Quantum Algorithms

Personal notes based on lecture material and assigned reading from Princeton's ELE 396: Quantum Computing, taught by Stephen Lyon.

Important Identities

N-bit Hadamard

$$H^{\otimes n}|\mathbf{0}\rangle = \frac{1}{\sqrt{2^n}} \sum_{z\in\{0,1\}^n} |\mathbf{z}\rangle$$

$$H^{\otimes n}|\mathbf{x}\rangle = \frac{1}{\sqrt{2^n}} \sum_{z\in\{0,1\}^n} (-1)^{\mathbf{x}\cdot\mathbf{z}}|\mathbf{z}\rangle$$

$U_f\colon |\mathbf{x}\rangle|y\rangle \to |\mathbf{x}\rangle|y \oplus f(x)\rangle$

$$U_f\left(\sum_{x\in\{0,1\}^n} |\mathbf{x}\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)\right) = \sum_{x\in\{0,1\}^n} (-1)^{f(\mathbf{x})}|\mathbf{x}\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

Deutsch-Jozsa

- Setup
    - Input: a black-box for computing unknown function $f\colon \{0,1\}^n \to \{0,1\}$
    - Details: f is either a constant or a balanced function
        - If it is constant, all inputs map to either 0 or 1
        - If it is balanced, exactly half the inputs map to 0 and the other half to 1
    - Problem: determine whether f is constant or balanced by making queries

- Input $|\psi_0\rangle = |\mathbf{0}\rangle|1\rangle$

- Apply (n+1)-bit Hadamard to $|\mathbf{0}\rangle|1\rangle$ resulting in

$$|\psi_1\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |\mathbf{x}\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

- Apply $U_f\colon |\mathbf{x}\rangle|y\rangle \to |\mathbf{x}\rangle|y \oplus f(x)\rangle$

$$
\begin{aligned}
|\psi_2\rangle &= U_f\left(\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|\boldsymbol{x}\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)\right) \\
&= \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}(-1)^{f(x)}|\boldsymbol{x}\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)
\end{aligned}
$$

- Apply n-bit Hadamard again

$$
\begin{aligned}
|\psi_3\rangle &= H^{\otimes n}\left(\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}(-1)^{f(x)}|\boldsymbol{x}\rangle\right)\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) \\
&= \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}(-1)^{f(x)}\,H^{\otimes n}|\boldsymbol{x}\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) \\
&= \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}(-1)^{f(x)}\frac{1}{\sqrt{2^n}}\sum_{z\in\{0,1\}^n}(-1)^{\boldsymbol{x}\cdot\boldsymbol{z}}|\boldsymbol{z}\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) \\
&= \frac{1}{2^n}\sum_{z\in\{0,1\}^n}\left(\sum_{x\in\{0,1\}^n}(-1)^{f(x)}(-1)^{\boldsymbol{x}\cdot\boldsymbol{z}}\right)|\boldsymbol{z}\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)
\end{aligned}
$$

- Measure input registers in computational basis ($|0\rangle, |1\rangle$)
  - Coefficient of $|\boldsymbol{z}\rangle = |\boldsymbol{0}\rangle$ is given by

$$
\sum_{x\in\{0,1\}^n}(-1)^{f(x)}(-1)^{\boldsymbol{x}\cdot\boldsymbol{z}} = \sum_{x\in\{0,1\}^n}(-1)^{f(x)}
$$

    - If $f(\boldsymbol{x})$ is balanced, this sum is 0.
    - If $f(\boldsymbol{x})$ is constant, this sum is 2^n.
  - If measurement yields $|\boldsymbol{0}\rangle$, $f(\boldsymbol{x})$ must be constant. If measurement yields any other value, $f(\boldsymbol{x})$ must be balanced

- Classical v. quantum algorithm analysis
  - Deterministic: classical requires $2^{n-1}+1$ queries, while quantum requires 1
  - Probabilistic: classical can solve Deutch-Jozsa with probability of error at most $\frac{1}{2}$ using 2 queries, and less than $\frac{1}{2^n}$ with $n+1$ queries
  - *Linear gap* in the case of exponentially small error (not that impressive!)

