IQC Institute for Quantum Computing · University of Waterloo · PI

Introduction to Quantum Information Processing

Lecture 11

Michele Mosca

Eigenvalue Estimation and Quantum Factoring

- Eigenvalue Estimation
- Quantum Factoring

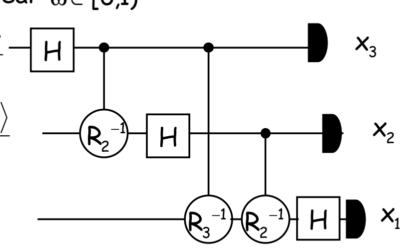
Quantum Phase Estimation

- For any real $\omega \in [0,1)$

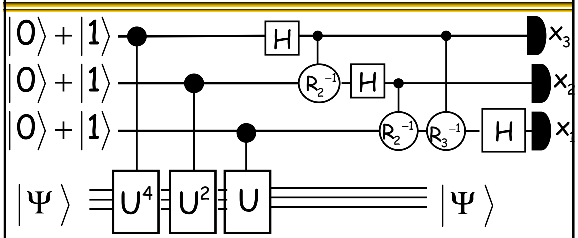
$$\frac{|0\rangle + e^{2\pi i(8\omega)}|1\rangle}{\sqrt{2}}$$

$$\frac{|0\rangle + e^{2\pi i(4\omega)}|1\rangle}{\sqrt{2}}$$

$$\frac{|0\rangle + e^{2\pi i(\omega)}|1\rangle}{\sqrt{2}}$$



- With high probability $\frac{4x_1+2x_2+x_1}{8} \approx \omega$



Eigenvalue kick-back

- Given U with eigenvector $|\Psi\rangle$ and eigenvalue $e^{2\pi i\omega}$ we thus have an algorithm that maps

$$|0\rangle|\Psi\rangle \xrightarrow{QFT\otimes I,\, c-U^{x},\, QFT^{-1}\otimes I} |\tilde{\omega}\rangle|\Psi\rangle$$

Example

- Let $G = Z_5^{*} = \{1,2,3,4\} \bmod 5$
- Then $1^1 \equiv 1,\ 2^4 \equiv 1,\ 3^4 \equiv 1,\ 4^2 \equiv 1$
- We can easily implement, for example, U_2

$U_2|001\rangle \rightarrow |010\rangle \qquad U_2^{2}|001\rangle \rightarrow |100\rangle$

$U_2^{3}|001\rangle \rightarrow |011\rangle \qquad U_2^{4}|001\rangle \rightarrow |001\rangle$

- The eigenvectors of U_2 include

$$|\Psi_k\rangle = \sum_{j=0}^{3} e^{-2\pi i \frac{jk}{4}} |2^j \bmod 5\rangle$$

Example

$$|\Psi_3\rangle$$
$$= |001\rangle + e^{-2\pi i \frac{3}{4}}|010\rangle + e^{-2\pi i \frac{6}{4}}|100\rangle + e^{-2\pi i \frac{9}{4}}|011\rangle$$
$$= |001\rangle + e^{-2\pi i \frac{3}{4}}|010\rangle + e^{-2\pi i \frac{2}{4}}|100\rangle + e^{-2\pi i \frac{1}{4}}|011\rangle$$

Example

$$U_2|\Psi_3\rangle$$
$$= |010\rangle + e^{-2\pi i \frac{3}{4}}|100\rangle + e^{-2\pi i \frac{2}{4}}|011\rangle + e^{-2\pi i \frac{1}{4}}|001\rangle$$
$$= e^{2\pi i \frac{3}{4}}(e^{-2\pi i \frac{3}{4}}|010\rangle + e^{-2\pi i \frac{2}{4}}|100\rangle + e^{-2\pi i \frac{1}{4}}|011\rangle + |001\rangle)$$
$$= e^{2\pi i \frac{3}{4}}|\Psi_3\rangle$$

Example

$$U_2|\Psi_0\rangle = |\Psi_0\rangle$$
$$U_2|\Psi_1\rangle = e^{2\pi i \frac{1}{4}}|\Psi_1\rangle$$
$$U_2|\Psi_2\rangle = e^{2\pi i \frac{2}{4}}|\Psi_2\rangle$$
$$U_2|\Psi_3\rangle = e^{2\pi i \frac{3}{4}}|\Psi_3\rangle$$
$$\frac{1}{2}\left(|\Psi_0\rangle + |\Psi_1\rangle + |\Psi_2\rangle + |\Psi_3\rangle\right) = |001\rangle$$

Example

$$c - U_2(|0\rangle + |1\rangle)|\Psi_0\rangle = (|0\rangle + |1\rangle)|\Psi_0\rangle$$

$$c - U_2(|0\rangle + |1\rangle)|\Psi_1\rangle = \left(|0\rangle + e^{2\pi i\frac{1}{4}}|1\rangle\right)|\Psi_1\rangle$$

$$c - U_2(|0\rangle + |1\rangle)|\Psi_2\rangle = \left(|0\rangle + e^{2\pi i\frac{2}{4}}|1\rangle\right)|\Psi_2\rangle$$

$$c - U_2(|0\rangle + |1\rangle)|\Psi_3\rangle = \left(|0\rangle + e^{2\pi i\frac{3}{4}}|1\rangle\right)|\Psi_3\rangle$$

