

QIP Exercises

1. Entanglement

a) Show that the state

$$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

is entangled. That is, show that no pair of single qubit states $|\phi\rangle, |\psi\rangle$ can satisfy that $|\phi\rangle \otimes |\psi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$.

b) Is the state $\frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|11\rangle$ entangled? what about $\frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|10\rangle$?

2. Distinguishing states

Alice prepares a qubit and chooses at random whether to generate one in state $|0\rangle$ or in state $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$. She sends the qubit to Bob, who tries to figure out which state he received.

Let B_θ be the basis for C^2 that is rotated by an angle of θ from the standard basis consisting of $|0\rangle, |1\rangle$. So if we let

$$|0_\theta\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle, \quad |1_\theta\rangle = -\sin\theta|0\rangle + \cos\theta|1\rangle$$

then $B_\theta = (|0_\theta\rangle, |1_\theta\rangle)$. Recall that measuring a qubit in basis B_θ can be thought of as asking the qubit which basis state it is in, and we say the result is 0 if the answer is $|0_\theta\rangle$ and 1 otherwise.

Suppose Bob measures the received qubit in basis B_0 . If the result was 0 he guesses that he received state $|0\rangle$, otherwise he guesses that he received $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$. What is the probability that he is right?

Suppose Bob measures instead in basis $B_{\pi/8}$. Again if the result was 0 his guess is state $|0\rangle$, and otherwise $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$. What is now the success probability?

Find the choice of θ for which measurement in basis B_θ gives the highest possible success probability.

3. Measuring EPR pairs

Consider a system containing two qubits. It lives in 4-dimensional space, and the standard basis ($|00\rangle, |01\rangle, |10\rangle, |11\rangle$) can be thought of as being constructed from the standard basis ($|0\rangle, |1\rangle$) for the first qubit and the same basis for the second, and then taking all pairwise tensor products (recall that $|00\rangle$, for instance, is short for $|0\rangle \otimes |0\rangle$).

In exactly the same way, we can construct a basis for the 4-dimensional space starting instead from the single qubit basis ($|0_\theta\rangle, |1_\theta\rangle$) for both the first and second qubit. The resulting basis is ($|0_\theta 0_\theta\rangle, |0_\theta 1_\theta\rangle, |1_\theta 0_\theta\rangle, |1_\theta 1_\theta\rangle$).

Suppose now that the two qubits are in the EPR state $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$. Show that for any θ :

$$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle = \frac{1}{\sqrt{2}}|0_\theta 0_\theta\rangle + \frac{1}{\sqrt{2}}|1_\theta 1_\theta\rangle$$

Use this to argue that if one of the qubits is measured in basis B_θ , the result is 0 with probability 1/2 and 1 with probability 1/2, and if the result is a bit b , then the other qubit is in the same state as the one measured, i.e., $|b_\theta\rangle$.

4. A game with classical players

Suppose Alice and Bob play the following game against a challenger Charlie:

1. Alice and Bob are allowed to meet before the game and agree on any (classical) strategy they want, but during the game they cannot communicate.
2. Charlie chooses two bits x, y at random, and gives x to Alice and y to Bob.
3. Alice outputs a bit a and Bob a bit b . Alice and Bob win the game if it is the case that $a \oplus b = x \wedge y$.

Show that there is no way Alice and Bob can win with probability larger than 3/4.

5. The game with quantum players

In this exercise, Alice and Bob play the same game, but now they are allowed to use quantum information when they meet before the game. Concretely, assume they prepare two qubits in the state $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$. Alice then takes one qubit with her, Bob takes the other.

Note that sharing parts of an entangled state as we do here does not allow to send information, so there is no trivial winning strategy in the line of Alice telling Bob which input bit she has. But still, there is a strategy that does better than any classical solution:

If Alice has input bit 0, she measures her qubit in basis $B_{\pi/4}$, if the bit is 1, she measures in basis B_0 . In any case, she outputs the measurement result.

If Bob has input bit 0, he measures his qubit in basis $B_{\pi/8}$, if the bit is 1, he measures in basis $B_{3\pi/8}$. In any case, he outputs the measurement result.

Use Exercise 3 to show that Alice and Bob wins this game with probability $\cos^2 \pi/8$. You may wonder why we have not specified whether Alice measures before Bob or Bob before Alice. The answer is that it doesn't matter – the distribution of results will be the same in both cases.

This result shows that quantum physics cannot be explained by “hidden classical variables”: Several physicists have tried to explain the observed correlation between measurements of EPR particles by assuming that the particles somehow “agreed on” some hidden classical information when the state was created, and that is then supposedly the reason why one particle can show the same measurement result as the other.

