1. The Bernstein-Vazirani problem.

(a) [2 points] Suppose \( f : \{0, 1\}^n \to \{0, 1\} \) is a function of the form

\[
  f(x) = x_1 s_1 + x_2 s_2 + \cdots + x_n s_n \mod 2
\]

for some unknown \( s \in \{0, 1\}^n \). Given a black box for \( f \), how many classical queries are required to learn \( s \) with certainty?

**Solution:** Clearly, \( n \) queries are sufficient, since

\[
  f(10\ldots0) = s_1, \quad f(010\ldots0) = s_2, \ldots, \quad f(00\ldots01) = s_n.
\]

But \( n \) queries are also necessary, since if we query \( f \) on only \( n-1 \) inputs, we only determine \( f \) on at most an \( (n-1) \)-dimensional subspace of \( \{0, 1\}^n \). Another way to see this is that if we only make \( n-1 \) queries, then we can only learn \( n-1 \) bits, whereas it takes \( n \) bits of information to specify \( s \).

(b) [3 points] Prove that for any \( n \)-bit string \( u \in \{0, 1\}^n \),

\[
  \sum_{v \in \{0, 1\}^n} (-1)^{u \cdot v} = \begin{cases} 2^n & \text{if } u = 00\ldots0 \\ 0 & \text{otherwise.} \end{cases}
\]

**Solution:** If \( u = 0 \) then every term is 1, so the sum is clearly \( 2^n \). Otherwise there is some bit of \( u \) that is a 1. Without loss of generality, suppose \( u_1 = 1 \); then

\[
  \sum_{v \in \{0, 1\}^n} (-1)^{u \cdot v} = \sum_{v \in \{0, 1\}^n} (-1)^{u_1 + u_2 v_2 + \cdots + u_n v_n} = \sum_{v_2, \ldots, v_n \in \{0, 1\}} (-1)^{u_2 v_2 + \cdots + u_n v_n} - \sum_{v_2, \ldots, v_n \in \{0, 1\}} (-1)^{u_2 v_2 + \cdots + u_n v_n} = 0.
\]

(c) [4 points] Let \( U_f \) denote a quantum black box for \( f \), acting as \( U_f|x\rangle y = |x\rangle y \oplus f(x) \) for any \( x \in \{0, 1\}^n \) and \( y \in \{0, 1\} \). Show that the output of the following circuit is the state \( |s\rangle(|0\rangle - |1\rangle)/\sqrt{2} \).

![Circuit Diagram]

**Solution:** Let \( |\rangle = (|0\rangle - |1\rangle)/\sqrt{2} \). Recall the effect of phase kickback:

\[
  |x\rangle|\rangle \xrightarrow{U_f} \frac{1}{\sqrt{2}}(|x\rangle|f(x)\rangle + |x\rangle|f(x)\rangle) = (-1)^{f(x)}|x\rangle|\rangle.
\]
2. A fast approximate QFT.

(a) [2 points] In class, we saw a circuit implementing the n-qubit QFT using Hadamard and controlled-$R_k$ gates, where $R_k|x\rangle = e^{2\pi i x/2^k}|x\rangle$ for $x \in \{0, 1\}$. How many gates in total does that circuit use? Express your answer both exactly and using $\Theta$ notation. (Recall that we say $f(n) \in \Theta(g(n))$ if $f(n) \in O(g(n))$ and $g(n) \in O(f(n))$.)

Solution: $1 + 2 + 3 + \cdots + n = n(n + 1)/2 \in \Theta(n^2)$

(b) [3 points] Let $cR_k$ denote the controlled-$R_k$ gate, with $cR_k|x, y\rangle = e^{2\pi i xy/2^k}|x, y\rangle$ for $x, y \in \{0, 1\}$. Show that $E(cR_k, I) \leq 2\pi/2^k$, where $I$ denotes the $4 \times 4$ identity matrix, and where $E(U, V) = \max_{\psi} \|U|\psi\rangle - V|\psi\rangle\|$. You may use the fact that $\sin x \leq x$ for any $x \geq 0$.

Solution: We have

$$cR_k - I = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & e^{2\pi i/2^k} & 0 \end{pmatrix} - \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & e^{2\pi i/2^k} & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & e^{2\pi i/2^k} - 1 \end{pmatrix}.$$ 

Letting $|\psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$ denote a general quantum state of two qubits, we have $(R_k - I)|\psi\rangle = d(e^{2\pi i/2^k} - 1)|11\rangle$. Clearly the norm of this state is maximized by taking $|d| = 1$, so that the norm is $|e^{2\pi i/2^k} - 1| = |e^{\pi i/2^k} (e^{\pi i/2^k} - e^{-\pi i/2^k})| = 2|\sin(\pi/2^k)| \leq 2\pi/2^k$. 

