

**2.111J/18.435J Quantum Computation Midterm Quiz Solutions**  
 (Given in class, with a page of notes allowed, on Thursday, October 27, 2005)

**1) Classical Logic**

Consider a binary function  $f$  from  $n$  bits to  $m$  bits. If one can write  $f(\mathbf{x}) = M\mathbf{x} + \mathbf{b}$ , where  $\mathbf{x}$  is a column vector of length  $n$ ,  $M$  is a  $m \times n$  matrix, and  $\mathbf{b}$  is a column vector of length  $m$ , then  $f$  is said to be *affine*. (All multiplication and addition in this problem is mod 2.)

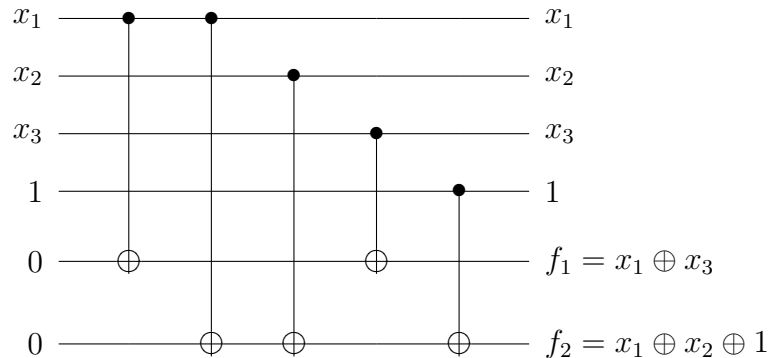
- (a) Let  $M = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$  and  $\mathbf{b} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ . Exhibit a circuit made only of CNOT gates that implements  $f(\mathbf{x}) = M\mathbf{x} + \mathbf{b}$ . (Your circuit can include more than 3 bits.)
- (b) Is  $f$  one-to-one? How is your answer to this question reflected in the form of your circuit in (a)?
- (c) Can any affine function  $f$  from  $n$  bits to  $m$  bits be constructed out of CNOT gates alone? (You are free to include more than  $\max\{m, n\}$  bits in these hypothetical circuits.) If so, why? If not, why not?

**Solution (1a)**

A circuit calculating the affine function

$$f(\mathbf{x}) = \begin{pmatrix} f_1(x_1, x_2, x_3) \\ f_2(x_1, x_2, x_3) \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} x_1 \oplus x_3 \\ x_1 \oplus x_2 \oplus 1 \end{pmatrix}$$

is readily constructed from CNOTs since a CNOT gate by definition simply add (mod 2) the value of its control bit to its target bit. Therefore, a straightforward circuit on 6 bits implementing this affine function  $f$  is



**Solution (1b)**

No,  $f$  is not one-to-one since it has 3 input bits and 2 output bits. Therefore,  $f$  has thus  $2^3 = 8$  possible inputs, but no matter what  $f$  is precisely, it has no more than  $2^2 = 4$  possible outputs. (With a moment's effort, one can verify that the range for this particular  $f$  does in

fact include all 4 two bit strings.) This fact is manifested in the reversible circuit exhibited in (1a) in the fact that only a subset of the circuit's bits encode logical outputs.

### Solution (1c)

Yes, circuits comprised only of CNOTs can handle any affine function since affine functions are simply prescriptions for a bunch of mod 2 additions and CNOTs again, by definition, simply add mod 2 the value of their control bits to their target bits. Indeed, the circuit exhibited in (1a) illustrates a straightforward approach that can handle any affine function. If  $f(\mathbf{x}) = M\mathbf{x} + \mathbf{b}$  where  $\mathbf{x}$  is a column vector of length  $n$ ,  $M$  is a  $m \times n$  matrix containing  $|M|$  ones, and  $\mathbf{b}$  is a column vector of length  $m$  containing  $|\mathbf{b}|$  ones, then you can implement  $f$  in a circuit with  $m + n + |\mathbf{b}|$  bits with  $|M| + |\mathbf{b}|$  CNOTs.

## 2) Single Qubit Operators

*Note on Conventions: In this problem, positive rotation angles correspond to counterclockwise rotations, and negative rotation angles correspond to clockwise rotations.*

- A qubit is rotated by  $\pi/2$  around the  $x$ -axis and then rotated by  $\pi/2$  around the  $y$ -axis. Write down the  $2 \times 2$  unitary matrix  $U$  corresponding to the net rotation.
- The net rotation  $U$  from (a) is expressible as a single rotation. By what angle? Around what axis?
- To lowest nonzero order in  $\epsilon$ , write down the  $2 \times 2$  unitary transformation  $U_\epsilon$  corresponding to a rotation of  $\epsilon$  around the  $x$ -axis, followed by a rotation of  $\epsilon$  around the  $y$ -axis, then a rotation of  $-\epsilon$  around the  $x$ -axis, and finally a rotation of  $-\epsilon$  around the  $y$ -axis.
- The net approximate rotation  $U_\epsilon$  from (c) is expressible as a single rotation. By what angle? Around what axis?