Bernstein-Vazirani

- Setup
  - Input: a black-box for computing unknown function $f\colon\{0,1\}^n \to \{0,1\}$
  - Details: $f(\boldsymbol{x}) = \boldsymbol{x}\cdot\boldsymbol{a}$
  - Problem: want to determine n-bit "secret" hard-coded value $\boldsymbol{a}$

- Same procedure
  - Know that $f(\boldsymbol{x}) = \boldsymbol{x} \cdot \boldsymbol{a}$

$$|\psi_3\rangle = \frac{1}{2^n} \sum_{z\in\{0,1\}^n} \left(\sum_{x\in\{0,1\}^n} (-1)^{f(x)} (-1)^{\boldsymbol{x}\cdot\boldsymbol{z}} \right) |\boldsymbol{z}\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$$

$$= \frac{1}{2^n} \sum_{z\in\{0,1\}^n} \left(\sum_{x\in\{0,1\}^n} (-1)^{\boldsymbol{x}\cdot\boldsymbol{a}} (-1)^{\boldsymbol{x}\cdot\boldsymbol{z}} \right) |\boldsymbol{z}\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$$

$$= \frac{1}{2^n} \sum_{z\in\{0,1\}^n} \left(\sum_{x\in\{0,1\}^n} (-1)^{(\boldsymbol{z}\oplus\boldsymbol{a})\cdot\boldsymbol{x}} \right) |\boldsymbol{z}\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$$

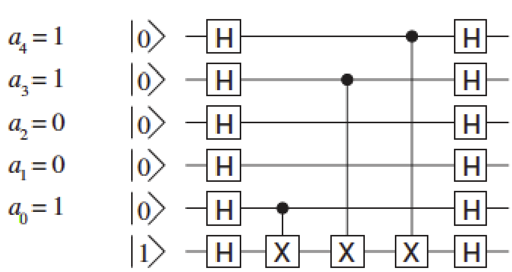
  - Measuring input register *always yields* $\boldsymbol{a}$, and so we are done!
    - Coefficient of $|\boldsymbol{z}\rangle = |\boldsymbol{a}\rangle$ is given by

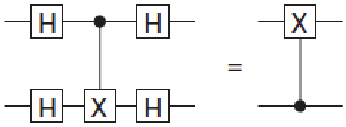
$$\sum_{x\in\{0,1\}^n} (-1)^{(\boldsymbol{z}\oplus\boldsymbol{a})\cdot\boldsymbol{x}} = \sum_{x\in\{0,1\}^n} (-1)^{\boldsymbol{0}} = 2^n$$

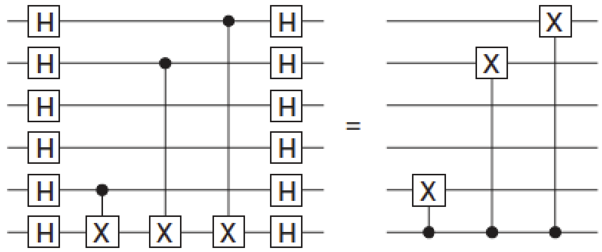
    - Coefficient of $|\boldsymbol{z}\rangle \neq |\boldsymbol{a}\rangle$ is given by

$$\sum_{x\in\{0,1\}^n} (-1)^{(\boldsymbol{z}\oplus\boldsymbol{a})\cdot\boldsymbol{x}} = \sum_{x\in\{0,1\}^n} (-1)^{\boldsymbol{b}\cdot\boldsymbol{x}} = 0$$

- A second way of looking at this problem exists
  - Circuit diagram
    - Key idea: $U_f: |\boldsymbol{x}\rangle|y\rangle \to |\boldsymbol{x}\rangle|y \oplus f(x)\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)} |\boldsymbol{x}\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$ can be represented as series of CNOTs on the output register, controlled by those input bits that correspond to nonzero bits of a
    - Applying n-bit Hadamards before and after U_f uncovers the hardcoded value of a in the blackbox







- Classical v. quantum algorithm analysis
    - Deterministic: classical computer must call subroutine n times to determine (n bits of) $\boldsymbol{a}$ while a quantum computer need only call the subroutine once

Simon's Problem

- Setup
    - Input: a black-box for computing unknown function $f\colon \{0,1\}^n \to \{0,1\}^{n-1}$
    - Details: $f(\boldsymbol{x}) = f(\boldsymbol{y})$ iff $\boldsymbol{y} = \boldsymbol{x} \oplus \boldsymbol{a}$
    - Problem: want to determine period $\boldsymbol{a}$ of $f(\boldsymbol{x})$

