

# 1 Quantum bits

🔗 PRESKILL: *chapter 2.1 and 2.2*

A wave function  $|\Psi\rangle$  in a two-dimensional Hilbert space (with basis vectors  $|0\rangle$  and  $|1\rangle$ ) has the general form

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle.$$

The coefficients  $\alpha$  and  $\beta$  are two arbitrary complex numbers.

a) To specify  $\alpha$  and  $\beta$  one needs 4 real numbers. Argue that 2 of those 4 numbers are superfluous for the specification of a physical state.

b) Show that, without loss of generality, one can write the state  $|\Psi\rangle$  in the form

$$|\Psi\rangle = \cos(\theta/2)|0\rangle + e^{i\phi}\sin(\theta/2)|1\rangle,$$

with real  $\theta$  and  $\phi$ . These are the spherical coordinates of a point on the unit sphere, called the *Bloch sphere*.

For an electron spin we can interpret the basis vectors  $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$  and  $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$  as, respectively, spin up  $|\uparrow\rangle$  or down  $|\downarrow\rangle$  along the  $z$ -axis.

c) Where do these two states lie on the Bloch sphere?

More generally the spin is oriented along the  $x$ ,  $y$ , or  $z$ -axis if it is an eigenfunction of the Pauli matrix

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

For later use we also define the unit matrix

$$\sigma_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

d) Where on the Bloch sphere lies a spin oriented along the  $x$  or  $y$ -axis?

A spin state that points in the direction of the unit vector  $\mathbf{n} = (n_x, n_y, n_z)$  is an eigenfunction with eigenvalue  $+1$  of

$$\mathbf{n} \cdot \boldsymbol{\sigma} \equiv n_x \sigma_x + n_y \sigma_y + n_z \sigma_z.$$

e) Derive that  $\mathbf{n}$  indicates the point on the Bloch sphere corresponding to that spin state.

f) A single qubit (spin-1/2) is in an unknown *pure* state  $|\psi\rangle$ , selected at random from an ensemble uniformly distributed over the Bloch sphere. We guess at random that the state is  $|\phi\rangle$ . On the average, what is the *fidelity*  $F \equiv |\langle\phi|\psi\rangle|^2$  of our guess?

## 2 Quantum gates

🔗 PRESKILL: *chapter 6.2*

The elementary operation (gate) of a quantum computer acts on a single qubit. It is a linear operation, which can be represented by a matrix multiplication,

$$|\Psi\rangle_{\text{out}} = U|\Psi\rangle_{\text{in}} \Leftrightarrow \begin{pmatrix} \alpha^{\text{out}} \\ \beta^{\text{out}} \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \alpha^{\text{in}} \\ \beta^{\text{in}} \end{pmatrix}.$$

a) Show that normalization of initial state  $|\Psi_{\text{in}}\rangle$  and final state  $|\Psi_{\text{out}}\rangle$  requires that  $U$  is a unitary matrix,

$$UU^\dagger = U^\dagger U = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

b) Are the Pauli matrices allowed as quantum gates? Explain what each Pauli matrix does to a point on the Bloch sphere.

c) Are these three gates independent, or can you construct one out of the other two?

The Hadamard gate has the form

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

d) What does this gate do to a point on the Bloch sphere?

e) Show that the combination of  $H$  and a single Pauli matrix (e.g.  $\sigma_x$ ) can be used to construct the other two Pauli matrices.

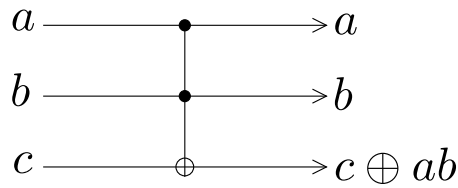
The most general gate rotates a point on the Bloch sphere by an angle  $\theta$  along the unit vector  $\mathbf{n}$ .

f) Demonstrate that this gate is given by

$$R_{\mathbf{n}}(\theta) = e^{-i(\theta/2)\mathbf{n}\cdot\boldsymbol{\sigma}} = \cos(\theta/2)\sigma_0 - i\sin(\theta/2)\mathbf{n}\cdot\boldsymbol{\sigma}.$$

An arbitrary quantum mechanical operation on  $n$  qubits is a  $2^n \times 2^n$  unitary matrix  $U$ . The elementary operations (gates) of a quantum circuit act only on 1 or 2 qubits. These are building blocks for gates that act on more than 2 qubits.

