Today's outline - February 09, 2023

- Walsh-Hadamard transformation
- Deutch's problem
- Quantum subroutines
- State-dependent phase shift

Reading Assignment: Reiffel: 7.4–7.6 Wong: 7.3–7.5

Homework Assignment #05:
due Tuesday, February 21, 2023

Exam #1 Tuesday, February 28, 2023
Covers Rieffel Chapters 2-5; Homeworks 1-4

The Walsh-Hadamard matrix

In the standard basis, the matrix representation of W is a $2^n \times 2^n$ matrix with entries given by

$$W_{sr} = W_{rs} = \frac{1}{\sqrt{2^n}}(-1)^{r\cdot s}, \qquad 0 \le r, s \le 2^n - 1$$

This states that for a given string $|r\rangle$ the $|r\rangle^{th}$ column and row of W is a set of ± 1 values that depend on the number of common one-bits between $|r\rangle$ and each possible value of $|s\rangle$

The $|r\rangle^{th}$ column is the the Walsh-Hadamard transformation applied to $|r\rangle$ and is given by

$$W|r\rangle = \sum_{s=0}^{2^n-1} W_{rs}|s\rangle = \frac{1}{\sqrt{2^n}}\sum_{s=0}^{2^n-1}(-1)^{r\cdot s}|s\rangle$$

$$W|r\rangle = (H\otimes\cdots\otimes H)(|r_{n-1}\rangle\otimes\cdots\otimes|r_0\rangle) = \frac{1}{\sqrt{2^n}}[|0\rangle + (-1)^{r_{n-1}}|1\rangle]\otimes\cdots\otimes[|0\rangle + (-1)^{r_0}|1\rangle]$$

$$= \frac{1}{\sqrt{2^n}}\sum_{s=0}^{2^n-1}(-1)^{s_{n-1}r_{n-1}}|s_{n-1}\rangle\otimes\cdots\otimes(-1)^{s_0 r_0}|s_0\rangle = \frac{1}{\sqrt{2^n}}\sum_{s=0}^{2^n-1}(-1)^{r\cdot s}|s\rangle$$

A simple example

Consider a 2-qubit system where we wish to define the Walsh-Hadamard transformation matrix

For each of the 4 possible states $|00\rangle$, $|01\rangle$, $|10\rangle$, and $|11\rangle$ we can generate the transformation by $W|r\rangle = (H \otimes H)|r\rangle$

$$W|00\rangle = \tfrac{1}{2}\left[(|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle)\right] = \tfrac{1}{2}\left[|00\rangle + |01\rangle + |10\rangle + |11\rangle\right]$$

$$W|01\rangle = \tfrac{1}{2}\left[(|0\rangle + |1\rangle) \otimes (|0\rangle - |1\rangle)\right] = \tfrac{1}{2}\left[|00\rangle - |01\rangle + |10\rangle - |11\rangle\right]$$

$$W|10\rangle = \tfrac{1}{2}\left[(|0\rangle - |1\rangle) \otimes (|0\rangle + |1\rangle)\right] = \tfrac{1}{2}\left[|00\rangle + |01\rangle - |10\rangle - |11\rangle\right]$$

$$W|11\rangle = \tfrac{1}{2}\left[(|0\rangle - |1\rangle) \otimes (|0\rangle - |1\rangle)\right] = \tfrac{1}{2}\left[|00\rangle - |01\rangle - |10\rangle + |11\rangle\right]$$

$$W = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

A simple example

Now let's generate the W matrix using the relation $W_{sr} = W_{rs} = \frac{1}{\sqrt{2^n}}(-1)^{r \cdot s}$ with $0 \leq r, s \leq 2^n - 1$

$\vert r\rangle$	$\vert s\rangle$	W_{sr}
$\vert 00\rangle$	$\vert 00\rangle$	1
$\vert 00\rangle$	$\vert 01\rangle$	1
$\vert 00\rangle$	$\vert 10\rangle$	1
$\vert 00\rangle$	$\vert 11\rangle$	1
$\vert 01\rangle$	$\vert 01\rangle$	-1
$\vert 01\rangle$	$\vert 10\rangle$	1
$\vert 01\rangle$	$\vert 11\rangle$	-1
$\vert 10\rangle$	$\vert 10\rangle$	-1
$\vert 10\rangle$	$\vert 11\rangle$	-1
$\vert 11\rangle$	$\vert 11\rangle$	1

$$W = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

This is the identical matrix generated by the first method

Quantum parallelism

Suppose that we have two registers of qubits, $|x\rangle$ and $|y\rangle$ of length n and m, respectively