### Solution (2a)

By definition,  $U = R_y(\pi/2)R_x(\pi/2) = e^{-i\pi\sigma_y/4}e^{-i\pi\sigma_x/4}$ . Since  $\sigma_x = \sigma_y^2 = \mathbb{I}$ , we may evaluate  $U$  with the following highly useful formula for  $e^{i\alpha M}$  (where  $\alpha$  is a scalar and  $M$  is a matrix):

$$M^2 = \mathbb{I} \implies e^{i\alpha M} = \cos(\alpha)\mathbb{I} + i \sin(\alpha)M.$$

Thus,

$$\begin{aligned} U &= [\cos(\pi/4)\mathbb{I} - i \sin(\pi/4)\sigma_y][\cos(\pi/4)\mathbb{I} - i \sin(\pi/4)\sigma_x] \\ &= (\mathbb{I} - i\sigma_y)(\mathbb{I} - i\sigma_x)/2 \\ &= (\mathbb{I} - i\sigma_y - i\sigma_x - \sigma_y\sigma_x)/2 \\ &= \frac{1}{2} \begin{pmatrix} 1+i & -1-i \\ 1-i & 1-i \end{pmatrix}. \end{aligned}$$

## Solution (2b)

A rotation  $R_{\hat{n}}(\theta)$  of an angle  $\theta$  around an arbitrary axis  $\hat{n} = (n_x, n_y, n_z)$  where  $n_x^2 + n_y^2 + n_z^2 = 1$  takes the form

$$\begin{aligned} R_{\hat{n}}(\theta) &= e^{-i\theta(n_x\sigma_x + n_y\sigma_y + n_z\sigma_z)/2} \\ &= \cos(\theta/2)\mathbb{I} - i\sin(\theta/2)(n_x\sigma_x + n_y\sigma_y + n_z\sigma_z) \\ &= \begin{pmatrix} \cos(\theta/2) - in_z\sin(\theta/2) & -(n_y + in_x)\sin(\theta/2) \\ (n_y - in_x)\sin(\theta/2) & \cos(\theta/2) + in_z\sin(\theta/2) \end{pmatrix} \end{aligned}$$

Therefore, upon examining the net rotation matrix from (2a),

$$U = \frac{1}{2} \begin{pmatrix} 1+i & -1-i \\ 1-i & 1-i \end{pmatrix},$$

we see  $R_{\hat{n}}(\theta)$  is defined by the equations:

$$\begin{aligned} \cos(\theta/2) &= 1/2 \\ n_x \sin(\theta/2) &= 1/2 \\ n_y \sin(\theta/2) &= 1/2 \\ n_z \sin(\theta/2) &= -1/2 \end{aligned}$$

The first equation implies that

$$\theta = 2 \arccos(1/2) = \pm 2\pi/3 + 4\pi k \text{ where } k \text{ is an integer}$$

and that

$$\sin(\theta/2) = \pm\sqrt{3}/2.$$

This in turn sets the axis

$$\begin{aligned} n_x &= \pm 1/\sqrt{3} \\ n_y &= \pm 1/\sqrt{3} \\ n_z &= \mp 1/\sqrt{3}. \end{aligned}$$

## Solution (2c)

By definition,  $U_\epsilon = R_y(-\epsilon)R_x(-\epsilon)R_y(\epsilon)R_x(\epsilon) = e^{i\epsilon\sigma_y/2}e^{i\epsilon\sigma_x/2}e^{-i\epsilon\sigma_y/2}e^{-i\epsilon\sigma_x/2}$ . Thus, expanding the exponentials in Taylor series

$$\begin{aligned} U_\epsilon &= (\mathbb{I} + i\epsilon\sigma_y/2 - \epsilon^2\mathbb{I}/8 + \dots)(\mathbb{I} + i\epsilon\sigma_x/2 - \epsilon^2\mathbb{I}/8 + \dots) \\ &\quad \times (\mathbb{I} - i\epsilon\sigma_y/2 - \epsilon^2\mathbb{I}/8 + \dots)(\mathbb{I} - i\epsilon\sigma_x/2 - \epsilon^2\mathbb{I}/8 + \dots) \\ &= \mathbb{I} + i\epsilon(\sigma_y + \sigma_x - \sigma_y - \sigma_x) - \epsilon^2 \begin{pmatrix} 4\mathbb{I}/8 + \sigma_y\sigma_x/4 - \sigma_y^2/4 - \sigma_y\sigma_x/4 \\ -\sigma_x\sigma_y/4 - \sigma_x^2/4 + \sigma_y\sigma_x/4 \end{pmatrix} \\ &= \mathbb{I} + \epsilon^2[\sigma_x, \sigma_y]/4 \\ &= \mathbb{I} + i\epsilon^2\sigma_z/2 \end{aligned}$$

