TUTORIAL 13

1 Assignment 9

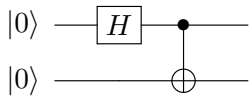
Recall Shor's code that was defined in the lecture:

$$|\bar{0}\rangle = \frac{1}{2\sqrt{2}}\left(|0^3\rangle + |1^3\rangle\right)^{\otimes 3},$$
$$|\bar{1}\rangle = \frac{1}{2\sqrt{2}}\left(|0^3\rangle - |1^3\rangle\right)^{\otimes 3}.$$

Show that this code cannot correct arbitrary acting on two qubits.

2 Exam from last year

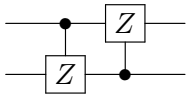
Problem 1 (Basic calculations)**.** 1. Consider the following circuit



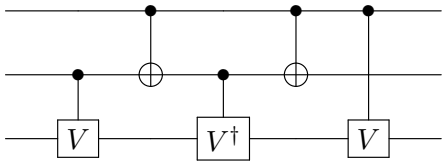
(a) Compute the two-qubit state $|\psi\rangle_{A_1A_2}$ after applying this circuit. Here A_1 denotes the top wire and A_2 the bottom wire.

(b) Compute the density matrix of the state on A_1, i.e., the partial trace over A_2 of the density operator $|\psi\rangle\langle\psi|_{A_1A_2}$ that we denote $\mathrm{tr}_{A_2}\left(|\psi\rangle\langle\psi|_{A_1A_2}\right)$.

2. Recall that $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ and the controlled version CZ is defined by $CZ(|0\rangle \otimes |\psi\rangle) = |0\rangle \otimes |\psi\rangle$ and $CZ(|1\rangle \otimes |\psi\rangle) = |1\rangle \otimes (Z|\psi\rangle)$. In circuit diagrams, CZ is denoted by a black dot on the control qubit connected with a Z gate for the target qubit. Compute the unitary defined by the following circuit:

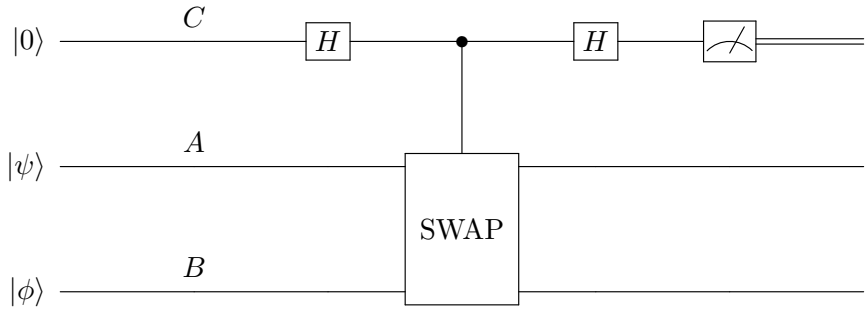


3. Let U be the unitary on three qubits computed by the following circuit



where V is a unitary on 1 qubit. Recall that $V^\dagger$ is the complex conjugate of V. For each $b_1, b_2 \in \{0, 1\}$, give the state $U(|b_1\rangle \otimes |b_2\rangle \otimes |\psi\rangle)$ as a function of V and $|\psi\rangle$. The state has a simple description. Here, $|\psi\rangle \in \mathbb{C}^2$ an arbitrary qubit state.

Problem 2 (SWAP test and application to quantum fingerprinting)**.** Assume we have two quantum registers A prepared in the state $|\psi\rangle \in \mathbb{C}^d$ and B prepared in the state $|\phi\rangle \in \mathbb{C}^d$. We would like to construct a circuit to estimate $|\langle\psi|\phi\rangle|^2$. The "SWAP test" is a procedure for doing this: use a qubit register C initialized in the state $|0\rangle$, apply a controlled-SWAP gate followed by a Hadamard on register C and then measure C as shown in the following circuit diagram:



The SWAP unitary on $\mathbb{C}^d \otimes \mathbb{C}^d$ is defined by $\mathrm{SWAP}(|i\rangle_A \otimes |j\rangle_B) = |j\rangle_A \otimes |i\rangle_B$ for any $i, j \in \{0, \ldots, d-1\}$. Here $|0\rangle_A, |1\rangle_A, \ldots, |d-1\rangle_A$ is a fixed orthonormal basis of $\mathbb{C}^d$ (and the same for B). The controlled-SWAP gate is defined as usual: if the control qubit is $|0\rangle$ nothing is done on the AB registers and if the control qubit is $|1\rangle$, the unitary SWAP is applied on the AB registers.

1. When $d = 2$, what is the dimension of the controlled-SWAP unitary? Write down the matrix for controlled-SWAP explicitly.

2. Show that for any states $|\psi\rangle \in \mathbb{C}^d, |\phi\rangle \in \mathbb{C}^d$, we have $\mathrm{SWAP}(|\psi\rangle_A \otimes |\phi\rangle_B) = |\phi\rangle_A \otimes |\psi\rangle_B$. (As the name suggests, the unitary exchanges the two registers A and B).

3. Compute the probability that the outcome of the measurement of the C register at the end of the circuit diagram is 0. This probability should be a function of $|\langle\psi|\phi\rangle|^2$.

4. Let $\epsilon \in (0, 1)$. Deduce a procedure that outputs a number that lies in the interval $[|\langle\psi|\phi\rangle|^2 - \epsilon, |\langle\psi|\phi\rangle|^2 + \epsilon]$ with probability at least $2/3$ by using multiple copies of $|\psi\rangle, |\phi\rangle$. How many copies of $|\psi\rangle$ and $|\phi\rangle$ do you use as a function of ϵ?

5. We now apply this procedure for a problem of testing equality also called fingerprinting. Suppose Alice has a bitstring $x \in \{0,1\}^m$ and Bob has a bitstring $y \in \{0,1\}^m$ and the Referee would like to know whether $x = y$ or $x \neq y$ while minimizing communication. Communication can only be between Alice and the Referee or Bob and the Referee (i.e., no communication between Alice and Bob). The objective is to design a protocol that allow the referee to correctly decide whether $x = y$ or $x \neq y$ for all possible choices of $x \in \{0,1\}^m$ and $y \in \{0,1\}^m$.

   (a) Give a protocol achieving this task and using m bits of communication from Alice to Referee and m bits from Bob to Referee (this protocol is supposed to be trivial).

   (b) In a quantum protocol, Alice can prepare a state $|\psi_x\rangle \in \mathbb{C}^d$ as a function of her bitstring x, and Bob a state $|\phi_y\rangle \in \mathbb{C}^d$ as a function of his bitstring y. The Referee receives both states $|\psi_x\rangle$ and $|\phi_y\rangle$ and can perform an arbitrary operation allowed by quantum theory and outputs 1 (corresponding to $x = y$) or 0 (corresponding to $x \neq y$). Design a quantum protocol satisfying the following properties:

   - (Cost) $d = \mathrm{poly}(m)$, i.e., d is polynomial in m. In other words, the number of qubits of communication used is $O(\log m)$.
   - (Correctness) For every $x, y \in \{0,1\}^m$, if $x = y$, the Referee outputs 1 with certainty and if $x \neq y$, the Referee outputs 0 with probability at least $\frac{2}{3}$

   Hint: You may want to use classical error correcting codes, in particular, you may use without proof the existence of codes of type $(n, \lfloor n/10 \rfloor)$ that have a minimum distance at least $\lfloor n/10 \rfloor$ for any $n \in \mathbb{N}_+$.