Chapter 10 Quantum Algorithms

Joe Song

November 20, 2019

The notes are loosely based on Chapter 10 of Dasgupta, Papadimitriou and Vazirani. Algorithms. 2008. McGraw-Hill. New York.

1 Qubits

Superposition principle: If a quantum system can be in one of two states, then it can also be in any linear combination of the two states.

1.1 A single qubit

The generic quantum state:

$$|a\rangle = a_0 |0\rangle + a_1 |1\rangle$$

a_0: a complex number, the amplitude of state $|0\rangle$
a_1: a complex number, the amplitude of state $|1\rangle$

with

$$|a_0|^2 + |a_1|^2 = 1$$

If measured, a qubit collapses to a classical single bit with the following probabilities:

$$\Pr(0) = |a_0|^2, \quad \Pr(1) = |a_1|^2$$

1.2 Double qubits

The generic quantum state

$$|a\rangle = a_{00} |00\rangle + a_{01} |01\rangle + a_{10} |10\rangle + a_{11} |11\rangle$$

with

$$|a_{00}|^2 + |a_{01}|^2 + |a_{10}|^2 + |a_{11}|^2 = 1$$

If measured, we get two classical bits with the following probabilities:

$$\Pr(00) = |a_{00}|^2, \quad \Pr(01) = |a_{01}|^2, \quad \Pr(10) = |a_{10}|^2, \quad \Pr(11) = |a_{11}|^2$$

1.3 Three qubits

The generic quantum state

$$|a\rangle = a_{000}\,|000\rangle + a_{001}\,|001\rangle + a_{010}\,|010\rangle + a_{011}\,|011\rangle + a_{100}\,|100\rangle + a_{101}\,|101\rangle + a_{110}\,|110\rangle + a_{111}\,|111\rangle$$

with

$$|a_{000}|^2 + |a_{001}|^2 + |a_{010}|^2 + |a_{011}|^2 + |a_{100}|^2 + |a_{101}|^2 + |a_{110}|^2 + |a_{111}|^2 = 1$$

If measured, we get three classical bits with probability:

$$\Pr(000) = |a_{000}|^2, \quad \Pr(001) = |a_{001}|^2, \quad \Pr(010) = |a_{010}|^2, \quad \Pr(011) = |a_{011}|^2$$

$$\Pr(100) = |a_{100}|^2, \quad \Pr(101) = |a_{101}|^2, \quad \Pr(110) = |a_{110}|^2, \quad \Pr(111) = |a_{111}|^2$$

A state of three (3) qubits can carry information about all eight (2^3) possible states of three classical bits!

quantum memory $\gg$ classical memory

2 Hadamard transform

1. Defintion:

$$H(|0\rangle) = \frac{1}{\sqrt{2}}\,|0\rangle + \frac{1}{\sqrt{2}}\,|1\rangle$$

$$H(|1\rangle) = \frac{1}{\sqrt{2}}\,|0\rangle - \frac{1}{\sqrt{2}}\,|1\rangle$$

2. Hadamard transform is linear:

$$H(a_0\,|0\rangle + a_1\,|1\rangle) = a_0 H(|0\rangle) + a_1 H(|1\rangle) = \frac{a_0 + a_1}{\sqrt{2}}\,|0\rangle + \frac{a_0 - a_1}{\sqrt{2}}\,|1\rangle$$

3. Hadamard transform is its own inverse:

$$
\begin{aligned}
&H(H(a_0 |0\rangle + a_1 |1\rangle)) && (1)\\
=&H\left(\frac{a_0 + a_1}{\sqrt{2}} |0\rangle + \frac{a_0 - a_1}{\sqrt{2}} |1\rangle\right) && (2)\\
=&\frac{\frac{a_0+a_1}{\sqrt{2}} + \frac{a_0-a_1}{\sqrt{2}}}{\sqrt{2}} |0\rangle + \frac{\frac{a_0+a_1}{\sqrt{2}} - \frac{a_0-a_1}{\sqrt{2}}}{\sqrt{2}} |1\rangle && (3)\\
=&a_0 |0\rangle + a_1 |1\rangle && (4)
\end{aligned}
$$

Applying Hadamard transform twice on a qubit will get back the original qubit!