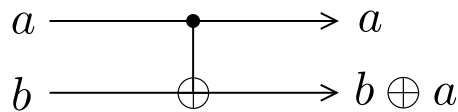
Example: The Toffoli gate is a 3-qubit gate that flips the third qubit  $c$  ( $0 \leftrightarrow 1$ ), if and only if the first two qubits  $a, b$  are both 1. The notation is



The encircled + means addition modulo 2.

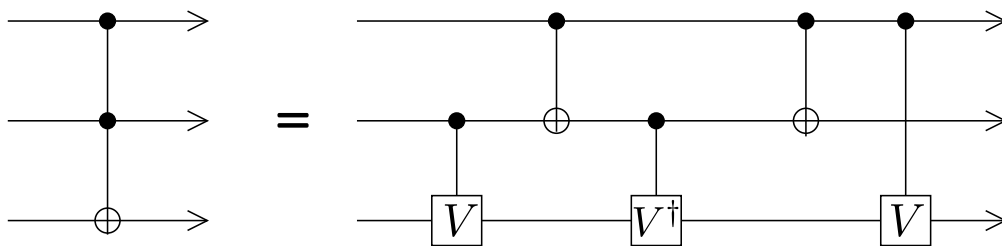
g) Explain that this diagram does what it should do.

Note that the CNOT gate can be represented in the same way by



In a classical computer it is not possible to construct the Toffoli gate out of gates that act only on 1 or 2 qubits. (At least not if the gates should be reversible.) In a quantum computer that is possible.

h) Show that



where  $V = \frac{1}{2} \begin{pmatrix} 1-i & 1+i \\ 1+i & 1-i \end{pmatrix}$ ,  $V^\dagger = \frac{1}{2} \begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix}$ , so that  $V^2 = \sigma_x$ .

### 3 Density matrix

PRESKILL: *chapter 2.3*

The expectation value of an operator  $M$  in the state  $|\Psi\rangle$  is  $\langle M \rangle = \langle \Psi | M | \Psi \rangle$ . We can write this as the trace of the product of the operator  $M$  and an operator  $\rho$ ,

$$\langle M \rangle = \text{tr } M\rho, \quad \rho = |\Psi\rangle\langle\Psi|.$$

The operator  $\rho$  is the density matrix corresponding to the state  $|\Psi\rangle$ .

a) Derive that  $\text{tr } \rho = 1$ ,  $\rho = \rho^\dagger$ ,  $\rho^2 = \rho$ . What are the eigenvalues of  $\rho$ ?

More generally, a system can consist of a mixture of states. If the state  $|\Psi_n\rangle$  occurs with probability  $p_n$ , then the density matrix is

$$\rho = \sum_n p_n |\Psi_n\rangle \langle \Psi_n|.$$

b) What is now the expectation value of  $M$ ?

c) Derive that it still holds that  $\text{tr } \rho = 1$ ,  $\rho = \rho^\dagger$ . However, unlike for a pure (not mixed) state, it no longer holds that  $\rho^2 = \rho$ .

d) Derive that  $\langle \Psi | \rho | \Psi \rangle \geq 0$  for each  $|\Psi\rangle$ . What restriction does this inequality impose on the eigenvalues of  $\rho$ ?

e) For a single qubit  $\rho$  is a  $2 \times 2$  matrix. Derive that  $\rho$  can be written in terms of the Pauli matrices in the form

$$\rho = \frac{1}{2} (\sigma_0 + \mathbf{a} \cdot \boldsymbol{\sigma}),$$

with a vector of real coefficients  $\mathbf{a} = (a_x, a_y, a_z)$ . Why is  $|\mathbf{a}| \leq 1$ ? What operation on  $\mathbf{a}$  corresponds to complex conjugation of  $\rho$ ? And what operation on  $\mathbf{a}$  corresponds to a unitary transformation of  $\rho$ ?

f) The vectors  $\mathbf{a}$  which satisfy  $|\mathbf{a}| \leq 1$  form a sphere, the Bloch sphere (or Bloch ball). Where on the Bloch sphere lies the density matrix  $\rho = |\Psi\rangle \langle \Psi|$  of a pure state? Derive this formula for the overlap of two pure states:  $|\langle \Psi_1 | \Psi_2 \rangle|^2 = \frac{1}{2} (1 + \mathbf{a}_1 \cdot \mathbf{a}_2)$ .

