DFT}:\; \tilde{f}_k \;\longrightarrow\; \tilde{f}_j = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} w^{jk} \tilde{f}_k$$

nonzero only when $j = \ell$

$$f_j = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} w^{jk} \tilde{f}_k = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} w^{jk} \left(\frac{1}{\sqrt{N}} \sum_{\ell=0}^{N-1} w^{-\ell k} f_\ell \right) = \frac{1}{N} \sum_{\ell}^{N-1} \overbrace{\sum_{k=0}^{N-1} w^{(j-\ell)k}} f_\ell = \sum_{\ell}^{N-1} f_\ell\, \delta_{j\ell} = f_j$$

$$\boxed{\frac{1}{N} \sum_{k=0}^{N-1} w^{(j-\ell)k} = \delta_{j\ell}}$$

$$\frac{1}{N} \sum_{k=0}^{N-1} w^{(j-\ell)k} = \begin{cases} \dfrac{1}{N} \dfrac{1 - \exp\left(\frac{2\pi i}{N}(j-\ell)N\right)}{1 - \exp\left(\frac{2\pi i}{N}\right)} = 0\,, & \text{if } j \neq \ell \\ 1\,, & \text{if } j = \ell \end{cases}$$

Discrete Fourier Transformation

- Convolution (circular convolution, periodic convolution, cyclic convolution)

$$(f * g)_i = \sum_{j=0}^{N-1} f_i \, g_{i-j} \,, \qquad \text{where } g_{-m} = g_{N-m} \text{ (periodic condition)}$$

- DFT turns convolution into point wise vector multiplication.

$$\text{DFT of } f * g = \tilde{c}_k = \tilde{f}_k \, \tilde{g}_k$$

$$\tilde{c}_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} w^{-jk} (f * g)_j = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} w^{-jk} \left(\sum_{i=0}^{N-1} f_i \, g_{j-i} \right)$$

δ_{mk}

$$= \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} w^{-jk} \sum_{i=0}^{N-1} \left(\frac{1}{\sqrt{N}} \sum_{\ell} w^{i\ell} \tilde{f}_\ell \right) \left(\frac{1}{\sqrt{N}} \sum_{m} w^{(j-i)m} \tilde{g}_m \right) = \frac{1}{\sqrt{N}^3} \sum_{j,i,\ell,m} \tilde{f}_\ell \, \tilde{g}_m \, w^{-jk} \, w^{i\ell} \, w^{jm} \, w^{-im} = \tilde{f}_k \, \tilde{g}_k$$

$\delta_{\ell m}$

$$\frac{1}{N} \sum_{k=0}^{N-1} w^{(j-\ell)k} = \delta_{j\ell}$$

$$w = \exp\left(\frac{2\pi i}{N} \right)$$

$$\text{DFT}: \; f_k \longrightarrow \tilde{f}_j = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} w^{-jk} f_k$$

$$\text{Inverse DFT}: \; \tilde{f}_k \longrightarrow \tilde{f}_j = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} w^{jk} \tilde{f}_k$$

Fast Fourier Transformation

- DFT: $O(N^2) = O((2^n)^2)$
- FFT: $O(N \log N) = O(2^n \log 2^n) = O(2^n \log n)$
- QFT: $O(n^2)$ where $N = 2^n$
- Best known QFT: $O(n \log n)$
  - "An improved quantum Fourier transform algorithm and applications" by L. Hales and S. Hallgren

Quantum Fourier Transformation

- Quantum analog of discrete Fourier transformation
- Used in Shor's algorithm, computing discrete logarithm, quantum phase estimation, algorithms for hidden subgroup problem
- Don Coppersmith (IBM) in 2002
  - https://arxiv.org/pdf/quant-ph/0201067.pdf

Quantum Fourier Transformation

- For classical discrete Fourier transformation

$$y_k = \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} w^{jk} x_j \qquad w = \exp\left(\frac{2\pi i}{2^n}\right) \qquad N = 2^n$$

- QFT is defined similarly $\quad F : \ |j\rangle \longrightarrow \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} w^{jk} |k\rangle = F|j\rangle$

- For arbitrary quantum states, $\quad F : \ |x\rangle = \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} x_j |j\rangle \longrightarrow |y\rangle = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} y_k |k\rangle$

$$F|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} x_j F|j\rangle = \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} x_j w^{jk} |k\rangle$$

- For a single quantum state, $\quad F|j\rangle = \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} w^{jk} |k\rangle \qquad F|j'\rangle = \frac{1}{\sqrt{2^n}} \sum_{j'=0}^{2^n-1} w^{j'k'} |k'\rangle$

$$\langle j'|F^\dagger F|j\rangle = \frac{1}{2^n} \sum_{k=0}^{2^n-1} \sum_{k'=0}^{2^n-1} w^{-j'k'} w^{jk} \langle k'|k\rangle = \frac{1}{2^n} \sum_{k=0}^{2^n-1} w^{(j-j')k} = \delta_{jj'}$$

$$\frac{1}{2^n} \sum_{k=0}^{2^n-1} w^{(j-\ell)k} = \delta_{j\ell}$$

$F^\dagger F = 1$ and QFT is a unitary transformation.

Quantum Fourier Transformation

For $$j = j_1 2^{n-1} + j_2 2^{n-2} + \cdots + j_n 2^0 = \sum_{i=1}^{n} j_i\, 2^{n-i}$$

$$k = k_1 2^{n-1} + k_2 2^{n-2} + \cdots + k_n 2^0 = \sum_{i=1}^{n} k_i\, 2^{n-i}$$

$$\frac{1}{2^n} \sum_{k=0}^{2^n-1} w^{(j-\ell)k} = \delta_{j\ell}$$

$$F\,|\,j\rangle = \frac{1}{\sqrt{2}^n} \sum_{k=0}^{2^n-1} w^{jk}\,|\,k\rangle = \frac{1}{\sqrt{2}^n} \sum_{k=0}^{2^n-1} \exp\!\left(\frac{2\pi i j}{2^n} \sum_{\ell=1}^{n} k_\ell 2^{n-\ell}\right) |\,k\rangle$$

$$w = \exp\!\left(\frac{2\pi i}{2^n}\right)$$

$$= \frac{1}{\sqrt{2}^n} \sum_{k=0}^{2^n-1} \exp\!\left(2\pi i j \sum_{\ell=1}^{n} k_\ell 2^{-\ell}\right) |\,k\rangle$$

$$= \frac{1}{\sqrt{2}^n} \sum_{k=0}^{2^n-1} \exp\!\left(2\pi i j k_1 2^{-1}\right) \exp\!\left(2\pi i j k_2 2^{-2}\right) \cdots \exp\!\left(2\pi i j k_n 2^{-n}\right) |\,k\rangle$$

$$= \frac{1}{\sqrt{2}^n} \sum_{k_1=0}^{1} \cdots \sum_{k_n=0}^{1} \exp\!\left(2\pi i j k_1 2^{-1}\right) \exp\!\left(2\pi i j k_2 2^{-2}\right) \cdots \underbrace{\exp\!\left(2\pi i j k_n 2^{-n}\right)}_{= |\,0\rangle + \exp\left(2\pi i j 2^{-n}\right) |\,1\rangle} |\,k_1\, k_2\, \cdots\, k_n\,\rangle$$

Quantum Fourier Transformation

$$F\,|j\rangle = \frac{1}{\sqrt{2}^n}\left(|0\rangle + \exp\!\left(\frac{2\pi i j}{2}\right)|1\rangle\right)\left(|0\rangle + \exp\!\left(\frac{2\pi i j}{2^2}\right)|1\rangle\right)\cdots\left(|0\rangle + \exp\!\left(\frac{2\pi i j}{2^n}\right)|1\rangle\right)$$

$$= \frac{1}{\sqrt{2}^n}\bigotimes_{k=1}^{n}\left(|0\rangle + \exp\!\left(\frac{2\pi i j}{2^k}\right)|1\rangle\right)$$

$j_i = 0\,,1$

$1 \le k \le n$

$0 \le j \le 2^n - 1$

- Binary fraction = expression in power of 1/2

In decimal form: $0.j_\ell\, j_{\ell+1}\,\cdots\, j_m = \frac{j_\ell}{2} + \frac{j_{\ell+1}}{2^2} + \cdots + \frac{j_m}{2^{m-\ell+1}}$

j is not necessarily an integer: $\frac{j}{2^k} = j_1\, j_2\,\cdots\, j_{n-k}\,\cdot\, j_{n-k+1}\,\cdots\, j_n = \sum_{\nu=1}^{n} j_\nu\, 2^{n-\nu-k}$

If $n = 8$ and $k = 3$, $j = j_1 2^7 + j_2 2^6 + j_3 2^5 + j_4 2^4 + j_5 2^3 + j_6 2^2 + j_7 2^1 + j_8 2^0$

$$\frac{j}{2^3} = j_1 2^4 + j_2 2^3 + j_3 2^2 + j_4 2^1 + j_5 2^0 + \underbrace{j_6 2^{-1} + j_7 2^{-2} + j_8 2^{-3}}_{\text{binary fraction: } 0\,.j_6 j_7 j_8}$$

$j_1 j_2 j_3 j_4 j_5 \cdot j_6 j_7 j_8$

Quantum Fourier Transformation

$$j = j_1 2^{n-1} + j_2 2^{n-2} + \cdots + j_{n-3} 2^3 + j_{n-2} 2^2 + j_{n-1} 2^1 + j_1 2^0 = \sum_{\nu=1}^{n} j_\nu 2^{n-\nu}$$

$$\frac{j}{2^k} = \frac{j_1 2^{n-1} + j_2 2^{n-2} + \cdots + j_{n-3} 2^3 + j_{n-2} 2^2 + j_{n-1} 2^1 + j_1 2^0}{2^k} = \sum_{\nu=1}^{n} \frac{j_\nu \, 2^{n-\nu}}{2^k} = \sum_{\nu=1}^{n} j_\nu \, 2^{n-\nu-k}$$

$$= j_1 j_2 \cdots j_{n-k} \,.\, j_{n-k+1} \cdots j_n$$

$$\exp\left(2\pi i \frac{j}{2^k}\right) = \exp\left(2\pi i \, 0\,.\, j_{n-k+1} \, \cdots \, j_n\right)$$

$$F\,|j\rangle = \frac{1}{\sqrt{2}^n} \left(|0\rangle + \exp\left(\frac{2\pi i j}{2}\right)|1\rangle\right) \left(|0\rangle + \exp\left(\frac{2\pi i j}{2^2}\right)|1\rangle\right) \cdots \left(|0\rangle + \exp\left(\frac{2\pi i j}{2^n}\right)|1\rangle\right)$$

$$= \frac{1}{\sqrt{2}^n} \bigotimes_{k=1}^{n} \left(|0\rangle + \exp\left(\frac{2\pi i j}{2^k}\right)|1\rangle\right) = \frac{1}{\sqrt{2}^n} \bigotimes_{k=1}^{n} \left(|0\rangle + \exp\left(2\pi i \, 0\,.\, j_{n-k-1} \, \cdots \, j_n\right)|1\rangle\right)$$

$$= \frac{1}{\sqrt{2}^n} \left(|0\rangle + \exp\left(2\pi i \, 0\,.\, j_n\right)|1\rangle\right) \left(|0\rangle + \exp\left(2\pi i \, 0\,.\, j_{n-1} j_{n-2}\right)|1\rangle\right)$$

$$\cdots \left(|0\rangle + \exp\left(2\pi i \, 0\,.\, j_1 j_2 \cdots j_n\right)|1\rangle\right)$$

Quantum Circuit for QFT

- $|j_\ell\rangle$ transforms into $\frac{1}{\sqrt{2}}\left[\,|0\rangle + \exp\left(2\pi i\, 0\,.j_\ell \cdots j_n\right)|1\rangle\right]$

$$= \frac{1}{\sqrt{2}}\left[\,|0\rangle + \underbrace{e^{2\pi i 0.j_\ell}}\,\underbrace{e^{2\pi i 0.0 j_{\ell+1}\cdots j_n}}|1\rangle\right]$$

$$\exp\left(2\pi i \frac{j_\ell}{2}\right) = \exp\left(\pi i j_\ell\right) = (-1)^{j_\ell}$$

use $R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{pmatrix}$

$$0.0 j_{\ell+1}\cdots j_n = \frac{0.j_{\ell+1}\cdots j_n}{2}$$

Controlled by the value of j_kth qubit.

if $\begin{cases} j_k = 0\,, & R_k = 1 \\ j_k = 1\,, & R_k \end{cases}$

$\boxed{\text{1st qubit:}}$ $|0\rangle + \exp\left(2\pi i\, 0\,.j_\ell \cdots j_n\right)|1\rangle$

