Week 12: Show me your 'phase’, Mr. Unitary: Quantum Fourier Transform, quantum phase estimation, Shor’s factoring algorithm, and quantum linear system (such as the HHL algorithm) and programming with IBM Qiskit

Fourier and Discrete Fourier Transform

- Fourier transform (continuous case) and inverse

$$\hat{f}(k) \equiv \int_{-\infty}^{\infty} dx\, f(x) e^{i2\pi xk} \qquad f(x) \equiv \int_{-\infty}^{\infty} dk\, \hat{f}(k) e^{-i2\pi xk}$$

- Discrete Fourier transform and inverse

$$f(x) \longrightarrow \hat{f}(k) \equiv \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} e^{i2\pi kx/N} f(x) \qquad \hat{f}(k) \longrightarrow f(x) = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{-i2\pi kx/N} \hat{f}(k)$$

integer $\sum_k \hat{f}(k)|k\rangle$

- Useful tools in Physics, Engineering, etc.

$N = 2^n$ ← # of qubits

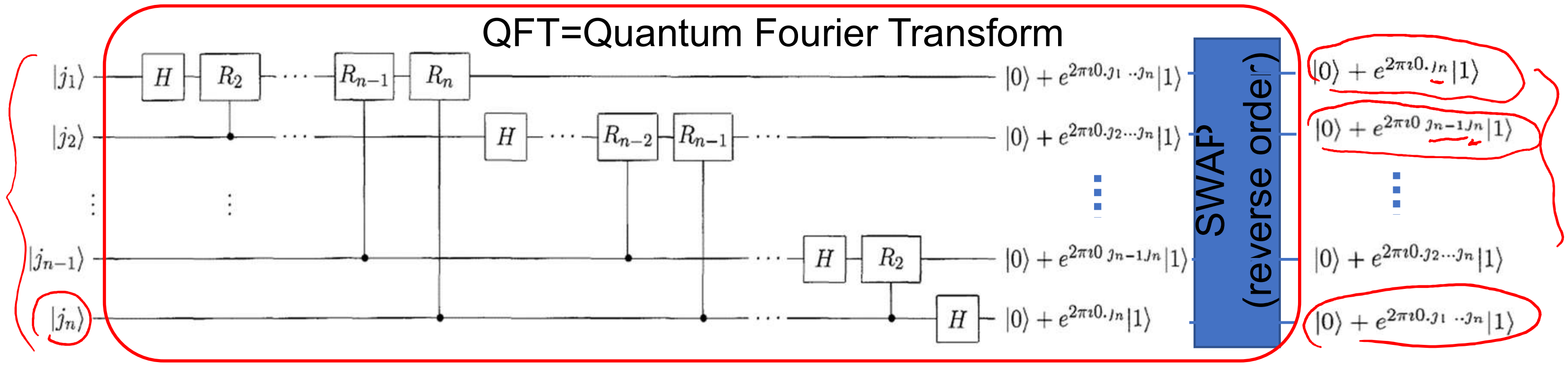
- Expect in the quantum regime:

$$|j\rangle \longrightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{i2\pi jk/N} |k\rangle$$

x $|j_1 j_2 \cdots j_n\rangle$ $|k_1 k_2 \cdots k_n\rangle$

Quantum Fourier Transform

$$|j = j_1 j_2 \ldots j_n\rangle \longrightarrow \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} e^{i2\pi jk/2^n} |k = k_1 k_2 \ldots k_n\rangle \qquad R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{i2\pi/2^k} \end{pmatrix}$$



$$j = \sum_{q=1}^{n} j_q\, 2^{n-q} \qquad k = \sum_{r=1}^{n} k_r\, 2^{n-r}$$

$$|\psi_{\rm QFT}\rangle = \frac{1}{2^{n/2}} \sum_{k's=\{0,1\}} e^{i2\pi \sum_{q,r=1}^{n} j_q 2^{n-q} k_r 2^{n-r}/2^n} |k = k_1 k_2 \ldots k_n\rangle$$

