Problem Set 2

Solution

1. [30/100] We proved that every unitary operation can be realized by a quantum circuit that uses only U_{CNOT} gates and 1-qubit gates. Show that it is not true that every bijective boolean function can be computed by a classical circuit that uses only CNOT gates and NOT gates.

   [Hint: use linear algebra over the field $\mathbb{F}_2$.]

   ## Solution:

   There are many possible approaches. The simplest one is to prove that the Toffoli gate
   $$(a, b, c) \to (a, b, ab \ \ XOR \ \ c)$$
   cannot be realized using NOT and CNOT. In a NOT gate, the transformation is
   $$x \to (1 \ \ XOR \ \ x)$$
   and in a CNOT gate it is
   $$(a, b) \to (a, a \ \ XOR \ \ b).$$

   So both gates are affine transformations over $\mathbb{F}_2$(Galois field of two elements), meaning that each bit of the output is an XOR of a subset of bits of the input and, possibly, the constant 1. A combination of affine transformation is still affine, so in a circuit made of CNOT gates and NOT gates each bit of the output is an affine function of the bits of the input.

   It remains to prove that a Toffoli gate is not an affine transformation. Note that if the Toffoli gate were affine then the transformation $a, b \to ab$ would be affine, while it is a quadratic transformation and so it cannot be affine.

Example :
If the Toffoli gate were affine, we could write (all operations in $\mathbb{F}_2$):

$$ab + c = xa + yb + zc + w$$

for some bits x, y, z, w. Now, if we set $a = b = c = 0$, we get $w = 0$. If we set $a = 0, b = 1, c = 0$, we have $y = 0$. If we set $a = 1, b = 1 + x, c = 0$, we have $1 + x = x$,which is a contradiction. $\square$

Another possible solution: [the number of bijective function using CNOT and NOT gates $(= 2^{n^2+n})$] $<$ [all possible number of bijective boolean functions $(= (2^n)!)$], for large n

2. [40/100] Let us say that an *efficient experiment* on a quantum state is a polynomial time quantum computation, followed by a measurement, followed by a polynomial time classical computation on the outcome of the measurement.

   For a binary string $x = (x_1, \ldots, x_n)$, let $mod3(x)$ be 0 if $\sum_i x_i \equiv 0 \pmod 3$ and let $mod3(x)$ be 1 otherwise. Show that there is an efficient experiment that distinguishes with high probability the quantum state $q_{uniform} := \frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} |x\rangle$ from the quantum state $q_{mod3} := \frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} (-1)^{mod3(x)} |x\rangle$. That is, there is an efficient experiment that outputs YES with higher probability (by an additive constant term) than when executed on $q_{uniform}$.

Solution:

Suppose we apply the Hadamard transform to a quantum state

$$\sum_x f(x)|x\rangle.$$

Noting that in general, for every $x \in \{0,1\}^n$,

$$H^{\otimes n}|x\rangle = \frac{1}{2^{n/2}} \sum_{s \in \{0,1\}^n} (-1)^{x_1 s_1 + \cdots + x_n s_n} |s\rangle,$$

we have

$$H^{\otimes n}\Big[\sum_x f(x)|x\rangle\Big] = \frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} \sum_{s \in \{0,1\}^n} f(x)(-1)^{x_1 s_1 + \cdots + x_n s_n} |s\rangle.$$

or simply,

$$\sum_s \hat{f}(s)|s\rangle.$$

In this new state, the amplitude $\hat{f}(00\dots0)$ of the all-zero string is

$$\frac{1}{2^{n/2}}\sum_{x\in\{0,1\}^n} f(x).$$

Thus, if we conduct a measurement, after applying the Hadamard transform, the state $|00\dots0\rangle$ will be measured with probability

$$\frac{1}{2^n}\Big|\sum_{x\in\{0,1\}^n} f(x)\Big|^2.$$

Now, consider $q_{uniform}$ as an initial quantum state. After the Hadamard transform, we will measure $|00\dots0\rangle$ with probability

$$\frac{1}{2^n}\Big|\sum_{x\in\{0,1\}^n} f(x)\Big|^2 = \frac{1}{2^n}\Big|\sum_{x\in\{0,1\}^n}\frac{1}{2^{n/2}}\Big|^2 = \frac{1}{2^n}\Big|2^n\frac{1}{2^{n/2}}\Big|^2 = 1.$$

