# Math 4981 Spring 2021
# Cryptography HW 11
# 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?

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 $\mathbf{U}_f$.

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.

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

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 $\mathbf{U}_{FT}|\Psi\rangle$.

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

   Specifically, prove that

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

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 rational numbers $a/b, c/d$ with $b, d < N$. Show that $\left|\frac{a}{b} - \frac{c}{d}\right| > \frac{1}{N^2}$.