Start with $|j\rangle = |j_1\rangle|j_2 j_3 \cdots j_n\rangle \xrightarrow{H_1} \frac{1}{\sqrt{2}}\Big(|0\rangle + (-1)^{j_1}|1\rangle\Big)|j_2 j_3 \cdots j_n\rangle$

$$= \frac{1}{\sqrt{2}}\Big(|0\rangle + e^{2\pi i\, 0.j_1}|1\rangle\Big)|j_2 j_3 \cdots j_n\rangle$$

$$\xrightarrow{\text{R}_2 \text{ on } \text{q}_1 \text{ with } \text{q}_2 \text{ control}} \frac{1}{\sqrt{2}}\Big(|0\rangle + e^{2\pi i\, 0.j_1} e^{2\pi i\, j_2/2^2}|1\rangle\Big)|j_2 j_3 \cdots j_n\rangle$$

$$= \frac{1}{\sqrt{2}}\Big(|0\rangle + e^{2\pi i\, 0.j_1 j_2}|1\rangle\Big)|j_2 j_3 \cdots j_n\rangle$$

Quantum Circuit for QFT

$$\xrightarrow{\mathrm{R_3\ on\ q_1\ with\ q_3\ control}} \frac{1}{\sqrt{2}}\Big(\,|0\rangle + e^{2\pi i\, 0.j_1 j_2 j_3}\,|1\rangle\Big)\,|j_2 j_3 \cdots j_n\rangle$$

$$\xrightarrow[\mathrm{to\ q_n}]{\mathrm{continue\ down}} \frac{1}{\sqrt{2}}\Big(\,|0\rangle + e^{2\pi i\, 0.j_1 j_2 j_3 \cdots j_n}\,|1\rangle\Big)\,|j_2 j_3 \cdots j_n\rangle$$

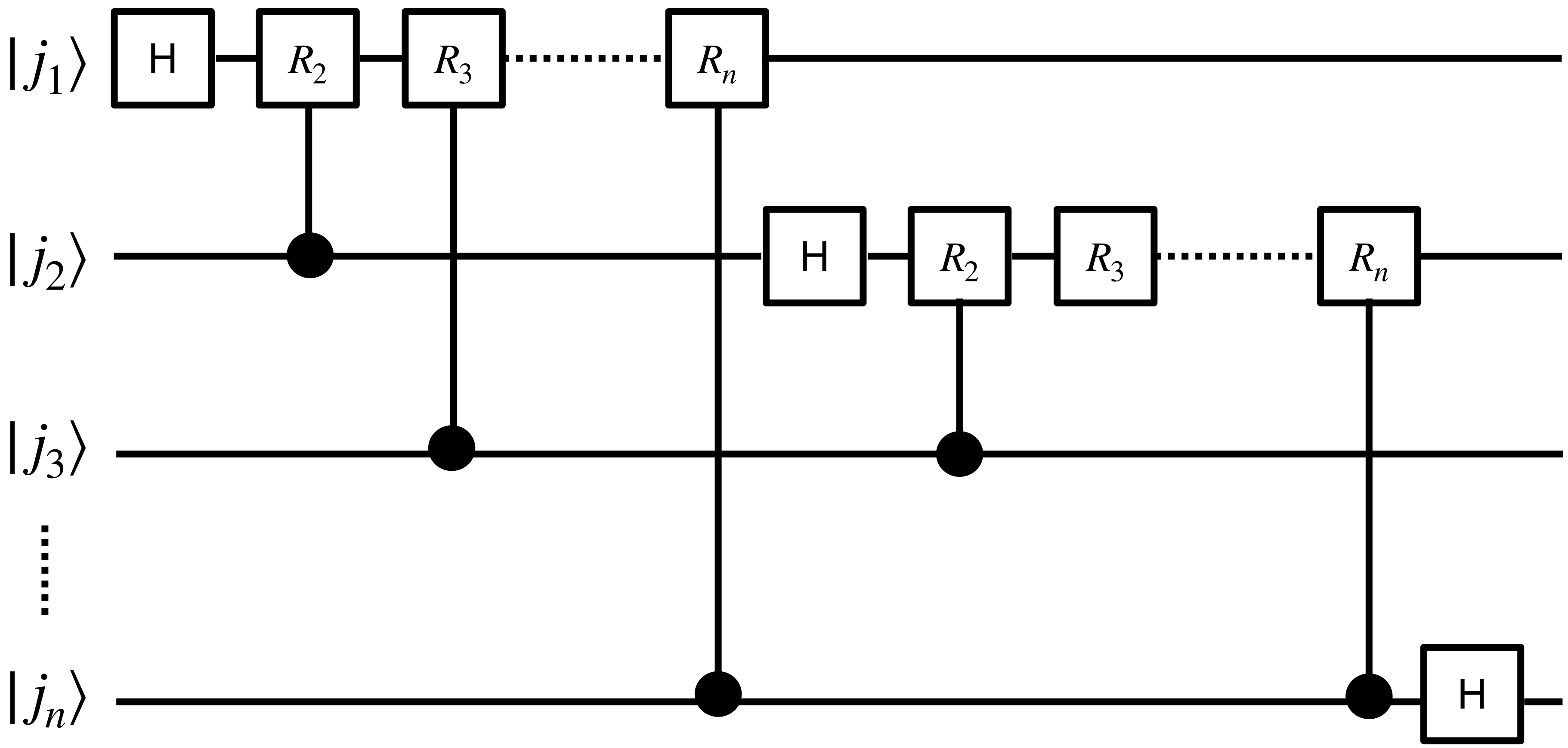
The entire procedure is repeated for all other qubits, $j_2\,, j_3\,, \cdots\ j_n$

$$\frac{1}{\sqrt{2}^n}\Big[\,|0\rangle + e^{2\pi i\, 0.j_1 \cdots j_n}\,|1\rangle\Big]\Big[\,|0\rangle + e^{2\pi i\, 0.j_2 \cdots j_n}\,|1\rangle\Big]\ \cdots\ \Big[\,|0\rangle + e^{2\pi i\, 0.j_n}\,|1\rangle\Big]$$

Use SWAP gate or relabel to obtain:
$$F\,|j\rangle = \frac{1}{\sqrt{2}^n}\bigotimes_{k=1}^{n}\left(\,|0\rangle + \exp\!\left(\frac{2\pi i j}{2^k}\right)|1\rangle\right)$$

$$\frac{1}{\sqrt{2}^n}\Big[\,|0\rangle + e^{2\pi i\, 0.j_n}\,|1\rangle\Big]\Big[\,|0\rangle + e^{2\pi i\, 0.j_2 \cdots j_n}\,|1\rangle\Big]\ \cdots\ \Big[\,|0\rangle + e^{2\pi i\, 0.j_1 \cdots j_n}\,|1\rangle\Big]$$

Quantum Circuit for QFT



$$\frac{1}{\sqrt{2}}\Big[\,|0\rangle + e^{2\pi i\,0.j_1\cdots j_n}\,|1\rangle\,\Big]$$

$$\frac{1}{\sqrt{2}}\Big[\,|0\rangle + e^{2\pi i\,0.j_2\cdots j_n}\,|1\rangle\,\Big]$$

$$\vdots$$

$$\frac{1}{\sqrt{2}}\Big[\,|0\rangle + (-1)^{j_n}\,|1\rangle\,\Big]$$

$$= \frac{1}{\sqrt{2}}\Big[\,|0\rangle + e^{2\pi i\,0.j_1}\,|1\rangle\,\Big]$$

How many gates are required?

$$\left.\begin{array}{ll} q_1\text{: H + (n-1) controlled R gates} & \rightarrow n \\ q_2\text{: H + (n-2) controlled R gates} & \rightarrow n-1 \\ \vdots & \vdots \\ q_n\text{: H + 0 controlled R gates} & \rightarrow 1 \end{array}\right\} \frac{n(n+1)}{2}$$

Also need $\mathcal{O}(n/2)$ SWAP gates

Overall scaling of QFT is $\mathcal{O}(n^2)$

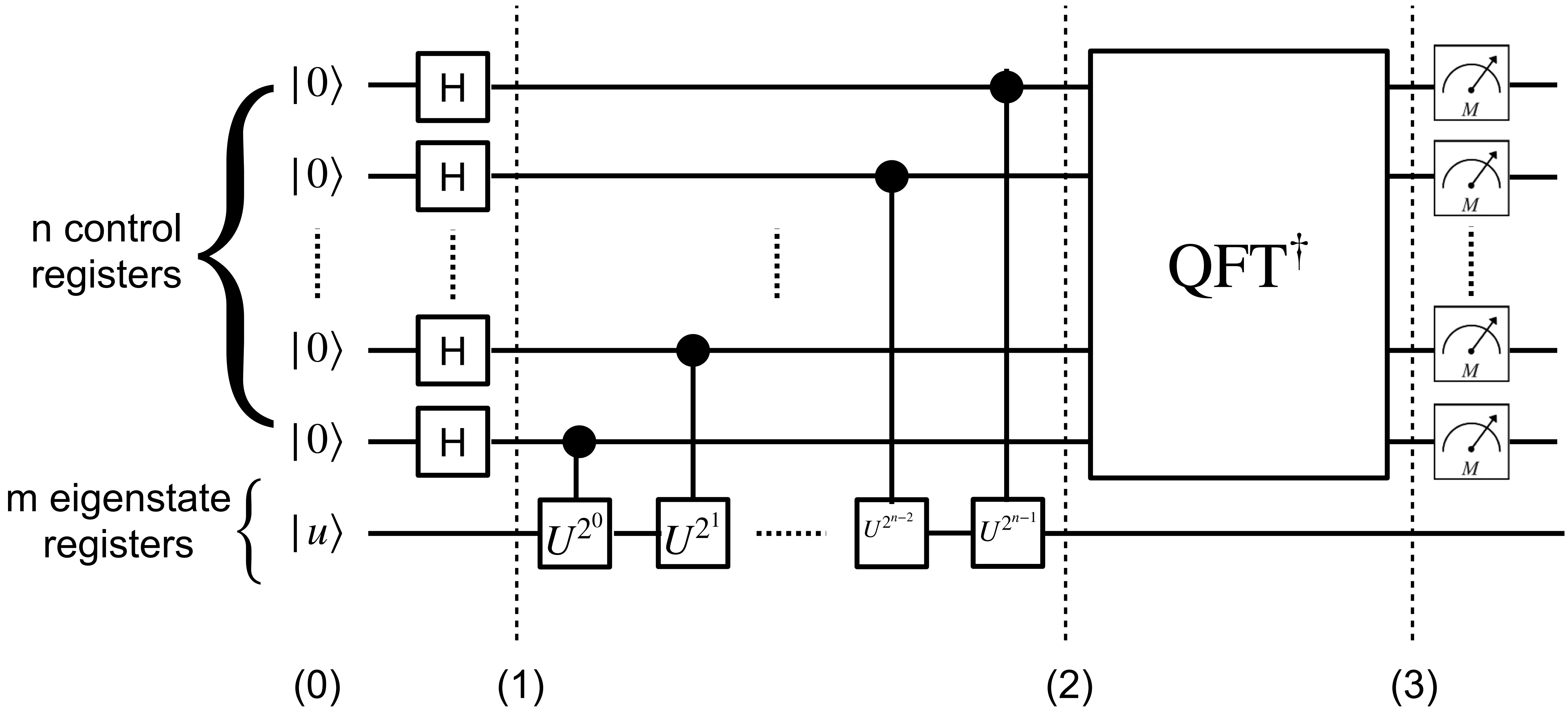
- Classical Fourier Transform scales as $\mathcal{O}(N^2) = \mathcal{O}((2^n)^2)$
- FFT: $\mathcal{O}(Nln(N))$ for $N = 2^n$

Quantum Phase Estimation and Finding Eigenvalues

- Good example of phase kickback and use of QFT
- Unitary operator $U: \;\; U|u\rangle = e^{i\phi}|u\rangle, \qquad 0 \le \phi < 2\pi$
- How to find eigenvalue? = How to measure the phase?
- How to find ϕ to a given level of precision?
- Find the best n-bit estimate of the phase ϕ