A linear transformation U_f which acts on the combined registers $|x\rangle \otimes |y\rangle$ acts on the registers as $U_f : |x, y\rangle \rightarrow |x, y \oplus f(x)\rangle$

This operator can also act on a superposition $\sum a_x |x\rangle$ as

$$U_f : \sum_x a_x |x, 0\rangle \quad \longrightarrow \quad \sum_x a_x |x, f(x)\rangle$$

Apply the U_f operator to the uniform superposition state obtained from the Walsh-Hadamard transformation

$$U_f : (W|0\rangle) \otimes |0\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle|0\rangle \quad \longrightarrow \quad \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle|f(x)\rangle$$

The resultant state is one where all 2^n $|f(x)\rangle$ values entangled with their corresponding input values, $|x\rangle$

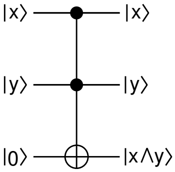
In principle, it is now possible to operate on all possible combinations simultaneously in an effect called quantum parallelism but other transformations must be applied to make it useful

The Toffoli gate

The Toffoli gate, computes the conjunction of two values, $|x\rangle$ and $|y\rangle$ with the output going to a register initially set to $|0\rangle$

First construct the universal superposition of the two input qubits

$$\begin{aligned} W(|00\rangle)\otimes|0\rangle &= \tfrac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\otimes\tfrac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\otimes|0\rangle \\ &= \tfrac{1}{2}(|000\rangle+|010\rangle+|100\rangle+|110\rangle) \end{aligned}$$



Applying the Toffoli gate, we have

$$\begin{aligned} T\left[W|00\rangle\otimes|0\rangle\right] &= T\left[\tfrac{1}{2}(|000\rangle+|010\rangle+|100\rangle+|110\rangle)\right] \\ &= \tfrac{1}{2}\left[|000\rangle+|010\rangle+|100\rangle+|111\rangle\right] \end{aligned}$$

While the entire truth table for the Toffoli gate is present in this entangled state, it is only possible to extract one value with a measurement of $|x\rangle\otimes|y\rangle$

Circuit complexity

A circuit family $\mathcal{C} = \{C_n\}$ is made up of circuits C_n indexed by their maximum input size, the circuit C_5 handles 5-qubit sized inputs

The circuit complexity of a circuit is the number of simple gates in the circuit

The complexity of a circuit family is the asymptotic number of simple gates expresesd in terms of the input size

Circuit complexity is important as it relates directly to the amount of resources required to perform the computation, thus a good model of circuit complexity is required when planning a quantum circuit

A valid model for circuit complexity must be both uniform and consistent

A quantum circuit family $\mathcal{C}$ is consistent if its circuits C_n gove consistent results: for all $m < n$, applying C_n to input $|x\rangle$ of size m must give the same result as applying C_m to the same input

A quantum circuit family $\mathcal{C}$ is polynomially uniform if there exists a polynomial $f(n)$ and a classical program that constructs the circuit C_n in at most $O(f(n))$ steps

Query complexity

The first quantum algorithms solve "black box" or "oracle" problems, where it is only possible to solve the problem by observing the output of the black box

A quantum black box behaves like the transformation U_f

$$U_f : \sum_x \alpha_x |x\rangle|y\rangle \quad \longrightarrow \quad \sum_x \alpha_x |x, f(x) \oplus y\rangle$$

The query complexity is defined as the number of times that the black box must be queried to solve the problem

If the query complexity of a black box is low, it is only of utility if its implementation is efficient, however, this approach is useful in setting lower bounds on the circuit complexity

If the query complexity is $\Omega(N)$, then the circuit complexity must be at least $\Omega(N)$

The value of black box problems in quantum computing was to demonstrate that a quantum algorithm has lower query complexity than a classical circuit that solves the same problem

Communication complexity

For communication problems, a complexity measure is the miniumum number of qubits that must be transmitted to accomplish a task

For example in the dense coding algorithm, complexity is related to the number of qubits that must be sent in order to communicate n bits of information

Classical protocols require the transmission of n bits while $n/2$ qubits plus an additional $n/2$ EPR pairs (or ebits) are needed for a quantum protocol

For quantum teleportation of n qubits, the number of classical bits sent is $2n$ plus an additional n ebits