### Solution (2d)

Noting that

$$R_z(\epsilon^2) = e^{-i\epsilon^2/2} = \cos(\epsilon^2/2)\mathbb{I} - i \sin(\epsilon^2/2)\sigma_z,$$

we see the net approximate rotation  $U_\epsilon = \mathbb{I} + i\epsilon^2\sigma_z/2$  is an  $O(\epsilon^2)$  approximation to a single rotation of  $-\epsilon^2$  around the  $z$ -axis.

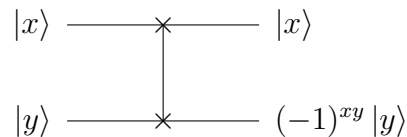
---

### 3) Cluster States

A *controlled phase gate* applies a phase of  $-1$  to  $|11\rangle$  and leaves all other logical states unchanged. That is,

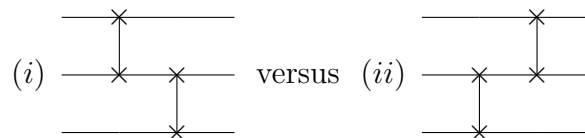
$$|00\rangle \rightarrow |00\rangle, \quad |01\rangle \rightarrow |01\rangle, \quad |10\rangle \rightarrow |10\rangle, \quad |11\rangle \rightarrow -|11\rangle$$

We depict controlled phase gates with the following diagram.

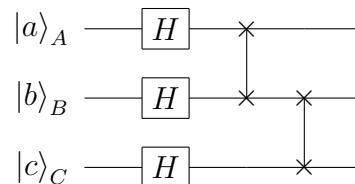


[Note that the phase factor  $(-1)^{xy}$  can just as well be associated with the output ket  $|x\rangle$ . Controlled phase gates are symmetric.]

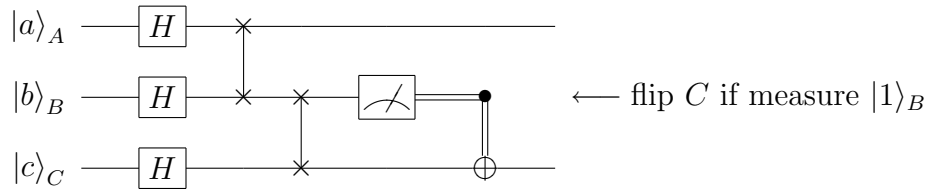
- (a) Show how to construct a CNOT using controlled phase gates and single qubit rotations.
- (b) How do the following two circuits differ in their effect?



- (c) What state is produced by the following circuit?



- (d) Consider extending the circuit in (c) by measuring qubit  $B$  in the  $\{|0\rangle, |1\rangle\}$  basis and then flipping the qubit  $C$  if the result of the measurement is  $|1\rangle_B$ .



What is the joint state of qubits  $A$  and  $C$  after this procedure...

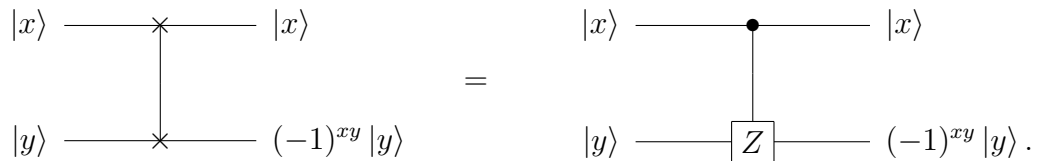
- (i) ... if measurement of qubit  $B$  yields  $|1\rangle_B$ ?
- (ii) ... if you do not yet know the measurement result for qubit  $B$ ?

**Solution (3a)**

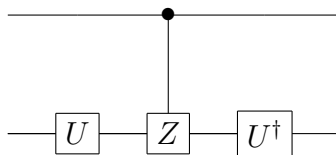
First, realize that a CNOT gate is equivalent to a controlled- $X$  gate.



Next, realize that a controlled phase gate is equivalent to a controlled- $Z$  gate.



Therefore, a gate of the following form

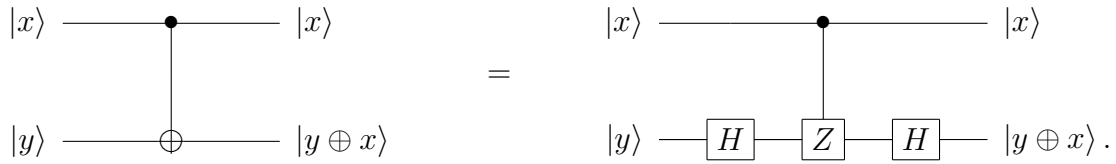


where  $X = UZU^\dagger$  will implement CNOT because  $U$  is unitary and thus if the control bit is 0 and thus the  $Z$  is not implemented, the fact  $UU^\dagger = \mathbb{I}$ , will ensure that the target qubit is unchanged as is desired.