$n-q-r \geq 0$

2^{n-q-r}

$$= \frac{1}{2^{n/2}} \otimes_{r=1}^{n} \left(\sum_{k_r=\{0,1\}} e^{i2\pi(\sum_q^n j_q k_r 2^{n-q-r})} |k_r\rangle \right)$$

$$= \frac{1}{2^{n/2}} \otimes_{r=1}^{n} \left(|0\rangle + e^{i2\pi(\sum_{q=n-r+1}^{n} j_q 2^{n-q-r})} |1\rangle \right)_r$$

$$\sum_{q=n-r+1}^{n} j_q 2^{n-q-r} = 0.j_{n-r+1} j_{n-r+2} \cdots j_n$$

$$= \frac{1}{2^{n/2}} \otimes_{r=1}^{n} \left(|0\rangle + e^{i2\pi(0.j_{n-r+1} j_{n-r+2} \cdots j_n)} |1\rangle \right)_r$$

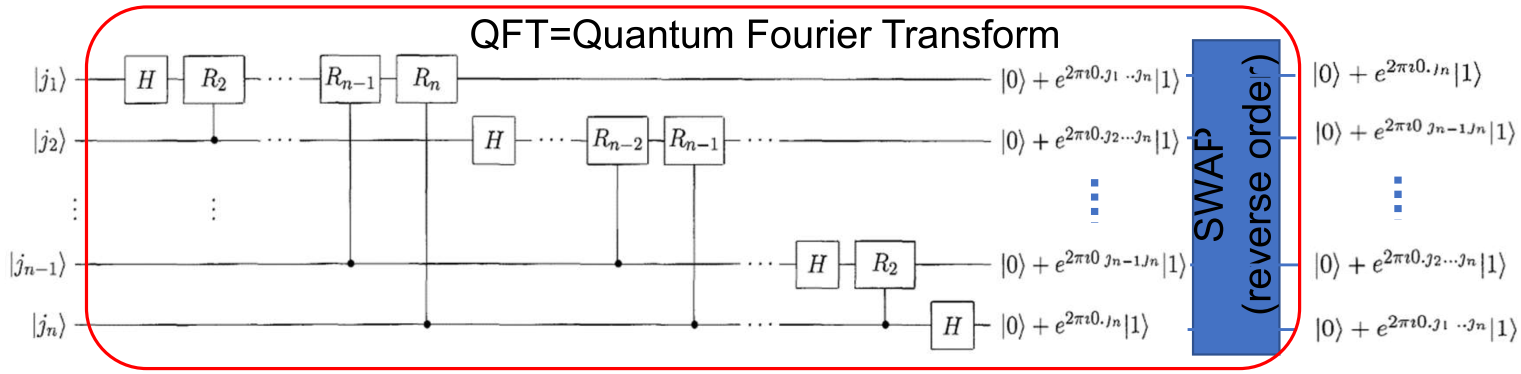
$$R^{[q\to r(q>r)]} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i2\pi/2^{q-r+1}} \end{pmatrix}$$

other papers may use $k = k_n k_{n-1} \cdots k_1$, be aware of convention

$$\sim (|0\rangle + e^{i2\pi 0.j_n}|1\rangle)(|0\rangle + e^{i2\pi 0.j_{n-1}j_n}|1\rangle)\ldots(|0\rangle + e^{i2\pi 0.j_1\cdots j_n}|1\rangle)$$

Quantum Fourier Transform

$$|j = j_1 j_2 \ldots j_n\rangle \longrightarrow \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} e^{i2\pi jk/2^n} |k = k_1 k_2 \ldots k_n\rangle \qquad R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{i2\pi/2^k} \end{pmatrix}$$



$$|\psi_{\rm QFT}\rangle = \frac{1}{2^{n/2}} \sum_{k's=\{0,1\}} e^{i2\pi \sum_{q,r=1}^{n} j_q 2^{n-q} k_r 2^{n-r}/2^n} |k = k_1 k_2 \ldots k_n\rangle$$

$$\sim (|0\rangle + e^{i2\pi 0.j_n}|1\rangle)(|0\rangle + e^{i2\pi 0.j_{n-1}j_n}|1\rangle)\ldots(|0\rangle + e^{i2\pi 0.j_1 \ldots j_n}|1\rangle)$$

