Math 4981 Spring 2021
Cryptography HW 11 Solutions
Due Thursday, April 8

1. Verify that $|\Psi\rangle = \frac{2}{7}|00\rangle + \frac{1-i}{7}|01\rangle + \frac{1+5i}{7}|10\rangle + \frac{4-i}{7}|11\rangle$ is a valid 2-qubit state. What is the probability of each possible measurement?

   Solution:

   We have

$$\begin{aligned} ||\Psi\rangle| &= \left|\frac{2}{7}\right| + \left|\frac{1-i}{7}\right| + \left|\frac{1+5i}{7}\right| + \left|\frac{4-i}{7}\right| \\ &= \frac{1}{7}\sqrt{4 + (1-i)(1+i) + (1+5i)(1-5i) + (4-i)(4+i)} \\ &= \frac{1}{7}\sqrt{4+1+1+1+25+16+1} = \frac{1}{7}\sqrt{49} = 1. \end{aligned}$$

   Thus this is a unit vector and so a valid 2-qubit state.

   We have

$$\begin{aligned} p(|00\rangle) &= \frac{4}{49} & p(|01\rangle) &= \frac{2}{49} \\ p(|10\rangle) &= \frac{26}{49} & p(|11\rangle) &= \frac{17}{49}. \end{aligned}$$

2. If $f : \{0,1\}^n \to \{0,1\}^m$ is a function with n bits of input and m bits of output, we can define a unitary operator $\mathbf{U}_f : \mathbb{C}^{2^{n+m}} \to \mathbb{C}^{2^{n+m}}$ by $\mathbf{U}_f\left(|x\rangle_n|y\rangle_m\right) = |x\rangle_n|f(x) \oplus y\rangle_m$. Given a fixed f, find a function $g : \{0,1\}^n \to \{0,1\}^m$ such that $\mathbf{U}_g$ is the inverse of $\mathbf{U}_f$.

   Solution:

   In fact $\mathbf{U}_f$ is its own inverse, since

$$\mathbf{U}_f\mathbf{U}_f(|x\rangle|y\rangle) = \mathbf{U}_f(|x\rangle|f(x) \oplus y\rangle) = |x\rangle|f(x) \oplus f(x) \oplus y\rangle = |x\rangle|0 \oplus y\rangle = |x\rangle|y\rangle.$$

3. Check explicitly that $\mathbf{H}^{\otimes n}|0\rangle_n = \frac{1}{2^{n/2}} \sum_{x \leq 0 < 2^n} |x\rangle_n$ is a unit vector.

   Solution:

$$\left\| \frac{1}{2^{n/2}} \sum_{x \leq 0 < 2^n} |x\rangle_n \right\| = \sqrt{\sum_{x=0}^{2^n-1} \frac{1}{2^{n/2}} \cdot \overline{\frac{1}{2^{n/2}}}}$$
$$= \sqrt{\sum_{x=0}^{2^n-1} \frac{1}{2^n}} = 1.$$

4. Suppose we have a unitary matrix $\mathbf{U}$ such that $\mathbf{U}(|\phi\rangle|0\rangle) \approx |\phi\rangle|\phi\rangle$ and $\mathbf{U}(|\psi\rangle|0\rangle) \approx |\psi\rangle|\psi\rangle$. Show that either $\langle\phi|\psi\rangle \approx 0$ or $\langle\phi|\psi\rangle \approx 1$.

   (Hint: $\left\langle \vec{u}_1 \otimes \vec{u}_2 \middle| \vec{v}_1 \otimes \vec{v}_1 \right\rangle = \langle \vec{u}_1 | \vec{v}_1 \rangle \cdot \langle \vec{u}_2 | \vec{v}_2 \rangle$.)