The necessary  $U$  for  $X = UZU^\dagger$  is the Hadamard transformation

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

So noting that  $H = H^\dagger$ , we conclude



### Solution (3b)

The two circuits do not differ in their effect.

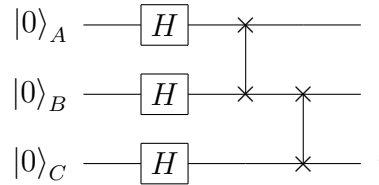


In circuit (i), the first controlled phase gate gives a phase factor  $(-1)^{xy}$  free associable with any of the qubits. This phase factor simply goes unchanged through the second controlled phase gate, which gives another phase factor  $(-1)^{yz}$ , again freely associable with any of the qubits. Thus, the net effect is just a phase factor  $(-1)^{yz}(-1)^{xy}$ .

In comparison, in circuit (ii), the first controlled phase gate gives a phase factor  $(-1)^{yz}$  free associable with any of the qubits. This phase factor goes unchanged through the second controlled phase gate, which gives another phase factor  $(-1)^{xy}$ , again freely associable with any of the qubits. Thus, the net effect is just a phase factor  $(-1)^{xy}(-1)^{yz}$ , which is equivalent to (i).

### Solution (3c)

After the Hadamards in



the computer's state is the superposition

$$|\psi\rangle = \frac{1}{2\sqrt{2}} \sum_{x=0}^1 \sum_{y=0}^1 \sum_{z=0}^1 (-1)^{ax \oplus by \oplus cz} |x\rangle_A \otimes |y\rangle_B \otimes |z\rangle_C.$$

Then, as described in (3b) the net effect of the two controlled phase gates is to give a phase

factor  $(-1)^{xy}(-1)^{yz}$ . Thus, the output is

$$|\psi\rangle_{\text{out}} = \frac{1}{2\sqrt{2}} \sum_{x=0}^1 \sum_{y=0}^1 \sum_{z=0}^1 (-1)^{ax \oplus by \oplus cz} (-1)^{xy} (-1)^{yz} |x\rangle_A \otimes |y\rangle_B \otimes |z\rangle_C.$$

### Solution (3d)

*Part (i):* In this case, we are told we obtain  $|1\rangle_B$  upon measuring qubit  $B$ . Thus, right after measurement, the state  $|\psi\rangle_{\text{out}}$  from (3c) collapses (either subjectively or objectively depending on your metaphysical leanings, but I digress) to the state containing only those 4 components which have  $|y = 1\rangle_B$ .

$$\begin{aligned} |\psi\rangle_{\text{measured } B=1} &= \frac{1}{2} \sum_{x=0}^1 \sum_{z=0}^1 (-1)^{ax \oplus b \oplus cz} (-1)^x (-1)^z |x\rangle_A \otimes |1\rangle_B \otimes |z\rangle_C \\ &= \left[ \frac{1}{\sqrt{2}} \sum_{x=0}^1 (-1)^{(1 \oplus a)x} |x\rangle_A \right] \otimes \left[ (-1)^b |1\rangle_B \right] \otimes \left[ \frac{1}{\sqrt{2}} \sum_{z=0}^1 (-1)^{(1 \oplus c)z} |z\rangle_C \right]. \end{aligned}$$

The classically controlled bit flip then acts on qubit  $C$  yielding

$$\begin{aligned} |\psi\rangle_{\text{final, if } B=1 \text{ known}} &= \left[ \frac{1}{\sqrt{2}} \sum_{x=0}^1 (-1)^{(1 \oplus a)x} |x\rangle_A \right] \otimes \left[ (-1)^b |1\rangle_B \right] \otimes \left[ \frac{1}{\sqrt{2}} \sum_{z=0}^1 (-1)^{(1 \oplus c)z} |z \oplus 1\rangle_C \right] \\ &= \left[ \frac{1}{\sqrt{2}} (|0\rangle_A + (-1)^{1 \oplus a} |1\rangle_A) \right] \otimes \left[ (-1)^b |1\rangle_B \right] \otimes \left[ \frac{1}{\sqrt{2}} (|1\rangle_C + (-1)^{1 \oplus c} |0\rangle_C) \right]. \end{aligned}$$