Example

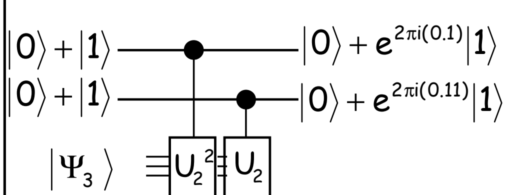
$$c - U_2{}^2(|0\rangle + |1\rangle)|\Psi_0\rangle = (|0\rangle + |1\rangle)|\Psi_0\rangle$$

$$c - U_2{}^2(|0\rangle + |1\rangle)|\Psi_1\rangle = \left(|0\rangle + e^{2\pi i\frac{2}{4}}|1\rangle\right)|\Psi_1\rangle$$

$$c - U_2{}^2(|0\rangle + |1\rangle)|\Psi_2\rangle = (|0\rangle + |1\rangle)|\Psi_2\rangle$$

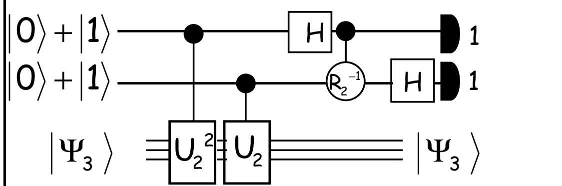
$$c - U_2{}^2(|0\rangle + |1\rangle)|\Psi_3\rangle = \left(|0\rangle + e^{2\pi i\frac{2}{4}}|1\rangle\right)|\Psi_3\rangle$$

Eigenvalue Kickback



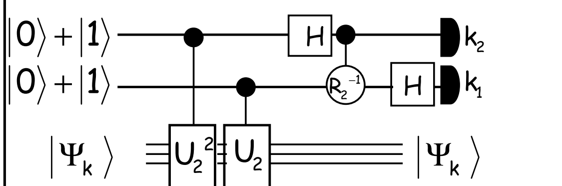
Eigenvalue Kickback

$3 = 2 \cdot 1 + 1$

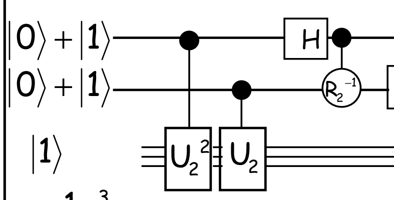


Eigenvalue Kickback

$k = 2k_1 + k_2$



Eigenvalue Kickback



$$\frac{1}{2}\sum_{k=0}^{3} |k\rangle |\Psi_k\rangle$$

$$= \frac{1}{2}\sum_{k=0}^{3} |\Psi_k\rangle$$

Example

- Let $a \in G = Z_N^*$ $a^r \equiv 1$
- We can easily implement

$U_a|x\rangle \to |ax\rangle$ $U_a^2|x\rangle = U_{a^2}|x\rangle \to |a^2x\rangle$

$U_a^{2^n}|x\rangle = U_{a^{2^n}}|x\rangle \to |a^{2^n}x\rangle$

- The eigenvectors of U_a include

$$|\Psi_k\rangle = \sum_{j=0}^{r-1} e^{-2\pi i\frac{jk}{r}}|a^j\rangle$$

Example

$$U_a|\Psi_k\rangle = U_a(|1\rangle + e^{-2\pi i\frac{k}{r}}|a\rangle + e^{-2\pi i\frac{2k}{r}}|a^2\rangle + \cdots + e^{-2\pi i\frac{(r-1)k}{r}}|a^{r-1}\rangle)$$
$$= |a\rangle + e^{-2\pi i\frac{k}{r}}|a^2\rangle + e^{-2\pi i\frac{2k}{r}}|a^3\rangle + \cdots + e^{-2\pi i\frac{(r-1)k}{r}}|a^r\rangle$$
$$= e^{2\pi i\frac{k}{r}}(|1\rangle + e^{-2\pi i\frac{k}{r}}|a\rangle + e^{-2\pi i\frac{2k}{r}}|a^2\rangle + \cdots + e^{-2\pi i\frac{(r-1)k}{r}}|a^{r-1}\rangle)$$
$$= e^{2\pi i\frac{k}{r}}|\Psi_k\rangle$$

Example

$$c - U_{a^{2^j}}(|0\rangle + |1\rangle)|\Psi_k\rangle = \left(|0\rangle + e^{2\pi i\frac{2^j k}{r}}|1\rangle\right)|\Psi_k\rangle$$

$$\frac{1}{\sqrt{r}}(|\Psi_0\rangle + |\Psi_1\rangle + |\Psi_2\rangle + \cdots + |\Psi_{r-1}\rangle) = |1\rangle$$