Deutch's algorithm

The first truly quantum algorithm was described by Deutch in 1985 and demonstrated that quantum computation could outperform classical computation

$$\begin{array}{ll} f(0) \longrightarrow 0; & f(1) \longrightarrow 0 \\ f(0) \longrightarrow 1; & f(1) \longrightarrow 1 \\ f(0) \longrightarrow 0; & f(1) \longrightarrow 1 \\ f(0) \longrightarrow 1; & f(1) \longrightarrow 0 \end{array}$$

This black box problem determines whether a function, f is constant or balanced

Classically, this would require two calls to the black box, one for each value of the input bit, but with a quantum algorithm, only one call is necessary

Implementation requires a two-qubit unitary transformation $U_f|x\rangle|y\rangle \rightarrow |x\rangle|y \oplus f(x)\rangle$

$$U_f : |x\rangle|0\rangle \longrightarrow |x\rangle|f(x)\rangle$$

Applying U_f to two qubits in the Hadamard basis gives

$$\begin{aligned} U_f|+-\rangle &= U_f\left[\tfrac{1}{2}\big(|0\rangle + |1\rangle\big)\big(|0\rangle - |1\rangle\big)\right] \\ &= \tfrac{1}{2}\Big[|0\rangle\big(|0 \oplus f(0)\rangle - |1 \oplus f(0)\rangle\big) + |1\rangle\big(|0 \oplus f(1)\rangle - |1 \oplus f(1)\rangle\big)\Big] \end{aligned}$$

Deutch's algorithm

$$\begin{aligned} U_f|+\rangle|-\rangle &= \frac{1}{2}\Big[|0\rangle\big(|0\oplus f(0)\rangle - |1\oplus f(0)\rangle\big) + |1\rangle\big(|0\oplus f(1)\rangle - |1\oplus f(1)\rangle\big)\Big] \\ &= \frac{1}{2}\sum_{x=0}^{1}|x\rangle\big(|0\oplus f(x)\rangle - |1\oplus f(x)\rangle\big) \end{aligned}$$

when $f(x)=0$ then $\frac{1}{\sqrt{2}}\big(|0\oplus f(x)\rangle - |1\oplus f(x)\rangle\big) \longrightarrow \frac{1}{\sqrt{2}}\big(|0\rangle - |1\rangle\big) = +|-\rangle$

but if $f(x)=1$ then $\frac{1}{\sqrt{2}}\big(|0\oplus f(x)\rangle - |1\oplus f(x)\rangle\big) \longrightarrow \frac{1}{\sqrt{2}}\big(|1\rangle - |0\rangle\big) = -|-\rangle$

Thus, in a more compact notation, we write

$$U_f|+\rangle|-\rangle = \frac{1}{\sqrt{2}}\sum_{x=0}^{1}(-1)^{f(x)}|x\rangle|-\rangle$$

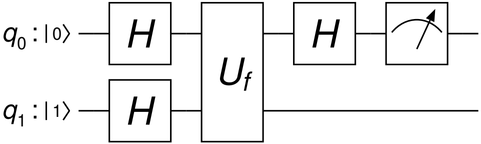
For $f(x)$ constant, both terms pick up the same phase shift and the state is $|+\rangle|-\rangle$

For $f(x)$ balanced, only one term picks up a phase shift, giving a result of $|-\rangle|-\rangle$

Deutch's algorithm

As a quantum circuit, Deutch's algorithm is implemented by

1. prepare two qubits: $q_0 = |0\rangle$ and $q_1 = |1\rangle$
2. apply the Hadamard transform to each qubit
3. apply the black box algorithm
4. apply the Hadamard transform to q_0
5. measure q_0 and interpret



(a) $q_0 = 0 \longrightarrow f(x)$ is constant

(b) $q_0 = 1 \longrightarrow f(x)$ is balanced

$$q_0 : |0\rangle \rightarrow |+\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big)$$

$$q_1 : |1\rangle \rightarrow |-\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle - |1\rangle\big)$$

$$U_f|+\rangle|-\rangle = \frac{1}{\sqrt{2}}\sum_{x=0}^{1}(-1)^{f(x)}|x\rangle|-\rangle$$

