CPSC 436Q: Homework 2

Due on Gradescope by 11:59pm on October 28, 2024

Rules.

1. Please try to solve the problems yourself first. If you get stuck, you may *consult* any resources (books, internet, peers, office hours, etc.) for solutions. Provided you *acknowledge* these resources, no marks will be deducted. However, you must write up your own solution *independently*, using your own words.[1]
2. Please write legibly, work that is illegible will be marked as incorrect. Latex is strongly recommended for legibility. (I also recommend using `https://www.overleaf.com/` if you're new to Latex.)
3. All answers should be justified.
4. If you spot any mistakes, please email me at `wdaochen@cs.ubc.ca`. Any corrections will be announced on Piazza.
5. The total number of points for non-bonus questions is $T = 32$. Credit policy for the bonus questions: suppose you receive x points for the bonus questions and y points for the non-bonus questions, then the total number of points you receive for this homework is $\min(x + y, T)$.

Homework

1. **Half-zeros versus all-zeros problem.**
   Let $n \in \mathbb{N}$ be even. Consider the function

$$f\colon \{x \in \{0,1\}^n \mid |x| = n/2\} \cup \{0^n\} \to \{0,1\} \tag{1}$$

   defined by $f(x) = 0$ if and only if $x = 0^n$ (recall this is the all-zeros string).

   (a) **(4 points)** Show that $D(f) = n/2 + 1$. [Hint: use a proof similar to what we did in class for $D(\mathrm{OR}_n)$. Do the equals sign in two parts, $\leq$ and $\geq$.]

   (b) **(2 points)** In class, we defined $R_\epsilon(f)$ for $\epsilon \in (0, 1/2)$. Suppose we define $R_0(f)$ in the same way but with ϵ set to 0. Show from the definitions that $R_0(f) = D(f)$. (Therefore, the randomized query complexity of f with zero error is equal to $n/2 + 1$ by the previous part.)

   (c) Recall the quantum phase oracle of x is the unitary U_x acting on $\mathbb{C}^{2n}$ defined by $U_x |i\rangle |b\rangle = (-1)^{x_i \cdot b} |i\rangle |b\rangle$ for all $i \in [n]$ and $b \in \{0,1\}$. Consider applying U_x to the state

$$|\psi\rangle |1\rangle \in \mathbb{C}^n \otimes \mathbb{C}^2 = \mathbb{C}^{2n}, \quad \text{where } |\psi\rangle \coloneqq \frac{1}{\sqrt{n}} \sum_{i=1}^{n} |i\rangle, \tag{2}$$

   and then measuring using $\{|\psi\rangle\langle\psi| \otimes \mathbb{1}_2, (\mathbb{1}_n - |\psi\rangle\langle\psi|) \otimes \mathbb{1}_2\}$, where the first projector in the set corresponds to output 0 and the second to 1. (This is often called "measuring the first register" using $\{|\psi\rangle\langle\psi|, \mathbb{1}_n - |\psi\rangle\langle\psi|)\}$ since the "$\otimes \mathbb{1}_2$" does nothing to the second register.)

   (4 points) Calculate the probability of the output being 0 as a function of x. Therefore, show that $Q_0(f) \leq 1$, where $Q_0(f)$ is defined in the same way as $Q_\epsilon(f)$ but with ϵ set to 0.

Remark 1. *Computing (a variant of) f goes by the name of the Deutsch-Jozsa problem, one of the foundational results in quantum computation that first established the possibility of large quantum speedup (if no error is allowed). Recall from the first homework that $R(f) = O(1)$ so the large speedup disappears if errors are allowed. Later, we will study Simon's problem in class which has a large quantum speedup even if errors are allowed.*

[1] GenAI tools like ChatGPT can occasionally solve these problems correctly. Like other resources, if you use it, please verify and understand its solution first. Also remember, you will not have access to any resources other than a pen in the final exam.

