CPSC 436Q: Homework 3

Due on Gradescope by 11:59pm on November 25, 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. **Consolidation of lecture material.**

   (a) **(2 points)** Linear algebra in $\mathbb{F}_2^k$. Show that the following three vectors *are* linearly independent as vectors in $\mathbb{R}^3$ (so span three dimensions) but *are not* linear independent as vectors in $\mathbb{F}_2^3$ (so span less than three dimensions). Write down the span of these vectors as vectors in $\mathbb{F}_2^3$.

   $$\begin{pmatrix}1\\1\\0\end{pmatrix}, \begin{pmatrix}0\\1\\1\end{pmatrix}, \begin{pmatrix}1\\0\\1\end{pmatrix}. \tag{1}$$

   (Recall that in the analysis of Simon's algorithm, linear algebra is done in $\mathbb{F}_2^k$. While most aspects of linear algebra in $\mathbb{F}_2^k$ and $\mathbb{R}^k$ are the same, e.g., row-rank = column rank and the rank-nullity theorem, this exercise shows that there can be subtle differences.)

   (b) **(2 points)** Show that the quantum Fourier transform QFT_M is unitary for any $M \in \mathbb{N}$. That is, show

   $$\mathrm{QFT}_M^\dagger \mathrm{QFT}_M = \mathbb{1}_M = \mathrm{QFT}_M \mathrm{QFT}_M^\dagger. \tag{2}$$

2. **Improving the period finding algorithm.**

   In fact, the quantum query complexity of finding the period r of a string x with symbols in $\mathbb{Z}_N$ is $O(1)$, i.e., constant, which is better than the $O(\ln\ln(N))$ we derived in class. We will walk through how this works in this problem. (Based on Problem 8 from Assignment 6 of Ryan O'Donnell's 2018 course.)

   Recall that the main subroutine of the quantum algorithm for period finding generates a number z of the form $j \cdot 2^n/r$ for some j uniformly at random from $\{0, 1, \ldots, r-1\}$. *Throughout this question, assume that r divides 2^n as in class.*

   By rejecting $z = 0$, we can readily modify the subroutine to generate a number z of the form $j \cdot 2^n/r$ for some j uniformly at random from $\{1, \ldots, r-1\}$. This would only incur a small constant overhead since $z = 0$ occurs with probability $1/r$ (which is $\leq 1/100$ if we wlog assume $r \geq 100$ as in class).

   In the following, all probabilities are over j_1, j_2 each independently chosen uniformly at random from $\{1, \ldots, r-1\}$.

   (a) **(2 points)** Show that for any fixed prime $p \in \mathbb{N}$,

   $$\Pr[p \text{ divides both } j_1 \text{ and } j_2] \leq \frac{1}{p^2}. \tag{3}$$

[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.

(b) **(2 points)** Show that

$$\Pr[j_1 \text{ and } j_2 \text{ are not coprime}] \leq \sum_{p \text{ prime}} \frac{1}{p^2}, \tag{4}$$

where the second infinite sum is over all primes $p \in \mathbb{N}$.

(c) **(2 points)** Show that

$$\sum_{p \text{ prime}} \frac{1}{p^2} \leq 0.99. \tag{5}$$

[Hint: you may use any of the results/methods in Basel problem Wiki concerning a different but similar sum.]

(d) **(4 points)** Using the previous parts, explain how to *modify* the last part of the period-finding algorithm from class (where we repeated the subroutine $10000 \ln \ln(N)$ times) so that the number of repeats (and hence queries) becomes *constant* yet the algorithm is still *correct* with probability at least 2/3. (You may assume the subroutine has already been modified not to generate $z = 0$ because this only incurs a small constant overhead, as explained above.) [Hint: the notion of gcd may be useful. For $x, y \in \mathbb{N}$, $\gcd(x, y)$ is the greatest common divisor of x and y, e.g., $\gcd(30, 24) = 6$, $\gcd(8, 9) = 1$, $\gcd(7, 21) = 7$.]

