QIC 710 Problem Set 4

1. Computation and un-computation.

(a) Let f be a permutation on $\{0,1\}^n$. Given classical circuits computing f and f^{-1}, using AND and NOT gates, give a reversible circuit that computes the map

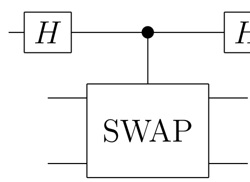
$$|x\rangle \otimes |0^n\rangle \mapsto |f(x)\rangle \otimes |0^n\rangle \ .$$

(b) Let p be a prime and g a generator for Z_p^*. Give an efficient quantum circuit that approximates the map

$$|x\rangle \mapsto |g^x \mod p\rangle$$

for $x \in \{0,1,\ldots,p-2\}$. (You may use extra ancilla qubits, but clean up the garbage. You may take as given any well-known efficient classical circuits.)

2. The "swap test."
Let SWAP be the unitary operator that maps $|\phi\rangle \otimes |\psi\rangle \mapsto |\psi\rangle \otimes |\phi\rangle$ for all $|\phi\rangle, |\psi\rangle$, i.e., it swaps the two registers. Let c-SWAP be the controlled SWAP operator.



Consider the above circuit, with input $|0\rangle\langle 0| \otimes \rho \otimes \sigma$ for some density matrices ρ, σ. Show that the measurement gives 0 with probability

$$\frac{1}{2}\big(1 + \mathrm{Tr}(\rho\,\sigma)\big) \ .$$

In particular, if $\rho = \sigma = |\psi\rangle\langle\psi|$ for some state $|\psi\rangle$, then the measurement gives 0 with certainty. If ρ and σ have orthogonal supports, e.g., $\rho = |\psi\rangle\langle\psi|$, $\sigma = |\phi\rangle\langle\phi|$ with $\langle\psi|\phi\rangle = 0$, then the measurement result is uniformly random.

3. The Pauli matrices are important in quantum information for numerous reasons, in particular because they are generators for the group of single-qubit transformations $SU(2)$ (the group of 2×2 unitary matrices with determinant $+1$), which also describe rotations of the Bloch sphere in three dimensions.

The Pauli matrices are defined as

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \ .$$

They satisfy $X^2 = Y^2 = Z^2 = \mathbf{1}$, $XY = iZ = -YX$, $YZ = iX = -ZY$ and $ZX = iY = -XZ$.

(a) For a Pauli P, let $R_P(2\theta) = e^{i\theta P}$, a rotation about the P axis in the Bloch sphere by angle 2θ. Using the fact/definition $e^M = \sum_{k=0}^{\infty} M^k/k!$, show that

$$R_X(2\theta) = e^{i\theta X} = \begin{pmatrix} \cos\theta & i\sin\theta \\ i\sin\theta & \cos\theta \end{pmatrix}$$

$$R_Y(2\theta) = e^{i\theta Y} = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}$$

$$R_Z(2\theta) = e^{i\theta Z} = \begin{pmatrix} \cos\theta + i\sin\theta & 0 \\ 0 & \cos\theta - i\sin\theta \end{pmatrix}$$

(b) Suppose you want $R_Z(\theta)$ but only have gates that perform $R_X(\frac{\pi}{2})$ and $R_Y(\theta)$. Show how to compose these gates to accomplish the desired rotation.