So the circuit behaves as follows:

\[ 0\rangle \rightarrow H^{\otimes n} \otimes I \rightarrow \frac{1}{\sqrt{2^n}} \sum_{x \in \{0, 1\}^n} |x\rangle \rightarrow \]

\[ U_f \rightarrow \frac{1}{\sqrt{2^n}} \sum_{x \in \{0, 1\}^n} (-1)^{f(x)} |x\rangle \rightarrow \]

\[ H^{\otimes n} \otimes I \rightarrow \frac{1}{\sqrt{2^n}} \sum_{x, y \in \{0, 1\}^n} (-1)^{f(x) + x \cdot y} |y\rangle \rightarrow \]

Now since $f(x) = x \cdot s$, the state is

\[ \frac{1}{2^n} \sum_{x, y \in \{0, 1\}^n} (-1)^{x \cdot (s \oplus y)} |y\rangle \rightarrow = \frac{1}{2^n} \sum_{y \in \{0, 1\}^n} \begin{cases} 2^n & \text{if } s = y \\ 0 & \text{otherwise} \end{cases} |y\rangle \rightarrow = |s\rangle \rightarrow \]

as claimed, where in the first step we have used part (b) and the fact that $s \oplus y = 0$ if and only if $s = y$.

Another method that does not rely on part (b) is to show that $H^{\otimes n}|s\rangle$ is the same as the state of the first $n$ qubits just after $U_f$ is applied.

(d) [1 point] What can you conclude about the quantum query complexity of learning $s$?

Solution: Since a computational basis measurement reveals $s$, we only need one quantum query to solve the problem.
(c) [5 points] Let $F$ denote the exact QFT on $n$ qubits. Suppose that for some constant $c$, we delete all the controlled-$R_k$ gates with $k > \log_2(n) + c$ from the QFT circuit, giving a circuit for another unitary operation, $\tilde{F}$. Show that $E(F, \tilde{F}) \leq \epsilon$ for some $\epsilon$ that is independent of $n$, where $\epsilon$ can be made arbitrarily small by choosing $c$ arbitrarily large. (Hint: Use equation 4.3.3 of KLM.)

**Solution:** For each qubit in the circuit, we have a sequence of controlled-$R_k$ gates with $k = 2$ up to some value depending on the index of the qubit. Of these gates, we omit the ones with $k > \log_2(n) + c$. So, using the fact that the error is additive, the total error in this part of the circuit is at most

$$\sum_{k=\lceil \log_2(n) + c \rceil}^{\infty} E(cR_k, I) = \sum_{k=\lceil \log_2(n) + c \rceil}^{\infty} \frac{2\pi}{2^k} = \frac{4\pi}{2^\lceil \log_2(n) + c \rceil} \leq \frac{4\pi}{2\log_2(n) + c} = \frac{4\pi}{2^n}.$$  

Since there are $n$ qubits in the circuit, and one such block of controlled-$R_k$ gates for each qubit, and again because the error is additive, the total error in the entire circuit is at most $4\pi/2^c$. This expression is independent of $n$, and can be made arbitrarily small by making $c$ arbitrarily large. (Indeed, we see that the value of $c$ needed to obtain error $\epsilon$ is $O(\log(1/\epsilon))$, which is quite favorable.)

(d) [1 point] For a fixed $c$, how many gates are used by the circuit implementing $\tilde{F}$? It is sufficient to give your answer using $\Theta$ notation.

**Solution:** $\Theta(n \log n)$

3. Implementing the square root of a unitary.

(a) [2 points] Let $U$ be a unitary operation with eigenvalues $\pm 1$. Let $P_0$ be the projection onto the +1 eigenspace of $U$ and let $P_1$ be the projection onto the −1 eigenspace of $U$. Let $V = P_0 + iP_1$. Show that $V^2 = U$.

**Solution:** We have

$$(P_0 + iP_1)^2 = P_0^2 + iP_0P_1 + iP_1P_0 - P_1^2 = P_0 - P_1 = U.$$  

(b) [2 points] Give a circuit of 1- and 2-qubit gates and controlled-$U$ gates with the following behavior (where the first register is a single qubit):

$$|0\rangle|\psi\rangle \rightarrow \begin{cases} |0\rangle|\psi\rangle & \text{if } U|\psi\rangle = |\psi\rangle \\ |1\rangle|\psi\rangle & \text{if } U|\psi\rangle = -|\psi\rangle. \end{cases}$$
Solution: This is simply phase estimation with one bit of precision, i.e., the Hadamard test:

\[
\begin{align*}
|0\rangle & \rightarrow H \cdot H \cdot |0\rangle \\
|\psi\rangle & \rightarrow U \cdot |\psi\rangle
\end{align*}
\]

(c) [4 points] Give a circuit of 1- and 2-qubit gates and controlled-\(U\) gates that implements \(V\), and show that it has the desired behavior. Your circuit may use ancilla qubits that begin and end in the \(|0\rangle\) state.