$(0.1)_2 = 0 + \frac{1}{2^1} + \cdots$

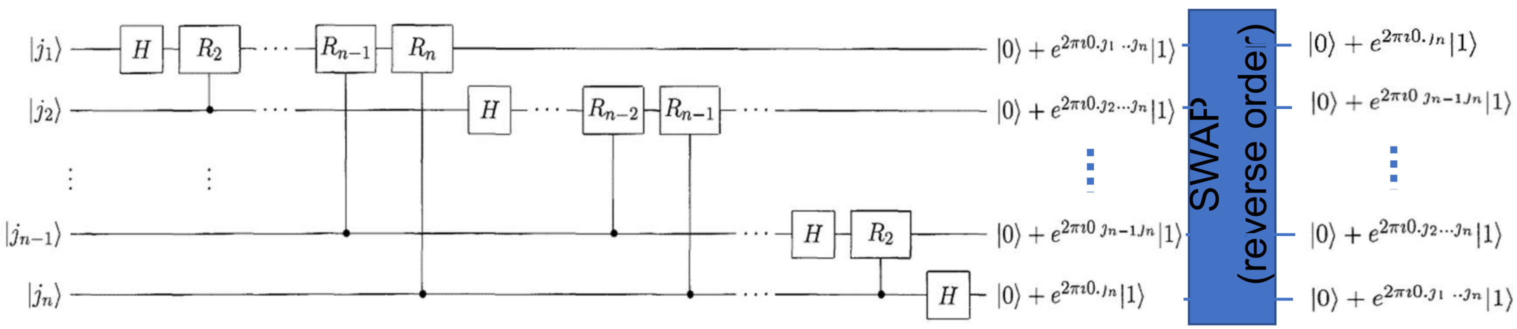
$(1.1)_2 = 1 + \frac{1}{2^1}$

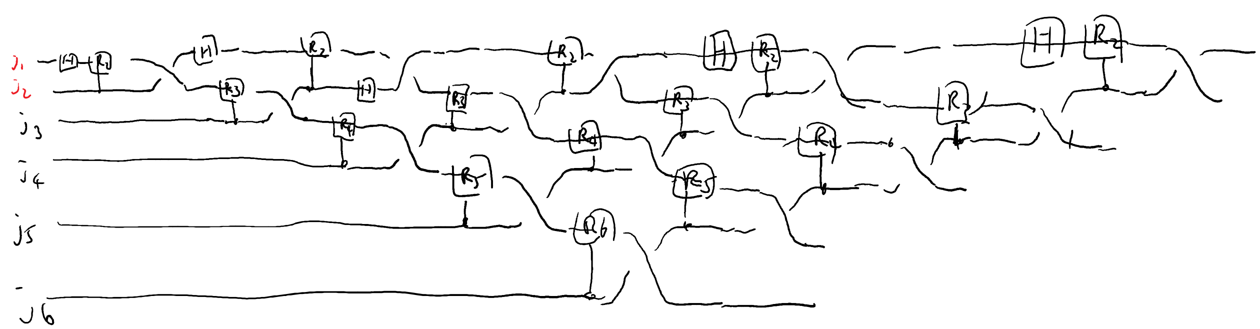
$e^{2\pi i \cdot 1} = 1$

This explains the swap, Hadamard & controlled phase gates

$$R^{[q \to r (q>r)]} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i2\pi/2^{q-r+1}} \end{pmatrix}$$

