Presentation Notes – Week 2

Private Reading: Quantum Computing
February 21, 2025
Oberlin College
Iago B. Mendes

1. Computational process

- Registers: Qbits used as input or output

$$|x\rangle_n |y\rangle_m \tag{1}$$

(for n input Qbits and m output Qbits)

- Definition of unitary actions:

$$\hat{U}_f(|x\rangle_n |y\rangle_m) = |x\rangle_n |y \oplus f(x)\rangle_m \tag{2}$$

"$\oplus$" = exclusive or (module-2 bitwise addition with no carrying)
Example: $1101 \oplus 0111 = 1010$
Note:

$$\hat{U}_f(|x\rangle_n |0\rangle_m) = (|x\rangle_n |f(x)\rangle_m) \tag{3}$$

$$\hat{U}_f(|x\rangle_n |1\rangle_m) = (|x\rangle_n |\tilde{f}(x)\rangle_m) \tag{4}$$

- Hadamard transformation:

$$
\begin{aligned}
(\hat{H} \otimes \hat{H})(|0\rangle \otimes |0\rangle) &= (\hat{H}|0\rangle)(\hat{H}|0\rangle) && (5)\\
&= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) && (6)\\
&= \frac{1}{2}(|0\rangle|0\rangle + |0\rangle|1\rangle + |1\rangle|0\rangle + |1\rangle|1\rangle) && (7)\\
&= \frac{1}{2}(|0\rangle_2 + |1\rangle_2 + |2\rangle_2 + |3\rangle_2) && (8)
\end{aligned}
$$

For n Qbits:

$$
\begin{aligned}
\hat{H}^{\otimes n}|0\rangle_n &= (\hat{H} \otimes \hat{H} \otimes \cdots \otimes \hat{H})|0\rangle_n && (9)\\
&= \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle_n && (10)
\end{aligned}
$$

- "Quantum parallelism":

$$
\begin{aligned}
\hat{U}_f(\hat{H}^{\otimes n} \otimes \hat{1}_m)(|0\rangle_n |0\rangle_m) &= \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} \hat{U}_f(|x\rangle_n |0\rangle_m) && (11)\\
&= \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle_n |f(x)\rangle_m && (12)
\end{aligned}
$$

Note: state depends on all 2^n evaluations of f
Wrong typical conclusion: "Where were all those calculations done? In parallel universes!"
This is the same mistake as saying that a superposed state is defined, but we don't know what it is.

State after measurement: $|x_0\rangle f(x_0)$
(we only have the evaluation of $f(x_0)$)

2. Deutsch's problem

- Let $f : \{0,1\} \to \{0,1\}$
- 4 possibilities:

$f(0)$	$f(1)$
0	0
0	1
1	0
1	1

- Question: is f constant?
- Classical computer: 2 evaluations
  - Find and compare the values of $f(0)$ and $f(1)$
- Quantum computer: 1 evaluation
  - Start with $|0\rangle|0\rangle$
  - Apply $(\hat{X} \otimes \hat{X})$

$$|1\rangle|1\rangle \tag{13}$$

  - Apply $(\hat{H} \otimes \hat{H})$

$$\frac{1}{2}(|0\rangle - |1\rangle)(|0\rangle - |1\rangle) \tag{14}$$

$$\frac{1}{2}(|0\rangle|0\rangle - |0\rangle|1\rangle - |1\rangle|0\rangle + |1\rangle|1\rangle) \tag{15}$$

  - Apply $\hat{U}_f$

$$\frac{1}{2}(|0\rangle|f(0)\rangle - |0\rangle|\tilde{f}(0)\rangle - |1\rangle|f(1)\rangle + |1\rangle|\tilde{f}(1)\rangle) \tag{16}$$

    * If $f = \text{const}$, $f(1) = f(0)$ and $\tilde{f}(1) = \tilde{f}(0)$

$$\frac{1}{2}(|0\rangle|f(0)\rangle - |0\rangle|\tilde{f}(0)\rangle - |1\rangle|f(0)\rangle + |1\rangle|\tilde{f}(0)\rangle) \tag{17}$$

$$\frac{1}{2}(|0\rangle - |1\rangle)(|f(0)\rangle - |\tilde{f}(0)\rangle) \tag{18}$$