g) Derive that the expectation value of the spin operator  $\mathbf{n} \cdot \boldsymbol{\sigma}$  along the direction  $\mathbf{n}$  is given by the inner product  $\mathbf{a} \cdot \mathbf{n}$ . Explain how you can use this property to measure the density matrix. Why is this not possible if you have only a single system at your disposal?

h) After randomly selecting a one-qubit pure state as in problem 1.f, we perform a measurement of the spin along the  $z$ -axis. This measurement prepares a state described by the density matrix

$$\rho = \langle \psi | P_\uparrow | \psi \rangle P_\uparrow + \langle \psi | P_\downarrow | \psi \rangle P_\downarrow.$$

Here  $P_{\uparrow\downarrow}$  is the projector onto the spin-up or spin-down states along the  $z$ -axis. On the average, with what fidelity  $F \equiv \langle \psi | \rho | \psi \rangle$  does this density matrix represent the initial state  $\psi$ ? (The improvement in  $F$  compared to the answer to problem 1.g is a crude measure of how much we learned by making the measurement.)

## 4 Entanglement

🔗 PRESKILL: *chapter 2.4*

The state  $|\Psi\rangle$  of two qubits  $A$  and  $B$  can be constructed out of the building blocks  $|0\rangle_A, |1\rangle_A, |0\rangle_B, |1\rangle_B$  of the individual qubits,

$$|\Psi\rangle = c_{00}|0\rangle_A|0\rangle_B + c_{01}|0\rangle_A|1\rangle_B + c_{10}|1\rangle_A|0\rangle_B + c_{11}|1\rangle_A|1\rangle_B.$$

a) Show that the condition of normalisation can be written as  $\text{tr}cc^\dagger = 1$ , with  $c$  the  $2 \times 2$  matrix with coefficients  $c_{ij}$ .

b) Why is it always possible to choose a new basis  $|\cdot\rangle'_A, |\cdot\rangle'_B$  such that

$$|\Psi\rangle = c'_{00}|0\rangle'_A|0\rangle'_B + c'_{11}|1\rangle'_A|1\rangle'_B,$$

with real positive  $c'_{00}, c'_{11}$ . (This is called the Schmidt decomposition.)

If I only do measurements on qubit  $A$ , then it suffices to know the reduced density matrix

$$\rho_A = \text{tr}_B|\Psi\rangle\langle\Psi|.$$

c) Derive that

$$(\rho_A)_{ij} = \sum_k c_{ik}c_{jk}^*, \text{ hence } \rho_A = cc^\dagger.$$

The qubits  $A$  and  $B$  are called “entangled” if  $\rho_A$  describes a mixed (not pure) state.

d) Show that  $\det\rho_A \neq 0$  ( $\det = \text{determinant}$ ) is a necessary and sufficient condition for entanglement.

e) Why is it equivalent to determine the entanglement from  $\rho_A$  or from  $\rho_B = \text{tr}_A|\Psi\rangle\langle\Psi|$ ?

A widely used measure of entanglement is the *concurrence*

$$\mathcal{C} = 2\sqrt{\det\rho_A}.$$

f) Derive that  $0 \leq \mathcal{C} \leq 1$ .

g) Consider the two-qubit state

$$|\Phi\rangle = \frac{1}{\sqrt{2}}|\uparrow\rangle_A\left(\frac{1}{2}|\uparrow\rangle_B + \frac{1}{2}\sqrt{3}|\downarrow\rangle_B\right) + \frac{1}{\sqrt{2}}|\downarrow\rangle_A\left(\frac{1}{2}|\downarrow\rangle_B + \frac{1}{2}\sqrt{3}|\uparrow\rangle_B\right).$$

Compute the partial density matrices  $\rho_A = \text{Tr}_B|\Phi\rangle\langle\Phi|$  and  $\rho_B = \text{Tr}_A|\Phi\rangle\langle\Phi|$ . Find the Schmidt decomposition of  $|\Phi\rangle$ .

## 5 Teleportation

🔗 PRESKILL: *chapter 4*

The basis  $|00\rangle, |01\rangle, |10\rangle, |11\rangle$  of two qubits from problem 4 is not entangled. Sometimes it is more convenient to use another basis,

$$|\beta_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}, \quad |\beta_{01}\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}, \quad |\beta_{10}\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}, \quad |\beta_{11}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}},$$

which *is* entangled. This basis is called the Bell basis.

a) Show that each of the four Bell states is maximally entangled (has concurrence = 1).

