Today's outline - February 14, 2023

- State-dependent amplitude and phase changes
- Deutch-Josza problem
- Bernstein-Vazirani problem

Reading Assignment: Reiffel: 7.7–7.8 Wong: 7.3–7.5

Homework Assignment #04:
due Friday, February 17, 2023

Exam #1 Tuesday, February 28, 2023
Covers Reiffel Chapters 2–5, HW# 1–4

State-dependent phase changes

Suppose we wish to apply a phase shift that depends on the state of a specific qubit, $|x\rangle \to e^{i\phi(x)}|x\rangle$ where there is an associated function $f : \mathbf{Z_n} \to \mathbf{Z_s}$ that is efficiently computable

The i^{th} bit of $f(x)$ is the i^{th} term of the binary expansion for the phase, $\phi(x) \approx 2\pi f(x)/2^s$

Given a transformation U_f that is efficient, it is possible to perform the state-dependent phase shift in $O(s)$ steps plus 2 invocations of U_f

Suppose that $f(x) = x$, we want a subroutine that changes the phase of an s-qubit standard basis state $|x\rangle$ by $\phi(x) = 2\pi x/2^s$ using the transformation

$$P(\phi) = T\left(-\tfrac{\phi}{2}\right) K\left(\tfrac{\phi}{2}\right) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix}$$

define $Phase\ |a[s]\rangle =$

1. **for** $i \in [0 \ldots s-1]$ — loop over all s bits in register $|a\rangle$
2. $P\left(\frac{2\pi}{2^i}\right)|a_i\rangle$ — apply the specified rotation to the i^{th} qubit

State-dependent phase changes

Using the subroutine $Phase : |a\rangle \rightarrow e^{i2\pi s/2^s}$ it is now possible to write a program that implements the n-qubit transformation $Phase_f : |x\rangle \rightarrow e^{i2\pi f(x)/2^s}$

	define $Phase_f\ |x[k]\rangle =$	
1.	**qubit** $a[s]$	create an s-qubit temporary register
2.	$U_f|x\rangle|a\rangle$	compute f in a
3.	$Phase\ |a\rangle$	perform phase shift by $2\pi a/2^s$
4.	$U_f^{-1}|x\rangle|a\rangle$	uncompute f

Step 2 entangles $|a\rangle$ with $|x\rangle$ and is set to the binary expansion of $\phi(x)$ for the desired phase shifts to $|x\rangle$

Step 3 changes the phase of $|a\rangle$ and also of $|x\rangle$ because they are entangled

Step 4 unentangles $|a\rangle$ from $|x\rangle$ leaving it in the desired state

State-dependent amplitude shifts

We wish to rotate each term in a superposition by a single qubit rotation $R(\beta(x))$ where $\beta(x)$ is state-dependent such that $|x\rangle \otimes |b\rangle \to |x\rangle \otimes (R(\beta(x))|b\rangle$

If $\beta(x) \approx 2\pi f(x)/2^s$ and $f : \mathbf{Z}_n \to \mathbf{Z}_s$ define a subroutine

define $Rot\ |a[s]\rangle|b[1]\rangle =$

1.	**for** $i \in [0 \ldots s-1]$	loop over all s bits in register $\|a\rangle$
2.	$\|a_i\rangle$ **control** $R\left(\frac{2\pi}{2^i}\right)\|b\rangle$	apply a controlled rotation to the $\|b\rangle$ qubit

The full program is thus

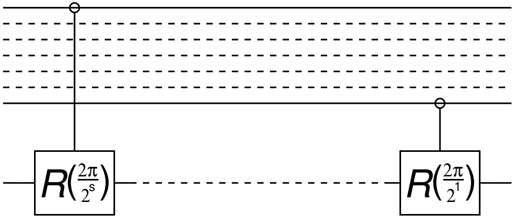
define $Rot_f\ |x[k]\rangle|b[1]\rangle =$