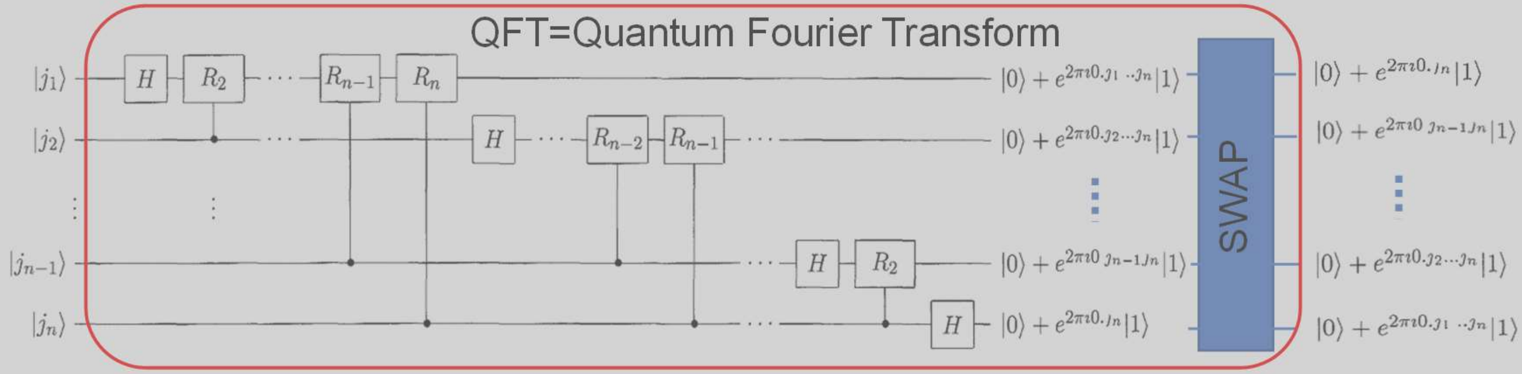
Swap can be implemented along the way

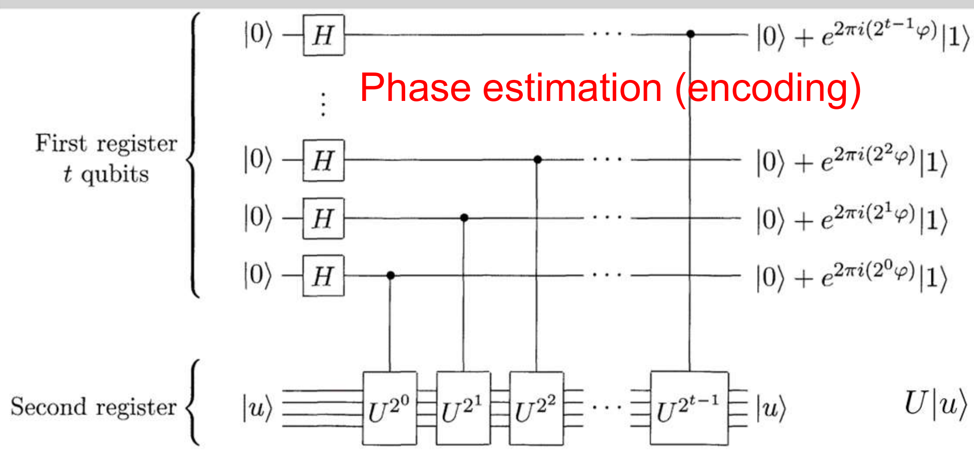




QFT and phase estimation

$$|j = j_1 j_2 \dots j_n\rangle \longrightarrow \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} e^{i2\pi jk/2^n} |k = k_1 k_2 \dots k_n\rangle \qquad R_n = \begin{pmatrix} 1 & 0 \\ 0 & e^{i2\pi/2^n} \end{pmatrix}$$





[from Nielsen & Chuang]

Almost same structure
➔ Apply inverse QFT
to extract phase

$$U|u\rangle = e^{-iHt}|u\rangle = e^{i2\pi\phi}|u\rangle$$

$$\phi = 0.\phi_1\phi_2 \dots \phi_t \dots$$

Distribution of measurement outcomes

- (1) Encode phase ϕ, (2) Inverse QFT, (3) Measurement in computational basis

- Example. phase/2π: $\phi = 0.096723759008708_{10} = 0.0001100011000010111001_2$

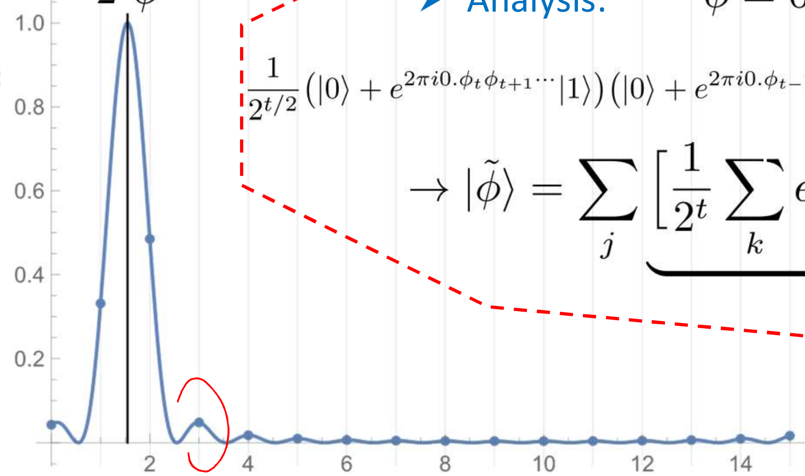
  Use t=4 qubits to encode phase ➔ $2^4\phi = 1.100011000010111001_2$

