QUANTUM CRYPTOGRAPHY
Master of Logic, University of Amsterdam, 2017
TEACHERS: Jan Czajkowski, Yfke Dulek, and Christian Schaffner

Practice problem set 10

You do not have to hand in these exercises, they are for practicing only.

Problem 1: Position verification with a flawed device

Imagine that Alice (one of the verifiers in a position-verification protocol) is unable to prepare BB84 states. Instead, she can only produce qubits in the standard basis $\{|0\rangle, |1\rangle\}$ and the Breidbart basis $\{|0_B\rangle, |1_B\rangle\}$, where $|0_B\rangle = \cos(\pi/8)|0\rangle + \sin(\pi/8)|1\rangle$, and $|1_B\rangle = \sin(\pi/8)|0\rangle - \cos(\pi/8)|1\rangle$.

(a) Drawing on your intuition, do you think it will become easier or harder for dishonest Waldo and Wenda to trick Alice and Bob? Or does it not matter?

(b) Now explicitly compute the probability that dishonest Waldo and Wenda can cheat if Alice sends $n = 1$ qubit (encoded in either the standard or the $\pi/8$ basis with probability $1/2$).

(c) Suppose Waldo and Wenda have no quantum memory. What is their winning probability of Alice sends n qubits?

Problem 2: Personalized position verification

Let's imagine Alice and Bob want something more than just position verification. Say they not only want to know that someone is at a given location but also that that person is specifically Waldo, and not anyone else (maybe Wenda). We will build a protocol to do just that. In order to identify Waldo, we will assume that Alice, Bob and Waldo share a secret key $k \in \{0,1\}^n$ ahead of time.

Construct a protocol that satisfies the following conditions:

(Correctness) If Waldo is at the claimed position, then he can convince Alice and Bob of this fact.

(Security I) If Waldo is helped by his companion Wenda (with whom he is unentangled), the probability that he can trick Alice and Bob (into thinking that he is at the location while he is not) is exponentially small in n.

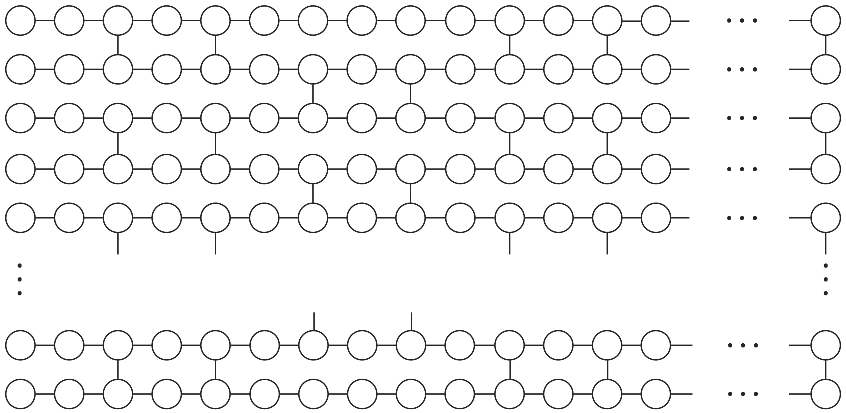
(Security II) Any impostor Willem cannot trick Alice and Bob into believing that he is Waldo at the claimed location except with probability exponentially small in n.

Problem 3: Universality of the brickwork state

Consider the "brickwork state", which was claimed in the lectures to be a universal resource for measurement-based quantum computation. In this exercise you will prove its universality. The $n \times m$ brickwork state is defined as a grid of n rows and m columns of $|+\rangle$ states, with CTRL-Z operations applied between the qubits as follows:

- For all $1 \leqslant i \leqslant n$ and all $1 \leqslant j < m$: between qubits (i,j) and $(i, j+1)$ (the horizontal connections)
- For all odd $1 \leqslant i \leqslant n$: and all $j \equiv 3 \mod 8$: between qubits (i,j) and $(i+1,j)$, and also between qubits $(i,j+2)$ and $(i+1,j+2)$.
- For all even $1 \leqslant i \leqslant n$: and all $j \equiv 7 \mod 8$: between qubits (i,j) and $(i+1,j)$, and also between qubits $(i,j+2)$ and $(i+1,j+2)$.

See also the image below, where the edges represent CTRL-Z operations.



Let M^θ denote the single-qubit measurement in the basis $\{|+_\theta\rangle, |-_\theta\rangle\}$, where $|+_\theta\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\theta}|1\rangle)$ and $|-_\theta\rangle = \frac{1}{\sqrt{2}}(|0\rangle - e^{i\theta}|1\rangle)$.

