Excursions in Computing Science: Week 7b. Quantum Computing

P. Hayden*
McGill University, Montreal, Canada

April 20, 2012

I. Prefatory Notes

1. The "strong" Church-Turing thesis, that any real-world computation can be efficiently simulated on a Turing Machine is a fundamental assumption of C.S.—but quantum computing provides a counterexample, by computing faster than a Turing Machine can in principle. (For Turing Machine, read PC with unbounded memory: see Week 11.)

2. Here is a switch-light question: is a light switch connected to a light? or: does this switch control that light?

Let $f : \{0,1\} \to \{0,1\}$ represent the connection: 0 means "off" and 1 means "on"; the 0 or 1 on the left of the $\to$ refer to the switch; the 0 or 1 on the right of the $\to$ refer to the light. $f(0)$ is the state of the light if the switch is off and $f(1)$ is the state of the light if the switch is on.

Then there is no effect on the light if $f(0) = f(1)$
and there is a connection if $f(0) \neq f(1)$.

The switch-light question becomes "does $f(0) = f(1)$ or does $f(0) \neq f(1)$?".

Classical computing requires two invocations to the function $f()$ to answer this question. We are going to see that quantum computing needs only one [Deu85].

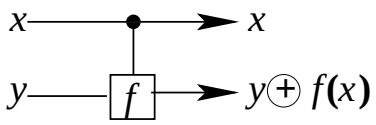
3. Logic circuits are built out of "gates", elementary components that can be used repeatedly to assemble the circuit. We will build a pre-quantum circuit to answer the switch-light question using a **not** gate and a specialized gate for the function, $f()$, that represents the switch. We will then build a quantum circuit to do the same thing using a **Hadamard** gate and the specialized gate for $f()$.

Here are the **not** and **Hadamard** gates, and a small circuit using $f()$ to produce $f()$ applied to one input "exclusively ored" with a second input.

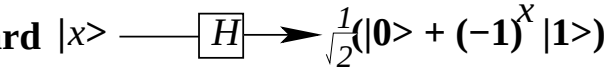
Transcribed by THM from a lecture on 2007/2/28 by PH.

not

switch



Hadamard



(The symbol $\oplus$ is the binary operator **xor** (exclusive-or), with the following truth-table (see Week 10)

x	y	$x \oplus y$
0	0	0
0	1	1
1	0	1
1	1	0

that is, $x \oplus y$ is 1 if and only if x and y differ.
This means that $f(0) \oplus f(1)$ is what we must calculate to answer the switch-light question: it is 0 if $f(0) = f(1)$ and 1 otherwise.
Note that $0 \oplus y = y$, $1 \oplus y =$ **not** y, and that $\oplus$ is commutative and associative.)

The **not** gate and the **switch** circuit with $f()$ are written as pre-quantum, with the variables x and y standing in for the truth values 0 and 1.

The **Hadamard** gate is for the quantum computer. The truth values and variables are written inside Dirac kets (see Week 6), which serve here purely to enable us to write combinations of them, such as $| 0 >| 1 >$, and not get them mixed up—they do not commute.

It is useful to spell out the notation shown for the Hadamard gate. Here it is with the variable x taking on its two possible values, 0 and 1.

$$\begin{aligned} H \mid 0 > &= \frac{1}{\sqrt{2}}(\mid 0 > + \mid 1 >) \\ H \mid 1 > &= \frac{1}{\sqrt{2}}(\mid 0 > - \mid 1 >) \end{aligned}$$

Or, again, here it is in matrix form, with $| 0 >$ represented as the vector $(1,0)^T$ and $| 1 >$ represented as $(0,1)^T$.

$$\begin{aligned} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \\ \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \end{aligned}$$