   Solution:

   Suppose we have a unitary matrix that does approximate cloning. Then we have

$$\left\langle \mathbf{U}(|\phi\rangle|0\rangle) \middle| \mathbf{U}(|\psi\rangle|0\rangle) \right\rangle \approx \left\langle |\phi\rangle|\phi\rangle \middle| |\psi\rangle|\psi\rangle \right\rangle$$
$$= \langle\phi|\psi\rangle \cdot \langle\phi|\psi\rangle = \big(\langle\phi|\psi\rangle\big)^2.$$

   But we know that $\mathbf{U}$ is unitary and thus preserves inner products, so we also have

$$\left\langle \mathbf{U}(|\phi\rangle|0\rangle) \middle| \mathbf{U}(|\psi\rangle|0\rangle) \right\rangle = \left\langle |\phi\rangle|0\rangle \middle| |\psi\rangle|0\rangle \right\rangle$$
$$= \langle\phi|\psi\rangle \cdot \langle 0|0\rangle = \langle\phi|\psi\rangle$$

   since $\langle 0|0\rangle = 1$. Thus we have

$$\big(\langle\phi|\psi\rangle\big)^2 \approx \langle\phi|\psi\rangle$$

   And thus $\langle\phi|\psi\rangle$ must be close to zero or close to 1, so this can't work for all vectors $|\phi\rangle, |\psi\rangle$.

5. Let $|\Psi\rangle = \frac{2}{7}|00\rangle + \frac{1-i}{7}|01\rangle + \frac{1+5i}{7}|10\rangle + \frac{4-i}{7}|11\rangle$ as in problem (1). Compute explicitly the quantum Fourier transform $\mathbf{U}_{FT}|\Psi\rangle$.

Solution:

$$\begin{aligned}
U_{FT}|00\rangle &= \frac{1}{2}\sum_{y=0}^{3}\exp(2\pi i\cdot 0\cdot y/4)|y\rangle_2 \\
&= \frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle \\
U_{FT}|01\rangle &= \frac{1}{2}\sum_{y=0}^{3}\exp(2\pi i\cdot 1\cdot y/4)|y\rangle_2 \\
&= \frac{1}{2}|00\rangle + \frac{i}{2}|01\rangle + \frac{-1}{2}|10\rangle + \frac{-i}{2}|11\rangle \\
U_{FT}|10\rangle &= \frac{1}{2}\sum_{y=0}^{3}\exp(2\pi i\cdot 2\cdot y/4)|y\rangle_2 \\
&= \frac{1}{2}|00\rangle + \frac{-1}{2}|01\rangle + \frac{1}{2}|10\rangle + \frac{-1}{2}|11\rangle \\
U_{FT}|00\rangle &= \frac{1}{2}\sum_{y=0}^{3}\exp(2\pi i\cdot 3\cdot y/4)|y\rangle_2 \\
&= \frac{1}{2}|00\rangle + \frac{-i}{2}|01\rangle + \frac{-1}{2}|10\rangle + \frac{i}{2}|11\rangle
\end{aligned}$$

and so

$$\begin{aligned}
U_{FT}|\Psi\rangle &= \frac{2}{7}U_{FT}|00\rangle + \frac{1-i}{7}U_{FT}|01\rangle + \frac{1+5i}{7}U_{FT}|10\rangle + \frac{4-i}{7}U_{FT}|11\rangle \\
&= \frac{1}{7}|00\rangle + \frac{1}{7}|01\rangle + \frac{1}{7}|10\rangle + \frac{1}{7}|11\rangle \\
&\quad + \frac{1-i}{14}|00\rangle + \frac{i+1}{14}|01\rangle + \frac{i-1}{14}|10\rangle + \frac{-1-i}{14}|11\rangle \\
&\quad + \frac{1+5i}{14}|00\rangle + \frac{-1-5i}{14}|01\rangle + \frac{1+5i}{14}|10\rangle + \frac{-1-5i}{14}|11\rangle \\
&\quad + \frac{4-i}{14}|00\rangle + \frac{-1-4i}{14}|01\rangle + \frac{i-4}{14}|10\rangle + \frac{4i+1}{14}|11\rangle \\
&= \frac{8+3i}{14}|00\rangle + \frac{1-8i}{14}|01\rangle + \frac{-2+7i}{14}|10\rangle + \frac{1-2i}{14}|11\rangle.
\end{aligned}$$

It's not necessary for this problem, but you can check that this is in fact a unit vector since

$$8^2 + 3^2 + 1^2 + 8^2 + 2^2 + 7^2 + 1^2 + 2^2 = 196 = 14^2.$$

6. Check that the quantum Fourier transform is unitary by showing that it sends an orthonormal basis to an orthonormal basis.