Since this is a product state, the state of qubits  $A$  and  $C$  considered without  $B$  is immediately seen to be

$$\begin{aligned} |\psi\rangle_{AC \text{ final, if } B=1 \text{ known}} &= (-1)^b \left[ \frac{1}{\sqrt{2}} (|0\rangle_A + (-1)^{1 \oplus a} |1\rangle_A) \right] \otimes \left[ \frac{1}{\sqrt{2}} (|1\rangle_C + (-1)^{1 \oplus c} |0\rangle_C) \right] \\ &= \frac{(-1)^b}{2} \left[ (-1)^{1 \oplus c} |00\rangle + |01\rangle + (-1)^{a \oplus c} |10\rangle + (-1)^{1 \oplus a} |11\rangle \right] \end{aligned}$$

*Part (i), Alternate Method:* At the risk of being pedantic, one can verify this by explicitly tracing out qubit  $B$  in the density matrix  $\rho_{ABC} = |\psi\rangle\langle\psi|_{\text{final, if } B=1 \text{ known}}$ . This partial trace is trivial since  $|\psi\rangle_{\text{final, if } B=1 \text{ known}}$  is a product state of the form  $|\psi\rangle_{ABC} = |\beta\rangle_B \otimes |\alpha\rangle_{AC}$ . (We need not even assume  $|\alpha\rangle_{AC}$  is itself a product state as it is in our case.) Thus,

$$\begin{aligned} \rho_{AC} &= \text{Tr}_B \{ \rho_{ABC} \} \\ &= \text{Tr}_B \{ (|\beta\rangle_B \otimes |\alpha\rangle_{AC}) ( \langle\beta|_B \otimes \langle\alpha|_{AC} ) \} \\ &= \langle\beta|\beta\rangle_B \otimes |\alpha\rangle\langle\alpha|_{AC} \\ &= |\alpha\rangle\langle\alpha|_{AC}. \end{aligned}$$

*Part (ii)*: If one wishes to proceed without resorting to the reduced density matrices, then one can argue as follows. In the state right before measurement,

$$|\psi\rangle_{\text{out}} = \frac{1}{2\sqrt{2}} \sum_{x=0}^1 \sum_{y=0}^1 \sum_{z=0}^1 (-1)^{ax \oplus by \oplus cz} (-1)^{xy} (-1)^{yz} |x\rangle_A \otimes |y\rangle_B \otimes |z\rangle_C,$$

all 8 components, though they differ in relative phase, have amplitudes of equal magnitude. There are 4 components including  $|0\rangle_B$  and 4 components including  $|1\rangle_B$ . Thus, there is a 50% chance of measuring  $|0\rangle_B$  and a 50% chance of measuring  $|1\rangle_B$ . In the former case, the measurement-controlled bit flip does not act, and in the latter case it does. Therefore, the final state coming out of this procedure is the *mixed* state

$$\rho_{AC} = \frac{1}{2} |\psi\rangle\langle\psi|_{AC \text{ final, if } B=1 \text{ known}} + \frac{1}{2} |\psi\rangle\langle\psi|_{AC \text{ final, if } B=0 \text{ known}}.$$

where from Part (i),

$$|\psi\rangle_{AC \text{ final, if } B=1 \text{ known}} = (-1)^b \left[ \frac{1}{\sqrt{2}} (|0\rangle_A + (-1)^{1 \oplus a} |1\rangle_A) \right] \otimes \left[ \frac{1}{\sqrt{2}} (|1\rangle_C + (-1)^{1 \oplus c} |0\rangle_C) \right].$$

As for  $|\psi\rangle_{AC \text{ final, if } B=0 \text{ known}}$ , we argue similarly to Part (i). Measurement of  $|0\rangle_B$  would collapse  $|\psi\rangle_{\text{out}}$  to the 4 components that contain  $|y=0\rangle_B$ ,

$$\begin{aligned} |\psi\rangle_{\text{measured } B=0} &= \frac{1}{2} \sum_{x=0}^1 \sum_{z=0}^1 (-1)^{ax \oplus cz} |x\rangle_A \otimes |0\rangle_B \otimes |z\rangle_C \\ &= \left[ \frac{1}{\sqrt{2}} \sum_{x=0}^1 (-1)^{ax} |x\rangle_A \right] \otimes \left[ |0\rangle_B \right] \otimes \left[ \frac{1}{\sqrt{2}} \sum_{z=0}^1 (-1)^{cz} |z\rangle_C \right]. \end{aligned}$$