2. **Randomized query complexity.**

(a) **(4 points)** Given $f\colon \{0,1\}^n \to \{0,1\}$, the sensitivity of f at $x \in \{0,1\}^n$, denoted $s_x(f)$, is defined to be the size of the set

$$\{i \in [n] \mid f(x) \neq f(x^i)\}, \tag{3}$$

where x^i denotes x with the ith bit flipped. (E.g., if $x = 001$, then $x^1 = 101$, $x^2 = 011$, $x^3 = 000$.) Then, the sensitivity of f is defined to be

$$s(f) \coloneqq \max_{x \in \{0,1\}^n} s_x(f). \tag{4}$$

Show that $s(\mathrm{OR}_n) = n$. Prove that for all $\epsilon \in (0, 1/2)$, and all $f\colon \{0,1\}^n \to \{0,1\}$, we have

$$R_\epsilon(f) \geq (1 - 2\epsilon)s(f). \tag{5}$$

[Hint: the proof is a generalization of what we did in class for $R(\mathrm{OR}_n^{0,1})$.]

(b) **(2 points)** The Majority function on $n \in \mathbb{N}$ bits is defined as $\mathrm{MAJ}_n\colon \{0,1\}^n \to \{0,1\}$; $\mathrm{MAJ}_n(x) = 1$ if and only if $|x| > n/2$. Show that $s(\mathrm{MAJ}_n) \geq \lceil n/2 \rceil$ for all $n \in \mathbb{N}$. (So $R_\epsilon(\mathrm{MAJ}_n) \geq (1 - 2\epsilon)\lceil n/2 \rceil$ by the previous part. $\lceil \cdot \rceil$ denotes the ceiling function.)

(c) **(4 points)** For this part, recall $R(\cdot) = R_{1/3}(\cdot)$ by definition, where the 1/3 refers to the probability of error being less than or equal to 1/3. In class, we showed $R(\mathrm{OR}_3) \leq 2$ and that $R(\mathrm{OR}_3) \geq (1 - 2 \cdot (1/3)) \cdot 3 = 1$. There's a gap! Show that in fact $R(\mathrm{OR}_3) = 2$ by considering a *different distribution* μ on $\{0,1\}^3$ and showing $\Pr[T^*(x) = \mathrm{OR}_3(x) \mid x \leftarrow \mu]$ is *strictly* less than 2/3 for *any* depth-1 DDT T^*. (We cannot use the same distribution as in class since that only gives a lower bound of $R(\mathrm{OR}_3) \geq 1$.) [Hint: there are not that many depth-1 DDTs and some of them may behave similarly depending on how you defined μ.]

3. **SWAP test.**

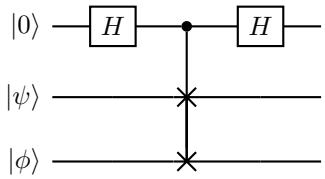
Let $n \in \mathbb{N}$. Let $|\psi\rangle \coloneqq \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle$ and $|\phi\rangle \coloneqq \sum_{x \in \{0,1\}^n} \beta_x |x\rangle$ be two n-qubit quantum states.

The cSWAP (pronounced "controlled-SWAP") gate implements the unitary acting on $\mathbb{C}^2 \otimes \mathbb{C}^{2^n} \otimes \mathbb{C}^{2^n}$ defined by

$$\mathrm{cSWAP}\,|0\rangle\,|x\rangle\,|y\rangle = |0\rangle\,|x\rangle\,|y\rangle \quad \text{and} \quad \mathrm{cSWAP}\,|1\rangle\,|x\rangle\,|y\rangle = |1\rangle\,|y\rangle\,|x\rangle\,, \tag{6}$$

for all $x, y \in \{0,1\}^n$.

(2 points) Compute the output of the following circuit, where the $\cdot - \times - \times$ symbol denotes the cSWAP gate, using Dirac notation throughout.



(2 points) Suppose we make the computational basis measurement on the first register, that is, we make the measurement defined by

$$\Pi_0 \coloneqq |0\rangle\langle 0| \otimes \mathbb{1}_{2^n} \otimes \mathbb{1}_{2^n} \quad \text{and} \quad \Pi_1 \coloneqq |1\rangle\langle 1| \otimes \mathbb{1}_{2^n} \otimes \mathbb{1}_{2^n}\,. \tag{7}$$

Show that the probability of measuring 0 is

$$\frac{1 + |\,\langle\psi|\phi\rangle\,|^2}{2}. \tag{8}$$

(The procedure involving the above circuit and measurement is known as the "SWAP test", which is an important primitive in quantum computing.)