- Input $|\psi_0\rangle = |\boldsymbol{0}\rangle_n |\boldsymbol{0}\rangle_{n-1}$
    - $|\boldsymbol{0}\rangle_n$ is the input register and $|\boldsymbol{0}\rangle_{n-1}$ is the output register

- Apply n-bit Hadamard to input

$$|\psi_1\rangle = \left(\frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |\boldsymbol{x}\rangle\right) |\boldsymbol{0}\rangle_{n-1}$$

- Apply $U_f\colon |\boldsymbol{x}\rangle|\boldsymbol{0}\rangle \to |\boldsymbol{x}\rangle|\boldsymbol{f}(\boldsymbol{x})\rangle$

$$|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |\boldsymbol{x}\rangle|\boldsymbol{f}(\boldsymbol{x})\rangle_{n-1}$$

- Measure output register
    - Some value of $|\boldsymbol{f}(\boldsymbol{x_0})\rangle$ corresponding to random $\boldsymbol{x_0}$ and $\boldsymbol{x_0} \oplus \boldsymbol{a}$
    - Resulting state

$$|\psi_3\rangle = \frac{1}{\sqrt{2}}(|\boldsymbol{x_0}\rangle + |\boldsymbol{x_0} \oplus \boldsymbol{a}\rangle)|\boldsymbol{f}(\boldsymbol{x_0})\rangle$$

- Apply n-bit Hadamard to input

$$|\psi_4\rangle = H^{\otimes n}\left(\frac{1}{\sqrt{2}}(|\boldsymbol{x_0}\rangle + |\boldsymbol{x_0} \oplus \boldsymbol{a}\rangle)\right)|\boldsymbol{f}(\boldsymbol{x_0})\rangle$$

$$= \frac{1}{\sqrt{2^{n+1}}} \sum_{y \in \{0,1\}^n} (-1)^{\boldsymbol{x_0} \cdot \boldsymbol{y}} + (-1)^{(\boldsymbol{x_0} \oplus \boldsymbol{a}) \cdot \boldsymbol{y}} |\boldsymbol{y}\rangle$$
$$= \frac{1}{\sqrt{2^{n+1}}} \sum_{y \in \{0,1\}^n} (-1)^{\boldsymbol{x_0} \cdot \boldsymbol{y}} + (-1)^{\boldsymbol{x_0} \cdot \boldsymbol{y}} (-1)^{\boldsymbol{a} \cdot \boldsymbol{y}} |\boldsymbol{y}\rangle$$
$$= \frac{1}{\sqrt{2^{n+1}}} \sum_{\boldsymbol{a} \cdot \boldsymbol{y} = 0} 2(-1)^{\boldsymbol{x_0} \cdot \boldsymbol{y}} \, |\boldsymbol{y}\rangle$$
$$= \frac{1}{\sqrt{2^{n-1}}} \sum_{\boldsymbol{a} \cdot \boldsymbol{y} = 0} (-1)^{\boldsymbol{x_0} \cdot \boldsymbol{y}} \, |\boldsymbol{y}\rangle$$

Note that $\boldsymbol{a} \cdot \boldsymbol{y}$ is a modulo-2 bitwise inner product. Clearly, if $\boldsymbol{a} \cdot \boldsymbol{y} = 1$, the second summation equals 0.

- Measure the input register
  - Yields random $|\boldsymbol{y}\rangle$ satisfying $\boldsymbol{a} \cdot \boldsymbol{y} = 0 \pmod 2$
  - Gives a linear equation in the bits of $\boldsymbol{a}$
    - E.x. $a_1 + a_3 + a_{11} = 0$
  - $n + 20$ invocations should yield n linearly independent equations (from which $\boldsymbol{a}$ can unambiguously be determined) with probability at least $1 - \frac{1}{10^6}$

- Classical v. quantum algorithm analysis
  - Classically: would have to feed subroutine $\sim 2^{\frac{n}{2}}$ different values of $\boldsymbol{x}$ for appreciable chance of finding a pair that XOR to **a** (birthday problem)
    - Exponential in number of bits n
  - Quantum: need only a linear number of invocations ($n + 20$) to have a very good chance of accurately determining $\boldsymbol{a}$
    - Note Simon's algorithm is a zero-error algorithm – though it possible that $n + 20$ invocations may not be sufficient to determine $\boldsymbol{a}$, there is no chance of getting an *incorrect answer*

