**COMS 4281 - Introduction to Quantum Computing** Fall 2024

# Practice Worksheet 6

This practice worksheet is intended to act as a review sheet for the midterm as well as give some practice for the more recently covered material. The midterm and final exam will have questions inspired by the worksheets.

## Problem 1: Basic Fourier math

Recall that the Fourier basis for $\mathbb{C}^N$ is comprised of the following states: for all $j = 0, 1, 2, \ldots N-1$,

$$|f_j\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \omega_N^{jk} \, |k\rangle$$

where

$$\omega_N = \exp\left(\frac{2\pi i}{N}\right)$$

is the $N$'th root of unity. It also can be written as

$$\omega_N = \cos\left(\frac{2\pi}{N}\right) + i \sin\left(\frac{2\pi}{N}\right) .$$

(a) Write out $\omega_2, \omega_3, \omega_4, \omega_8$ in terms of algebraic numbers (e.g., numbers of the form $1, -1, i, 2+i, \sqrt{3}/2$, etc.).

(b) What is $\omega_2^0 + \omega_2^1$? That is, $\omega_2^0$ is $\omega_2$ to the zeroth power, $\omega_2^1$ is $\omega_2$ to the first power, etc.

(c) What is $\omega_3^0 + \omega_3^1 + \omega_3^2$?

(d) What is $\omega_8^0 + \cdots + \omega_8^7$?

(e) Let $j$ be an integer that is not a multiple of $N$. Prove that

$$\left(1 - \omega_N^j\right) \sum_{k=0}^{N-1} \omega_N^{jk} = 0 .$$

(f) Use this to conclude that

$$\sum_{k=0}^{N-1} \omega_N^{jk} = \begin{cases} 0 & \text{if } j \text{ is not a multiple of } N \\ N & \text{if } j \text{ is a multiple of } N \end{cases}$$

(g) Show that the Fourier basis vectors $\{|f_0\rangle, \ldots, |f_{N-1}\rangle\}$ forms an orthonormal basis.

## Problem 2: Order Finding algorithm

Recall that the Order Finding problem is as follows: given two nonnegative integers $(x, N)$ where $0 \le x < N$ and $\gcd(x, N) = 1$ (meaning that the only thing that divides both $x$ and $N$ is 1), find the smallest integer $r$ such that $x^r = 1 \mod N$.

(a) What is the order $r$ of $x = 7$, when taken modulo $N = 15$?

(b) What is the order $r$ of $x = 3$, when taken modulo $N = 11$?

Recall the unitary matrix acting on $\mathbb{C}^N$ such that

$$U_x |y\rangle = |xy \mod N\rangle \ .$$

Here we use the standard basis of $\mathbb{C}^N$ which is $\{|0\rangle, |1\rangle, \ldots, |N-1\rangle\}$. Let $x = 3, N = 11, y = 4$.

(c) Compute $U_x^k |y\rangle$ for $k = 0, 1, 2, \ldots, 10$.

(d) For these choices of $x, N, y$, write out a formula for $U_x^k |y\rangle$ for general $k$.

**Problem 3: Outer products**

We will get some practice with outer products. For the following, write the matrix form of the given expression, and identify the well-known name for that matrix.

(a) $|1\rangle\langle 0| + |0\rangle\langle 1|$

(b) $\sqrt{2}\Big( |+\rangle\langle -| \ + \ |0\rangle\langle 1| \Big)$

(c) $|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X$.

(d) Let $U$ be an arbitrary single-qubit gate. Describe the high-level functionality of the matrix

$$|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U$$

as a quantum gate. We often call this gate the "controlled-$U$" gate, or abbreviated by $cU$.

(e) $\sum_{x \in \{0,1\}^n} |x\rangle\langle x|$. Note that this is a matrix acting on $n$ qubits.

(f) $\sum_{0 \le j,k < N} \exp\Big( -\frac{2\pi i jk}{N} \Big) |j\rangle\langle k|$. Note that this matrix acts on $\mathbb{C}^N$.

**Problem 4: Grover search**

(a) Show that the Grover diffusion operator $R = 2\,|+\rangle\langle +|^{\otimes n} - I$ is a unitary matrix.

(b) Show that $R = H^{\otimes n}\Big(2\,|0\rangle\langle 0|^{\otimes n} - I\Big)H^{\otimes n}$, where $|0\rangle\langle 0|^{\otimes n}$ is the outer product of $|0\rangle^{\otimes n}$ with itself.

(c) Show that the unitary operator $2\,|0\rangle\langle 0|^{\otimes n} - I$ is the same as $O_h$, the phase oracle corresponding to the boolean function $h : \{0,1\}^n \to \{0,1\}$ where

$$h(x) = \begin{cases} 0 & \text{if } x = 0 \cdots 0 \\ 1 & \text{otherwise} \end{cases} .$$

(d) Suppose $f : \{0,1\}^n \to \{0,1\}$ has $M$ solutions $x$ such that $f(x) = 1$. Suppose we run Grover's algorithm with $k$ iterations, and then measure the state of the algorithm. What is the probability that a solution is produced as an outcome (as a function of $n, M, k$)?