Quantum Information – Problem Set 1

Advanced Quantum Mechanics – KU Leuven
Lecturer: Aidan Chatwin-Davies (aidan.chatwindavies@kuleuven.be)

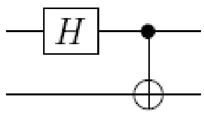
18 November 2020

Problem 1: Quantum gate warm-up

a) Recall that the *computational basis* is the basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ and the *Bell basis* is the basis consisting of the maximally entangled states

$$
\begin{aligned}
|\Phi_\pm\rangle &= \frac{1}{\sqrt{2}}\left(|00\rangle \pm |11\rangle\right) \\
|\Psi_\pm\rangle &= \frac{1}{\sqrt{2}}\left(|01\rangle \pm |10\rangle\right).
\end{aligned}
$$

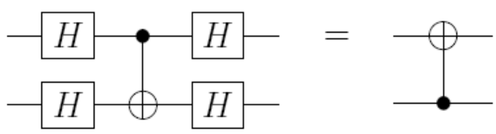
Show that the following circuit maps the computational basis onto the Bell basis:

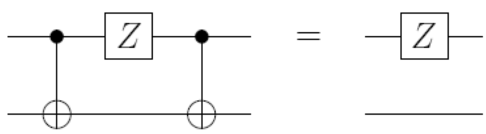


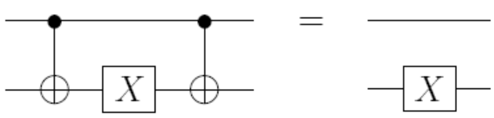
Recall that the matrix representation of the Hadamard gate, H, in the computational basis is given by

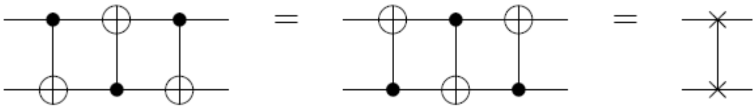
$$
H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.
$$

b) Demonstrate the following equalities:









(The very last gate denotes the SWAP gate, i.e. $\mathrm{SWAP}|x\rangle|y\rangle = |y\rangle|x\rangle$.)

Problem 2: Grover Search

Some quantum algorithms, like the quantum factoring algorithm and the quantum solution to Simon's problem, are so dramatic because they constitute an exponential speed-up over the best known classical algorithm. Grover Search, on the other hand, does not offer an exponential speed-up, but it is striking in its extremely broad generality.

Grover Search is an algorithm that implements an unstructured database search: Given a database that contains N entries (with no duplicates), find a particular marked entry, ω. In other words, we assume that we are given an oracle that computes a function, f_ω, such that

$$f_\omega(x) = \begin{cases} 0 & x \neq \omega \\ 1 & x = \omega \end{cases} . \tag{1}$$

Moreover, assume that querying f_ω incurs no computational cost (it's "easy" to evaluate f_ω). Not knowing which entry is the marked entry ω, our task is to determine this by querying f_ω.

For example, think back to the days when telephone books were still relevant. It is easy to look up someone's phone number if you know their name, because the database of (name, number) pairs is sorted in alphabetical order—it's a structured database. However, it's a tricky task to find the *name* corresponding to a certain number. In this example, the marked entry is a particular name ω, and you "implement" the function f_ω by taking a name, looking up the corresponding phone number (an easy task given the phone book), and comparing it to the given phone number.

a) Classically, what is an optimal strategy for finding ω in an unstructured database with N unique entries by querying f_ω? What is the smallest number of times you must query f_ω before the probability of having found ω exceeds $1/2$?

b) For convenience, suppose that the database entries are n-bit strings and that there are $N = 2^n$ entries (i.e. each unique n-bit string appears in the database exactly once). Now suppose we are given a quantum oracle; that is, a unitary U_{f_ω} that acts on $n+1$ qubits as

$$U_{f_\omega}|x\rangle|y\rangle = |x\rangle|y \oplus f_\omega(x)\rangle. \tag{2}$$

($x \equiv x_1 x_2 \cdots x_n$ denotes a n-bit string and y is a single bit.) Recall from the lectures that $U_{f_\omega}|x\rangle|-\rangle = (-1)^{f_\omega(x)}|x\rangle|-\rangle$. Therefore, if we always prepare the last qubit in the state $|-\rangle$ and then discard it, we are really just implementing the unitary operation

$$U_\omega : |x\rangle \mapsto (-1)^{f_\omega(x)}|x\rangle. \tag{3}$$

We can therefore compactly write

$$U_\omega = I - 2|\omega\rangle\langle\omega|. \tag{4}$$

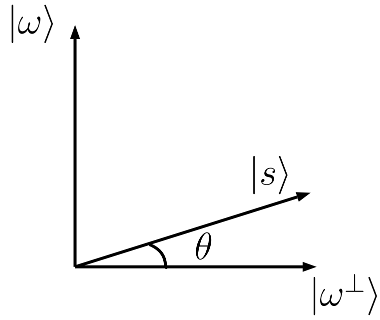
Convince yourself that this is true.

c) Let

$$|s\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle. \tag{5}$$

What is the value of $\langle\omega|s\rangle$?

