QUANTUM ALGORITHMS
FINAL EXAM

PROF. MATTHEW MOORE

DUE: 2021-05-11 AT 10:00

Name: ______________________________________

Instructions

- You may make use of any non-human assistance — any book, the web (but do not ask for help online), etc. Solutions must be self-contained.
- Solutions given with little or no justification may receive little or no credit.
- Solutions will be graded based on correctness, quality, and presentation. Turn in something that you are proud of.
- There are 3 problems. **Submit only 2 for grading.**

"I pledge on my honor that I have neither given nor received unauthorized aid on this assignment."

Signature: ______________________________________

1. Let $\mathbb{G}$ be a finite Abelian group such that

$$\mathbb{G} \cong \prod_{i=1}^{k} \mathbb{Z}/m_i\mathbb{Z}$$

by the Fundamental Theorem of Finitely Generated Abelian Groups. Regard elements $g \in G$ as tuples $g = (g_i) \in \prod \mathbb{Z}/m_i\mathbb{Z}$. Recall that the Quantum Fourier Transform for $\mathbb{G}$ was defined

$$\mathcal{F}_{\mathbb{G}} \coloneqq \frac{1}{\sqrt{|\mathbb{G}|}} \sum_{g,h \in G} \mu(g,h) \left| g \right\rangle \left\langle h \right|$$

where

$$\mu(g,h) \coloneqq \prod_{i=1}^{k} \omega_{m_i}^{g_i h_i}, \qquad \omega_{m_i} \coloneqq \exp(2\pi i/m_i).$$

Show that $\mathcal{F}_{\mathbb{G}} = \bigotimes_{i=1}^{k} \mathcal{F}_{\mathbb{Z}/m_i\mathbb{Z}}$.

2. Recall that the Kronecker product of *matrices* A and B is defined

$$A * B := \begin{pmatrix} a_{11}B & \cdots & a_{1n}B \\ \vdots & & \vdots \\ a_{m1}B & \cdots & a_{mn}B \end{pmatrix}, \qquad A = (a_{ij}),$$

and that given a *linear operator* $C : \mathbb{T} \to \mathbb{U}$, we denote the matrix of C relative to some specified ordered bases for $\mathbb{T}$ and $\mathbb{U}$ as $[C]$.

Let $\mathbb{V}, \mathbb{W}, \mathbb{X}, \mathbb{Y}$ be vector spaces with respective ordered bases

$$\mathcal{V} = \{\, |v_1\rangle, |v_2\rangle \,\}, \qquad \mathcal{W} = \{\, |w_1\rangle, |w_2\rangle, |w_3\rangle \,\},$$
$$\mathcal{X} = \{\, |x_1\rangle, |x_2\rangle, |x_3\rangle \,\}, \qquad \mathcal{Y} = \{\, |y_1\rangle, |y_2\rangle \,\}.$$

Define linear operators $D : \mathbb{V} \to \mathbb{W}$ and $E : \mathbb{X} \to \mathbb{Y}$ by

$$D|v_1\rangle = |w_1\rangle + |w_2\rangle + |w_3\rangle, \qquad E|x_1\rangle = |y_1\rangle - |y_2\rangle,$$
$$D|v_2\rangle = 2|w_2\rangle - |w_3\rangle, \qquad E|x_2\rangle = 2|y_2\rangle,$$
$$E|x_3\rangle = |y_1\rangle + |y_2\rangle.$$

Show that $[D] * [E] = [D \otimes E]$, where the bases for $\mathbb{V} \otimes \mathbb{X}$ and $\mathbb{W} \otimes \mathbb{Y}$ are the usual lexicographically ordered bases. You may do this by direct calculation if you wish.

3. Given a group $\mathbb{G}$, recall that the discrete logarithm problem takes as input elements $a, b \in G$ such that $b^s = a$, and outputs the number s. Recall that the quantum solution to the discrete logarithm problem involves running the eigenvalue estimation circuit in series using the operators U_b and $U_a^\dagger$.

(i) Show that the state in the circuit before passing through the two inverse Quantum Fourier Transform blocks is proportional to

$$\sum_{x,y\in\{0,1\}^n} \left|x, y, b^x a^{-y}\right\rangle .$$

(ii) Carefully show that the state after passing through the two inverse Quantum Fourier Transform blocks but before measurement is proportional to

$$\sum_{\substack{z,w\in\{0,1\}^n \\ sw+z=0}} |z, w\rangle \otimes \sum_{k=1}^{m} \exp(-2\pi i(kw)/2^n) \left|b^k\right\rangle ,$$

where m is the period/order of b in $\mathbb{G}$. [*Hint: use* $b^s = a$.]

(iii) Conclude that measuring the top two registers of the circuit produces pairs $|u, v\rangle$ such that $b^u a^{-v} = 1$. Explain how to use such pairs to find s.