Solution: Using the circuit from part (b), we coherently compute the eigenvalue of \(U\) in an ancilla register. Then, according to part (a), we apply a phase of \(i\) if the eigenvalue is \(-1\), and no phase otherwise. Finally, we uncompute the eigenvalue. This circuit is as follows:

\[
\begin{align*}
|0\rangle & \rightarrow H \cdot H \cdot T^2 \cdot H \cdot H \cdot |0\rangle \\
|\psi\rangle & \rightarrow U \cdot U \cdot V \cdot |\psi\rangle
\end{align*}
\]

Note that we can uncompute the eigenvalue with a controlled-\(U\) gate since \(U^2 = I\).

4. Fourier transforms and composite systems. Recall that the quantum Fourier transform on \(n\) qubits is defined as the transformation

\[
|x\rangle \mapsto \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{2\pi i x y / 2^n} |y\rangle
\]

where we identify \(n\)-bit strings and the integers they represent in binary. More generally, for any nonnegative integer \(N\), we can define the quantum Fourier transform modulo \(N\) as the transformation

\[
|x\rangle \xrightarrow{F_N} \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{2\pi i x y / N} |y\rangle
\]

where the state space is \(\mathbb{C}^N\), with orthonormal basis \(\{|0\rangle, |1\rangle, \ldots, |N-1\rangle\}\).

(a) [3 points] Show that \(F_N\) is a unitary transformation.

Solution: It suffices to show that the Fourier basis states

\[
|\tilde{x}\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{2\pi i x y / N} |y\rangle
\]

are orthonormal. We have

\[
\langle \tilde{x'} | \tilde{x}\rangle = \frac{1}{N} \sum_{y, y'=0}^{N-1} e^{2\pi i (x y - x' y') / N} \langle y' | y \rangle = \frac{1}{N} \sum_{y=0}^{N-1} e^{2\pi i (x - x') y / N}.
\]
For $x = x'$ this is equal to 1 since all $N$ terms in the sum are equal to 1. But for $x \neq x'$,

$$
\sum_{y=0}^{N-1} \left( e^{2\pi i (x-x')/N} \right)^y = \frac{e^{2\pi i (x-x')/N} - 1}{e^{2\pi i (x-x')/N} - 1} = 0
$$

since $x - x'$ is an integer. Therefore

$$
\langle \tilde{x}' | \tilde{x} \rangle = \begin{cases} 
    1 & x = x' \\
    0 & \text{otherwise}
\end{cases}
$$
as desired.

(b) [1 point] Write $F_5$ in matrix form.

Solution:

$$
F_5 = \frac{1}{\sqrt{5}} \begin{pmatrix} 
1 & 1 & 1 & 1 & 1 \\
1 & e^{2\pi i/5} & e^{4\pi i/5} & e^{6\pi i/5} & e^{8\pi i/5} \\
1 & e^{4\pi i/5} & e^{8\pi i/5} & e^{2\pi i/5} & e^{6\pi i/5} \\
1 & e^{6\pi i/5} & e^{2\pi i/5} & e^{8\pi i/5} & e^{4\pi i/5} \\
1 & e^{8\pi i/5} & e^{6\pi i/5} & e^{4\pi i/5} & e^{2\pi i/5} 
\end{pmatrix}
$$

(c) [3 points] Show that $F_2 \otimes F_3 \cong F_6$, where $\cong$ denotes equivalence up to a permutation of the rows and columns (not necessarily the same permutation for the rows as for the columns).

Solution: We have

$$
F_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 
1 & 1 \\
1 & -1 
\end{pmatrix},
$$

$$
F_3 = \frac{1}{\sqrt{3}} \begin{pmatrix} 
1 & 1 & 1 \\
1 & e^{2\pi i/3} & e^{4\pi i/3} \\
1 & e^{4\pi i/3} & e^{2\pi i/3} 
\end{pmatrix},
$$