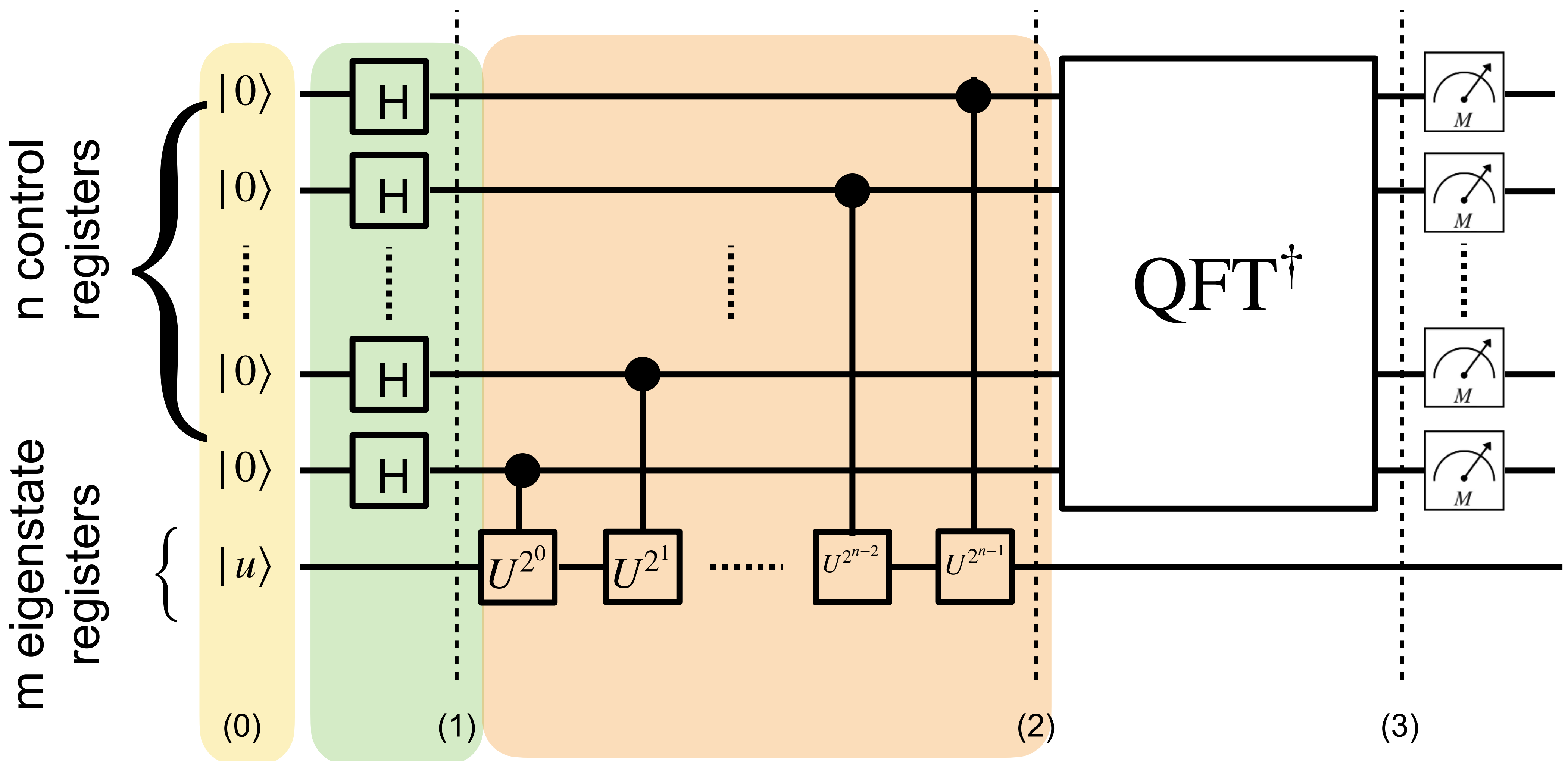
$$U^{2j}|u\rangle = \left(e^{i\phi}\right)^{2^j}|u\rangle = e^{i\phi\, 2^j}|u\rangle$$

Quantum Circuit for QPE



$$\mathrm{QPE} = H + \text{controlled} - U^{2^j} + \mathrm{QFT}^\dagger$$

Quantum Circuit for QPE



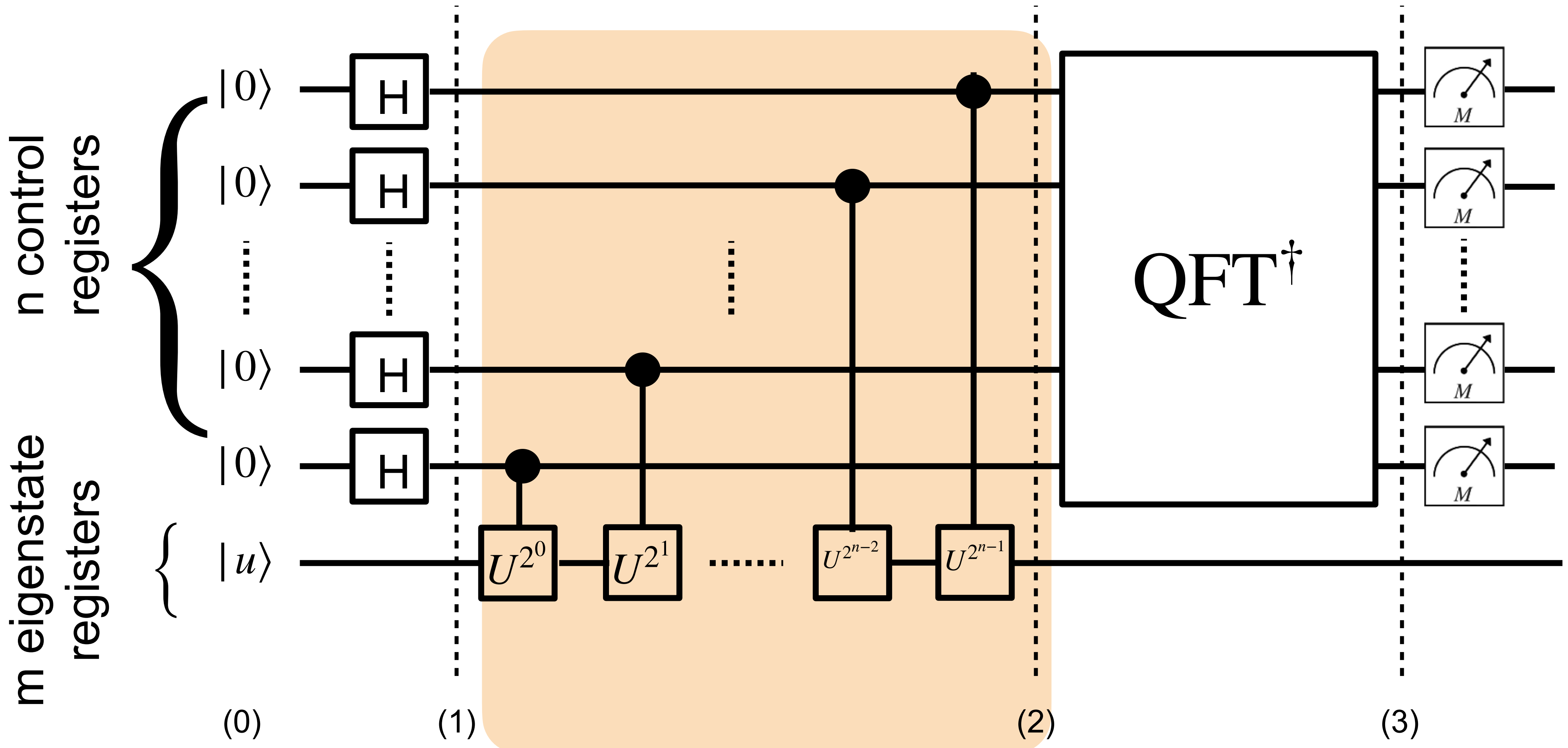
$$\mathrm{QPE} \;= H + \text{controlled} - U^{2^j} + \mathrm{QFT}^\dagger$$

$$|\psi_0\rangle = |0\rangle^{\otimes n} \otimes |u\rangle$$

$$|\psi_1\rangle = \Big(H|0\rangle\Big)^{\otimes n} \otimes |u\rangle = \frac{1}{\sqrt{2}^n}\Big(|0\rangle + |1\rangle\Big)^{\otimes n} \otimes |u\rangle$$

$$|\psi_2\rangle = \prod_{j=0}^{n-1} \mathrm{CU}^{2^j} \frac{1}{\sqrt{2}^n}\Big(|0\rangle + |1\rangle\Big)^{\otimes n} \otimes |u\rangle$$

Quantum Circuit for QPE



$$|\psi_2\rangle = \prod_{j=0}^{n-1} \mathrm{CU}^{2^j} \frac{1}{\sqrt{2}^n}\Big(|0\rangle + |1\rangle\Big)^{\otimes n} \otimes |u\rangle$$

$$U^{2j}|u\rangle = \left(e^{i\phi}\right)^{2^j}|u\rangle = e^{i\phi\, 2^j}|u\rangle$$

$$\frac{1}{\sqrt{2}}\Big(|0\rangle + |1\rangle\Big) \otimes |u\rangle \xrightarrow{\mathrm{CU}^{2^j}} \frac{1}{\sqrt{2}}\Big(|0\rangle \otimes |u\rangle + U^{2^j}|1\rangle \otimes |u\rangle\Big)$$

$$= \frac{1}{\sqrt{2}}\Big(|0\rangle + e^{i\phi\, 2^j}|1\rangle\Big) \otimes |u\rangle$$

Quantum Circuit for QPE

$$|\psi_2\rangle = \frac{1}{\sqrt{2}^n}\Big(|0\rangle + e^{i\phi\,2^{n-1}}|1\rangle\Big)\Big(|0\rangle + e^{i\phi\,2^{n-2}}|1\rangle\Big)\cdots\Big(|0\rangle + e^{i2\phi}|1\rangle\Big)\Big(|0\rangle + e^{i\phi}|1\rangle\Big)\otimes|u\rangle$$

$$= \frac{1}{\sqrt{2}^n}\sum_{y=0}^{2^n-1}\underbrace{e^{i\phi y}}\,|y\rangle\otimes|u\rangle$$

Phase kick-back: phase factor $e^{i\phi y}$ has been propagated back from the second eigenstate register to the first control register

$$\mathrm{QFT}\,|a\rangle = \frac{1}{\sqrt{2}^n}\sum_{k=0}^{2^n-1} e^{2\pi i a/2^n}\,|k\rangle \longrightarrow \frac{2\pi i a}{2^n} = i\phi \longrightarrow \boxed{\phi = 2\pi\Big(\frac{a}{2^n}+\delta\Big)}$$

$$a = a_{n-1}a_{n-2}\cdots a_0$$

- $\frac{2\pi a}{2^n}$ is the best n-bit binary approximation of ϕ .
- $0 \le |\delta| \le \frac{1}{2^{n+1}}$ is the associated error.

$$\mathrm{QFT}^{-1}|y\rangle = \frac{1}{\sqrt{2}^n}\sum_{x=0}^{2^n-1} e^{-2\pi i x y/2^n}\,|x\rangle$$

$$|\psi_3\rangle = \mathrm{QFT}^{-1}|\psi_2\rangle = \frac{1}{2^n}\sum_{x=0}^{2^n-1}\sum_{y=0}^{2^n-1} e^{2\pi i (a-x)y/2^n}\, e^{2\pi i \delta y}\,|x\rangle\otimes|u\rangle$$

Operate only n control register.

Quantum Circuit for QPE

$$|\psi_3\rangle = \mathrm{QFT}^{-1}|\psi_2\rangle = \frac{1}{2^n}\sum_{x=0}^{2^n-1}\sum_{y=0}^{2^n-1} e^{2\pi i(a-x)y/2^n} e^{2\pi i\delta y}|x\rangle\otimes|u\rangle$$

Operate only n control register.

(1) If $\delta = 0$, $\quad \frac{1}{2^n}\sum_{y=0}^{2^n-1}\exp\left(\frac{2\pi i(a-x)y}{2^n}\right) = \delta_{ax} \longrightarrow |\psi_3\rangle = |a\rangle\otimes|u\rangle \longrightarrow \phi = \frac{2\pi a}{2^n}$

(2) If $\delta \neq 0$, Measuring 1st register and getting the state $|x\rangle = |a\rangle$ is the best n-bit estimate of ϕ. The corresponding probability is $P_a = |C_a|^2 \geq \frac{4}{\pi^2} \approx 0.405$

Quantum Circuit for QPE

$$|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} e^{2\pi i x\phi} |x\rangle \otimes |u\rangle$$

$$\mathrm{QFT}^{-1}|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{-2\pi i x y/2^n} |y\rangle$$

$$|\psi_3\rangle = \mathrm{QFT}^{-1}|\psi_2\rangle = \frac{1}{2^n} \sum_{x=0}^{2^n-1} \sum_{y=0}^{2^n-1} e^{2\pi i x(\phi - y/2^n)} |y\rangle \otimes |u\rangle$$

Probability of observing $|y\rangle$ = $P(y) = \left| \frac{1}{2^n} \sum_{x=0}^{2^n-1} e^{2\pi i x(\phi - y/2^n)} \right|^2 = \frac{1}{2^{2n}} \left| \frac{1 - r^{2^n}}{1 - r} \right|^2, \quad r \equiv \exp\left[2\pi i \left(\phi - \frac{y}{2^n}\right)\right]$