(2 points) Suppose a stranger gives you k n-qubit states $|\psi_1\rangle, \ldots, |\psi_k\rangle$ with the promise that either

(a) For all $i \in [k]$,

$$|\psi_i\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle\,, \tag{9}$$

or

(b) There exists $S \subseteq \{0,1\}^n$ of size $|S| = 2^{n-1}$ such that for all $i \in [k]$,

$$|\psi_i\rangle = \frac{1}{\sqrt{2^{n-1}}} \sum_{x \in S} |x\rangle \,. \tag{10}$$

(The stranger does not tell you what S is.)

The stranger also does not tell you which case you're in. Nonetheless, show that for all $k \geq 20$ there is a procedure involving the SWAP test that, in either case, can help you correctly decide the case you're in with probability $\geq 99/100$.

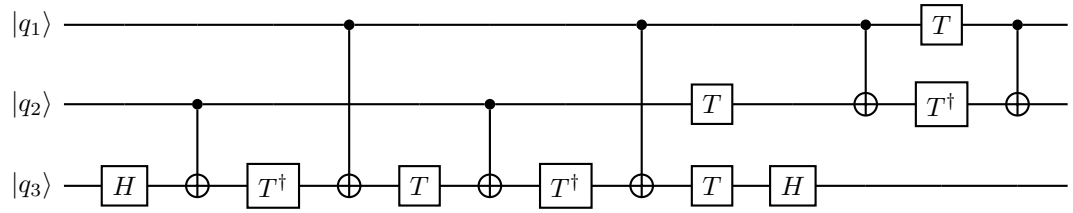
Remark 2. *The last part of the question illustrates that a quantum state $\sum_x \alpha_x |x\rangle$ behaves very differently from the probability distribution that assigns probability $|\alpha_x|^2$ to x. In the probabilistic analogue of this problem, the first case would correspond to k samples each chosen uniformly randomly from $\{0,1\}^n$, and the second case would correspond to k samples each chosen uniformly randomly from some $S \subseteq \{0,1\}^n$ of size $|S| = 2^{n-1}$. If you don't know what S is, distinguishing between these cases with probability $\geq 99/100$ would require $k = \Omega(2^n)$.*

4. **A circuit identity.**

The $T^\dagger$ gate implements the unitary

$$\begin{pmatrix} 1 & 0 \\ 0 & e^{-i\pi/4} \end{pmatrix}. \tag{11}$$

(a) **(4 points)** The following circuit C is an alternative way of implementing the Toffoli gate using only H, T, CNOT, and $T^\dagger$ gates. For *two* bitstrings $q_1q_2q_3 \in \{0,1\}^3$ *of your choice*, verify $C|q_1q_2q_3\rangle = \text{Toffoli}\,|q_1q_2q_3\rangle$. (If you did this for all of the eight possible 3-bit strings, then you would fully verify that the following circuit implements the Tofolli gate but hopefully you get the idea from doing two.)



(b) **(2 points)** Explain why the above implies that the Toffoli gate can also be implemented using only H, T, and CNOT gates (without $T^\dagger$ gates).

5. **Bonus questions.**

(a) **Randomized query complexity continued.** Q2(c) shows that that the general result $R_\epsilon(\text{OR}_n) \geq (1-2\epsilon)n$ is not tight for $\epsilon = 1/3$ and $n = 3$.
(4 points) Can you improve the general result, i.e., give a better lower bound on $R_\epsilon(\text{OR}_n)$ for all $\epsilon \in (0, 1/2)$ and $n \in \mathbb{N}$?

(b) **Circuit compilation.** The S gate implements the unitary

$$\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}. \tag{12}$$

(4 points) Prove or disprove the following statement.
For all unitaries $U \in \mathbb{C}^{2\times 2}$ and for all $\epsilon > 0$, there exists a quantum circuit on 1 qubit defined by a finite sequence of H (Hadamard) and S gates such that the unitary $V \in \mathbb{C}^{2\times 2}$ implemented by the quantum circuit satisfies

$$\|V - U\|_F \leq \epsilon, \tag{13}$$

where $\|\cdot\|_F$ denotes the Frobenius norm, i.e.,

$$\left\| \begin{pmatrix} a & b \\ c & d \end{pmatrix} \right\|_F := \sqrt{|a|^2 + |b|^2 + |c|^2 + |d|^2}. \tag{14}$$

[To receive any credit for this problem, you must prove/disprove from first principles. You may not invoke well-known theorems.]

Remark 3. *In the jargon, this question is asking whether the gate set $\{H, S\}$ is universal for single-qubit unitaries.*