Thus, since the measurement conditioned bit flip does not act in this case,

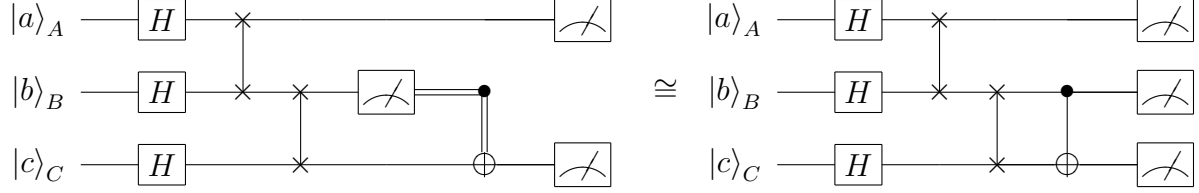
$$\begin{aligned} |\psi\rangle_{AC \text{ final, if } B=0 \text{ known}} &= \left[ \frac{1}{\sqrt{2}} (|0\rangle_A + (-1)^a |1\rangle_A) \right] \otimes \left[ \frac{1}{\sqrt{2}} (|0\rangle_C + (-1)^c |1\rangle_C) \right] \\ &= \frac{1}{2} \left[ |00\rangle + (-1)^c |01\rangle + (-1)^a |10\rangle + (-1)^{a \oplus c} |11\rangle \right] \end{aligned}$$

*Part (ii), Alternate Method*: In this case where we do not know the result of the measurement it is less of a pedantic overkill, and in fact probably a pedagogically useful exercise, to use the full apparatus of reduced density matrices. After all, reduced density matrices are precisely the mathematical tools defined to deal with the problem of when classical uncertainty arises as to the quantum state of a system because that system has been “measured” by interacting with another system which one cannot examine.

Before proceeding, since it’s simpler to write down gate operations on pure states than on mixed states, it is useful to invoke what Nielsen and Chuang dub “The Principle of Deferred Measurement”:

Measurements can always be moved from an intermediate stage of a quantum circuit to the end of the circuit; if the measurement results are used at any stage of the circuit then the classically controlled operations can be replaced by conditional quantum operations [p. 186].

In our case, this means that the following two circuits are equivalent.



Right before measurement, the state of the qubits in the circuit depicted on the right is

$$|\psi\rangle = \frac{1}{2\sqrt{2}} \sum_{xyz} (-1)^{ax \oplus by \oplus cz} (-1)^{xy} (-1)^{yz} |x\rangle_A \otimes |y\rangle_B \otimes |z \oplus y\rangle_C.$$

Thus, tracing out qubit  $B$  yields,

$$\begin{aligned} \rho_{AC} &= \text{Tr}_B\{|\psi\rangle\langle\psi|\} \\ &= \frac{1}{8} \text{Tr}_B \left\{ \left( \sum_{x'y'z'} (-1)^{ax' \oplus by' \oplus cz'} (-1)^{x'y'} (-1)^{y'z'} |x'\rangle_A \otimes |y'\rangle_B \otimes |z' \oplus y'\rangle_C \right) \right. \\ &\quad \left. \times \left( \sum_{xyz} (-1)^{ax \oplus by \oplus cz} (-1)^{xy} (-1)^{yz} \langle x|_A \otimes \langle y|_B \otimes \langle z \oplus y|_C \right) \right\} \\ &= \frac{1}{8} \sum_{xx'yy'zz'} \left[ \begin{array}{l} (-1)^{(y' \oplus a)x' \oplus by' \oplus (y' \oplus c)z'} \\ \times (-1)^{(y \oplus a)x \oplus by \oplus (y \oplus c)z} \end{array} \right] |x'\rangle\langle x|_A \otimes \langle y'|y\rangle_B \otimes |z' \oplus y'\rangle\langle z \oplus y|_C \end{aligned}$$

The inner products  $\langle y'|y\rangle_B = \delta_{y',y}$  leave only the  $y = y'$  terms.

$$\begin{aligned} \rho_{AC} &= \frac{1}{8} \sum_{xx'zz'} \left( \sum_y \left[ \begin{array}{l} (-1)^{(y \oplus a)x' \oplus by \oplus (y \oplus c)z'} \\ \times (-1)^{(y \oplus a)x \oplus by \oplus (y \oplus c)z} \end{array} \right] |x'\rangle\langle x|_A \otimes |z' \oplus y\rangle\langle z \oplus y|_C \right) \\ &= \left( \begin{array}{l} \frac{(-1)^b}{8} \sum_{xx'zz'} \left[ (-1)^{(1 \oplus a)(x' \oplus x)} (-1)^{(1 \oplus c)(z' \oplus z)} \right] |x'\rangle\langle x|_A \otimes |z' \oplus 1\rangle\langle z \oplus 1|_C \\ + \frac{1}{8} \sum_{x'z'xz} \left[ (-1)^{a(x' \oplus x)} (-1)^{c(z' \oplus z)} \right] |x'\rangle\langle x|_A \otimes |z'\rangle\langle z|_C \end{array} \right) \\ &= \left( \begin{array}{l} \frac{1}{2} \left[ \frac{(-1)^b}{2} \sum_{xx'} (-1)^{(1 \oplus a)(x' \oplus x)} |x'\rangle\langle x|_A \right] \otimes \left[ \frac{(-1)^b}{2} \sum_{zz'} (-1)^{(1 \oplus c)(z' \oplus z)} |z' \oplus 1\rangle\langle z \oplus 1|_C \right] \\ + \frac{1}{2} \left[ \frac{1}{2} \sum_{xx'} (-1)^{a(x' \oplus x)} |x'\rangle\langle x|_A \right] \otimes \left[ \frac{1}{2} \sum_{zz'} (-1)^{c(z' \oplus z)} |z'\rangle\langle z|_C \right] \end{array} \right) \\ &= \frac{1}{2} |\psi\rangle\langle\psi|_{AC \text{ final, if } B=1 \text{ known}} + \frac{1}{2} |\psi\rangle\langle\psi|_{AC \text{ final, if } B=0 \text{ known}} \end{aligned}$$