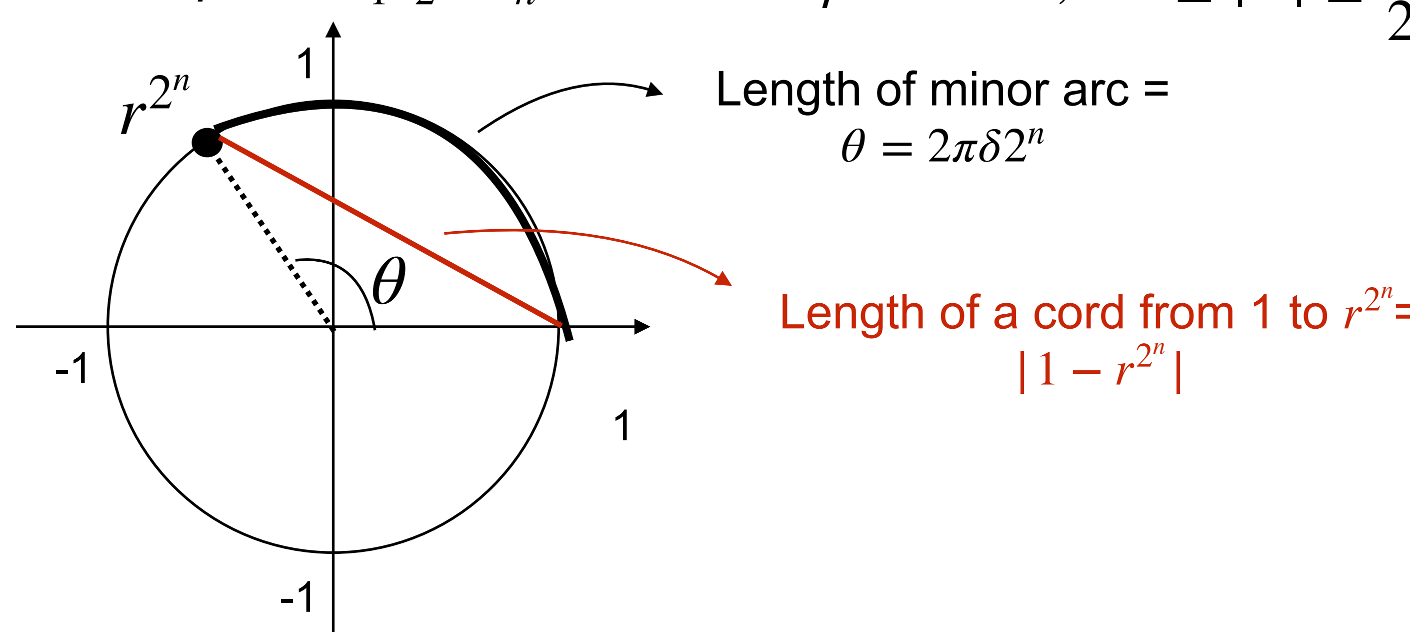
(1) If $\phi = \frac{y}{2^n}$, $\quad |\psi_3\rangle = |y\rangle \otimes |u\rangle \quad P(\phi = \frac{y}{2^n}) = 100\,\%$

(2) If $\phi \neq \frac{y}{2^n}$, $\quad$ closest n − bit approximation to $\phi = 0.\nu_1\nu_2\cdots\nu_n = \equiv \nu \qquad \phi - \nu \equiv \delta, \quad 0 \le |\delta| \le \frac{1}{2^{n+1}}$

$$r \equiv \exp\left[2\pi i \left(\phi - \frac{y}{2^n}\right)\right] = \exp(2\pi i \delta)$$

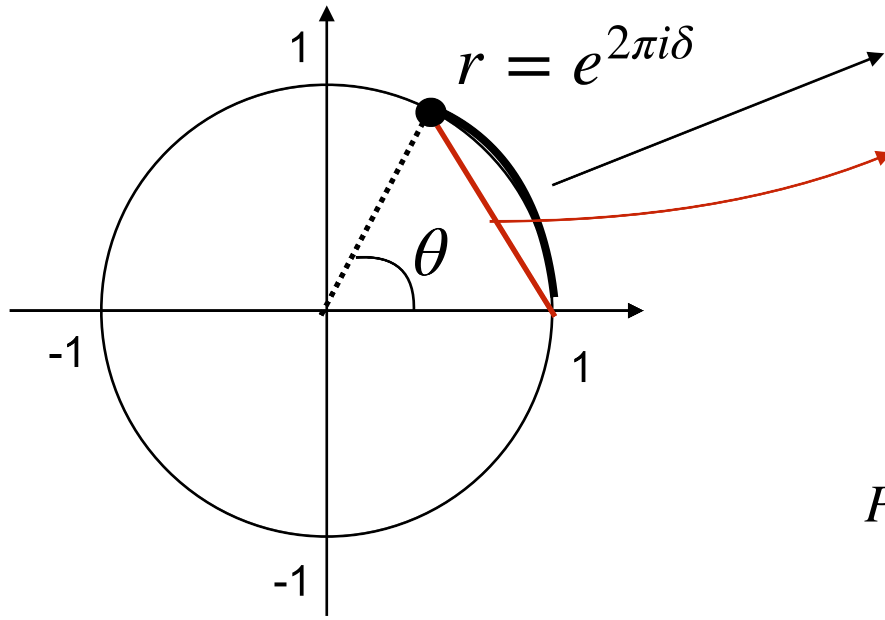
$$P(y) = \frac{1}{2^{2n}} \left| \frac{1 - r^{2^n}}{1 - r} \right|^2,$$

$$r^{2^n} = \left[\exp(2\pi i \delta)\right]^{2^n} = \exp(2\pi i \delta 2^n) = e^{i\theta}$$



$$\frac{\text{length of minor arc}}{\text{length of cord}} = \frac{2\pi\delta 2^n}{|1 - r^{2^n}|} \le \frac{\text{half circumference}}{\text{diameter}} \le \frac{\pi R}{2R} = \frac{\pi}{2} \longrightarrow |1 - r^{2^n}| \ge 4\delta 2^n$$

Quantum Circuit for QPE



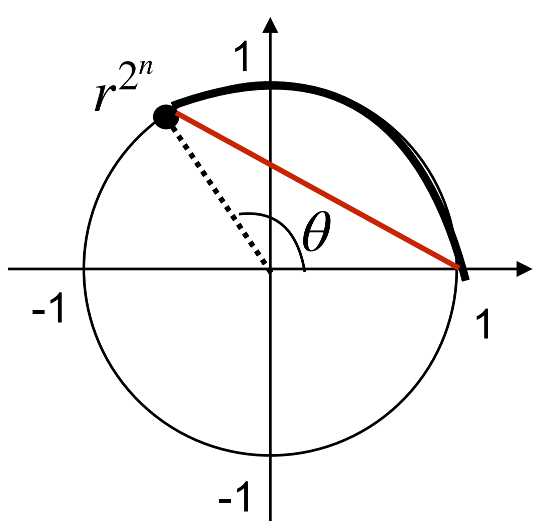
Length of minor arc = $\theta = 2\pi\delta 2^n$

Length of a cord from 1 to $r = |1-r|$

$$\frac{\text{length of minor arc}}{\text{length of cord}} = \frac{2\pi\delta}{|1-r|} > 1\,, \qquad |1-r| < 2\pi\delta$$

$$P(y) = \frac{1}{2^{2n}}\left|\frac{1-r^{2^n}}{1-r}\right|^2 \geq \frac{1}{2^{2n}}\left(\frac{4\delta 2^n}{2\pi\delta}\right)^2 = \frac{4}{\pi^2} > 0.405$$

- We will get the correct answer with probability greater than a constant.
- Probability of getting incorrect outcome can be calculated using $|\delta| > \frac{1}{2^{n+1}}$



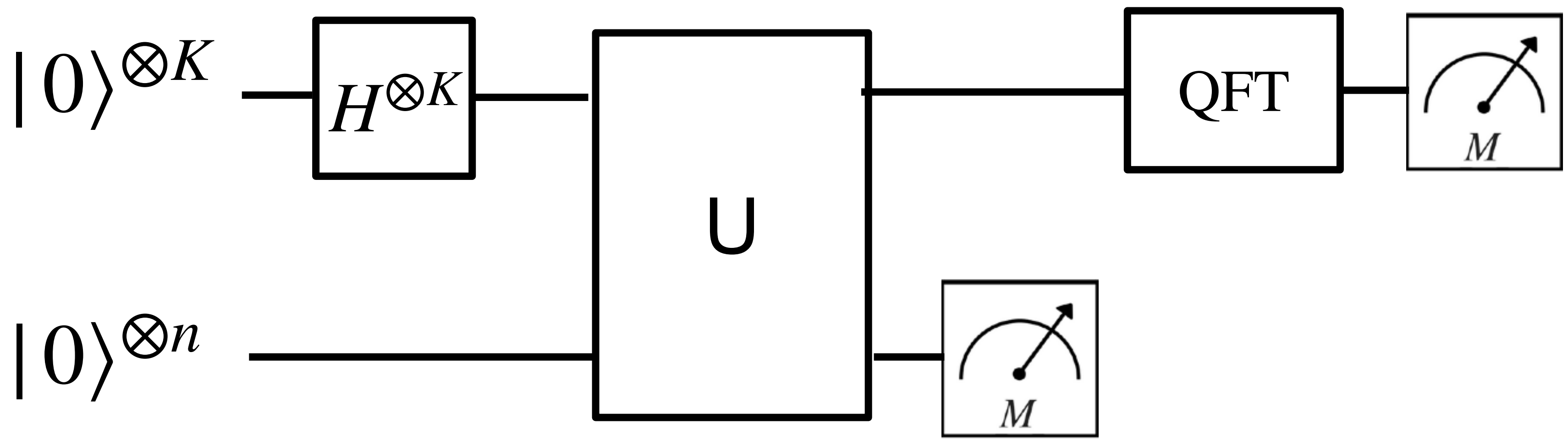
$$|1-r^{2^n}| < 2 \qquad \frac{\text{length of minor arc}}{\text{length of cord}} = \frac{2\pi\delta}{|1-r|} < \frac{\pi}{2}\,, \qquad |1-r| > 4\pi\delta$$

$$P(y) = \frac{1}{2^{2n}}\left|\frac{1-r^{2^n}}{1-r}\right|^2 \leq \frac{1}{2^{2n}}\left(\frac{2}{4\delta}\right)^2 = \frac{1}{2^{2n}(2\delta)^2}$$

If $\delta = \frac{c}{2^n}$, $P(c) \leq \frac{1}{4c^2}$

- N-bit estimate of phase ϕ is obtained with a high probability.
- Need to repeat the calculation multiple times.
- Increasing n will increase the probability of success (not obvious but true).
- Increasing n (# of qubits) will improve the precision of the phase estimate.

Shor's algorithm



$y = f(x) = a^x \pmod{\mathrm{N}}$

Discrete Logarithm Problem

- All standard public key encryption system and digital signature schemes are based on either factoring or discrete logarithm problem.
- $\mathbb{Z}_p^*$: group of integers $\{1, 2, \cdots, p-1\}$ under multiplication modulo p.
  - b: generator of $\mathbb{Z}_p^*$ (any b relatively prime to $p-1$ will work)
  - The discrete logarithm of $y \in \mathbb{Z}_p^*$ with respect to base b is the element $x \in \mathbb{Z}_p^*$ such that $b^x = y \pmod{p}$.
- Discrete logarithm problem: Given a prime p, a base $b \in \mathbb{Z}_p^*$ and an arbitrary element $y \in \mathbb{Z}_p^*$, find an $x \in \mathbb{Z}_p^*$ such that $b^x = y \pmod{p}$
  - Find the discrete logarithm of $y \in \mathbb{Z}_p^*$ with respect to base b such that $b^x = y \pmod{p}$
  - For a large p, this problem is computationally difficult to solve.
  - It is a special case of Abelian hidden subgroup problem.
  - Can be generalized to arbitrary finite cyclic groups.

