MTAT.05.024 Quantum Crypto

Assoc. Prof. Dirk Oliver Theis

Shahla Novruzova

Homework # 1

Handed out:	Tue Feb. 27
Due:	Tue March 5, 10:00
As PDF by email to	`shahla.novruzova@ut.ee`
subject:	`QCRY-HW1-`*lastname*

1 Orthonormal bases

Definition. The "computational (orthonormal) basis" of the Hilbert space of an n-qubit quantum register consists of the states $|x\rangle$, where x ranges over all elements of $\{0,1\}^n$, i.e., length-n bit strings. For example, for a single qubit, we get the familiar ONB $|0\rangle, |1\rangle$.

(a) 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 solution here.)

(b) Write the following 2-qubit states as superposition of the basis defined in (a):

- $|00\rangle$

  (Your solution here.)

- $|01\rangle$

  (Your solution here.)

- $|11\rangle$

  (Your solution here.)

2 Measurement I

A computational basis measurement of a single qubit has possible outcomes $0, 1$. If the single qubit is in state

$$\psi = \alpha_0 |0\rangle + \alpha_1 |1\rangle ,$$

then the probability of outcome 0 is $|\alpha_0|^2$ and the probability of outcome 1 is is $|\alpha_1|^2 = 1 - |\alpha_0|^2$.

For each of the following states, give the measurement probabilities of the outcomes:

(a) $|0\rangle$ ....

(b) $|1\rangle$ ....

(c) $|+\rangle$ ....

(d) $|-\rangle$ ....

(e) $|\circlearrowleft\rangle$ ....

(f) $|\circlearrowright\rangle$ ....

3 Measurement II

A computational basis measurement of the *left* one of two qubits has possible outcomes $0, 1$. If the two qubits are in the state

$$\psi = \alpha_{00} |00\rangle + \alpha_{01} |01\rangle + \alpha_{10} |10\rangle + \alpha_{11} |11\rangle ,$$

then the probability of outcome 0 is

$$|\alpha_{00}|^2 + |\alpha_{01}|^2$$

and the probability of outcome 1 is

$$|\alpha_{10}|^2 + |\alpha_{11}|^2 = 1 - \left(|\alpha_{00}|^2 + |\alpha_{01}|^2\right) .$$

For each of the states in item (a) of exercise 1, give the measurement probabilities of the outcome of measuring the left qubit.

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

4 Tensor products

Recall from the lecture the fact that that $(\phi, \psi) \to \phi \otimes \psi$ is "bi-linear", i.e.,

- For each fixed ϕ the mapping $\psi \mapsto \phi \otimes \psi$ is linear;
- For each fixed ψ the mapping $\phi \mapsto \phi \otimes \psi$ is linear.

Use this to expand the following 2-qubit states in the computational basis (i.e., $|0\rangle \otimes |0\rangle$, $|0\rangle \otimes |1\rangle$, $|1\rangle \otimes |0\rangle$, $|1\rangle \otimes |1\rangle$):

(a) $|0\rangle \otimes |+\rangle$ ......

(b) $|+\rangle \otimes |1\rangle$ ......

(c) $|+\rangle \otimes |+\rangle$ ......

(d) $|+\rangle \otimes |-\rangle$ ......

(e) $|-\rangle \otimes |+\rangle$ ......

(f) $|-\rangle \otimes |-\rangle$ ......

The construction of the basis in item (a) of exercise 1 can be carried out with $+/-$ instead of $0/1$:

- $(|+\rangle \otimes |+\rangle + |-\rangle \otimes |-\rangle)/\sqrt{2}$
- $(|+\rangle \otimes |+\rangle - |-\rangle \otimes |-\rangle)/\sqrt{2}$
- $(|+\rangle \otimes |-\rangle + |-\rangle \otimes |+\rangle)/\sqrt{2}$
- $(|+\rangle \otimes |-\rangle - |-\rangle \otimes |+\rangle)/\sqrt{2}$

(g) Creative writing. If a 2-qubit quantum register is in the state

$$\Big(\big((|00\rangle + |11\rangle)/\sqrt{2}\big) + \big((|+\rangle \otimes |+\rangle + |-\rangle \otimes |-\rangle)/\sqrt{2}\big)\Big)/\sqrt{2}$$

— what does that mean?