CPSC 436Q: Homework 3

Due on Gradescope by 11:59pm on December 1, 2025

Rules.

1. Please try to solve the problems yourself first. If you get stuck, you may *consult* any *non-GenAI* resources (books, Wikipedia, lecture notes, 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. Answers suspected of being from GenAI will receive zero credit unless you can demonstrate understanding upon appeal.
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 to receive any credit.
4. The total number of points for non-bonus questions is $T = 16$. Credit policy for bonus questions: suppose you receive x points for bonus questions and y points for non-bonus questions, then the total number of points you receive for this homework is $\min(x + y, T)$. Points for bonus questions are generally harder to earn.
5. If you spot any mistakes, please email me at `wdaochen@cs.ubc.ca`. Any corrections will be announced on Piazza.

Homework

1. **Improving the order finding algorithm.** (Based on Problem 8 from Assignment 6 of Ryan O'Donnell's 2018 course.)

   Recall that the main quantum circuit for factoring was repeated $O(1/\gamma)$ times, where γ is the probability that a uniformly random element in $\{0, 1, \ldots, r-1\}$ is coprime to r, and $1/\gamma$ can be bounded by $O(\log \log N)$.

   In this exercise, we'll walk through a different approach to shave off this $O(\log \log N)$ factor.

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

   By rejecting if $n = 0$, we can readily modify the subroutine to generate a number of the form $n \cdot M/r$ for some n chosen uniformly at random from $\{1, \ldots, r-1\}$. *This would only incur a small constant overhead, which you should henceforth ignore.*

   In the following, all probabilities are over n_1, n_2 each chosen independently and uniformly at random from $\{1, \ldots, r-1\}$.

   (a) **(2 points)** Show that for any fixed prime p,

   $$\Pr[p \text{ divides both } n_1 \text{ and } n_2] \leq \frac{1}{p^2}. \tag{1}$$

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

   $$\Pr[n_1 \text{ and } n_2 \text{ are not coprime}] \leq \sum_{p \text{ prime}} \frac{1}{p^2}, \tag{2}$$

   where the infinite sum is over all primes p.

   (c) **(2 points)** Use integration to show

   $$\sum_{p \text{ prime}} \frac{1}{p^2} \leq 0.9. \tag{3}$$

   Hint: integration represents area under a curve.

   (d) **(4 points)** Using the previous parts, explain how to *modify* the order-finding algorithm from class so that the quantum circuit is only repeated a *constant* number of times, yet the algorithm is still *correct* with probability at least a constant, say 0.99. Hint: it may help to consider $\gcd(n_1 \cdot M/r,\ n_2 \cdot M/r)$.

2. **Running Shor's algorithm yourself.**

   Let $N = 21$. In this case, N is small enough for you to run Shor's three-step algorithm as described in class. You do not need to use a quantum computer to find orders for such small N.

   (a) **(2 points)** Run the algorithm assuming that you chose $a = 2$ initially. Describe what happens each step.

   (b) **(2 points)** Repeat the above but now assuming that you chose $a = 5$ initially.

3. **Stabilizers of 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 four matrices:

$$\begin{array}{ccccccccc} X & \otimes & Z & \otimes & Z & \otimes & X & \otimes & I \\ I & \otimes & X & \otimes & Z & \otimes & Z & \otimes & X \\ X & \otimes & I & \otimes & X & \otimes & Z & \otimes & Z \\ Z & \otimes & X & \otimes & I & \otimes & X & \otimes & Z \end{array} \quad , \tag{4}$$

   where

$$I \coloneqq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad X \coloneqq \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \text{and} \quad Z \coloneqq \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{5}$$

   (2 points) Show that any pair of the four matrices in eq. (4) commute. (We say two square matrices A, B of the same size commute if $AB = BA$.) Hint: how does XZ relate to ZX?

4. **Bonus question: random vectors in $\mathbb{F}_2^n$.** In class, we showed that the probability $P_{K,n}$ of K vectors, each chosen uniformly at random from $\mathbb{F}_2^n$, spanning n dimensions is at least $1 - 2^{n-K}$. When $K = n$, this bound is trivial.

   (4 points) Derive an exact formula for $P_{n,n}$ and show that it is, in fact, at least $1/4$ for all positive integers n.