$f(x)$	$U_f\|q_0\rangle\|q_1\rangle$	q_0
$f(0) \rightarrow 0;\quad f(1) \rightarrow 0$	$+\|+\rangle\|-\rangle$	$\|+\rangle \rightarrow \|0\rangle$
$f(0) \rightarrow 1;\quad f(1) \rightarrow 1$	$-\|+\rangle\|-\rangle$	$\|+\rangle \rightarrow \|0\rangle$
$f(0) \rightarrow 0;\quad f(1) \rightarrow 1$	$+\|-\rangle\|-\rangle$	$\|-\rangle \rightarrow \|1\rangle$
$f(0) \rightarrow 1;\quad f(1) \rightarrow 0$	$-\|-\rangle\|-\rangle$	$\|-\rangle \rightarrow \|1\rangle$

Quantum subroutines

Subroutines are useful in quantum computing as they are for classical computations and often they utilize temporary qubits

These temporary qubits must be uncomputed as leaving them in the system could easily lead to entanglement which would destroy the computation

A subroutine that computes $\sum_i \alpha_i |x_i\rangle$ must not compute $\sum_i \alpha_i |x_i\rangle|y_i\rangle$ and simply throw away the qubits that store $|y_i\rangle$ unless it is certain that there is no entanglement with $|x_i\rangle$

There is no entanglement when we can write

$$\sum_i \alpha_i |x_i\rangle|y_i\rangle = \Big(\sum_i \alpha_i |x_i\rangle\Big) \otimes |y_i\rangle$$

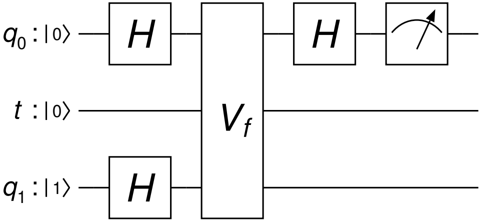
this is possible only when $|y_i\rangle \equiv |y_j\rangle$ for all values of i and j

For this reason, it is essential to uncompute $|y_i\rangle$ inside the subroutine before the output qubits are transmitted

Entanglement problems

Suppose the internal temporary computation, $|t\rangle$ in the Deutch example is made explicit in a transformation V_f such that

$$V_f : |x, t, y\rangle \rightarrow |x, t \oplus x, y \oplus f(x)\rangle$$



Deutch's algorithm now will not function properly

$$q_0 : |0\rangle \rightarrow |+\rangle = \tfrac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big), \qquad |t\rangle : |0\rangle, \qquad q_1 : |1\rangle \rightarrow |-\rangle = \tfrac{1}{\sqrt{2}}\big(|0\rangle - |1\rangle\big)$$

$$V_f(|+\rangle|0\rangle|-\rangle) = V_f\left(\frac{1}{\sqrt{2}}\sum_{x=0}^{1}|x\rangle|0\rangle|-\rangle\right) = \frac{1}{\sqrt{2}}\sum_{x=0}^{1}(-1)^{f(x)}|x\rangle|x\rangle|-\rangle$$

For $f(x)$ constant or balanced the V_f transformation yields

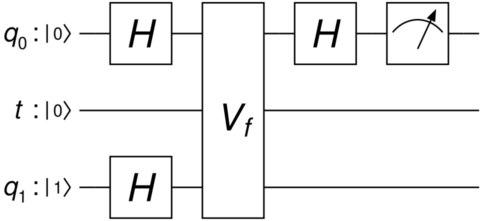
$$f(x)\ \text{constant} \quad \longrightarrow \quad V_f(|+\rangle|0\rangle|-\rangle) = (|00\rangle + |11\rangle)|-\rangle$$

$$f(x)\ \text{balanced} \quad \longrightarrow \quad V_f(|+\rangle|0\rangle|-\rangle) = (|00\rangle - |11\rangle)|-\rangle$$

Entanglement problems

$f(x)$ constant $\longrightarrow V_f(|+\rangle|0\rangle|-\rangle) = (|00\rangle + |11\rangle)|-\rangle$

$f(x)$ balanced $\longrightarrow V_f(|+\rangle|0\rangle|-\rangle) = (|00\rangle - |11\rangle)|-\rangle$



The final step of applying the Hadamard transformation to q_0 uses the $H \otimes I \otimes I$ transformation which yields

$f(x)$ constant $$H \otimes I \otimes I(|00\rangle + |11\rangle)|-\rangle = \tfrac{1}{2}(|00\rangle + |10\rangle + |01\rangle - |11\rangle)|-\rangle$$