But such hidden classical information exactly corresponds to Alice and Bob trying to win the game from Exercise 4 using a classical strategy. As we have seen, EPR pairs can do better than any such strategy, so therefore there is no classical explanation for the behavior of EPR pairs - assuming, of course, that the success probability of $\cos^2 \pi/8$ can be verified experimentally, which has indeed been done.

6. Different types of Oracles

Some definitions:

For any function $f : \{0, 1\}^n \rightarrow \{0, 1\}^m$, U_f is the standard quantum

operator computing f , i.e.,

$$U_f(|x\rangle|z\rangle) = |x\rangle|z \oplus f(x)\rangle.$$

If $m = 1$, the operator O_f is defined as

$$O_f(|x\rangle) = (-1)^{f(x)} |x\rangle.$$

We will use CU_f and CO_f to denote the controlled versions of these operators, i.e., these operations take as additional input a control q-bit c , such that

$$CU_f(|c\rangle|x\rangle|z\rangle) = |c\rangle|x\rangle|z \oplus f(x)\rangle \text{ if } c = 1 \text{ and } |c\rangle|x\rangle|z\rangle \text{ otherwise.}$$

Similarly, $CO_f(|c\rangle|x\rangle) = (-1)^{f(x)}|c\rangle|x\rangle$ if $c = 1$ and $|c\rangle|x\rangle$ otherwise.

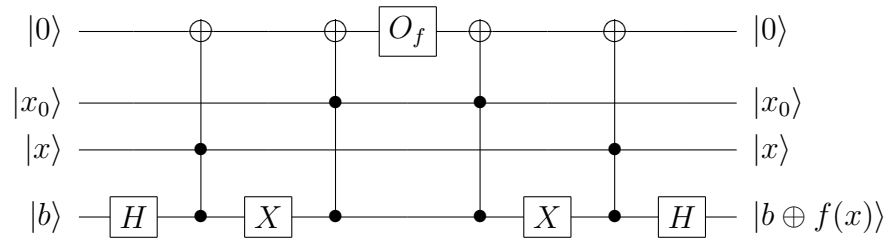
In this exercise, f will be a boolean function, $f : \{0, 1\}^n \rightarrow \{0, 1\}$. The textbook uses both the operators U_f and O_f , switching back and forth according to what is convenient. Part of the justification for this is that given access to U_f , O_f can be implemented by a single call to U_f , namely

$$U_f(|x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}}) = (-1)^{f(x)} |x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

where the last q-bit is returned to the same state, so it can be considered as an auxiliary variable and can be ignored, “seen from the outside”. This is a so-called black-box construction: the circuit and the auxiliary state we use to implement O_f are the same for any function f .

It is natural to ask if it is also easy to implement U_f , given access to O_f , and indeed this is necessary for some of the lower bounds in the book to be valid in general. To some extent, the answer is yes. The construction below is not a black-box construction, however. It requires that we know the value of $f(x_0)$ for some x_0 . For simplicity, we assume that in fact $f(x_0) = 0$.

Question 6.1 Argue that the circuit below on the given input state will produce an output state as specified and hence implements the U_f operator (for simplicity, the circuit is drawn as it looks when f takes only 1 input bit. In general, we would need $4n$ Toffoli gates instead of 4 – but still only one O_f).



The above result is good enough in practice: in a concrete application, it is perfectly reasonable to assume that we know at least one function value. It is no coincidence, however, that the construction is not black-box. In fact, there is no black-box construction implementing U_f based on O_f , as we shall see. Here is the first step:

Question 6.2 Show that there is no black-box construction implementing CO_f based on O_f , working for any function f . Hint: assume we had such a construction, which we can think of as a circuit that uses some number t of calls to O_f . Note that this circuit is the same, no matter what the function is. Consider what this construction would do if f is the constant function $f(x) = 1$ for all x . Consider separately the case where the control bit is 0 and where it is 1, and derive a contradiction by showing that t would have to be both even and odd.

The two next black-box constructions show that adding a control bit is easy if we start from U_f instead:

Question 6.3 Make a black-box construction using 2 calls to U_f and one Toffoli gate to implement CU_f .

Question 6.4 Make a black-box construction using 2 calls to CU_f and one Z gate to implement CO_f .

The last two questions imply that if we had a black-box construction implementing U_f based on O_f , we would have a black-box construction implementing CO_f based on O_f , but this contradicts question 6.2.

Exercise 7

Show that for any linear operator M , it holds that $M^\dagger M$ is a positive operator. First, argue that $M^\dagger M$ is Hermitian - and therefore has only real eigenvalues. Next, consider the number $\langle v | M^\dagger M | v \rangle$ where v is an eigenvector of $M^\dagger M$ with eigenvalue λ , and show that $\lambda \geq 0$.

Exercise 8

Consider the example of a measurement given as a POVM in N& C, that can distinguish between $|0\rangle$ and $|+\rangle$, and either gives guaranteed correct output or "I don't know".