(a) Starting with the state $|\psi\rangle \otimes |+\rangle$, and performing a control-Z followed by a measurement M^θ on the first qubit, what is the state $|\psi'\rangle$ of the second qubit? Assume the measurement outcome is $|+_\theta\rangle$.

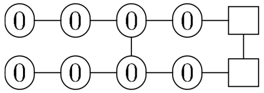
Express the unitary that maps $|\psi\rangle \to |\psi'\rangle$ in terms of the Hadamard gate and $U_z(\theta)$, the rotation of θ around the z axis of the Bloch sphere:

$$U_z(\theta) = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{bmatrix}.$$

(b) Show that for any given angle θ and any Pauli $X^s Z^t$, there exists a θ' (expressed in terms of θ, s, and t) such that measuring $M^{\theta'}$ is equivalent to applying $X^s Z^t$ and then measuring M^θ. (Here, equivalence is intended in terms of the outcome probabilities and post-measurement state on the remaining qubits. You should assume that the measured qubit is destroyed.)

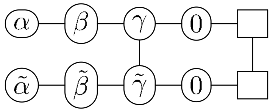
Conclude that if the measurement outcome was $|-_\theta\rangle$ instead of $|+_\theta\rangle$ in the previous subexercise, we can correct the output state to the computed state $|\psi'\rangle$ by measurement only.

(c) Use the result from the previous subexercise to determine the effect of the following *measurement pattern*. The two left-most qubits are the input qubits (in an arbitrary two-qubit pure state $|\psi\rangle$), all other qubits are initialized in the $|+\rangle$ state. The output lands into the only two unmeasured qubits, represented by the two squares.

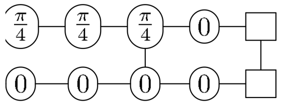


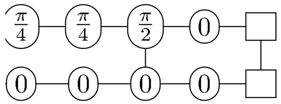
(d) In the above measurement pattern, change *one* measurement angle in order to implement the gate $T \otimes I$.

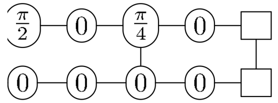
(e) Which two-qubit unitary is implemented by the following, more general, measurement pattern?

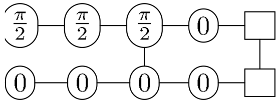

α β γ 0
$\tilde{\alpha}$ $\tilde{\beta}$ $\tilde{\gamma}$ 0

(f) Armed with the knowledge from the previous question, determine which of the following measurement patterns implements a Hadamard gate on the top qubit.

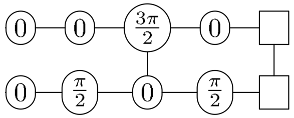


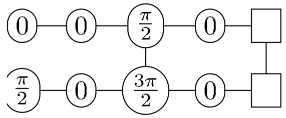


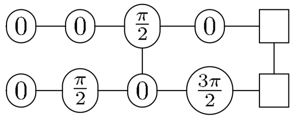


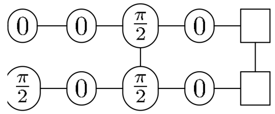


(g) We now know the measurement patterns for T and H. For universal quantum computation, we only need to find the pattern for CNOT. Which of the following patterns achieves CNOT with the top qubit as control?









(h) Describe how to perform CNOT between non-adjacent rows in the brickwork state.

Problem 4: Computing on encrypted quantum data

Alice wants Bob to perform some quantum circuit for her. She encrypts her n-qubit state using a quantum one-time pad. Call the X-keys $\vec{a} = (a_1, ..., a_n)$ and the Z-keys $\vec{b} = (b_1, ..., b_n)$. She then sends the encrypted state to Bob. In this exercise, you will investigate how Bob can perform the gates $X, Z, H, P, CNOT$, and T on this state in such a way that Alice can, at the end, decrypt the state to the desired outcome: the circuit applied to her input. Bob should not learn anything about Alice's input. During the computation, Alice can perform classical computations on her keys.

(a) Bob performs the Clifford gates $(X, Z, H, P, CNOT)$ by directly applying them to the encrypted qubits. Describe in detail the classical computations Alice must perform to update her keys.

(b) For the rest of this exercise, consider $n = 1$. Let $X^a Z^b \rho Z^b X^a$ describe the state of the qubit. Find expressions for p, x and z (in terms of 0, 1, a, and b) such that

$$TX^a Z^b = P^p X^x Z^z T.$$

(c) P^p is an error on the output state: Bob cannot continue his computation correctly without removing it first. However, Bob does not know p and therefore he cannot perform $(P^p)^\dagger$. Should Alice tell him p? Why or why not?