You can produce these states starting from a non-entangled basis, by using two gates: The Hadamard gate and the CNOT gate. The Hadamard gate rotates the first qubit,  $|x\rangle \rightarrow 2^{-1/2}(|0\rangle + (-1)^x|1\rangle)$ . The CNOT gate (controlled NOT) exchanges  $0 \leftrightarrow 1$  at the second qubit, but only if the first qubit is 1.

b) Show that  $|ij\rangle \rightarrow |\beta_{ij}\rangle$ .

Suppose that Alice and Bob have met to produce the state  $|\beta_{00}\rangle$  and then have separated, each taking 1 qubit. Alice wants to use this entangled pair to transmit to Bob the unknown state  $\alpha|0\rangle + \beta|1\rangle$  of a second qubit in her possession.

c) Why can't Alice just measure  $\alpha$  and  $\beta$  and send the result to Bob?

The state of the 3 qubits (2 with Alice, 1 with Bob) reads

$$|\Psi\rangle = 2^{-1/2} [\alpha(|00\rangle + |11\rangle)|0\rangle + \beta(|00\rangle + |11\rangle)|1\rangle].$$

Alice sends both her qubits through a CNOT gate, with the unknown qubit as the control, and then sends her unknown qubit through a Hadamard gate. She finally measures both her qubits.

d) Specify for each of the four outcomes 00, 01, 10, 11 of the measurement of Alice, what is the resulting state of Bob's qubit.

Alice communicates to Bob the result of her measurement.

e) Indicate how Bob can use that knowledge to bring his qubit in the state  $\alpha|0\rangle + \beta|1\rangle$  (without actually knowing that state!). This completes the "teleportation".

To communicate the result of her measurement to Bob, Alice must send a message. This takes time and ensures that teleportation does not exceed the speed of light. Suppose that

Bob tries to extract some information from his qubit *after* Alice's measurement but *before* her message has arrived.

f) Calculate the reduced density matrix of Bob,  $\rho_B = \text{tr}_A \rho$ , and show that  $\rho_B$  contains no information at all about the unknown qubit  $\alpha|0\rangle + \beta|1\rangle$ .

Alice must destroy her qubit to transmit its state to Bob. This is an example of the general "no-cloning theorem".

g) Show that it is not possible to construct a gate that can clone an arbitrary unknown qubit  $|\Psi\rangle$ , that is to say

$$|\Psi\rangle|0\rangle \rightarrow |\Psi\rangle|\Psi\rangle$$

is not possible.

## 6 Bell inequality

In problem 4 we encountered the concurrence  $\mathcal{C}$  as a measure of the degree of entanglement of two qubits  $A, B$  in the pure state

$$|\Psi\rangle = \sum_{ij} c_{ij} |i\rangle_A |j\rangle_B, \quad \mathcal{C} = 2|\det c|.$$

If you dispose of a large number of pairs  $A, B$  in the same state, then you can measure the concurrence from the mean correlation of spin  $A$  and spin  $B$ . The Bell inequality is a way to distinguish classical from quantum mechanical correlations.

The recipe is as follows: Choose two unit vectors  $\mathbf{a}, \mathbf{a}'$  along which to measure spin  $A$ , and two more  $\mathbf{b}, \mathbf{b}'$  for spin  $B$ . Measure for each combination of vectors the spin correlator

$$C_{nm} = \langle \Psi | (\mathbf{n} \cdot \boldsymbol{\sigma}_A) (\mathbf{m} \cdot \boldsymbol{\sigma}_B) | \Psi \rangle,$$

where  $\boldsymbol{\sigma}_A$  acts on spin  $A$  and  $\boldsymbol{\sigma}_B$  on spin  $B$ . Combine the results to obtain the Bell parameter

$$\mathcal{B} = C_{ab} + C_{a'b} + C_{ab'} - C_{a'b'}.$$

Maximize  $\mathcal{B}$  by varying  $\mathbf{a}, \mathbf{b}, \mathbf{a}', \mathbf{b}'$ . The maximum  $\mathcal{B}_{\max}$  gives the concurrence via

$$\mathcal{B}_{\max} = 2\sqrt{1 + \mathcal{C}^2}.$$

Let us prove this.

a) Why can you restrict yourself, without loss of generality, to states of the form  $|\Psi\rangle = \alpha|00\rangle + \beta|11\rangle$  (with real  $\alpha$  and  $\beta$ )?