The three operators defining the measurement are

$$E_0 = \frac{\sqrt{2}}{1 + \sqrt{2}} |-\rangle\langle -|, \quad E_+ = \frac{\sqrt{2}}{1 + \sqrt{2}} |1\rangle\langle 1|, \quad E_? = I - E_0 - E_+$$

You must show that operators of the measurement are positive. Remember that the eigenvalues λ of an operator A satisfies for eigenvector v : $Av = \lambda v$ which means that $(A - \lambda I)v = 0$, which has solutions iff $\text{Det}(A - \lambda I) = 0$. In our case it corresponds to a quadratic equation in λ that can be solved to find the eigenvalues of A. Knowing the eigenvalues of A is sufficient to assess its positivity.

Verify that the constant $c = \sqrt{2}/(1 + \sqrt{2})$ in front of operators E_+ and E_0 is as large as possible if we want $E_?$ to be positive. In other words, if $E_+ = c|1\rangle\langle 1|$ and $E_0 = c|-\rangle\langle -|$, for $c > \sqrt{2}/(1 + \sqrt{2})$ then $I - E_+ - E_0$ cannot be positive.

Exercise 9

Consider the following method for encrypting qubits: A and B share a key consisting of two random bits b_0, b_1 . To encrypt a qubit in state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, A will compute $X^{b_0} Z^{b_1} |\psi\rangle$ and send this state to B .

1. Describe how B can recover the state $|\psi\rangle$.
2. Compute the density matrix describing the state A sends as seen by an observer who does not know b_0, b_1 . Use your result to argue that the observer has no idea what $|\psi\rangle$ is.

3. Suppose you are guaranteed that the coordinates α, β of the input state are real. Show how the state can be encrypted with the same security using only a single shared and random bit.

Exercise 10

Find the operator-sum representation associated to the quantum operation applied to a single qubit q as follows: the environment applies a control-not gate to the qubit q together with another qubit initially in state $|0\rangle$ where q is the target and $|0\rangle$ is the control. Same question if the environment is initially in state $|+\rangle$ instead of $|0\rangle$.

Exercise 11

Show that the 2 quantum operations $\{X/\sqrt{2}, Z/\sqrt{2}\}$ and $\{H/\sqrt{2}, H'/\sqrt{2}\}$ are identical where H is the Hadamard transform and H' is the transform that maps $|0\rangle$ to $-|-\rangle$ and $|1\rangle$ to $|+\rangle$.

Exercise 12

Consider the bitflip code from N&C section 10.1.1. Assume we try to decode by simply performing a standard measurement in the computational basis on all three qubits. Show that this can work to reconstruct the original 1-qubit state if it was classical, i.e., it was $|0\rangle$ or $|1\rangle$. Give an example of a state where it would fail.

Exercise 13

Consider a codeword in the Shor code, i.e., the 9 qubits resulting from encoding some 1 qubit state. Divide the 9 qubits into 3 blocks of 3 consecutive qubits. Show that the Shor code can correct for three bit flips, if they occur in different blocks.

Exercise 14

Suppose you are told that a phaseflip occurred on one of the first three qubits in a Shor codeword. Show that this can be corrected for by applying Z to all three qubits.

Exercise 15

Show that any two different CSS codewords $|\xi_{x,z,v_k}\rangle, |\xi_{x',z',v_{k'}}\rangle$ are orthogonal (refer to Section 8 of the QMref note). Hint: argue that the pair (x, v_k) determines a coset of C_2 in the set of all n -bit vectors, and use this to argue that if $(x, v_k) \neq (x', v_{k'})$, the codewords are orthogonal because they are superpositions over disjoint sets of basis states. Then argue that $|\xi_{x,z,v_k}\rangle, |\xi_{x,z',v_k}\rangle$ are orthogonal by directly writing down an expression for the inner product $\langle \xi_{x,z,v_k} | \xi_{x,z',v_k} \rangle$. To argue that this expression is 0, you can use the result of Exercise 10.25 from N&C.

Exercise 16

Show the codewords states for the CSS codewords $|\xi_{x,z,v_k}\rangle$ satisfy

$$2^{-n/2} \sum_{j \in \{0,1\}^n} |j\rangle |j\rangle = 2^{-n/2} \sum_{v_k \in C_{1/2}, x \in C_{all/1}, z \in C_{all/2}^\perp} |\xi_{v_k,z,x}\rangle |\xi_{v_k,z,x}\rangle$$

Hint: you can make use of the following fact without proof: For any linear code C , any non-zero $u \in C$ and set $\{z_i\}$ of representatives for cosets of C^\perp , it holds that

$$\sum_i (-1)^{u \cdot z_i} = 0$$

Furthermore, do not be afraid of working with the horrible looking expression that results when you plug in the definition of $|\xi_{x,z,v_k}\rangle$, arranging the summation order correctly will help..