d) Define the unitary operator $U_s = 2|s\rangle\langle s| - I$, as well as an operator $R = U_s U_\omega$ called the *Grover iteration*. What is the action of R on $|s\rangle$ in the plane spanned by $|\omega\rangle$ and $|s\rangle$? (*Hint:* It is helpful to denote $\langle\omega|s\rangle \equiv \sin\theta$.)



e) What is the action of R^k on $|s\rangle$ $(k \in \mathbb{Z}, k > 0)$?

f) After applying R to $|s\rangle$ k times, we measure the resulting state. What value should we choose for k so that, with high probability, the outcome of the measurement is $|\omega\rangle$? How does this scale with N? Compare your answer here to the answer from part a). (*Hint:* For N large, $\sin\theta \approx \theta$.)

Extra Problem: Distance measures

Adapted from Exercise 2.7 of J. Preskill, Lecture Notes for Ph219/CS219: Quantum Information and Computation, *Chapter 2 (2013 edition).*

In many cases, we would like to be able to meaningfully quantify how "close" two quantum states are to each other. For example, if we are trying to correct errors made during a quantum computation, we would like to quantify how close the post-recovery state is to the original state. In this problem, we will see why the 1-norm is a good measure of closeness.

Consider two quantum states described by density operators ρ and $\tilde{\rho}$ in a N-dimensional Hilbert space, and consider the complete orthogonal measurement $\{E_a : a = 1, 2, \ldots, N\}$, where the E_a's are one-dimensional projectors satisfying

$$\sum_{a=1}^{N} E_a = I. \tag{6}$$

When the measurement is performed, outcome a occurs with probability $p_a = \operatorname{Tr} \rho E_a$ if the state is ρ and with probability $\tilde{p}_a = \operatorname{Tr} \tilde{\rho} E_a$ if the state is $\tilde{\rho}$.

The (normalized) L^1 distance between the two probability distributions is defined as

$$d(p, \tilde{p}) \equiv \|p - \tilde{p}\|_1 \equiv \frac{1}{2} \sum_{a=1}^{N} |p_a - \tilde{p}_a|. \tag{7}$$

This distance is zero if the two distributions are identical, and attains its maximum value of one if the two distributions have support on disjoint sets.

a) Show that

$$d(p,\tilde{p}) \leq \frac{1}{2}\sum_{i=1}^{N}|\lambda_i|, \tag{8}$$

where the λ_i's are the eigenvalues of the Hermitian operator $\rho - \tilde{\rho}$. *Hint:* Working in the basis in which $\rho - \tilde{\rho}$ is diagonal, find an expression for $|p_a - \tilde{p}_a|$, and then find an upper bound on $|p_a - \tilde{p}_a|$. Finally, use the completeness property Eq. (6) to bound $d(p,\tilde{p})$.

b) Find a choice for the orthogonal projectors $\{E_a\}$ that saturates the upper bound Eq. (8).

Define a distance $d(\rho,\tilde{\rho})$ between density operators as the maximal L^1 distance between the corresponding probability distributions that can be achieved by any orthogonal measurement. From the results of (a) and (b), we have found that

$$d(\rho,\tilde{\rho}) = \frac{1}{2}\sum_{i=1}^{N}|\lambda_i|. \tag{9}$$

c) The trace norm, or Schatten 1-norm $\|A\|_1$ of an operator A is defined as

$$\|A\|_1 \equiv \mathrm{Tr}\left[(A^\dagger A)^{1/2}\right]. \tag{10}$$

How can the distance $d(\rho,\tilde{\rho})$ be expressed as the 1-norm of an operator?

Now suppose that the states ρ and $\tilde{\rho}$ are pure states $\rho = |\psi\rangle\langle\psi|$ and $\tilde{\rho} = |\tilde{\psi}\rangle\langle\tilde{\psi}|$. If we adopt a suitable basis in the space spanned by the two vectors, and appropriate phase conventions, then these vectors can be expressed as

$$|\psi\rangle = \begin{pmatrix} \cos\theta/2 \\ \sin\theta/2 \end{pmatrix} \qquad |\tilde{\psi}\rangle = \begin{pmatrix} \sin\theta/2 \\ \cos\theta/2 \end{pmatrix}. \tag{11}$$

d) Express the distance $d(\rho,\tilde{\rho})$ in terms of the angle θ.

e) Express $\||\psi\rangle - |\tilde{\psi}\rangle\|^2$ (where $\|\cdot\|$ denotes the Hilbert space norm, i.e., the 2-norm $\||\psi\rangle\| = \sqrt{\langle\psi|\psi\rangle}$) in terms of θ, and by comparing with the results of (d), derive the bound

$$d(|\psi\rangle\langle\psi|, |\tilde{\psi}\rangle\langle\tilde{\psi}|) \leq \||\psi\rangle - |\tilde{\psi}\rangle\|. \tag{12}$$

f) Why is $\||\psi\rangle - |\tilde{\psi}\rangle\|$ *not* a good measure of the distinguishability of the pure quantum states ρ and $\tilde{\rho}$? *Hint:* Remember that quantum states are *rays*.