Quantum Error Correction

- quant-ph/9705052, Stabilizer codes and quantum error correction, Caltech PhD thesis by D. Gottesman
- John Preskill
  - Quantum Computation
  - http://theory.caltech.edu/~preskill/ph229/

Simple Classical (Bitflip) Error Correction

- Classically error correction is not necessary
  - Hardware for one bit is huge on an atomic scale
  - State 0 and 1 are so different that the probability of an unwanted flip is tiny.
- Error correction is needed for transmitting signal over long distance where it attenuates and can be corrupted by noise.
- Suppose we send one bit through a channel.
- Use redundancy:

$$|0\rangle \longrightarrow |000\rangle$$
$$|1\rangle \longrightarrow |111\rangle$$

called codewords

- Apply majority rule:

$$\{000,001,010,100\} \rightarrow 0$$
$$\{111,110,101,011\} \rightarrow 1$$

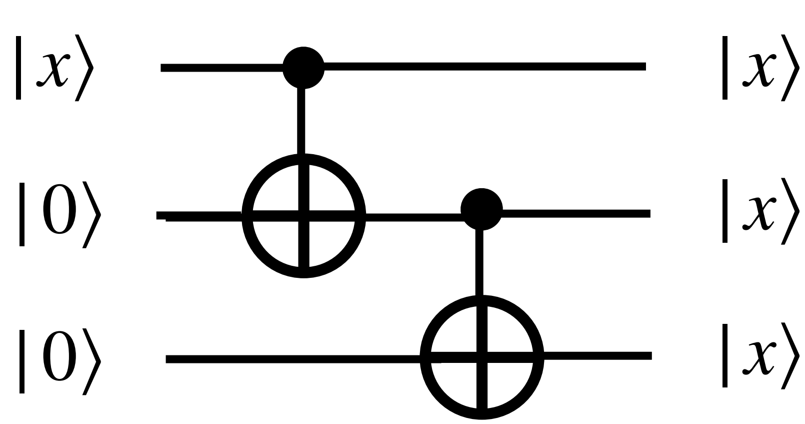
- Flip probability is p: $p^3 + 3(1-p)p^2 = 3p^2 - 2p^3 \leq p, \text{ if } p < 1/2$

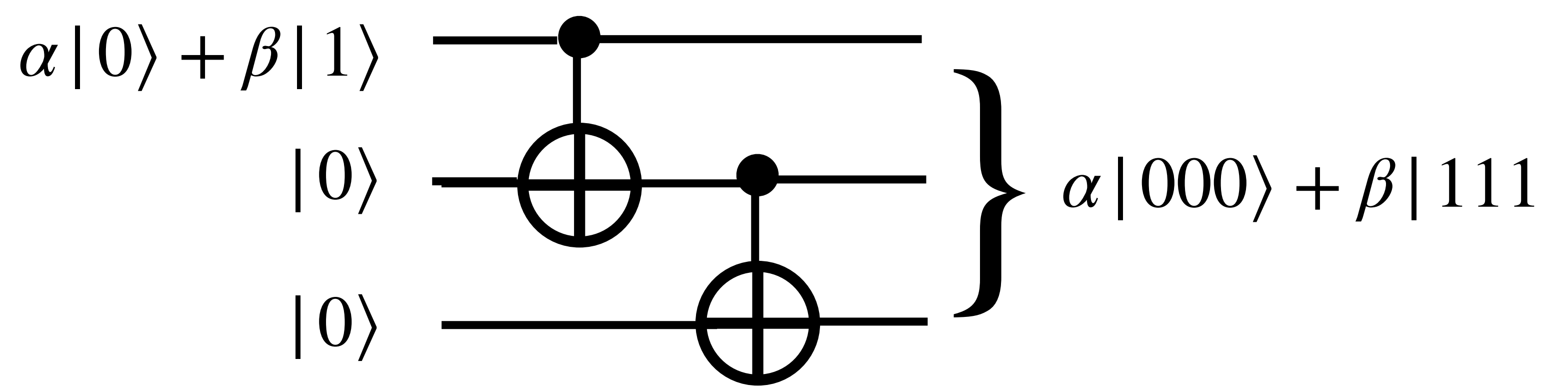
Quantum Error Correction

- QEC is essential and QC requires error correction
  - Physical system for a single qubit is small (often on an atomic scale) so any small external interference can disrupt the quantum system
- Measurement destroys quantum information
  - Checking for error is problematic.
  - Monitoring means measuring which would alter quantum states
- More general types of error can occur
  - (ex) phase error: $\frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big) \longrightarrow \frac{1}{\sqrt{2}}\big(|0\rangle + e^{i\phi}|1\rangle\big)$
- Errors are continuous
  - Unlike all or nothing bit flip errors for classical bits, errors ion qubits can grow continuously out of the uncorrupted state.

Bit Flip Error Correction

- If the error rate is low, we hope to correct them by tailing the number of qubits as the classical case.





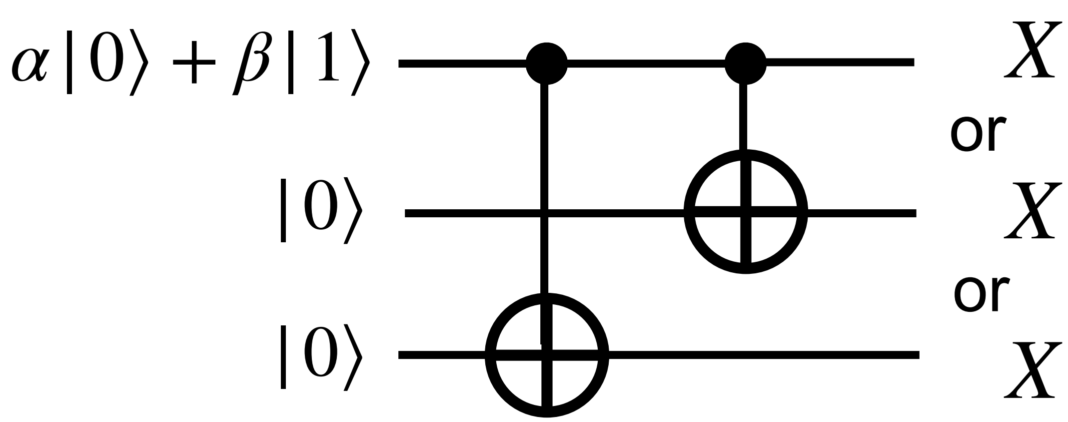
$\alpha|0\rangle+\beta|1\rangle \longrightarrow \alpha|000\rangle+\beta|111\rangle$ is not a clone of the input state

$$\left(\alpha|0\rangle+\beta|1\rangle\right)^{\otimes 3}=\alpha^3|000\rangle+\alpha^2\beta(|001\rangle+|010\rangle+|100\rangle)$$

$$+\alpha\beta^2(|110\rangle+|101\rangle+|011\rangle)+\beta^3|111\rangle$$

Bit Flip Error Correction

- Assume that no more than one qubit is flipped (reasonable approximation if the error rate is small)



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

$$|\psi_1\rangle = \alpha|100\rangle + \beta|011\rangle = X_1|\psi\rangle \quad \text{qubit 1 flipped}$$

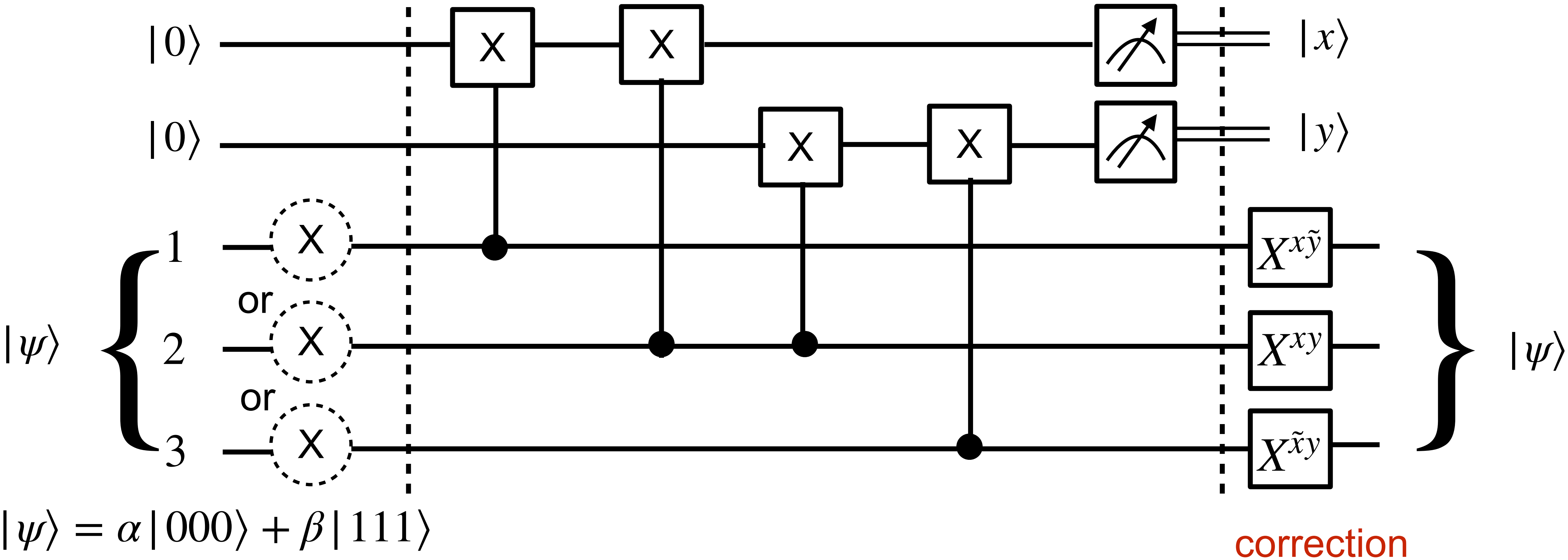
$$|\psi_2\rangle = \alpha|010\rangle + \beta|101\rangle = X_2|\psi\rangle \quad \text{qubit 2 flipped}$$

$$|\psi_3\rangle = \alpha|001\rangle + \beta|110\rangle = X_3|\psi\rangle \quad \text{qubit 3 flipped}$$

$\longrightarrow$ four states are called “syndromes”

- Classically to determine if one of the bits is flipped, we just have to look at them. However quantum mechanically, if we measure $|\psi\rangle$, we get $|000\rangle$ with probability $|\alpha|^2$ and $|111\rangle$ with $|\beta|^2$ which destroys the coherent superposition.
- Need to couple the codeword qubits to ancilla qubits and measure those, which does not destroy the coherent superposition.

Bit Flip Error Correction



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

$|\psi\rangle$: codeword $|000\rangle$ $\rightarrow$ no ancilla flipped $\rightarrow$ $x = 0 = y$

codeword $|000\rangle$ $\rightarrow$ both ancillas flipped $\rightarrow$ $x = 0 = y$

$|\psi_1\rangle$: codeword $|100\rangle$ $\rightarrow$ x flipped, y not flipped $\rightarrow$ $x = 1,\ y = 0$

codeword $|011\rangle$ $\rightarrow$ x flipped, y flipped twice $\rightarrow$ $x = 1,\ y = 0$

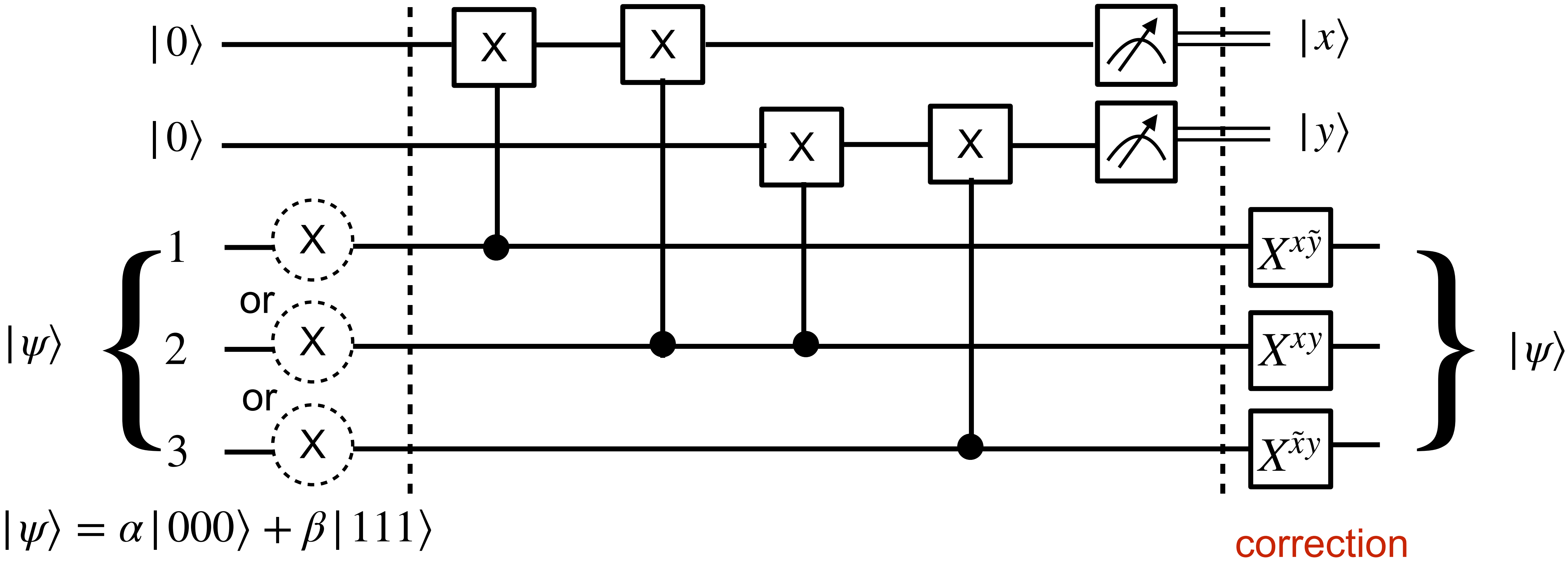
$|\psi_2\rangle$: codeword $|010\rangle$ $\rightarrow$ x and y flipped once $\rightarrow$ $x = 1 = 1$

codeword $|101\rangle$ $\rightarrow$ x and y flipped once $\rightarrow$ $x = 1 = 1$