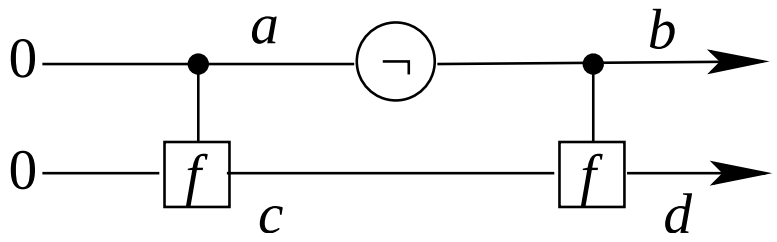
Note that H is its own inverse:

$$\begin{aligned} \mid 0 > &\rightarrow \frac{1}{\sqrt{2}}(\mid 0 > + \mid 1 >) \rightarrow \frac{1}{2}(\mid 0 > + \mid 1 > + (\mid 0 > - \mid 1 >)) = \mid 0 > \\ \mid 1 > &\rightarrow \frac{1}{\sqrt{2}}(\mid 0 > - \mid 1 >) \rightarrow \frac{1}{2}(\mid 0 > + \mid 1 > - (\mid 0 > - \mid 1 >)) = \mid 1 > \end{aligned}$$

or

$$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

4. Here is the pre-quantum circuit to answer the switch-light question, using only the pre-quantum **not** gate and the **xor** circuit involving $f()$.



The values at points a, b, c and d are

a 0

b 1

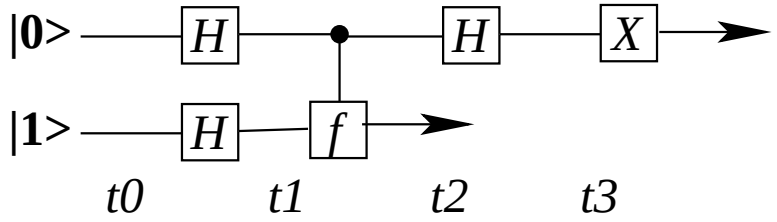
c $0 \oplus f(0) = f(0)$

d $f(0) \oplus f(1)$

so that d answers the switch-light question.

Note that the pre-quantum circuit must use $f()$ twice.

5. Here is the quantum-mechanical circuit to answer the switch-light question, using only the **Hadamard** gate and the **xor** circuit involving $f()$. (X is the operation of measuring the result, which converts from the quantum state to macroscopic observation.)



We can write the values at the various times t_0, t_1, t_2 and t_3 as combinations |upper>|lower>—and we can see why this notation is useful and why juxtaposition of kets is not commutative.

t_0

$$| 0 >| 1 >$$

t_1

$$\begin{aligned} H \mid 0 > H \mid 1 > &= \frac{1}{\sqrt{2}}(| 0 > + | 1 >)\frac{1}{\sqrt{2}}(| 0 > - | 1 >) \\ &= \frac{1}{2}(| 0 >| 0 > - | 0 >| 1 > + | 1 >| 0 > - | 1 >| 1 >) \end{aligned}$$

For steps t_2 and t_3 we will consider two cases.

Case i: $f(0) = f(1) \stackrel{\text{def}}{=} c$

t_2

$$\begin{aligned} & \frac{1}{2}(\mid 0 >\mid 0 \oplus c > - \mid 0 >\mid 1 \oplus c > + \mid 1 >\mid 0 \oplus c > - \mid 1 >\mid 1 \oplus c >) \\ = \; & \frac{1}{2}(\mid 0 >\mid c > - \mid 0 >\mid 1 \oplus c > + \mid 1 >\mid c > - \mid 1 >\mid 1 \oplus c >) \\ = \; & \frac{1}{\sqrt{2}}(\mid 0 > + \mid 1 >)\frac{1}{\sqrt{2}}(\mid c > - \mid 1 \oplus c >) \end{aligned}$$

t_3

$$\mid 0 > \frac{1}{\sqrt{2}}(\mid c > - \mid 1 \oplus c >)$$

(The result for t_3 follows because H is its own inverse: check this!)

