Homework #9. Due Tue 10/23.

#1 – Let $0 \leq x, z < 2^n$ be two numbers in the range indicated. Prove that the sum

$$\sum_{y=0}^{2^n-1} (-1)^{(x\oplus z)\cdot y}$$

is equal to $2^n$ if $x = z$ and is equal to zero if $x \neq z$.

#2 – Recall

$$H^\otimes n |x\rangle = \frac{1}{2^{n/2}} \sum_{y=0}^{2^n-1} (-1)^{x\cdot y} |y\rangle.$$ 

Check, using #1 above, that applying $H^\otimes n$ twice to any basis vector $|x\rangle$ yields $|x\rangle$. Is it true that any real symmetric unitary matrix $U$ must satisfy $U^2 = I$? Is $H^\otimes n$ unitary? Is it real? Is it symmetric?

#3 – Confirm that the unitary operator $(-I + 2A)$ found in the text can be implemented as $H^\otimes n$ followed by Phase followed by $H^\otimes n$. Here, Phase is defined by the rule:

$$\text{Phase}|x\rangle = \begin{cases} |x\rangle & \text{if } x = 0 \\ -|x\rangle & \text{if } x \neq 0 \end{cases}.$$ 

#4 – Exercise 6.3.1.

#5 – Exercise 6.3.3.

Ninth week summary

Tue 10/9. We went over Handout 9, and then analyzed the quantum circuit associated with Simon’s Periodicity algorithm. In that algorithm we take as given a Boolean function

$$F : \{0, 1\}^n \rightarrow \{0, 1\}^n$$
(note the range) satisfying this property: for some $c \in \{0, 1\}^n$,

$$F(x) = F(y) \iff x = y \oplus c.$$ 

We are given a component $U_F$ to use in our quantum circuit, and the problem is to find $c$. Each time we execute the circuit, we obtain after measurement an $x$ which satisfies $x \cdot c = 0$. With enough such $x$’s we can solve for $c$.

Wed 10/10. We finished up Simon – there was a handout with the circuit.

Thu 10/11. Took care of one loose end from yesterday: we use Simon’s algorithm until we obtain $n - 1$ linearly independent vectors $x$ such that $x \cdot c = 0$. Then, we have enough information to solve for $c$. We derived the fact that the expected number of times it is necessary to sample before obtaining enough $x$’s is $n - 1$ plus a quantity bounded by 1.7. Turning to Grover, we handed out a copy of the Grover circuit as found in the Nielsen-Chuang text. The latter analyzes why $\sqrt{2^n}$ is the right number of times to iterate the loop in the algorithm, whereas our text decides that analysis is beyond its scope. We were in the midst of checking that the two algorithms (our text, and N-C text) are in fact the same.

**Tenth week topics**

Tue 10/16. Finish the check that the two Grover algorithms we have before us are in fact the same. This means comparing the two operators $H^\otimes n \text{Phase} H^\otimes n$ from N-C with the operator $-I + 2A$ found in our text. Let’s see an example using the 2-trick approach: phase inversion, followed by invert about the mean.

Turning to the deeper analysis, consider the 2-dim plane spanned by the uniform superposition and the solution vector. Interpret the operator being iterated geometrically as a reflection around first the one, then the other; the net effect being a rotation. This should allow us to see why $\sqrt{2^n}$ is the right number of times to repeat.