Denote the length of  $\mathbf{a} + \mathbf{a}'$  as  $2\cos\theta$  with  $0 \leq \theta \leq \pi/2$ . Define two new vectors  $\mathbf{c}, \mathbf{c}'$  by

$$\mathbf{a} + \mathbf{a}' = 2\mathbf{c}\cos\theta, \quad \mathbf{a} - \mathbf{a}' = 2\mathbf{c}'\sin\theta.$$

b) Explain why  $\mathbf{c}$  and  $\mathbf{c}'$  have length 1 and why they are orthogonal.

Now you may immediately maximize

$$\mathcal{B} = 2\cos\theta \langle\Psi|(\mathbf{c}\cdot\boldsymbol{\sigma}_A)(\mathbf{b}\cdot\boldsymbol{\sigma}_B)|\Psi\rangle + 2\sin\theta \langle\Psi|(\mathbf{c}'\cdot\boldsymbol{\sigma}_A)(\mathbf{b}'\cdot\boldsymbol{\sigma}_B)|\Psi\rangle$$

over  $\theta$ .

c) Derive that

$$\max_{\theta} \mathcal{B} = 2 \left[ \langle\Psi|(\mathbf{c}\cdot\boldsymbol{\sigma}_A)(\mathbf{b}\cdot\boldsymbol{\sigma}_B)|\Psi\rangle^2 + \langle\Psi|(\mathbf{c}'\cdot\boldsymbol{\sigma}_A)(\mathbf{b}'\cdot\boldsymbol{\sigma}_B)|\Psi\rangle^2 \right]^{1/2}.$$

In what follows we will take coplanar vectors, say all in the  $x$ - $z$  plane:  $\mathbf{b} = (\sin\phi, 0, \cos\phi)$ ,  $\mathbf{b}' = (\sin\phi', 0, \cos\phi')$ ,  $\mathbf{c} = (\sin\gamma, 0, \cos\gamma)$ ,  $\mathbf{c}' = (-\cos\gamma, 0, \sin\gamma)$ . (We will skip the proof that the coplanar arrangement maximizes  $\mathcal{B}$ .)

d) Maximize over  $\phi, \phi', \gamma$  (in that order) to reach the desired result,

$$\mathcal{B}_{\max} = 2\sqrt{1 + 4(\alpha\beta)^2}.$$

A non-entangled state has  $\mathcal{B}_{\max} = 2$ . The Bell inequality

$$\mathcal{B} \leq 2$$

holds for all classical correlations. John Bell constructed this inequality as a way to demonstrate experimentally that quantum mechanical correlations can not be described in classical terms.

The argument goes as follows. In a classical description the Bell parameter can be found by measuring the spin polarisation  $P_n$  along the axes  $\mathbf{n} = \mathbf{a}, \mathbf{a}', \mathbf{b}, \mathbf{b}'$ . The measurement of spin  $A$  is assumed to leave spin  $B$  undisturbed (locality), so we can consider each measurement separately. The spin polarisation  $P_n$  is  $+1$  if the spin is  $\uparrow$  along  $\mathbf{n}$  and  $-1$  if it is  $\downarrow$ .

e) Show that

$$P_a P_b + P_{a'} P_b + P_a P_{b'} - P_{a'} P_{b'} = \pm 2.$$

f) Explain why  $\mathcal{B} \leq 2$ .



## 7 Quantum key distribution

📖 PRESKILL: *chapter 4.2* or *chapter 4.5* in the update.

Securely encoded communications between two parties (“Alice” and “Bob”) are possible if they have previously exchanged a private key, a random string of bits used to encrypt a message. (The encryption could be as simple as adding each bit in the key to each bit in the message.) Quantum key distribution provides for a method to ensure that this key cannot be intercepted and read without being noticed during the exchange. The security is fundamentally a consequence of the no-cloning theorem, so it is ensured by the laws of physics.

If Alice and Bob share entangled qubits, all they have to do is to measure their qubits to create a shared private key without having to exchange any qubits.

a) Explain how this would work. Why can’t they use this method to directly transmit the information itself?

