CSCE689: FDNS of Post-Quantum Crypto

Exercise 1

Texas A&M U, Fall 2018 — *September 7, 2018*

Lecturer: Fang Song — *Due: September 18, 2018*

Instructions. This is for your own practice only. For each of the four problems, you are required to turn in your work for selected subproblems of you own choice. It will not be graded, and it counts towards your participation grade. Download the TeX file if you want to typeset your solutions using LaTeX.

1. (Basic Algebra) Let X, Y, Z be the Pauli operators.
   (a) (complex number) For complex number $c = a + bi$, recall that the real and imaginary parts of c are denoted $Re(c) = a$ and $Im(c) = b$.
   - Prove that $c + c^* = 2 \cdot Re(c)$.
   - Prove that $|c|^2 := cc^* = a^2 + b^2$.
   - What is the polar form of $c = \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}i$? Use the fact that $e^{i\theta} = \cos\theta + i\sin\theta$?

   (b) (Trace) Recall the trace of a matrix $M = (m_{ij})_{n\times n}, m_{ij} \in \mathbb{C}$ is defined by $\mathrm{tr}(M) := \sum_{i=1}^{n} m_{ii}$.
   - What is $\mathrm{tr}(X|0\rangle\langle 1|)$?
   - Show that $\mathrm{tr}(YZ) = \mathrm{tr}(ZY)$. Prove that this holds for general matrices: any $n \times n$ matrices M and N, $\mathrm{tr}(MN) = \mathrm{tr}(NM)$.

   (c) (Inner product)
   - Let $|\phi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{i}{\sqrt{2}}|1\rangle$. $|\psi\rangle = \sqrt{\frac{1}{3}}|0\rangle - \sqrt{\frac{2}{3}}|1\rangle$. Calculate $\langle\phi|\psi\rangle$.
   - Show that $X = |0\rangle\langle 1| + |1\rangle\langle 0|$. Express Y, Z in this outer product form too. Calculate $\langle 1|X|0\rangle$ (using linearity).

   (d) (Tensor product) Recall the *tensor product* of two matrices A and B is $A \otimes B := (a_{ij}B)$.
   - Write out the 4×4 matrix representing $X \otimes Y$. Does it equal $Y \otimes X$?
   - Show that $(A \otimes B)^\dagger = A^\dagger \otimes B^\dagger$.
   - Show that $(A \otimes B)(C \otimes D) = AC \otimes BD$.
   - Show that if U and V are unitary matrices, then so is $U \otimes V$.

2. (Quantum states and gates)
   (a) In each case, describe the resulting state. $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$.
   i) Apply H to the qubit $\frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$.
   ii) Apply H to the first qubit of state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

iii) Apply H to both qubits of $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

iv) Apply $\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}$ to both qubits of state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

(b) Let $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

i) Suppose we have a qubit and we first apply X and then Z. Is it equivalent to first applying Z and then X?

ii) Suppose we have two qubits. We apply X to both and then Z to both. Is it equivalent to applying Z to both and then applying X to both? Determine your answer by explicitly computing $X \otimes X$, $Z \otimes Z$, and their products both ways.

(c) (SWAP gate) A SWAP gate takes two inputs a and b and outputs b and a; i.e., it swaps the values of two input registers. Show how to build a SWAP gate using only CNOT gates. (Hint: you'll need 3 of them.)

3. (Product states versus entangled states) In each of the following, either express the 2-qubit state as a tensor product of 1-qubit states or prove that it cannot be expressed this way.

(a) $\frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle - \frac{1}{2}|11\rangle$

(b) $\frac{3}{4}|00\rangle + \frac{\sqrt{3}}{4}|01\rangle + \frac{\sqrt{3}}{4}|10\rangle + \frac{1}{4}|11\rangle$

4. (Distinguishing states by local measurements) Suppose Alice and Bob are physically separated from each other, and are each given one of the qubits of some 2-qubit state. They are required to distinguish between State I and State II with only local measurements. Namely they can each perform a local (one-qubit) unitary operation and then a measurement (in the computational basis) of their own qubit. After their measurements, they can send only classical bits to each other. (This is usually referred to as LOCC: local operation and classical communication.) In each case below, either give a perfect distinguishing procedure (that never errs) or explain why there is no perfect distinguishing procedure (i.e., that for any procedure the success probability must be less than 1).

(a) State I: $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$; State II: $\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$

(b) State I: $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$; State II: $\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$

(c) State I: $\frac{1}{\sqrt{2}}(|00\rangle + i|11\rangle)$; State II: $\frac{1}{\sqrt{2}}(|00\rangle - i|11\rangle)$