as previously derived by a method admittedly requiring a lot less arithmetic.

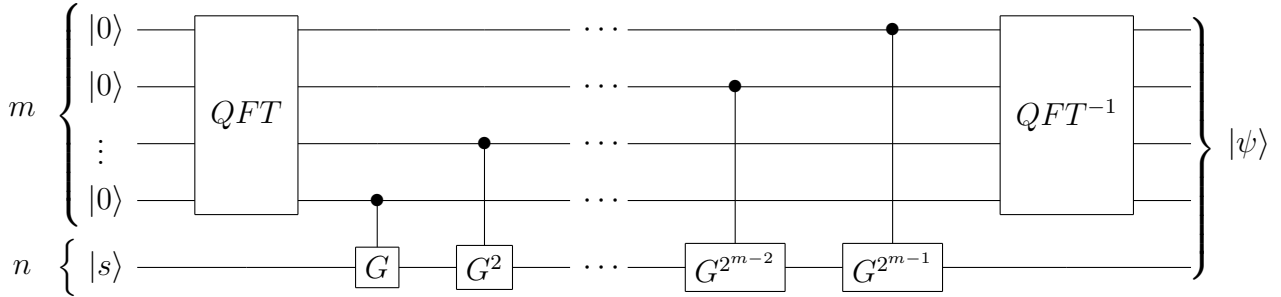
#### 4) Quantum Phase Estimation for Grover's Algorithm

Let  $G$  denote the Grover step:

$$\boxed{G} \iff (\mathbb{I} - 2|s\rangle\langle s|)(2|w\rangle\langle w| - \mathbb{I}),$$

where  $N = 2^n$ ,  $|w\rangle$  is the target state, and  $|s\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$ .

(a) What is the output of the following circuit?



(b) Suppose  $m = n$ . What information do you get by measuring the first  $m$  bits of  $|\psi\rangle$ ? After measurement, what state is registered by the second  $n$  bits of  $|\psi\rangle$ ?

(c) How do your conclusions for part (b) change if  $m \ll n$ ? If  $m \gg n$ ?

#### Solutions (4a) and (4b)

This circuit is the quantum phase estimation circuit for the Grover step  $G$ , a unitary operator. Thus, by design, the circuit outputs eigenvectors and (approximate) eigenvalues of  $G$ , which we shall denote by  $G|\theta_j\rangle = e^{i\theta_j}|\theta_j\rangle$ . [As  $G$  is unitary, all its eigenvalues are on the unit circle in the complex plane, and thus can be expressed in the form  $e^{i\theta_j}$  where  $\theta_j \in [0, 2\pi)$ .]

More specifically, the output of the  $n$ -qubit register will be an eigenvector  $|\theta_j\rangle$  of  $G$  and the accompanying output of the  $m$ -qubit register is, with high probability, an excellent  $m$ -bit binary fraction approximation  $0.k_1k_2\dots k_m$  to the phase angle of the corresponding eigenvalue  $\theta_j/2\pi$ .

Now, recall the orthonormal basis  $\{|w\rangle, |r\rangle\}$  where  $|r\rangle = \frac{1}{\sqrt{N-1}} \sum_{x \neq w} |x\rangle$  is the equal superposition over all states other than the search target, yields a very useful expression for the Grover step.

$$G = \cos \theta (|w\rangle\langle w| + |r\rangle\langle r|) + \sin \theta (|w\rangle\langle r| - |r\rangle\langle w|) = \begin{pmatrix} \cos \theta & \sin \theta \\ -\sin \theta & \cos \theta \end{pmatrix},$$

where  $\theta = \arccos \left( 1 - \frac{2}{N} \right)$ .