1.	**qubit** $a[s]$	create an s-qubit temporary register
2.	$U_f\|x\rangle\|a\rangle$	compute f in a
3.	$Rot\ \|a, b\rangle$	perform rotation by $2\pi a/2^s$
4.	$U_f^{-1}\|x\rangle\|a\rangle$	uncompute f

State-dependent amplitude shifts

define $Rot_f\ |x[k]\rangle|b[1]\rangle =$

1. **qubit** $a[s]$ — create an s-qubit temporary register
2. $U_f|x\rangle|a\rangle$ — compute f in a
3. $Rot\ |a, b\rangle$ — perform rotation by $2\pi a/2^s$
4. $U_f^{-1}|x\rangle|a\rangle$ — uncompute f



The Deutsch-Jozsa problem

This is a multi-qubit generalization of the Deutsch problem where a function is balanced if an equal number of input values return 0 and 1

Given a function $f : \mathbf{Z}_{2^n} \mapsto \mathbf{Z}_2$ that is known to be either constant or balanced, and a quantum oracle $U_f : |x\rangle|y\rangle \to |x\rangle|y \oplus f(x)\rangle$, determine whether the function f is constant or balanced

Start by using the $\phi = \pi$ phase change subroutine to negate terms of the superposition of basis vectors $|x\rangle$ with $f(x) = 1$ which returns

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} (-1)^{f(i)} |i\rangle$$

Next apply the Walsh transform to $|\psi\rangle$ recalling that for a vector $|r\rangle$, the Walsh transform is

$$W|r\rangle = \frac{1}{\sqrt{N}} \sum_{s=0}^{N-1} (-1)^{r \cdot s} |s\rangle$$

$$|\phi\rangle = W|\psi\rangle = \frac{1}{N} \sum_{i=0}^{N-1} \left((-1)^{f(i)} \sum_{j=0}^{N-1} (-1)^{i \cdot j} |j\rangle \right)$$

For each vector $|i\rangle$ in the sum that makes up $|\psi\rangle$, the Walsh transform applies a sign change depending on the number of common 1 bits between $|i\rangle$ and $|j\rangle$

The Deutsch-Jozsa problem

$$|\phi\rangle = \frac{1}{N}\sum_{i=0}^{N-1}\left((-1)^{f(i)}\sum_{j=0}^{N-1}(-1)^{i\cdot j}|j\rangle\right)$$

For constant $f(x)$, $|\phi\rangle = |0\rangle$

For balanced $f(x)$, $|\phi\rangle = |j\rangle \neq |0\rangle$

For constant f, $(-1)^{f(i)} = (-1)^{f(0)}$ is a global phase and can be pulled out of the sum

$$|\phi\rangle = (-1)^{f(0)}\frac{1}{N}\sum_{j=0}^{N-1}\left(\sum_{i=0}^{N-1}(-1)^{i\cdot j}\right)|j\rangle$$

But $$\sum_{x=0}^{N-1}(-1)^{x\cdot y} = \begin{cases} N & y = 0 \\ 0 & y \neq 0 \end{cases}$$

$$= (-1)^{f(0)}\frac{1}{N}\sum_{i=0}^{N-1}(-1)^{i\cdot 0}|0\rangle = (-1)^{f(0)}|0\rangle$$

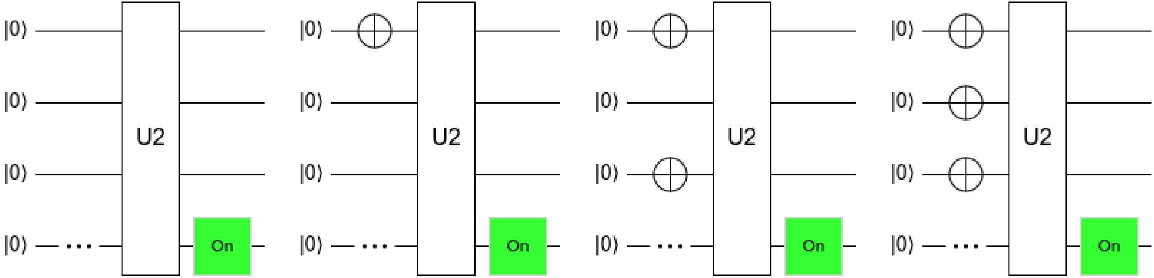
For balanced f, $f(i) = 0$ when $i \in X_0$ and the two internal sums must cancel when $|j\rangle = |0\rangle$ but not otherwise