Eigenvalue kick-back

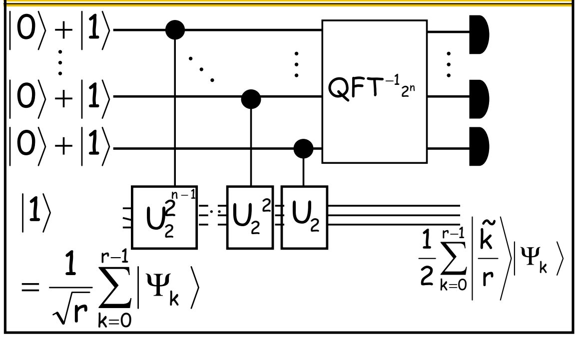
- Given U with eigenvectors $|\Psi_k\rangle$ and respective eigenvalues $e^{2\pi i \frac{k}{r}}$ we thus have an algorithm that maps

$$|0\rangle|\Psi_k\rangle \rightarrow \left|\frac{\tilde{k}}{r}\right\rangle|\Psi_k\rangle$$

and therefore

$$|0\rangle\sum_k \alpha_k|\Psi_k\rangle = \sum_k \alpha_k|0\rangle|\Psi_k\rangle \rightarrow \sum_k \alpha_k\left|\frac{\tilde{k}}{r}\right\rangle|\Psi_k\rangle$$

Eigenvalue Estimation



Eigenvalue kick-back

- Measuring the first register of

$$\sum_k \frac{1}{\sqrt{r}}\left|\frac{\tilde{k}}{r}\right\rangle|\Psi_k\rangle$$

is equivalent to measuring $\left|\frac{\tilde{k}}{r}\right\rangle$ with probability $\frac{1}{r}$

Quantum Factoring

- The security of many public key cryptosystems used in industry today relies on the difficulty of factoring large numbers into smaller factors.
- Factoring the integer N into smaller factors can be reduced to the following task:

Given integer a, find the smallest positive integer r so that $a^r \equiv 1 \bmod N$

(aside: how does factoring reduce to order-finding??)

- The most common approach for factoring integers is the difference of squares technique:
  - "Randomly" find two integers x and y satisfying $x^2 = y^2 \bmod N$
  - So N divides $x^2 - y^2 = (x - y)(x + y)$
  - Hope that $\gcd(N, x - y)$ is non-trivial
- If r is even, then let $x = a^{r/2} \bmod N$

so that $x^2 = 1^2 \bmod N$

Quantum Factoring

Since we know how to efficiently multiply by a mod N, we can efficiently implement

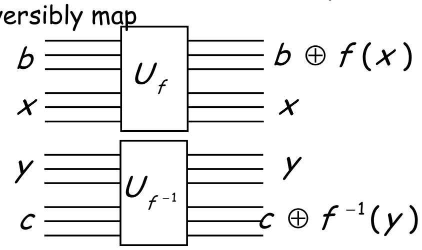
$$U_a|x\rangle = |ax\rangle$$

Note that $U_a^r|x\rangle = |a^r x\rangle = |x\rangle$

i.e. $U_a^r = I$

(Aside: more on reversible computing)

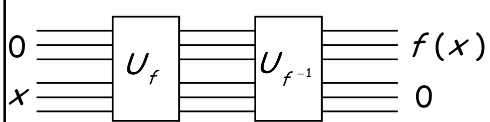
If we know how to efficiently compute f and f^{-1} then we can efficiently and reversibly map



(Aside: more on reversible computing)

And therefore we can efficiently map

$$|x\rangle \rightarrow |f(x)\rangle$$



Interesting eigenvalues

If $U_a^r = I$ then the eigenvalues of U_a are of the form $e^{2\pi i \frac{k}{r}}$

$$U_a|\psi_k\rangle = e^{i2\pi\frac{k}{r}}|\psi_k\rangle$$

$$|\psi_k\rangle = \sum_{j=0}^{r-1} e^{i2\pi j\frac{k}{r}}|a^j\rangle$$

Checking the eigenvalues

$$U_a|\psi_k\rangle = \sum_{j=0}^{r-1} e^{-i2\pi j\frac{k}{r}} U_a|a^j\rangle$$

$$= \sum_{j=0}^{r-1} e^{-i2\pi j\frac{k}{r}}|a^{j+1}\rangle = e^{i2\pi\frac{k}{r}}\left(\sum_{j=1}^{r} e^{-i2\pi j\frac{k}{r}}|a^j\rangle\right)$$

$$= e^{i2\pi\frac{k}{r}}\left(\sum_{j=0}^{r-1} e^{-i2\pi j\frac{k}{r}}|a^j\rangle\right) = e^{i2\pi\frac{k}{r}}|\psi_k\rangle$$

Finding r

For most integers k, a good estimate of $\frac{k}{r}$ (with error at most $\frac{1}{2r^2}$) allows us to determine r (even if we don't know k). (using continued fractions)