4. Quantum parallelism: create a superposition of all possible 2^n states

By applying tensor product on the Hadamard transform of $|0\rangle$:

$$
\begin{aligned}
&(H \otimes H \otimes \cdots \otimes H) |00\ldots0\rangle && (5)\\
=&\frac{1}{\sqrt{2^n}}[(|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) \otimes \cdots \otimes (|0\rangle + |1\rangle)] && (6)\\
=&\frac{1}{\sqrt{2^n}}(|0\ldots00\rangle + |0\ldots01\rangle + |0\ldots10\rangle + \cdots + |1\ldots11\rangle) && (7)\\
=&\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle && (8)
\end{aligned}
$$

Tensor product:

$$
(|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) = |00\rangle + |01\rangle + |10\rangle + |11\rangle
$$

5. Generally,

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

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

3 Solving a linear equation

Given $f(x) = u \cdot x \mod 2$. x is an input binary number of n-bits. u is an unknown binary number of n bits. Design an algorithm to determine u.

---

procedure find-u($f(x)$)

$x = 0\ldots01$

for $i \in 1,\ldots,n$:

  $u[i] = f(x)$

  $x = x << 1$ (shift left by 1 bit)

return u

Runtime: $O(n^2)$

4 Quantum algorithm solution

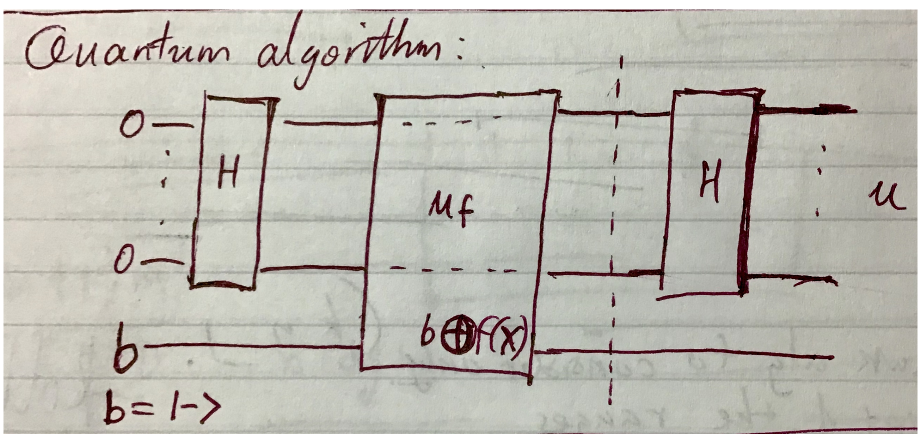

Figure 1: Quantum algorithm solution to linear equations. Runtime is constant in three steps.

Define

$$|-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

$$
\begin{aligned}
|-\rangle \oplus f(x) &= \frac{1}{\sqrt{2}}\,|0 \oplus f(x)\rangle - \frac{1}{\sqrt{2}}\,|1 \oplus f(x)\rangle && (9)\\
&= \begin{cases} \frac{1}{\sqrt{2}}\,|0 \oplus 0\rangle - \frac{1}{\sqrt{2}}\,|1 \oplus 0\rangle & f(x) = 0 \\ \frac{1}{\sqrt{2}}\,|0 \oplus 1\rangle - \frac{1}{\sqrt{2}}\,|1 \oplus 1\rangle & f(x) = 1 \end{cases} && (10)\\
&= \begin{cases} \frac{1}{\sqrt{2}}\,|0\rangle - \frac{1}{\sqrt{2}}\,|1\rangle & f(x) = 0 \\ \frac{1}{\sqrt{2}}\,|1\rangle - \frac{1}{\sqrt{2}}\,|0\rangle & f(x) = 1 \end{cases} && (11)\\
&= \begin{cases} |-\rangle & f(x) = 0 \\ -\,|-\rangle & f(x) = 1 \end{cases} && (12)\\
&= (-1)^{f(x)}\,|-\rangle && (13)
\end{aligned}
$$

After U_f, we have all $n+1$ qubits as

$$
\begin{aligned}
& H(|0\rangle) \otimes [|-\rangle \oplus f(x)] && (14)\\
=& \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle \otimes (-1)^{f(x)}\,|-\rangle && (15)\\
=& \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{f(x)}\,|x\rangle\,|-\rangle && (16)\\
=& \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{u \cdot x}\,|x\rangle\,|-\rangle && (17)
\end{aligned}
$$

After the second Hadamard transform on the first n-bits $|x\rangle$, we get

$$
H\left[\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{u \cdot x}\,|x\rangle\,|-\rangle\right] = |u\rangle
$$