The following approach can be used if sharing entangled qubits is impractical. To create the random bit string for the private key, Alice randomly prepares qubits in the states  $|0\rangle$  or  $|1\rangle$ . She then sends these qubits to Bob, but before doing so she randomly selects half of the qubits and acts on these with a Hadamard gate. She only tells Bob which qubits went through the Hadamard gate after he has received them.

b) How does Bob recover the random bit string originally prepared by Alice? Why can he only do that after he has learned which qubits Alice had sent through the Hadamard gate?

c) An eavesdropper (“Eve”) has intercepted the message in which Alice tells Bob which qubits she sent through the Hadamard gate. Suppose that Eve is also able to intercept the qubits on their way from Alice to Bob. Explain why she cannot use this knowledge to find the private key without Alice and Bob noticing the intrusion.

A mathematical argument for the security of this quantum key distribution goes as follows. Suppose Eve intercepts the qubits from Alice, in one of the four states  $|\phi_1\rangle = |0\rangle$ ,  $|\phi_2\rangle = |1\rangle$ ,  $|\phi_3\rangle = H|0\rangle$ ,  $|\phi_4\rangle = H|1\rangle$ , and operates on them in a quantum computer in some state  $\Phi_0$ . The operation should be such that the qubits from Alice are not affected, so that she can send them onward to Bob without anyone noticing. This operation has the general form

$$U(|\phi_\mu\rangle|\Phi_0\rangle) = |\phi_\mu\rangle|\Phi_\mu\rangle$$

for some unitary operator  $U$ . By measuring the final state  $\Phi_\mu$  of the quantum computer Eve hopes to learn something about the state  $\phi_\mu$  of the qubit she intercepted.

d) Show that, because unitary operations preserve inner products,  $\Phi_1 = \Phi_2 = \Phi_3 = \Phi_4$ , so Eve learns nothing.

## 8 Quantum algorithms

🔗 PRESKILL: *chapter 6.3*

Suppose you have a “black box” (an “oracle” in computer jargon) that evaluates a function  $f(x)$ . The integer  $x$  varies from 0 to  $2^N - 1$ . For each  $x$  the number  $f(x)$  is either 0 or 1. You do not know which  $f$  has been programmed in the black box, but you do know that  $f$  belongs to one of these two classes:

- class C:  $f$  is constant, taking on the same value for each  $x$ .
- class B:  $f$  is balanced, taking on the values 0 and 1 equally often.

a) If the black box is a classical computer, how often should it be consulted to determine with certainty the class of  $f$ ?

Deutsch and Jozsa have discovered that for a quantum computer one single consultation suffices. We examine in this problem a slight variation of the Deutsch-Jozsa algorithm, that needs  $N$  instead of  $N + 1$  qubits.

Initially all  $N$  qubits are in the state  $|0\rangle$ . Act with a Hadamard gate on each qubit.

b) Explain why the resulting state can be written as

$$(H|0\rangle)^N = 2^{-N/2} \sum_{x=0}^{2^N-1} |x\rangle.$$

Because the black box is quantum mechanical, you are not allowed to describe its operation by

$$\sum_x |x\rangle \rightarrow \sum_x |f(x)\rangle.$$

c) Why not?

Instead we describe its operation by

$$\sum_x |x\rangle \rightarrow \sum_x (-1)^{f(x)} |x\rangle.$$

d) Why is this allowed?

On each of the  $N$  qubits that comes out of the black box we act again with a Hadamard gate. Finally we measure them.

e) Show that they are all 0 if  $f$  is of class C.

f) Show that at least one qubit is 1 if  $f$  is of class B.

The Deutsch-Jozsa algorithm is a curiosity. It does not solve any “useful” problem. The Simon algorithm goes further. The unknown function  $f : x \rightarrow y$ , with  $x, y \in 0, 1, 2, \dots, 2^N - 1$  is periodic and you wish to find the period  $a$ . This algorithm is at the basis of Shor’s code breaker.

More precisely, for any pair  $x \neq x'$  it is given that  $f(x) = f(x')$  if and only if  $x' = x \oplus a$ , with  $1 \leq a \leq 2^{N-1}$ . The symbol  $\oplus$  indicates that you write  $x$  and  $a$  in binary notation and then add bits modulo 2. For example  $01011 \oplus 11001 = 10010$ .

g) Show that  $x \oplus a \oplus a = x$ .