* If $f \neq$ const, $f(1) = \tilde{f}(0)$ and $\tilde{f}(1) = f(0)$

$$\frac{1}{2}(|0\rangle|f(0)\rangle - |0\rangle|\tilde{f}(0)\rangle - |1\rangle|\tilde{f}(0)\rangle + |1\rangle|f(0)\rangle) \tag{19}$$

$$\frac{1}{2}(|0\rangle + |1\rangle)(|f(0)\rangle - |\tilde{f}(0)\rangle) \tag{20}$$

- Apply $(\hat{H} \otimes \hat{1})$
Note: Hadamard only on the input register

* $f =$ const:

$$\frac{1}{2}\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle - |0\rangle + |1\rangle)(|f(0)\rangle - |\tilde{f}(0)\rangle) \tag{21}$$

$$\frac{1}{\sqrt{2}}|1\rangle(|f(0)\rangle - |\tilde{f}(0)\rangle) \tag{22}$$

* $f \neq$ const:

$$\frac{1}{2}\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle + |0\rangle - |1\rangle)(|f(0)\rangle - |\tilde{f}(0)\rangle) \tag{23}$$

$$\frac{1}{\sqrt{2}}|0\rangle(|f(0)\rangle - |\tilde{f}(0)\rangle) \tag{24}$$

Answer to problem: $f =$ const if and only if the input register is 1!
Note: the output register has no use because it can be $f(0)$ or $\tilde{f}(0)$

- Trade-off: in the quantum computation above, we don't find the actual value of the function. That is, we don't know $f(0)$ or $f(1)$. Therefore, we have only eliminated 2 options out of the 4 possibilities for f.

3. Bernstein-Vazirani problem

- Let $0 \leq a, x < 2^n$ and $f(x) = a \cdot x = a_0 x_0 \oplus a_1 x_1 \oplus \ldots$
- Question: what is a?
- Classical computer: n evaluations of f
  - Find each bit of a with $a \cdot 2^m$ for $0 \leq m < n$
  Note: only the mth bit in 2^m is 1, all the others are 0
- Quantum computer: 1 evaluation
  - We can use the same process as before, but the circuit explanation below is more intuitive.

– Represent an implementation of $\hat{U}_f$

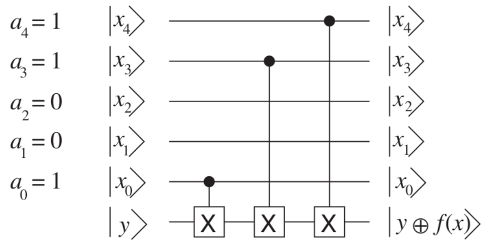

Figure 1

In the example above, $a = 11001 = 25$

– Sandwich the $\hat{U}_f$ gate with Hadamard gates

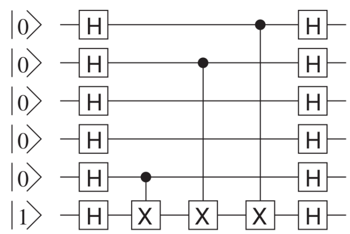

Figure 2

– Use the identity $(\hat{H}_i\hat{H}_j)\hat{C}_{ij}(\hat{H}_i\hat{H}_j) = \hat{C}_{ji}$

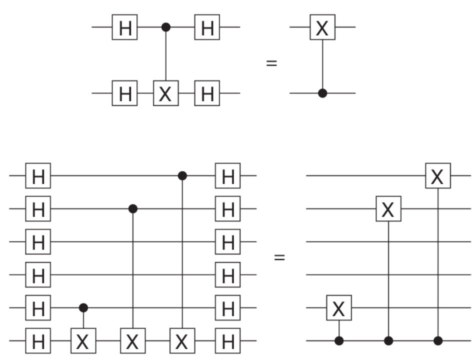

Figure 3

– Now that the output register is the control bit for all cNOT gates, we can create a copy of a in the input registers by setting the output bit to 1

Mathematically:

$$\hat{H}^{\otimes(n+1)}\hat{U}_f\hat{H}^{\otimes(n+1)}|0\rangle_n|1\rangle_1 = |a\rangle_n|1\rangle_1 \tag{25}$$

- Note: we went from $O(n)$ in the classical computer to $O(1)$ in the quantum computer. In Simon's problem, we go from $O(2^{n/2})$ to $O(n)$.