(Surely, this result can be obtained from direct calculation: if we apply the Hadamard transform to a quantum state $q_{uniform} := \frac{1}{2^{n/2}}\sum_{x\in\{0,1\}^n}|x\rangle$, we get $H^{\otimes n}\Big[\frac{1}{2^{n/2}}\sum_{x\in\{0,1\}^n}|x\rangle\Big] = \bigotimes_{i=1}^{n} H\Big[\frac{1}{\sqrt{2}}[|0\rangle+|1\rangle]\Big] = \bigotimes_{i=1}^{n}|0\rangle = |00\dots0\rangle$).

Thus, we see that if we start from $q_{uniform}$, then we will measure $|00\dots0\rangle$ with probability 1, and if we start from other states, we will measure $|00\dots0\rangle$ with probability 0.

Next, consider q_{mod3} as an initial quantum state. After the Hadamard transform, we will measure $|00\dots0\rangle$ with probability

$$\begin{aligned}
\frac{1}{2^n}\Big|\sum_{x\in\{0,1\}^n} f(x)\Big|^2 &= \frac{1}{2^n}\Big|\sum_{x\in\{0,1\}^n}\frac{1}{2^{n/2}}(-1)^{mod3(x)}\Big|^2 = \frac{1}{2^{2n}}\Big|\sum_{x\in\{0,1\}^n}(-1)^{mod3(x)}\Big|^2 \\
&= \Big[\mathbb{P}\Big(\sum_i x_i(mod3)=0\Big) - \mathbb{P}\Big(\sum_i x_i(mod3)\neq 0\Big)\Big]^2 \\
&= \frac{1}{9}+o(1)
\end{aligned}$$

where the probabilities are over a random $x\in\{0,1\}^2$. In short, if we start from q_{mod3}, we can claim the probability of measuring $|00\dots0\rangle$ is at most

$$\frac{1}{9}+o(1).$$

Hence, our experiment has distinguishing probability

$$\frac{8}{9}+o(1).$$

The claim about the probabilities can be proved, for example, by considering a three-state Markov chain that has the state space $\{0, 1, 2\}$, that starts at time 0 in the state 0, and whose state X_t at time t is equal to X_{t-1} with probability 1/2 and to $X_{t-1} + 1(mod 3)$ with probability 1/2. The chain is connected and aperiodic, so it has a constant mixing time. After n steps, X_n is $1/2^{\Omega(n)}$-close to the uniform distribution. But the distribution of X_n is precisely the distribution of $\sum_i x_i$

3. [30/100] Consider a quantum circuit that, on an n-qubit input, first applies an Hadamard gate to each input bit, and applies quantum Fourier transform over $\mathbb{Z}_{2^n}$. If we give the state $|00\ldots0\rangle$ as an input to the circuit, what is the output state?

Solution:

• Apply the Hadamard transform:

$$H^{\otimes n}|00\ldots0\rangle = \bigotimes_{i=1}^{n}\left[\frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big)\right] = \frac{1}{2^{n/2}}\sum_{x\in\{0,1\}^n}|x\rangle = \frac{1}{2^{n/2}}\sum_{j=0}^{2^n-1}|j\rangle.$$

• Apply the quantum Fourier transform. The Fourier coefficient of all-zero state:

$$\frac{1}{2^n}\sum_{k=0}^{2^n-1}e^{2\pi i k0/2^n} = 1.$$

which implies that the output state is $|00\ldots0\rangle$.