✓ Two best probable outcomes: 0001_2 (prob= 0.331695) and 0010_2 (prob= 0.48531)

Prob

= $|\alpha_j|^2$

$2^t\phi$



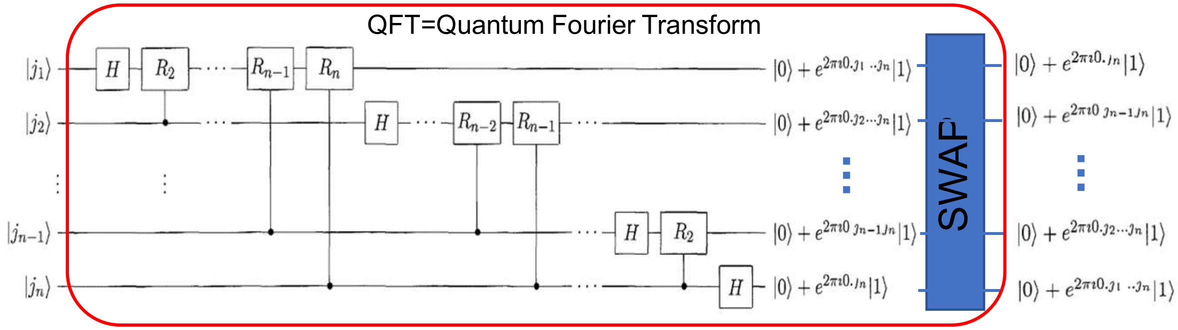
j=0 (0000_2) to 15 (1111_2)

➢ Analysis: $\phi = 0.\phi_1\phi_2\cdots\phi_t\cdots$

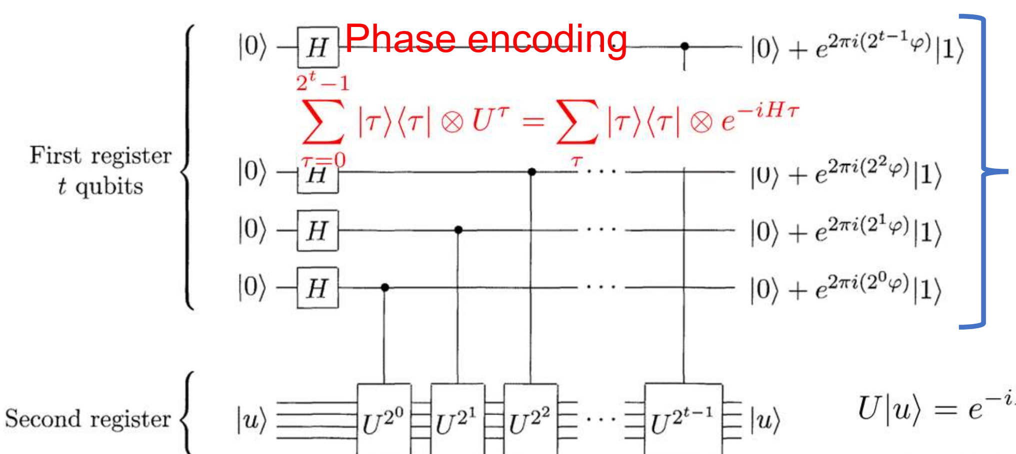
$$\frac{1}{2^{t/2}}\left(|0\rangle + e^{2\pi i 0.\phi_t\phi_{t+1}\cdots}|1\rangle\right)\left(|0\rangle + e^{2\pi i 0.\phi_{t-1}\phi_t\cdots}|1\rangle\right)\cdots\left(|0\rangle + e^{2\pi i 0.\phi_1\phi_2\cdots}|1\rangle\right)$$

$$\rightarrow |\tilde{\phi}\rangle = \sum_j \underbrace{\left[\frac{1}{2^t}\sum_k e^{2\pi i k(\phi - j/2^t)}\right]}_{\alpha_j} |j\rangle$$

Quantum Phase Estimation



- Accurate to $t - \log_2\left(2 + \frac{1}{2\epsilon}\right)$ binary digits with a probability > 1-ϵ



[from Nielsen & Chuang]