   Specifically, prove that

$$\left\langle \mathbf{U}_{FT}|x_1\rangle \middle| \mathbf{U}_{FT}|x_2\rangle \right\rangle = \begin{cases} 1 & x_1 = x_2 \\ 0 & x_1 \neq x_2 \end{cases}$$

   Solution:

For any x_1, x_2, we can compute

$$\begin{aligned}\Big\langle \mathbf{U}_{FT}|x_1\rangle \Big| \mathbf{U}_{FT}|x_2\rangle \Big\rangle &= \left\langle \frac{1}{2^{n/2}} \sum_{y=0}^{2^n-1} \exp(2\pi i \cdot x_1 \cdot y/2^n)|y\rangle_n \middle| \frac{1}{2^{n/2}} \sum_{y=0}^{2^n-1} \exp(2\pi i \cdot x_2 \cdot y/2^n)|y\rangle_n \right\rangle \\ &= \frac{1}{2^n} \sum_{y=0}^{2^n-1} \exp(2\pi i \cdot x_1 \cdot y/2^n)\overline{\exp(2\pi i \cdot x_w \cdot y/2^n)} \\ &= \frac{1}{2^n} \sum_{y=0}^{2^n-1} \exp(2\pi i \cdot x_1 \cdot y/2^n - 2\pi i \cdot x_w \cdot y/2^n) \\ &= \frac{1}{2^n} \sum_{y=0}^{2^n-1} \exp(2\pi i (x_1 - x_2) y/2^n).\end{aligned}$$

Now, if $x_1 = x_2$, this is just

$$\frac{1}{2^n} \sum_{y=0}^{2^n-1} \exp(2\pi i (0) y/2^n) = \frac{1}{2^n} \sum_{y=0}^{2^n-1} 1 = 1.$$

If $x_1 \neq x_2$, then it's some constant integer k. Then we have

$$\Big\langle \mathbf{U}_{FT}|x_1\rangle \Big| \mathbf{U}_{FT}|x_2\rangle \Big\rangle = \frac{1}{2^n} \sum_{y=0}^{2^n-1} \exp\left(2\pi i y \frac{k}{2^n}\right) \qquad = \frac{1}{2^n} \sum_{y=0}^{2^n-1} \exp\left(2\pi i \frac{k}{2^n}\right)^y$$

Since $\exp(2\pi i k/2^n)$ is a nth root of unity, it's a common fact that this sum is zero. There are a few different ways you could argue this; I'm happy for you to just say that for each complex number we get this way, we also get the complex number on the opposite side of the circle and they cancel out.

But you can also make arguments from the theory of polynomials, as you can see e.g. at `https://math.stackexchange.com/questions/891875/proof-that-sum-of-complex-unit-root`

7. In the proof of Shor's algorithm, we claimed there is at most one rational number with denominator less than N in a window of width $1/N^2$. We want to prove that.

   Suppose we have (distinct) rational numbers $a/b, c/d$ with $1 \leq b, d < N$. Show that $\left|\frac{a}{b} - \frac{c}{d}\right| > \frac{1}{N^2}$.

   Solution: We have $\frac{a}{b} - \frac{c}{d} = \frac{ad-bc}{db}$. Since $a/b \neq c/d$ (which I forgot to include in the original problem statement, sorry), we know that $ad - bc \neq 0$; and since it's an integer, we have $|ad - bc| \geq 1$. Since $b, d < N$ we have $bd < N^2$ and $\frac{1}{bd} > \frac{1}{N^2}$, and thus

$$\left|\frac{a}{b} - \frac{c}{d}\right| = \frac{|ad - bc|}{bd} > \frac{1}{N^2}.$$