$|\psi_3\rangle$: codeword $|001\rangle$ $\rightarrow$ x not flipped, y flipped $\rightarrow$ $x = 0,\ y = 1$

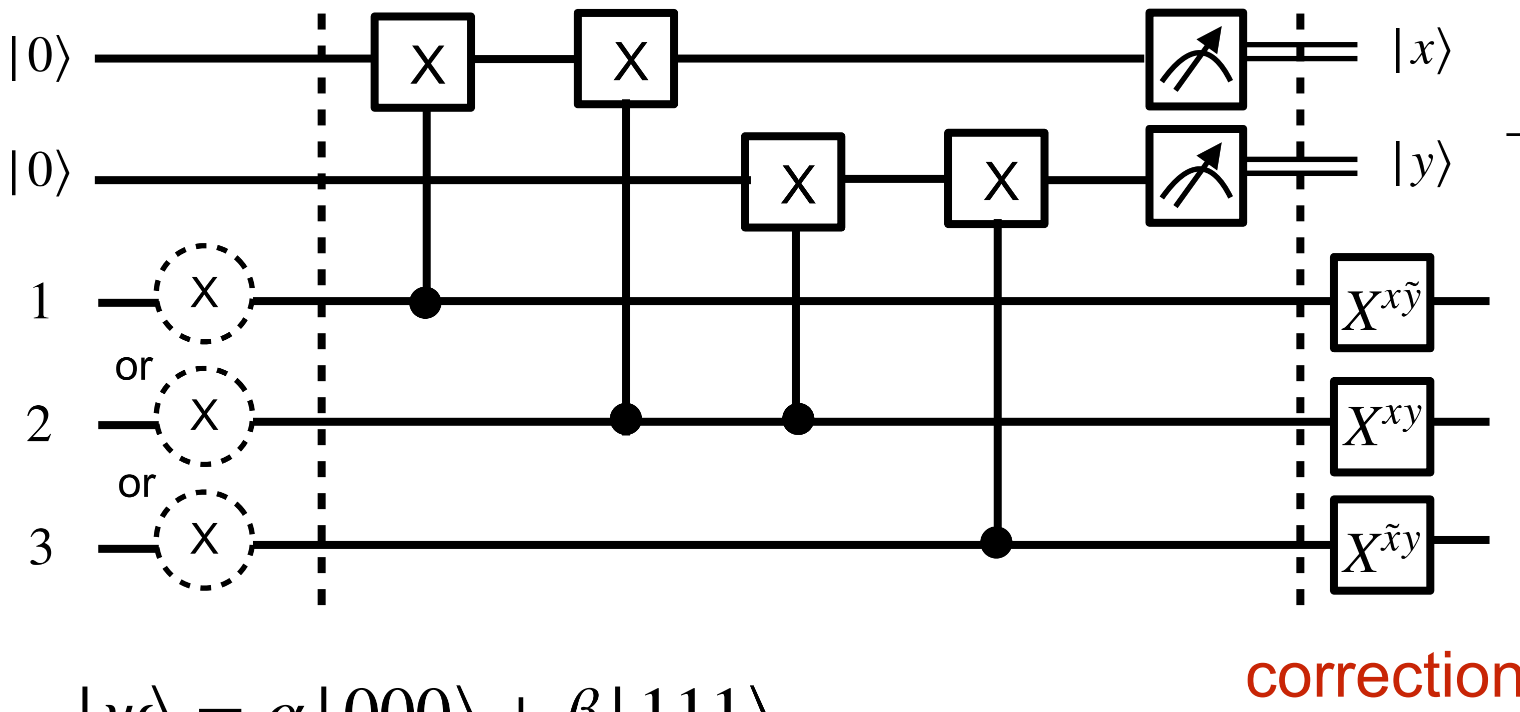
codeword $|110\rangle$ $\rightarrow$ x flipped twice, y flipped $\rightarrow$ $x = 0,\ y = 1$

Bit Flip Error Correction



Syndromes	Bit flipped	x	y
$\|\psi\rangle = \alpha\|000\rangle + \beta\|111\rangle$	None	0	0
$\|\psi_1\rangle = \alpha\|100\rangle + \beta\|011\rangle$	1	1	0
$\|\psi_2\rangle = \alpha\|010\rangle + \beta\|101\rangle$	2	1	1
$\|\psi_3\rangle = \alpha\|001\rangle + \beta\|110\rangle$	3	0	1

Bit Flip Error Correction



Syndromes	Bit flipped	x	y
$\|\psi\rangle = \alpha\|000\rangle + \beta\|111\rangle$	None	0	0
$\|\psi_1\rangle = \alpha\|100\rangle + \beta\|011\rangle$	1	1	0
$\|\psi_2\rangle = \alpha\|010\rangle + \beta\|101\rangle$	2	1	1
$\|\psi_3\rangle = \alpha\|001\rangle + \beta\|110\rangle$	3	0	1

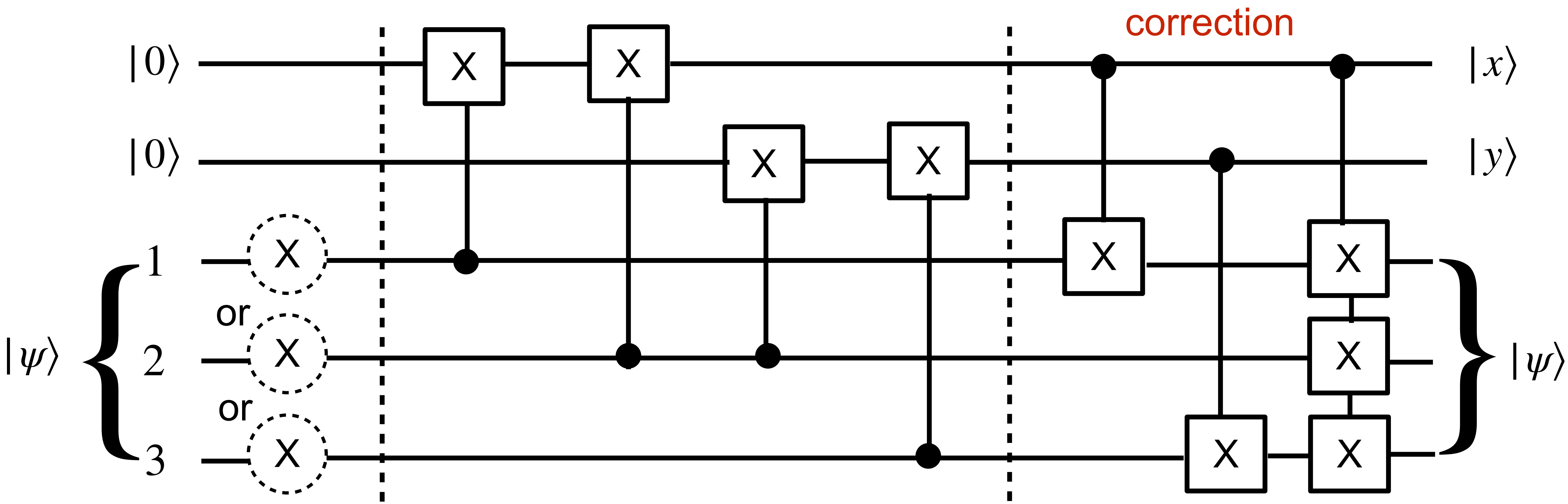
$$|\psi\rangle = \alpha|000\rangle + \beta|111\rangle$$

$X^{x\tilde{y}}$ gate on qubit 1, only if x=1 and y=0 $\rightarrow$ correcting $|\psi_1\rangle$

X^{xy} gate on qubit 2, only if x=1 and y=1 $\rightarrow$ correcting $|\psi_2\rangle$

$X^{\tilde{x}y}$ gate on qubit 3, only if x=0 and y=0 $\rightarrow$ correcting $|\psi_3\rangle$

Bit Flip Error Correction



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

$X^{x\tilde{y}}$ gate on qubit 1, only if x=1 and y=0 $\rightarrow$ correcting $|\psi_1\rangle$

X^{xy} gate on qubit 2, only if x=1 and y=1 $\rightarrow$ correcting $|\psi_2\rangle$

$X^{\tilde{x}y}$ gate on qubit 3, only if x=0 and y=0 $\rightarrow$ correcting $|\psi_3\rangle$

- What if errors in quantum circuits can arise continuously from zero? (Assume the error rate is small)

$$|\psi\rangle \quad \longrightarrow \quad \left[1 + \left(\epsilon_1 X_1 + \epsilon_2 X_2 + \epsilon_3 X_3\right)\right] |\psi\rangle \qquad\qquad \epsilon_i \in \mathbb{C}\,,\ |\epsilon_i| \ll 1$$

Stabilizer Formalism

- Useful method for error correction of arbitrary error.
- Consider two Hermitian operators, Z_1Z_2 and Z_2Z_3

$$Z_i^2 = I_{2\times2} \qquad Z_1Z_2 = Z_2Z_1 \qquad (Z_1Z_2)^2 = I_{2\times2} \qquad (Z_2Z_3)^2 = I_{2\times2}$$

$$\longrightarrow \quad A^2 = I_{2\times2} \quad \longrightarrow \quad \text{eigenvalues} = \pm 1 \qquad Ax = \lambda x \qquad A^2x = \lambda^2 x = x \qquad \lambda^2 = 1$$

$$\longrightarrow \quad [Z_1Z_2, Z_2Z_3] = 0 \qquad Z_1Z_3 \text{ and } Z_2Z_3 \text{ have the same eigenvectors.}$$

Syndromes	Z_1Z_2	Z_2Z_3	x	y
$\vert\psi\rangle = \alpha\vert 000\rangle + \beta\vert 111\rangle$	1	1	0	0
$\vert\psi_1\rangle = \alpha\vert 100\rangle + \beta\vert 011\rangle = X_1\vert\psi\rangle$	-1	1	1	0
$\vert\psi_2\rangle = \alpha\vert 010\rangle + \beta\vert 101\rangle = X_2\vert\psi\rangle$	-1	-1	1	1
$\vert\psi_3\rangle = \alpha\vert 001\rangle + \beta\vert 110\rangle = X_3\vert\psi\rangle$	1	-1	0	1

$$Z_1Z_2 = (-1)^x$$

$$Z_2Z_3 = (-1)^y$$

- Syndromes are eigenvectors of Z_1Z_2 and Z_2Z_3.
- Stabilizers are operators whose eigenvalues distinguish the different syndromes.

Properties of Stabilizers and Syndromes

- Syndromes are eigenvectors of $Z_1 Z_2$ and $Z_2 Z_3$.
- Stabilizers are operators whose eigenvalues distinguish the different syndromes.
- Eigenvalues of a stabilizer in a syndrome is +1 or -1.
- Eigenvalues of all stabilizers are +1 in the uncorrupted syndrome $|\psi\rangle$.
- Operators for the stabilizers are built out of the single qubit operators Z_i and X_i.
- Syndromes with a single qubit error are obtained by acting on the uncorrupted syndrome with X_i, Y_i and Z_i operators.
- For a general stabilizer A_α and a syndrome state $|\psi_\beta\rangle = B_\beta|\psi\rangle$, A_α either commutes or anti-commutes with B_β.
  - B_β involves a single Pauli's operator (X, Y or Z).
  - A_α involves a product of Pauli's operators (X's, and Z's b/c $Y = iXZ$).

Properties of Stabilizers and Syndromes

- If $[A_\alpha, B_\beta] = 0,\ A_\alpha|\psi_\beta\rangle = +1|\psi_\beta\rangle$ and eigenvalue of the stabilizer A_α in state $|\psi_\beta\rangle$ is +1.

  $-A_\alpha|\psi\rangle = A_\alpha B_\beta|\psi\rangle = B_\beta A_\alpha|\psi\rangle = B_\beta|\psi\rangle = |\psi\rangle$
- If $\{A_\alpha, B_\beta\} = 0,\ A_\alpha|\psi_\beta\rangle = -1|\psi_\beta\rangle$

  $-A_\alpha|\psi\rangle = A_\alpha B_\beta|\psi\rangle = -B_\beta A_\alpha|\psi\rangle = -B_\beta|\psi\rangle = -|\psi\rangle$
- Syndromes must be eigenvectors of all stabilizers → stabilizers must commute each other
- How to determine efficiently if a stabilizer commutes or anti-commutes with the operator which generates a corrupted syndrome out of the uncorrupted syndrome?
- For the case of 3-qubit bit-flip code, stabilizers are Z_1Z_2 and Z_2Z_3.
- Operators which generate the corrupted syndromes from the uncorrupted syndrome: X_1, X_2 and X_3.