Quantum Fourier Transform

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

Shor's Algorithm

- Input $|\psi_0\rangle = |0\rangle_n |0\rangle_{n_0}$
  - n is often $2n_0$

- Apply n-bit Hadamard

$$|\psi_1\rangle = (H^{\otimes n}|0\rangle_n)\left(|0\rangle_{n_0}\right) = \left(\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle_n\right)\left(|0\rangle_{n_0}\right)$$

- Apply $U_f: |x\rangle|0\rangle \rightarrow |x\rangle|z^x \pmod{pq}\rangle$

$$|\psi_2\rangle = U_f\left(\left(\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle_n\right)\left(|0\rangle_{n_0}\right)\right) = \frac{1}{\sqrt{2^n}}\sum_{y=0}^{2^n-1}|x\rangle_n\left(|f(x)\rangle_{n_0}\right)$$

  - z is randomly selected from [2, N-1]

- Measure output register, leaving input register in superposition of values which give that particular output

$$|\psi_3\rangle = \left(\frac{1}{\sqrt{M}}\sum_{k=0}^{m-1}|x_0 + kr\rangle_n\right)\left(|f(x_0)\rangle_{n_0}\right)$$

- Now apply the Quantum Fourier Transform (U_{QFT}) to the input register

$$\begin{aligned}|\psi_4\rangle = U_{QFT}\left(\frac{1}{\sqrt{M}}\sum_{k=0}^{m-1}|x_0 + kr\rangle_n\right) &= \frac{1}{\sqrt{M}}\sum_{k=0}^{m-1}\left(\frac{1}{\sqrt{2^n}}\sum_{y=0}^{2^n-1}e^{\frac{2\pi i(x_0+kr)y}{2^n}}|y\rangle_n\right)\\ &= \sum_{y=0}^{2^n-1}\frac{1}{\sqrt{M2^n}}\sum_{k=0}^{m-1}e^{\frac{2\pi i(x_0+kr)y}{2^n}}|y\rangle_n\\ &= \sum_{y=0}^{2^n-1}e^{\frac{2\pi i x_0 y}{2^n}}\frac{1}{\sqrt{M2^n}}\left(\sum_{k=0}^{m-1}e^{\frac{2\pi ikry}{2^n}}\right)|y\rangle_n\end{aligned}$$

- Measuring the QFTed input register yields $|y\rangle_n$ with probability

$$p(y) = \left|e^{\frac{2\pi i x_0 y}{2^n}}\frac{1}{\sqrt{M2^n}}\left(\sum_{k=0}^{m-1}e^{\frac{2\pi ikry}{2^n}}\right)\right|^2 = \frac{1}{M2^n}\left|\sum_{k=0}^{m-1}e^{\frac{2\pi ikry}{2^n}}\right|^2$$

- Note that $p(y)$ is strongly peaked where $\frac{ry}{2^n}$ is an integer
  - Assuming m is large enough,

$$\sum_{k=0}^{m-1}e^{\frac{2\pi ikry}{2^n}}$$

averages out to 0, *except* when $e^{\frac{2\pi ikry}{2^n}} \cong 1$

- Alternatively, y is likely near $j\frac{2^n}{r}$ where j is an integer
- If we use $2n_o = n$ bits, $> 40\%$ probability that measured y is within $\frac{1}{2}$ of $j\frac{2^n}{r}$

- Determine partial sums of continued fractions expansions of $\frac{y}{2^n}$
  - Denominators of continued fractions are candidates for r (order of z mod N)
    - Test $z^r \equiv 1$ (mod N) to verify
  - Given r
    - There is a 50% chance that r is even
    - If so, $\gcd(z^{r/2} + 1, N)$ is a nontrivial factor of N
      - This follows from: $(z^{r/2} + 1)(z^{r/2} - 1) \equiv 0$ (mod N)
    - If not, select new z and repeat

Grover's Algorithm

- Setup
  - Input: a blackbox for computing unknown function $f: \{0,1\}^n \to \{0,1\}$
  - Details: $f(x) = 1$ if $x = a$ and $f(x) = 0$ if $x \neq a$
  - Problem: want to determine secret a, where $0 \leq a \leq N$

- Classical approach
  - Guess possible values of a
    - Assumption: can't do better than random guessing
  - Need $\sim\frac{N}{2}$ guesses on average