Note that at t_3 the upper channel always has the value $\mid 0 >$, which is the result we want if $f(0) = f(1)$,

Case ii: $f(0) \stackrel{\text{def}}{=} c; f(1) = c' = 1 \oplus c$

t_2

$$\begin{aligned} & \frac{1}{2}(\mid 0 >\mid 0 \oplus c > - \mid 0 >\mid 1 \oplus c > + \mid 1 >\mid 0 \oplus 1 \oplus c > - \mid 1 >\mid 1 \oplus 1 \oplus c >) \\ = \; & \frac{1}{2}(\mid 0 >\mid c > - \mid 0 >\mid 1 \oplus c > + \mid 1 >\mid 1 \oplus c > - \mid 1 >\mid c >) \\ = \; & \frac{1}{\sqrt{2}}(\mid 0 > - \mid 1 >)\frac{1}{\sqrt{2}}(\mid c > - \mid 1 \oplus c >) \end{aligned}$$

t_3

$$\mid 1 > \frac{1}{\sqrt{2}}(\mid c > - \mid 1 \oplus c >)$$

Note that at t_3 the upper channel always has the value $\mid 1 >$, which is the result we want if $f(0) \neq f(1)$,

So the upper channel answers the switch-light question in both cases—and we used $f()$ only once.

6. We can abstract from this to a discussion of *state spaces*.

The pre-quantum state space is

$$\sum_{x,y} c_{x,y} \mid x >\mid y >= \{\mid 0 >\mid 0 >, \mid 0 >\mid 1 >, \mid 1 >\mid 0 >, \mid 1 >\mid 1 >, \}$$

with $c_{x,y} \in \{0, 1\}$ and $\sum_{x,y} c_{x,y} = 1$.

The quantum state space is

$$\sum_{x,y} c_{x,y} \mid x >\mid y >$$

with $c_{x,y} \in \mathcal{C}$, the 2-numbers, and $\sum_{x,y} \mid c_{x,y} \mid^2 = 1$.

(This quantum-mechanical (QM) state space permits "unreal" states such as

$$\frac{1}{\sqrt{2}}(\mid 0 >\mid 0 > - \mid 1 >\mid 1 >)$$

which cannot be factored in the way we did above at time t_2, and are thus "entangled". Such states underly the puzzles of EPR, supported by the experiments of Aspect et al. and Gisin. Note that under QM, locality and realism are inconsistent with each other: locality means there are no instant effects (faster than lightspeed); realism means we can isolate parts of the system.)

7. Developments after Deutsch's seminal 1985 paper

- 1993: potential ability to crack most public-key encryptions by factoring large integers, but also—
- unbreakable cryptography;
- search an unordered list of n elements in $\mathcal{O}(\sqrt{(}\backslash))$ time;
- Feb. 2007: speed up game tree search (e.g., chess) by factor $\sqrt{(}n)$, where n is roughly the number of moves that would need to be checked.

8. Physical construction of quantum computers

- ion trap: ions are qbits: gates by laser, e.g., H by shining the light for half the time needed to cause a transition;
- nuclear spins in molecules are qbits: gates by changing bonds;
- up to 13 qbits from liquid states of MRI (magnetic resonance imaging);
- superconductors on the surface of liquid helium

Note: the bottleneck is in the measurement step: parallelism ends at the boundary between QM and pre-quantum physics.

9. Summary

(These notes show the trees. Try to see the forest!)

A quantum computer can compare $f(0)$ and $f(1)$ by invoking $f()$ only once, while a pre-quantum computer must invoke it twice.

II. The Excursions

You've seen lots of ideas. Now *do* something with them!

1. What is the relationship between the Hadamard matrix, H, and the rotation operators $R_z(\pi)$ and $R_y(\pi/2)$ from Week 6?
2. Look up Einstein, Podolsky and Rosen's thought experiment, "EPR" (1935), and the experiments of Alain Aspect et al. (1982) and of Nicolas Gisin (1984).
3. Any part of the lecture that needs working through.

References

[Deu85] David Deutsch. Quantum theory, the Church-Turing principle and the universal quantum computer. *Proc. R. Soc. Lond.*, A400:97–117, 1985.