$$
F_6 = \frac{1}{\sqrt{6}} \begin{pmatrix} 
1 & 1 & 1 & 1 & 1 & 1 \\
1 & e^{\pi i/3} & e^{2\pi i/3} & e^{4\pi i/3} & e^{5\pi i/3} \\
1 & e^{2\pi i/3} & e^{4\pi i/3} & e^{2\pi i/3} & e^{4\pi i/3} \\
1 & e^{4\pi i/3} & e^{2\pi i/3} & e^{4\pi i/3} & e^{2\pi i/3} \\
1 & e^{5\pi i/3} & e^{4\pi i/3} & e^{2\pi i/3} & e^{\pi i/3} 
\end{pmatrix},
$$

and

$$
F_2 \otimes F_3 = \frac{1}{\sqrt{6}} \begin{pmatrix} 
1 & 1 & 1 & 1 & 1 & 1 \\
1 & e^{2\pi i/3} & e^{4\pi i/3} & e^{2\pi i/3} & e^{4\pi i/3} \\
1 & e^{4\pi i/3} & e^{2\pi i/3} & e^{4\pi i/3} & e^{2\pi i/3} \\
1 & e^{6\pi i/3} & e^{2\pi i/3} & e^{4\pi i/3} & e^{2\pi i/3} \\
1 & e^{8\pi i/3} & e^{2\pi i/3} & e^{4\pi i/3} & e^{2\pi i/3} 
\end{pmatrix} = \frac{1}{\sqrt{6}} \begin{pmatrix} 
1 & 1 & 1 & 1 & 1 & 1 \\
1 & e^{2\pi i/3} & e^{4\pi i/3} & e^{2\pi i/3} & e^{4\pi i/3} \\
1 & e^{4\pi i/3} & e^{2\pi i/3} & e^{4\pi i/3} & e^{2\pi i/3} \\
1 & e^{6\pi i/3} & e^{2\pi i/3} & e^{4\pi i/3} & e^{2\pi i/3} \\
1 & e^{8\pi i/3} & e^{2\pi i/3} & e^{4\pi i/3} & e^{2\pi i/3} 
\end{pmatrix}.
We can obtain $F_6$ from $F_2 \otimes F_3$ by sending rows 1, 2, 3, 4, 5, 6 to rows 1, 6, 2, 4, 3, 5, respectively, and columns 1, 2, 3, 4, 5, 6 to columns 1, 5, 3, 4, 2, 6, respectively.

(d) [3 points] Show that $F_N \otimes F_M \cong F_{NM}$ does not hold in general.

Solution: The simplest counterexample is as follows:

$$F_2 \otimes F_2 = \frac{1}{2} \begin{pmatrix}
1 & 1 & 1 & 1 \\
1 & -1 & 1 & -1 \\
1 & 1 & -1 & -1 \\
1 & -1 & -1 & 1
\end{pmatrix},$$

but

$$F_4 = \frac{1}{2} \begin{pmatrix}
1 & 1 & 1 & 1 \\
1 & i & -1 & -i \\
i & -1 & 1 & -1 \\
i & -i & -1 & i
\end{pmatrix}$$

cannot be obtained by permuting the rows and columns of $F_2 \otimes F_2$, simply because the set of entries is different.

(e) [5 bonus points] Show that if $N$ and $M$ are relatively prime, then $F_N \otimes F_M \cong F_{NM}$.

Solution: We have

$$F_N \otimes F_M = \frac{1}{\sqrt{NM}} \sum_{x,y=0}^{N-1} e^{2\pi i xy/N} |y\rangle \langle x| \otimes \sum_{x',y'=0}^{M-1} e^{2\pi i x'y'/M} |y'\rangle \langle x'|$$

$$= \frac{1}{\sqrt{NM}} \sum_{x,y=0}^{N-1} \sum_{x',y'=0}^{M-1} e^{2\pi i (Mx+Nx')/NM} |y,y\rangle \langle x,x'|,$$

and for comparison,

$$F_{NM} = \frac{1}{\sqrt{NM}} \sum_{z,w=0}^{NM-1} e^{2\pi i zw/NM} |w\rangle \langle z|.$$

By the Chinese remainder theorem, when $N$ and $M$ are coprime there is a bijection between $\mathbb{Z}_N \times \mathbb{Z}_M$ and $\mathbb{Z}_{NM}$ given by $(x,x') \leftrightarrow Mx + Nx' \mod NM$. Applying this bijection to the above expression for $F_{NM}$ (which corresponds to applying the same permutation to the rows and columns) gives

$$= \frac{1}{\sqrt{NM}} \sum_{x,y=0}^{N-1} \sum_{x',y'=0}^{M-1} e^{2\pi i (M^2 xy + N^2 x'y')/NM} |y,y\rangle \langle x,x'|$$

and for comparison,

$$= \frac{1}{\sqrt{NM}} \sum_{x,y=0}^{N-1} \sum_{x',y'=0}^{M-1} e^{2\pi i (M^2 xy + N^2 x'y')/NM} |y,y\rangle \langle x,x'|.$$

To get an expression that looks like $F_N \otimes F_M$, we can replace $x \rightarrow x/M \mod N$ and $x' \rightarrow x'/N \mod M$; these result in permutations of the columns since $M$ and $N$ are relatively prime, so $M$ has a multiplicative inverse modulo $N$ and vice versa.
5. Factoring 21.