Properties of Stabilizers and Syndromes

- How to determine efficiently if a stabilizer commutes or anti-commutes with the operator which generates a corrupted syndrome out of the uncorrupted syndrome?
- For the case of 3-qubit bit-flip code, stabilizers are Z_1Z_2 and Z_2Z_3.
- Operators which generate the corrupted syndromes from the uncorrupted syndrome: X_1, X_2 and X_3.
  - X_1 commutes with $Z_2Z_3 \longleftrightarrow [X_1, Z_2Z_3] = 0.$ $\because$ no sites in common
    $\rightarrow \; Z_2Z_3\,|\psi_1\rangle = +1\,|\psi_1\rangle$
  - X_2 has one common site with Z_2Z_3. $\;\rightarrow\; X_2Z_2Z_3 = -Z_2X_2Z_3 = -Z_2Z_3X_2$
    $\rightarrow \; \{X_1, Z_2Z_3\} = 0 \rightarrow \; Z_2Z_3\,|\psi_2\rangle = -\,|\psi_2\rangle$

Stabilizer Formalism

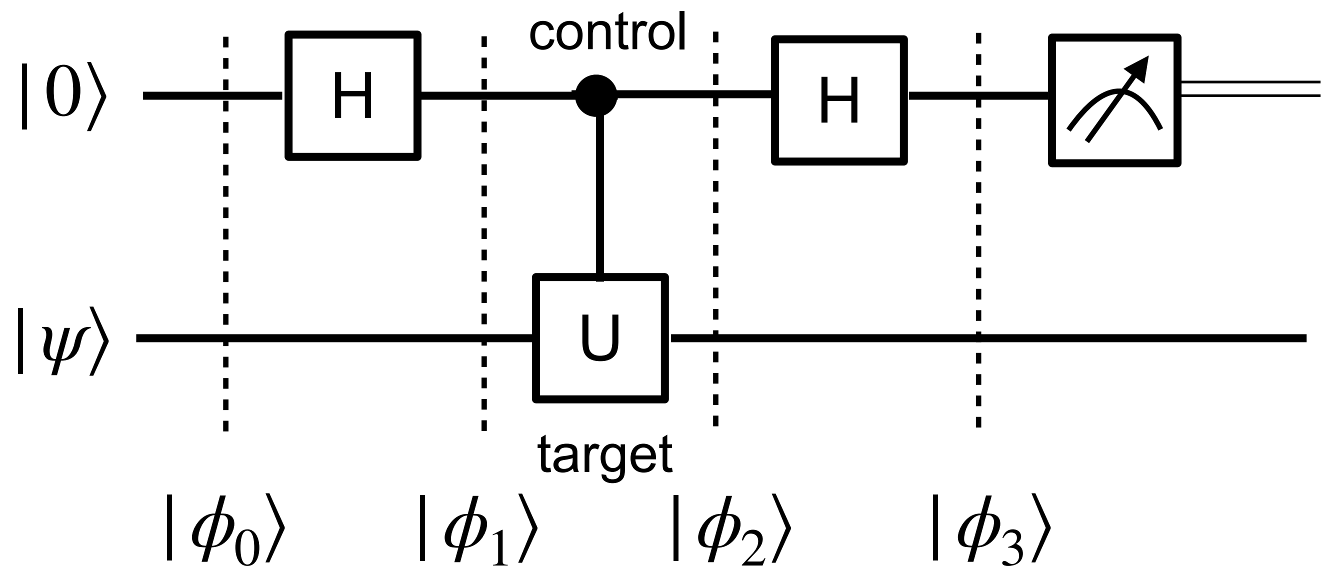
- In the stabilizer formalism, we need to construct a set of Hermitian operators (stabilizers) which satisfy the following properties
  - They square to 1 (so eigenvalues are ± 1).
  - They mutually commute (so they have the same eigenvectors).
  - The syndromes are eigenstates.
  - The uncorrupted syndrome has eigenvalue +1 for all stabilizers.
  - The set of ± 1 eigenvalues of the stabilizers uniquely specifies the syndrome.
  - Whether the eigenvalue is +1 or -1 is easily determined from the commutation properties of the stabilizer with respect to the operator which generate the corruption in the syndrome.

Stabilizer Formalism: Circuits

- Circuit which will measure the eigenvalues of stabilizers and hence determine which syndromes have occurred.

$$U = U^\dagger$$

$$U|\psi_\pm\rangle = \pm|\psi_\pm\rangle$$



$$|\psi\rangle \equiv \alpha_+|\psi_+\rangle + \alpha_-|\psi_-\rangle$$

$$|\phi_0\rangle = |0\rangle \otimes |\psi\rangle = \alpha_+|0\psi_+\rangle + \alpha_-|0\psi_-\rangle$$

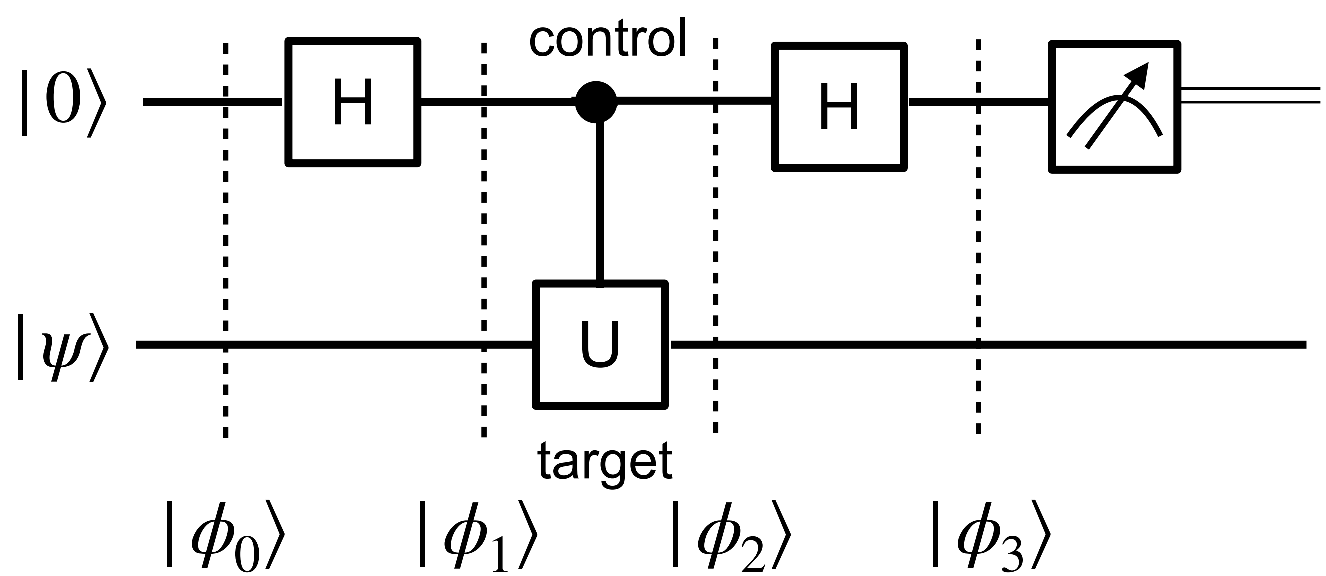
$$|\phi_1\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big) \otimes |\psi\rangle = \frac{\alpha_+}{\sqrt{2}}\Big[|0\psi_+\rangle + |1\psi_+\rangle\Big] + \frac{\alpha_-}{\sqrt{2}}\Big[|0\psi_-\rangle + |1\psi_-\rangle\Big]$$

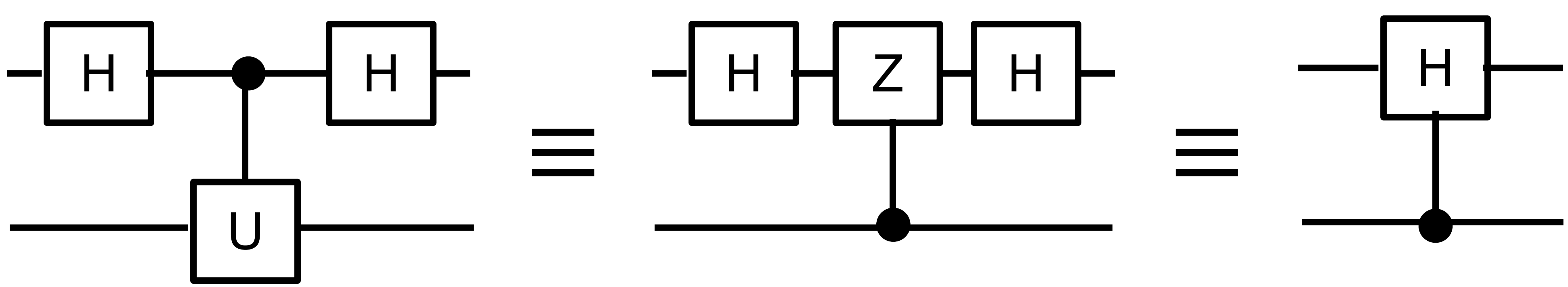
$$|\phi_2\rangle = \frac{\alpha_+}{\sqrt{2}}\Big(|0\psi_+\rangle + |1\psi_+\rangle\Big) + \frac{\alpha_-}{\sqrt{2}}\Big(|0\psi_-\rangle - |1\psi_-\rangle\Big)$$

$$|\phi_3\rangle = \alpha_+|0\psi_+\rangle + \alpha_-|1\psi_-\rangle$$

Stabilizer Formalism: Circuits

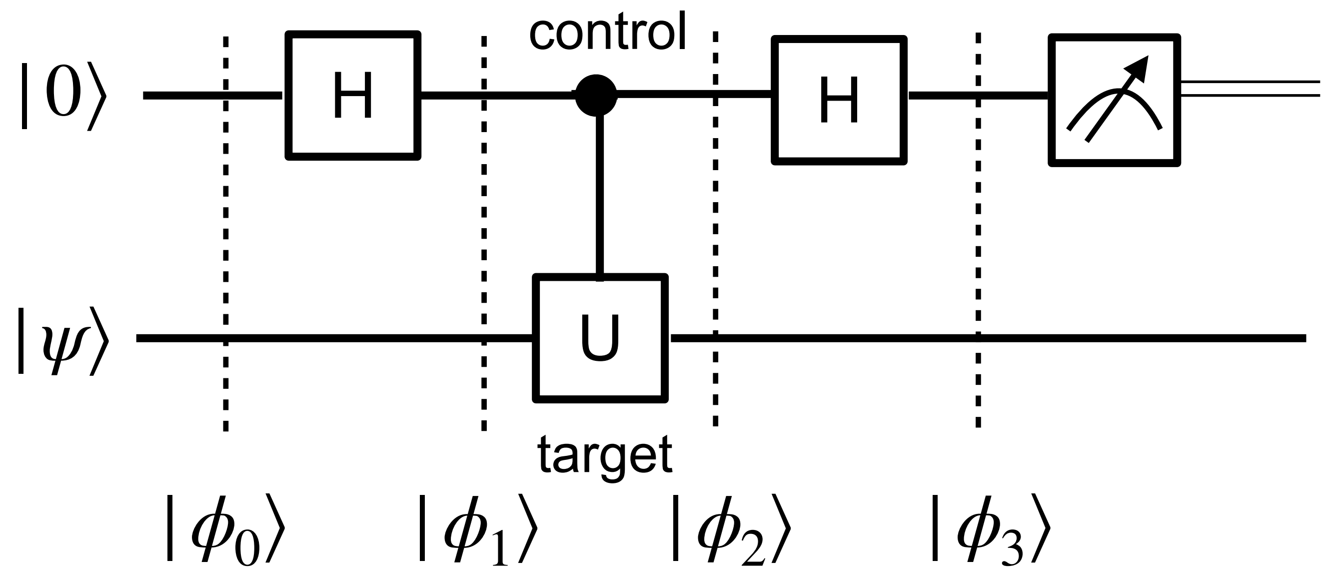
- If a measurement of the upper qubit gives $|0\rangle$ (with probability $|\alpha_+|^2$), the lower qubit will be in state $|\psi_+\rangle$.
- If a measurement of the upper qubit gives $|1\rangle$ (with probability $|\alpha_-|^2$), the lower qubit will be in state $|\psi_-\rangle$.
- ∴ control bit tells us which eigenstates of U the target qubit is in.