ϵ is error probability

Apply inverse of QFT will yield the first few digits of the phase ϕ

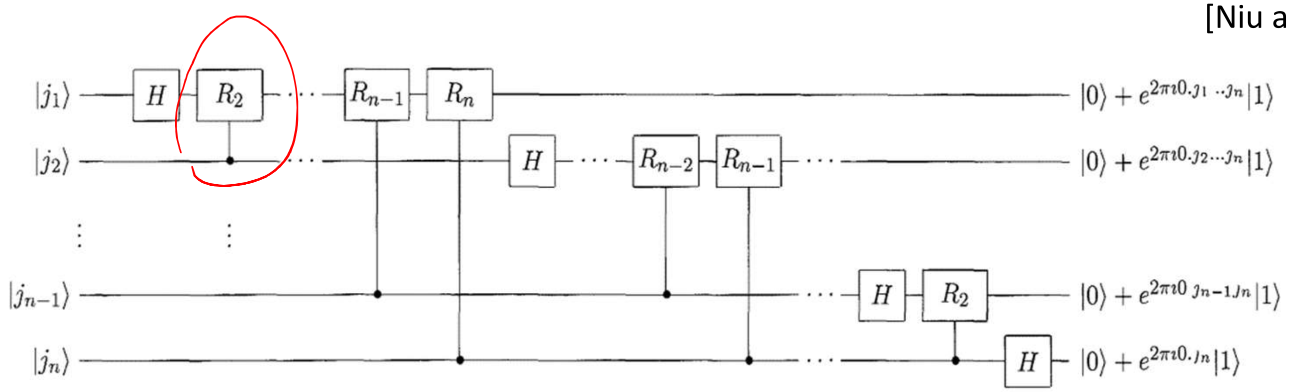
$$U|u\rangle = e^{-iHt}|u\rangle = e^{i2\pi\phi}|u\rangle$$

$$\phi = 0.\phi_1\phi_2\ldots.\phi_t\ldots$$

Semiclassical QFT and iterative QPE

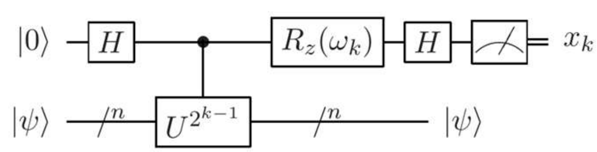
- If QFT or iQFT is the last step, then controlled phase gates can be replaced by 0/1 measurement followed by classical controlled phase gates

[Niu and Griffiths, PRL '96]



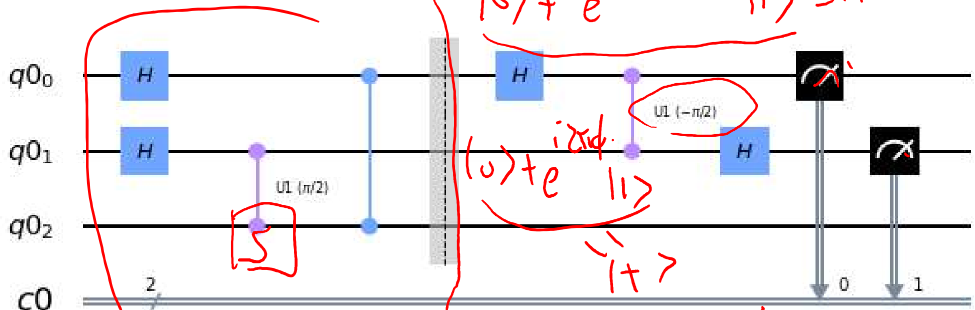
[Dobšíček, Johansson, Shumeiko, Wendin, PRA '07]

- Based on this, an iterative quantum phase estimation was developed

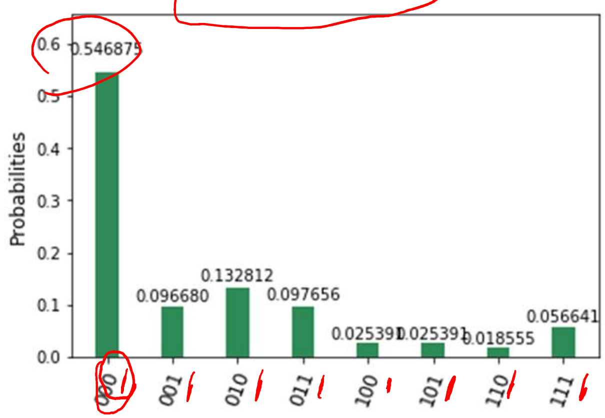


Phase estimation for gate S

1. case 0 phase (input of qubit 3 is |0> of S)