$f(x)$ balanced $$H \otimes I \otimes I(|00\rangle - |11\rangle)|-\rangle = \tfrac{1}{2}(|00\rangle + |10\rangle - |01\rangle + |11\rangle)|-\rangle$$

The q_0 qubit can be measured to be $|0\rangle$ or $|1\rangle$ with equal probability in both cases since two of the terms do not cancel but by uncomputing the t qubit, the states would be left as

$f(x)$ constant $$H \otimes I \otimes I(|00\rangle + |10\rangle)|-\rangle = \tfrac{1}{2}(|00\rangle + \cancel{|10\rangle} + |00\rangle - \cancel{|10\rangle})|-\rangle = |0\rangle|0\rangle|-\rangle$$

$f(x)$ balanced $$H \otimes I \otimes I(|00\rangle - |10\rangle)|-\rangle = \tfrac{1}{2}(\cancel{|00\rangle} + |10\rangle - \cancel{|00\rangle} + |10\rangle)|-\rangle = |1\rangle|0\rangle|-\rangle$$

Phase change for a subspace

Suppose we have a superposition state given by $|\psi\rangle = \sum a_i|i\rangle$

We wish to change the phase of every term $|i\rangle$ in the superposition if $|i\rangle \in X$ where X is a subset of the entire space $\{0, 1, \dots, N-1\}$

The goal is to find an efficient implementation of the transformation S_X^ϕ where

$$S_X^\phi \sum_{x=0}^{N-1} a_x|x\rangle = \sum_{x\in X} a_x e^{i\phi}|x\rangle + \sum_{x\notin X} a_x|x\rangle$$

Clearly it is possible to find a brute force implementation using the methods of Chapter 5, however we want an efficient implementation to determine if a state is in a specific subspace

We want a function $f(x) : \mathbf{Z}_{2^n} \to \mathbf{Z}_2$ that takes the natural numbers (represented by $\mathbf{Z}$) modulo 2^n into the natural numbers modulo 2 such that

$$f(x) = \begin{cases} 1 & x \in X \\ 0 & x \notin X \end{cases}$$

The depends on being able to compute membership in X efficiently but if this is possible with a quantum transformation U_f then through the use of a temporary qubit, it is possible to compute S_X^ϕ

Phase change for a subspace

The procedure is to use the temporary qubit to compute $f(x)$, then use the result of $f(x)$ to apply the phase change and finally uncompute the temporary qubit to avoid entanglement

The pseudo-code (Box 6.2 in text) is as follows

```
define $Phase_f(\phi)|x[k]\rangle =$
    qubit $a[1]$                       create a single qubit $a$ and set it to $|0\rangle$
    $U_f|x, a\rangle$                  compute $f(x) \longrightarrow a$
    $K(\frac{\phi}{2})|a\rangle$       apply a phase shift
    $T(-\frac{\phi}{2})|a\rangle$      apply a phase rotation
    $U_f^{-1}|x, a\rangle$             uncompute $f(x)$ to disentangle $a$
```

The TK sequence serves to apply a rotation only if a is equal to $|1\rangle$

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

Phase change of π

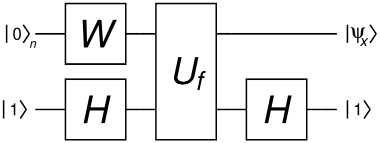
For the special case of $\phi = \pi$ there is an even simpler implementation

S^{π}_{X} can be implemented by starting with the temporary qubit b in a superposition state
$b : |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

Suppose the initial state is given by

$$|\psi\rangle = \sum_{x\in X} a_x|x\rangle + \sum_{x\notin X} a_x|x\rangle$$

$$\begin{aligned} U_f(|\psi\rangle \otimes |-\rangle) &= U_f\left(\sum_{x\in X} a_x|x\rangle \otimes |-\rangle\right) + U_f\left(\sum_{x\notin X} a_x|x\rangle \otimes |-\rangle\right) \\ &= -\left(\sum_{x\in X} a_x|x\rangle \otimes |-\rangle\right) + \left(\sum_{x\notin X} a_x|x\rangle \otimes |-\rangle\right) = (S^{\pi}_{X}|\psi\rangle) \otimes |-\rangle \end{aligned}$$



The circuit starts with a uniform superposition of an n-qubit register and an acilla qubit in the $|1\rangle$ state to create the superposition $|\psi_X\rangle = \sum(-1)^{f(x)}|x\rangle$