3. **Running Shor's algorithm yourself.** Recall the description of Shor's algorithm from the bottom of pg. 31 of my notes involving five steps. For *small* N, we can run it ourselves. In this exercise, take N to be 21.

(a) **(3 points)** Run the algorithm supposing that you chose $a = 2$ at the third step. Describe what happens at each step. You do *not* necessarily have to perform your computations using the red text in my notes. In the fourth step, you should compute $\mathrm{ord}_N(a)$ using any (classical) method you can think of, e.g., brute force is fine.[2]

(b) **(3 points)** Repeat the above but now supposing that you chose $a = 5$ at the third step.

4. **No quantum advantage for parity.** The $\mathrm{PARITY}_n \colon \{0,1\}^n \to \{0,1\}$ function is defined by

$$\mathrm{PARITY}(x) = x_1 \oplus x_2 \oplus \cdots \oplus x_n. \tag{6}$$

(**4 points**) Show that $\mathrm{Adv}(\mathrm{PARITY}_n) = \Omega(n)$.

5. **The five-qubit code.** *You can do this question before we cover quantum error correction.* (Based on Problem 4 from Assignment 5 of Andrew Childs's 2019 course.) Consider the following two five-qubit states:

$$\begin{aligned} |0_L\rangle \coloneqq \frac{1}{4}(&|00000\rangle \\ &+ |10010\rangle + |01001\rangle + |10100\rangle + |01010\rangle + |00101\rangle \\ &- |11000\rangle - |01100\rangle - |00110\rangle - |00011\rangle - |10001\rangle \\ &- |01111\rangle - |10111\rangle - |11011\rangle - |11101\rangle - |11110\rangle) \end{aligned}$$

and

$$\begin{aligned} |1_L\rangle \coloneqq \frac{1}{4}(&|11111\rangle \\ &+ |01101\rangle + |10110\rangle + |01011\rangle + |10101\rangle + |11010\rangle \\ &- |00111\rangle - |10011\rangle - |11001\rangle - |11100\rangle - |01110\rangle \\ &- |10000\rangle - |01000\rangle - |00100\rangle - |00010\rangle - |00001\rangle). \end{aligned}$$

(a) **(4 points)** Show that $|0_L\rangle$ and $|1_L\rangle$ are eigenstates (i.e., eigenvectors) with eigenvalue $+1$ of each of the following four matrices:

$$\begin{array}{ccccccccc} X & \otimes & Z & \otimes & Z & \otimes & X & \otimes & I \\ I & \otimes & X & \otimes & Z & \otimes & Z & \otimes & X \\ X & \otimes & I & \otimes & X & \otimes & Z & \otimes & Z \\ Z & \otimes & X & \otimes & I & \otimes & X & \otimes & Z \end{array}, \tag{7}$$

where

$$I \coloneqq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad X \coloneqq \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \text{and} \quad Z \coloneqq \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{8}$$

[Hint: you can show this without explicitly checking every case.]

(b) **(2 points)** Show that any pair of the four matrices in eq. (7) commute. (We say two square matrices A, B of the same size commute if $AB = BA$.)

[2] Of course, this step wouldn't be efficient classically as N gets large!

(c) **(2 points)** Show that $X_L \coloneqq X \otimes X \otimes X \otimes X \otimes X$ and $Z_L \coloneqq Z \otimes Z \otimes Z \otimes Z \otimes Z$ satisfy

$$X_L |0_L\rangle = |1_L\rangle\,, \quad X_L |1_L\rangle = |0_L\rangle\,, \quad Z_L |0_L\rangle = |0_L\rangle\,, \quad \text{and} \quad Z_L |1_L\rangle = -|1_L\rangle\,. \tag{9}$$

6. **Bonus question. (4 points)** In class, we showed that the probability $P_{K,k}$ of K vectors, each chosen uniformly at random from $\mathbb{F}_2^k$, spanning k dimensions is at least $1 - 2^{k-K}$. When $K = k$, this bound is trivial. Derive an exact formula for $P_{k,k}$ and show that it is, in fact, at least $1/4$ for any $k \in \mathbb{N}$.