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

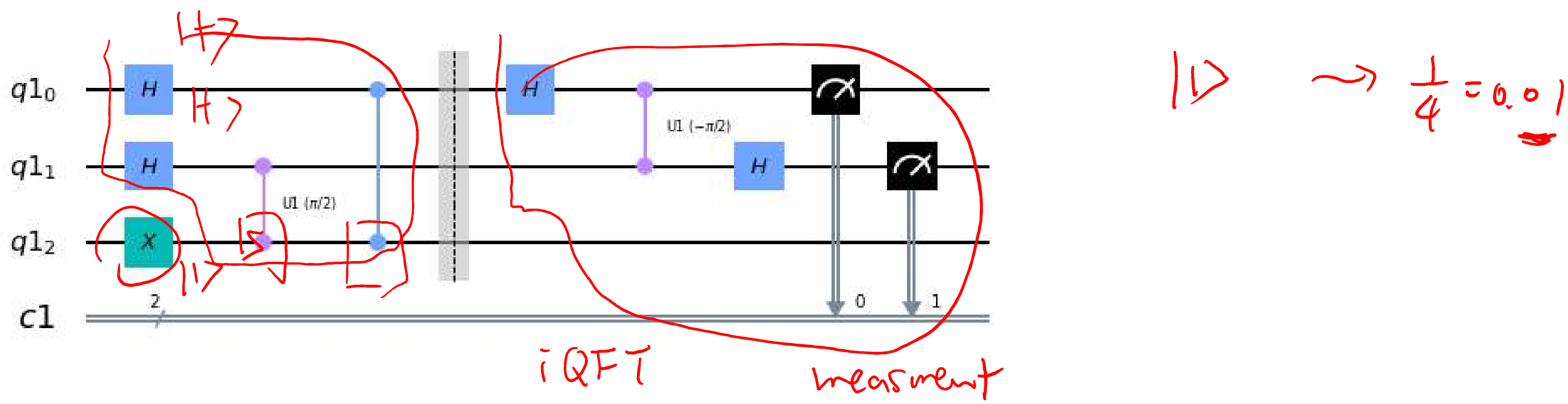


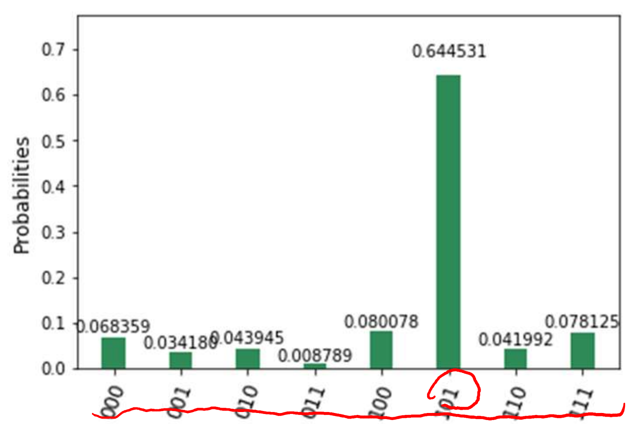
On ibmq_16_rueschlikon

Note: previous circuit run had also measured qubit[2]]; thus three bits of label.

Phase estimation for gate S

2. case pi/2 phase (input of qubit 3 is |1> of S)





On `ibmq_16_rueschlikon`

Note: previous circuit run had also measured qubit[2]]; thus three bits of label.

Supposed to be 100% at 101; error is substantial

Application of QPE

- Approximate projection to eigenstates
- Order and period finding
- Shor's factoring algorithm
- Discrete logarithm

  $$f(x_1, x_2) = a^{sx_1 + x_2} \bmod N \qquad b = a^s \Longrightarrow s = ?$$
  $$f(x_1 + q, x_2 - q\, s) = f(x_1, x_2)$$

- Hidden subgroup problem

  $$U|g\rangle|h\rangle = |g\rangle|h \oplus f(g)\rangle$$
  f is constant on the cosets of a subgroup K ➔ find K

- Harrow-Hassidim-Lloyd (HHL) quantum linear system and related algorithms
- Quantum SVD