In addition to the  $N$  qubits we need a second set of  $N$  qubits (called ancilla’s = helper or servant, in the jargon). Initially all  $2N$  qubits are 0, then the first  $N$  qubits are each sent through a Hadamard gate and subsequently they are acted upon with the following operation:

$$\sum_x |x\rangle|0\rangle \rightarrow \sum_x |x\rangle|f(x)\rangle.$$

Measure the  $N$  ancilla’s.

h) Suppose you measure  $f(x_0)$ . In which superposition of states are the first  $N$  qubits?

Send the first  $N$  qubits through a Hadamard gate and measure them.

i) Explain that the result  $x_1$  of that measurement is orthogonal to  $a$ , meaning that  $x_1 \odot a = 0$ , with  $\odot$  the bitwise multiplication.

By repeating the whole algorithm some  $N$  times you obtain  $N$  independent equations from which you can solve for  $a$ .

A more general search algorithm was discovered by Grover. The function  $f(x)$  of the oracle now returns  $x$  if  $x \neq a$  but it returns  $-x$  if  $x = a$ . The corresponding unitary is

$$U = 1 - 2|a\rangle\langle a| \text{ with } a \in \{0, 1, 2, \dots, 2^N - 1\}.$$

Classically, you would have to query the oracle an order  $\mathcal{N} = 2^N$  times before you would with high probability find the value  $a$  you are looking for, but on a quantum computer you can reduce this to order  $\sqrt{\mathcal{N}}$ . The first step is again to send the  $N$  qubits through a Hadamard gate and thus prepare the state  $|s\rangle = \mathcal{N}^{-1/2} \sum_{x=0}^{\mathcal{N}-1} |x\rangle$ . Then we query the oracle and subsequently apply the unitary  $V = 2|s\rangle\langle s| - 1$ . Iterate  $T$  times to obtain the final state


$$|\psi_T\rangle = (VU)^T |s\rangle.$$

Finally measure  $|\psi_T\rangle$ .

j) Explain why the iteration  $|\psi_{n+1}\rangle = VU|\psi_n\rangle$  rotates the state over an angle  $\theta \approx 2\mathcal{N}^{-1/2}$  in the plane spanned by the two vectors  $|s\rangle$  and  $|a\rangle$ . *Hint: it is easiest to first consider the effect of  $VU$  when it acts on a vector  $|a_\perp\rangle$  in the  $s$ - $a$  plane that is perpendicular to  $a$ .*

k) Explain that after  $T \approx \frac{1}{4}\pi\sqrt{\mathcal{N}}$  steps the measurement of  $|\psi_T\rangle$  will result in the desired value  $a$  with high probability.

## 9 Quantum error correction

 PRESKILL: chapter 7.1–7.4

We wish to protect a single qubit against the occurrence of a single error. The error could be a bit flip ( $\sigma_x$ ), a phase shift ( $\sigma_z$ ), or the combination of a bit flip and a phase shift ( $\sigma_y = i\sigma_x\sigma_z$ ).

Let us first restrict the error to a bit flip. A classical bit can be protected against a single bit flip by encoding it in three bits. The code is a simple repetition,

$$0 \rightarrow 000, 1 \rightarrow 111.$$

a) Explain how parity checking allows you to correct for a flip of one of the three bits.

Similarly, a quantum bit can be protected against a  $\sigma_x$  error by encoding it in three qubits,

$$|0\rangle \rightarrow |0\rangle|0\rangle|0\rangle, |1\rangle \rightarrow |1\rangle|1\rangle|1\rangle.$$

b) Construct a circuit that encodes the state  $\alpha|0\rangle + \beta|1\rangle$  as  $\alpha|0\rangle|0\rangle|0\rangle + \beta|1\rangle|1\rangle|1\rangle$ .

c) Suppose we know that at most one of the three qubits in the encoded state has flipped. Explain how a measurement of the two observables  $S_1 = \sigma_z \otimes \sigma_z \otimes 1$  and  $S_2 = 1 \otimes \sigma_z \otimes \sigma_z$  allows you to determine which of the qubits has flipped — without disturbing the encoded state. A  $\sigma_x$  operation on the flipped qubit then allows you to recover the original state.

The same code can correct for a phase shift ( $\sigma_z$ ) instead of a bit flip error, if we apply a Hadamard gate to each of the three qubits in the encoded state.

d) Explain why this works. What are the two observables that we have to measure in this case to determine the error?