- Input $|\psi_0\rangle = |\mathbf{0}\rangle|1\rangle$

- Apply (n+1)-bit Hadamard

$$|\psi_1\rangle = H^{\otimes(n+1)}|\mathbf{0}\rangle|1\rangle = \frac{1}{\sqrt{2^n}}\sum_{z\in\{0,1\}^n}|\boldsymbol{z}\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$
$$= |\phi\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

- Apply blackbox $U_f: |\boldsymbol{x}\rangle|y\rangle \to |\boldsymbol{x}\rangle|y \oplus f(x)\rangle$

$$|\psi_2\rangle = U_f\left(|\phi\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)\right)$$

$$
\begin{aligned}
&= \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} |\boldsymbol{x}\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \\
&= \frac{1}{\sqrt{2^n}} \left(\sqrt{2^n - 1}\, |a_\perp\rangle - |a\rangle \right)_n \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \\
&= |\phi'\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)
\end{aligned}
$$

where

$$|\phi\rangle = H^{\otimes n} |\mathbf{0}\rangle = \frac{1}{\sqrt{2^n}} \left(\sqrt{2^n - 1}\ |a_\perp\rangle + |a\rangle \right)$$

$$|a_\perp\rangle = \frac{1}{\sqrt{2^n - 1}} \sum_{x \neq a} |\boldsymbol{x}\rangle$$

Applying U_f thus reflects the state $|\phi\rangle$ across the axis $|a_\perp\rangle$ to $|\phi'\rangle$

We can express U_f as the operator $V = I - 2|a\rangle\langle a|$ since

$$
\begin{aligned}
V|\phi\rangle &= V \left(\frac{1}{\sqrt{2^n}} \left(\sqrt{2^n - 1}\ |a_\perp\rangle + |a\rangle \right) \right) \\
&= |\phi\rangle - 2|a\rangle \left(\frac{1}{\sqrt{2^n}} \sqrt{2^n - 1}\ \langle a|a_\perp\rangle + \frac{1}{\sqrt{2^n}} \langle a|a\rangle \right) \\
&= |\phi\rangle - \frac{2}{\sqrt{2^n}} |a\rangle \\
&= |\phi'\rangle
\end{aligned}
$$

- Next, we reflect $|\phi'\rangle$ around $|\phi\rangle$ with the operator $W = -(I - 2|\phi\rangle\langle\phi|)$
    - Note that to reflect around $|a_\perp\rangle$ we subtracted twice the projection along $|a\rangle$, which is equivalent to reflecting around $|a\rangle$ and then negating
    - To reflect around $|\phi\rangle$, we thus reflect around $|\phi_\perp\rangle$ and negate

Note that

$$
\begin{aligned}
W &= -(I - 2|\phi\rangle\langle\phi|) \\
&= -H^{\otimes n} H^{\otimes n} + 2H^{\otimes n} |0\rangle\langle 0|) H^{\otimes n} \\
&= -H^{\otimes n} (I - 2|0\rangle_n \langle 0|_n) H^{\otimes n} \\
&= -H^{\otimes n} W' H^{\otimes n}
\end{aligned}
$$

But $W' = I - 2|0\rangle_n\langle 0|_n = \begin{pmatrix} -1 & & \cdots & & 0 \\ & 1 & & & \\ \vdots & & 1 & & \vdots \\ & & & \ddots & \\ 0 & & \cdots & & 1 \end{pmatrix}$

Crucially, W' has a circuit implementation.

Now our state $W|\phi'\rangle = WV|\phi\rangle$ makes an angle of 3θ with respect to $|a_\perp\rangle$ where previously it made an angle of θ

- We repeat the previous two steps until $(WV)^n|\phi\rangle$ is approximately equal to $|a\rangle$. Note that each iteration adds 2θ to the angle between $|\phi^{(k)}\rangle$ and $|a_\perp\rangle$.

  Then approximately

$$m = \frac{\pi/2}{2\theta} = \frac{\pi}{4\theta}$$

  iterations are needed to yield $|a\rangle$. But $\theta = \sin^{-1}\frac{1}{\sqrt{2^n}} \cong \frac{1}{\sqrt{2^n}}$, so m comes out to be

$$\frac{\pi}{4}\sqrt{2^n} = \pi\sqrt{2^{n-4}} = O(\sqrt{N})$$