(a) [2 points] Suppose that, when running Shor’s algorithm to factor the number 21, you choose the value \(a = 2\). What is the order \(r\) of \(a \mod 21\)?

**Solution:** We have \(r = 6\), which can be seen as follows:

\[
\begin{align*}
2^1 &\equiv 2 \mod 21 \\
2^2 &\equiv 4 \mod 21 \\
2^3 &\equiv 8 \mod 21 \\
2^4 &\equiv 16 \mod 21 \\
2^5 &\equiv 32 \equiv 11 \mod 21 \\
2^6 &\equiv 11 \cdot 2 \equiv 1 \mod 21 .
\end{align*}
\]

(b) [3 points] Give an expression for the probabilities of the possible measurement outcomes when performing phase estimation with \(n\) bits of precision in Shor’s algorithm.

**Solution:** As discussed in class, the distribution of outcomes for estimating a phase \(\varphi\) is

\[
\Pr(y) = \frac{1}{2^{2n}} \frac{\sin^2\left(\frac{2^n \varphi}{2^n}\right)}{\sin^2\left(\frac{\varphi}{n} - \frac{\pi y}{2^n}\right)}
\]

(or \(\Pr(y) = \delta_{\varphi,2\pi y/2^n}\) if \(\varphi\) is \(2\pi\) times an \(n\)-bit binary fraction). In the version of Shor’s algorithm based on phase estimation, we perform phase estimation on the input state

\[
|1\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} |u_k\rangle,
\]

where

\[
|u_k\rangle = \frac{1}{\sqrt{r}} \sum_{x=0}^{r-1} e^{2\pi i k x / r} |a^x \mod N\rangle
\]

is an eigenstate of the multiplication-by-\(a\) map with eigenvalue \(e^{2\pi i k / r}\). Thus we see the phase estimation distribution with \(\varphi = 2\pi k / r\) with probability \(1/r\). In other words, we have

\[
\Pr(y) = \frac{1}{2^{2n}} \sum_{k=0}^{r-1} \frac{\sin^2\left(\frac{2^n \varphi}{r}\right)}{\sin^2\left(\frac{\varphi}{r} - \frac{\pi y}{2^n}\right)}
\]

(interpreting the term in the sum as \(2^{2n}\) in the case where this expression gives \(0/0\)).

(c) [2 points] In the execution of Shor’s algorithm considered in part (a), suppose you perform phase estimation with \(n = 7\) bits of precision. Plot the probabilities of the possible measurement outcomes obtained by the algorithm. You are encouraged to use software to produce your plot.

**Solution:** Putting \(n = 7\) and \(r = 6\) in the answer for the previous part, we find the following:
Observe that the distribution is peaked around integer multiples of $128/6 \approx 21.3$.

(d) [2 points] Compute $\gcd(21, a^{r/2} - 1)$ and $\gcd(21, a^{r/2} + 1)$. How do they relate to the prime factors of 21?

Solution: Using Euclid's algorithm, we have $\gcd(21, a^{r/2} - 1) = \gcd(21, 7) = 7$ and $\gcd(21, a^{r/2} + 1) = \gcd(21, 9) = \gcd(3, 9) = 3$. These are the two prime factors of 21.

(e) [3 points] How would your above answers change if instead of taking $a = 2$, you had taken $a = 5$?

Solution: With $a = 5$ we again have order $r = 6$, since

$$
\begin{align*}
5^1 &\equiv 5 \mod 21 \\
5^2 &\equiv 25 \equiv 4 \mod 21 \\
5^3 &\equiv 4 \cdot 5 \equiv 20 \mod 21 \\
5^4 &\equiv 20 \cdot 5 \equiv 16 \mod 21 \\
5^5 &\equiv 16 \cdot 5 \equiv 17 \mod 21 \\
5^6 &\equiv 17 \cdot 5 \equiv 1 \mod 21.
\end{align*}
$$

In other words, the result of part (a) is the same, and consequently, the result of part (b) is the same too. However, for part (c) we have $\gcd(21, 5^3 - 1) = 1$ and $\gcd(21, 5^3 + 1) = 21$, so with this choice of $a$ the algorithm would fail.

Total points: 51