$$|\phi\rangle = \frac{1}{N}\sum_{j=0}^{N-1}\left(\sum_{i\in X_0}(-1)^{i\cdot j} - \sum_{i\notin X_0}(-1)^{i\cdot j}\right)|j\rangle$$

This solves the Deutsch-Jozsa problem with a single call to U_f which is exponentially better than the classical solution

Deutsch-Jozsa – Quirk implementation

$$U_f : |x, y\rangle \to |x, y \oplus f(x)\rangle \qquad U_f : |x, 0\rangle \to |x, f(x)\rangle$$



https://tinyurl.com/3zujxrte

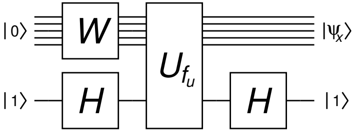
The Bernstein-Vazirani problem

The Bernstein-Vazirani problem is to determine the value of an unknown string u of bit length n using only queries of the form $q \cdot u$

The quantum algorithm can solve this using a single query to a transformation U_{f_u} where $f_u(q) = q \cdot u \mod 2$ and

$$U_{f_u} : |q\rangle|b\rangle \mapsto |q\rangle|b \oplus f_u(q)\rangle$$

This is solved by starting with the circuit that was used to apply the $\phi = \pi$ phase change which gives



$$|\psi_X\rangle = \frac{1}{\sqrt{N}} \sum_{q=0}^{N-1} (-1)^{f_u(q)} |q\rangle = \frac{1}{\sqrt{N}} \sum_{q=0}^{N-1} (-1)^{u \cdot q} |q\rangle$$

If the Walsh-Hadamard transformation is now applied to $|\psi_X\rangle$ we have

$$W|\psi_X\rangle = W \left(\frac{1}{\sqrt{N}} \sum_{q=0}^{N-1} (-1)^{u \cdot q} |q\rangle \right) = \frac{1}{\sqrt{N}} \sum_{q=0}^{N-1} (-1)^{u \cdot q} W|q\rangle = \frac{1}{N} \sum_{q=0}^{N-1} (-1)^{u \cdot q} \left(\sum_{z=0}^{N-1} (-1)^{q \cdot z} |z\rangle \right)$$

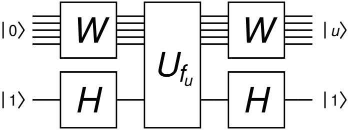
The Bernstein-Vazirani problem

$$
\begin{aligned}
W|\psi_X\rangle &= \frac{1}{N}\sum_{q=0}^{N-1}(-1)^{u\cdot q}\left(\sum_{z=0}^{N-1}(-1)^{q\cdot z}|z\rangle\right) \\
&= \frac{1}{N}\sum_{z=0}^{N-1}\left(\sum_{q=0}^{N-1}(-1)^{(u\oplus z)\cdot q}|z\rangle\right) \\
&= \frac{1}{N}\sum_{q=0}^{N-1}(-1)^{q\cdot 0}|u\rangle = \frac{1}{N}N|u\rangle = |u\rangle
\end{aligned}
$$

But from the discussion of the Hanning distance, we have that

$$(-1)^{u\cdot q+q\cdot z} \equiv (-1)^{(u\oplus z)\cdot q}$$

And the internal sum is zero unless $u \oplus z \equiv 0$ so only the term where $z \equiv u$ remains



This illustrates a common interpretation of how quantum circuits work, that is using parallelism to perform a computation on all possible inputs then manipulate the resulting superposition to get the result

https://tinyurl.com/fx3nyxj2