MTAT.07.024 Quantum Crypto

Assoc. Prof. Dirk Oliver Theis

Shahla Novruzova

Homework # 1

Handed out:	Tue Feb. 25
Due:	Tue March 4, 10:00
As PDF by email to	`shahla.novruzova@ut.ee`
subject:	`QCRY-HW1-`*lastname*

1 Warm-up: Bell states (20 pts)

Verify that the following four 2-qubit states form an ONB:

- $(|00\rangle + |11\rangle)/\sqrt{2}$
- $(|00\rangle - |11\rangle)/\sqrt{2}$
- $(|01\rangle + |10\rangle)/\sqrt{2}$
- $(|01\rangle - |10\rangle)/\sqrt{2}$

(Your calculations here.)

2 Warm-up: Exponential of Hermitian unitaries (20 pts)

Let A be a Hermitian (i.e., $A^\dagger = A$) unitary (i.e., $A^\dagger = A^{-1}$) operator. Prove that, for all $\theta \in \mathbb{R}$,

$$\exp(i\theta A) = \cos\theta \cdot \mathbb{1} + i \sin\theta \cdot A. \tag{1}$$

Recall:

- $\exp(X) = \sum_{k=0}^{\infty} \frac{X^k}{k!}$
- $\cos(X) = \sum_{j=0}^{\infty} \frac{(-1)^j}{(2j)!} X^{2j}$
- $\sin(X) = \sum_{j=0}^{\infty} \frac{(-1)^j}{(2j+1)!} X^{2j+1}$

(Your calculation here.)

0. Before starting, Alice and Bob share a pair of qubits (i.e., each of them has one qubit) in the state
$$\big(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle\big)/\sqrt{2}.$$
1. Alice is given 2 bits $x, z \in \{0, 1\}$ with the task to send them to Bob.
2. Alice does the following: If $x = 1$, apply an `X`-gate to her qubit.
3. Alice does the following: If $z = 1$, apply a `Z`-gate to her qubit.
4. Alice sends her qubit to Bob.
5. Bob now has both qubits.
6. Bob applies a `CNOT` gate with control on the qubit he received from Alice and target on his own qubit.
7. Bob applies a Hadamard basis-change gate to Alice's qubit.
8. Bob measures both qubits in the computational basis, and sets
   - $z' :=$ outcome from Alice's qubit
   - $x' :=$ outcome from his own qubit.

Figure 1: Efficient communication protocol with prior entanglement: 2 bits = 1 qubit + entangled resource

3 Efficient communication using entanglement (35 pts)

Consider the quantum communication protocol in Fig. 1.

Recall that

- $X = |+\rangle\langle+| - |-\rangle\langle-|$ and $Z = |0\rangle\langle 0| - |1\rangle\langle 1|$;
- The unitary for the Hadamard basis change gate is $|0\rangle\langle+| + |1\rangle\langle-| = |+\rangle\langle 0| + |-\rangle\langle 1|$;
- "Apply U to the left-most qubit" means, apply $U \otimes \mathbb{1}$ to the combined system;
- The unitary operator for `CNOT` with control on the left qubit and target on the right qubit is:
$$|0\rangle\langle 0| \otimes \mathbb{1} + |1\rangle\langle 1| \otimes X.$$

Verify that the protocol is correct: For every choice of x, z, with probability 1, Bob ends up with $x' = x$ and $z' = z$.

(Your solution here.)

4 No-cloning theorem (25 pts)

Suppose Alice has a qubit in an unknown state. She wants to send the qubit to Bob, but also keep a copy for herself. Let's say that a "cloning operator" is a mapping $E\colon \mathbb{C}^2 \to \mathbb{C}^2 \otimes \mathbb{C}^2$ with the property
$$E\psi = \psi \otimes \psi. \tag{2}$$

Alice wants a cloning operator — but not being Elon Musk, she's subject the rules of quantum mechanics, so her E must be a *linear* operator.

Prove that linear cloning operators don't exist.

(Your solution here.)