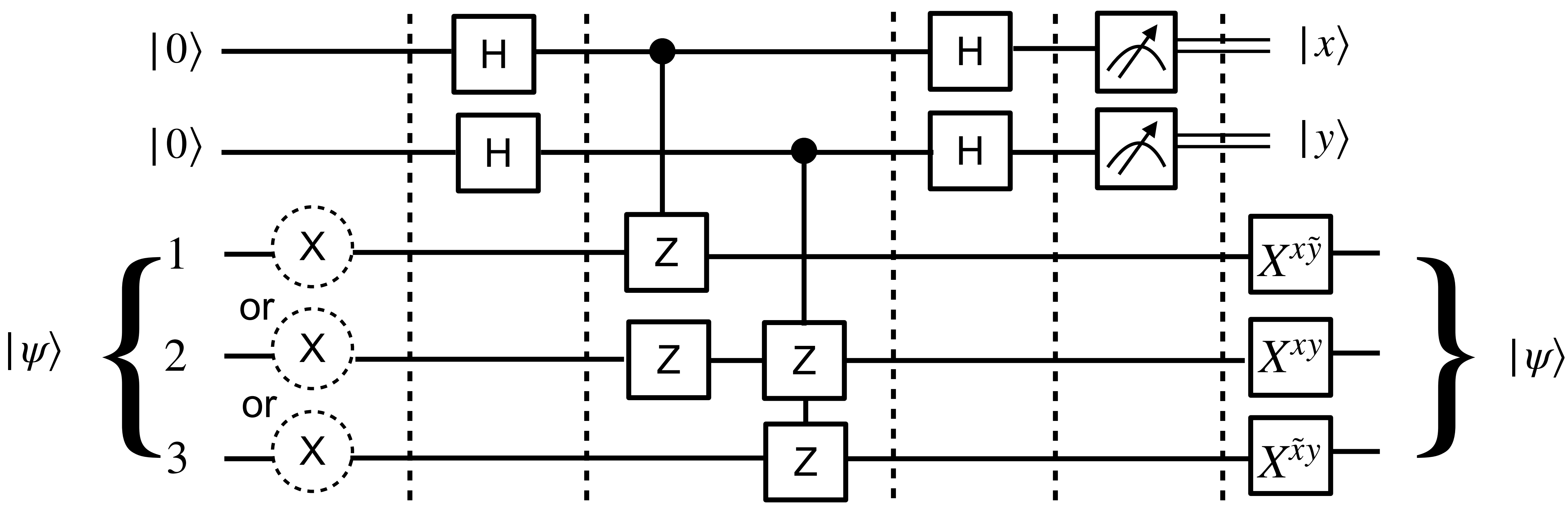


$$H^2 = 1$$
$$HZH = X$$

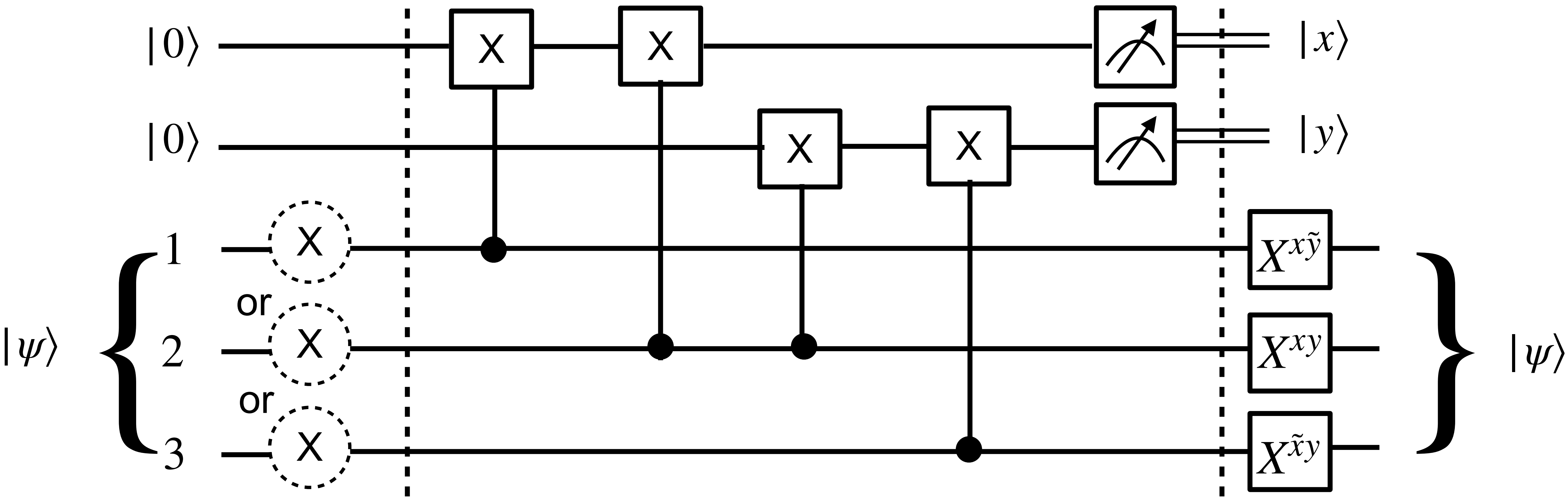
Bitflip code for 3 qubits



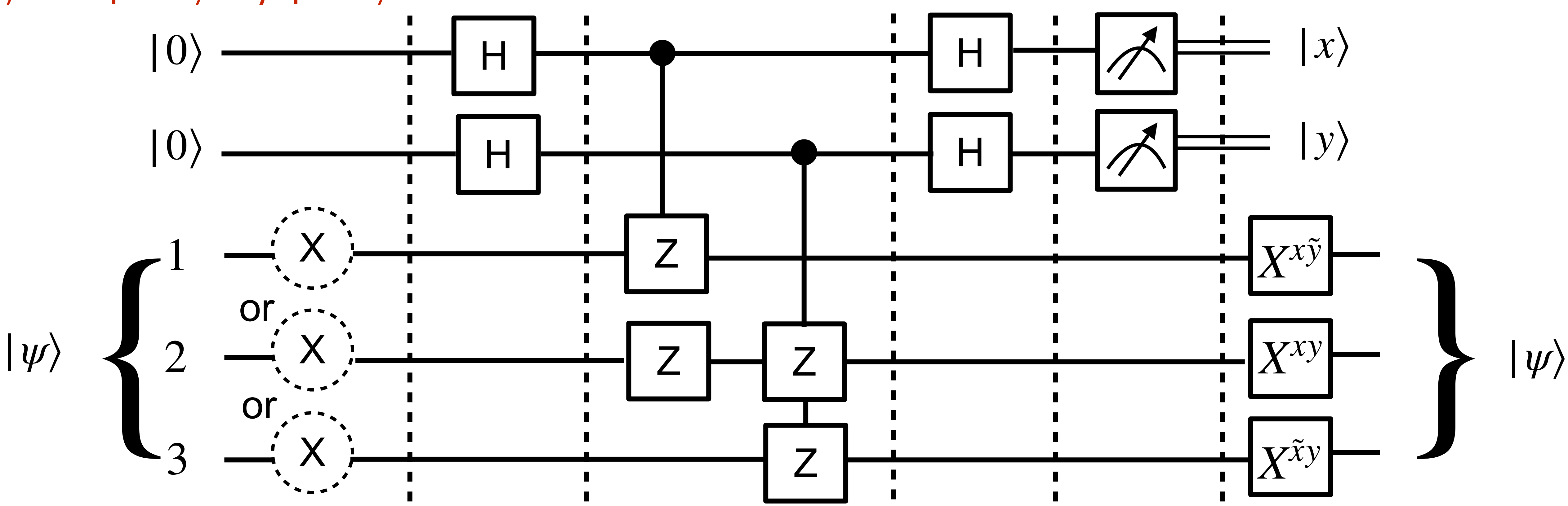
$|\psi\rangle = \alpha|000\rangle + \beta|111\rangle$



Bitflip code for 3 qubits



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



Phase Flip

- With some probability p, the relative phase of $|0\rangle$ and $|1\rangle$ is flipped.

Phase Flip

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \longrightarrow \alpha|0\rangle - \beta|1\rangle$$

$$\begin{pmatrix}\alpha\\ \beta\end{pmatrix} \longrightarrow Z\begin{pmatrix}\alpha\\ \beta\end{pmatrix} = \begin{pmatrix}\alpha\\ -\beta\end{pmatrix}$$ in Z-basis (computational basis)

Bit Flip

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \longrightarrow \alpha|1\rangle + \beta|0\rangle$$

$$X|0\rangle = |1\rangle$$
$$X|1\rangle = |0\rangle$$

$$\begin{pmatrix}\alpha\\ \beta\end{pmatrix} \longrightarrow X\begin{pmatrix}\alpha\\ \beta\end{pmatrix} = \begin{pmatrix}\beta\\ \alpha\end{pmatrix}$$

- Phase flip error model can be turned into the bit-flip error model by transforming to the ± basis (X basis).

$$|+\rangle = \frac{1}{\sqrt{2}}\Big(|0\rangle + |1\rangle\Big) \qquad |-\rangle = \frac{1}{\sqrt{2}}\Big(|0\rangle - |1\rangle\Big)$$

Transformation is Hadamard:

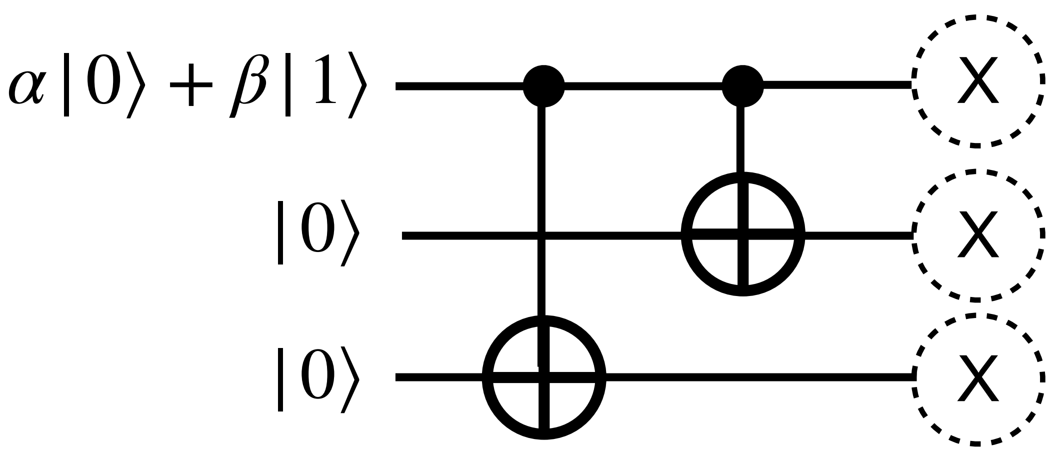
$$H|0\rangle = |+\rangle \qquad H|+\rangle = |0\rangle$$
$$H|1\rangle = |-\rangle \qquad H|-\rangle = |1\rangle$$

Phase Flip

- In the X-basis, roles of X and Z are interchanged.

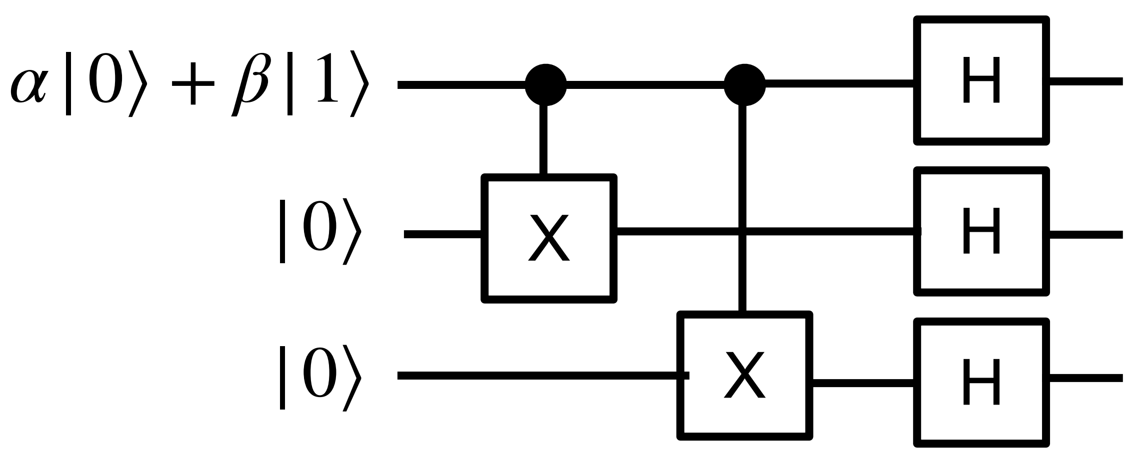
	In computational basis (Z-basis)	In X-basis	
Bit-flip	$X\|0\rangle = \|1\rangle$ $X\|1\rangle = \|0\rangle$	$Z\|+\rangle = \|-\rangle$ $Z\|-\rangle = \|+\rangle$	Phase-flip
Phase-flip	$Z\|0\rangle = \|0\rangle$ $Z\|1\rangle = -\|1\rangle$	$X\|+\rangle = \|+\rangle$ $X\|-\rangle = -\|-\rangle$	Bit-flip

- Stabilizers to detect phase errors involve X-operations as opposed to those used to detect bit-flip errors which involve Z-operators.



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

Circuit to encode 3-qubit bit-flip code acting on a linear combination of $|0\rangle$ and $|1\rangle$



$\alpha|+++\rangle + \beta|---\rangle$

Encoding circuit for the 3-qubit phase flip