The eigenvalues of  $G$  are now easily found.

$$\det\{G - \lambda_{\pm}\mathbb{I}\} = 0 \implies \lambda_{\pm}^2 - 2\lambda_{\pm} \cos \theta + 1 = 0 \implies \lambda_{\pm} = \frac{2 \cos \theta \pm \sqrt{4 \cos^2 \theta - 4}}{2} = e^{\pm i\theta},$$

where, again,  $\theta = \arccos\left(1 - \frac{2}{N}\right)$ .

To solve for the corresponding eigenvectors of  $G$ , note that

$$\begin{pmatrix} \cos \theta & \sin \theta \\ -\sin \theta & \cos \theta \end{pmatrix} \begin{pmatrix} 1 \\ \pm i \end{pmatrix} = \begin{pmatrix} \cos \theta \pm i \sin \theta \\ -\sin \theta \pm i \cos \theta \end{pmatrix} = e^{\pm i\theta} \begin{pmatrix} 1 \\ \pm i \end{pmatrix}.$$

Thus, we find that the eigenvectors and eigenvalues of  $G$  are

$$|\theta_{\pm}\rangle = \frac{1}{\sqrt{N}}(|w\rangle \pm i|r\rangle) \text{ with eigenvalue } e^{\pm i\theta}, \text{ where } \theta = \arccos\left(1 - \frac{2}{N}\right).$$

So we have succeeded in finding the possible outputs of the circuit. One will measure either:

- the  $n$ -qubit register to be in the state  $|\theta_{+}\rangle$  and the  $m$ -qubit register to be in a state  $|k_1 k_2 \dots k_m\rangle$  such that, with high probability  $0.k_1 k_2 \dots k_m$  is close to the best possible  $m$ -bit binary fraction approximation to  $\theta/2\pi$ , or
- the  $n$ -qubit register to be in the state  $|\theta_{-}\rangle$  and the  $m$ -qubit register to be in a state  $|k_1 k_2 \dots k_m\rangle$  such that, with high probability  $0.k_1 k_2 \dots k_m$  is close to the best possible  $m$ -bit binary fraction approximation to  $1 - \theta/2\pi$ .

In order to determine the probabilities of each outcome, we must decompose the starting state of the  $n$ -qubit register  $|s\rangle \equiv \sum_{x=0}^{N-1} |x\rangle$  in terms of the eigenvectors  $\{|\theta_{+}\rangle, |\theta_{-}\rangle\}$ . Noting that

$$|w\rangle = \frac{1}{\sqrt{2}}(|\theta_{+}\rangle + |\theta_{-}\rangle) \quad \text{and} \quad |r\rangle = \frac{1}{i\sqrt{2}}(|\theta_{+}\rangle - |\theta_{-}\rangle).$$

and thus

$$\begin{aligned} |s\rangle &\equiv \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle \\ &= \frac{1}{\sqrt{N}} |w\rangle + \sqrt{\frac{N-1}{N}} |r\rangle \\ &= \frac{1}{\sqrt{2N}} (|\theta_{+}\rangle + |\theta_{-}\rangle) - i \sqrt{\frac{N-1}{2N}} (|\theta_{+}\rangle - |\theta_{-}\rangle) \\ &= \frac{1}{\sqrt{2N}} \left[ (1 - i\sqrt{N-1}) |\theta_{+}\rangle + (1 + i\sqrt{N-1}) |\theta_{-}\rangle \right] \end{aligned}$$

Hence there is a 50% chance of the measuring  $|\theta_{+}\rangle$  scenario and a 50% chance of the measuring  $|\theta_{-}\rangle$  scenario.

### Solution (4c)

The basic scenarios do not change as  $m$  changes relative to  $n$ . Regardless of the value of  $m$  it is the case that one will measure either

- the  $n$ -qubit register to be in the state  $|\theta_+\rangle$  and the  $m$ -qubit register to be in a state  $|k_1k_2\dots k_m\rangle$  such that, with high probability  $0.k_1k_2\dots k_m$  is close to the best possible  $m$ -bit binary fraction approximation to  $\theta/2\pi$ , or
- the  $n$ -qubit register to be in the state  $|\theta_-\rangle$  and the  $m$ -qubit register to be in a state  $|k_1k_2\dots k_m\rangle$  such that, with high probability  $0.k_1k_2\dots k_m$  is close to the best possible  $m$ -bit binary fraction approximation to  $1 - \theta/2\pi$ .

Of course, the quality of the approximation of  $\theta$  increases as  $m$  increases. In this regard, note that  $m$ -bit approximations when  $m \ll n$  are essentially worthless since the best  $m$ -bit approximation to  $\theta/2\pi$  in this case is trivially 0. To see this, realize that since  $\cos \theta = (1 - 2/N) = (1 - 2^{1-n})$  is very close to 1 for even modest  $n$ , we can use the formula  $\cos \theta = 1 - \theta^2/2 + O(\theta^4)$  to make a very accurate estimate  $\theta = \sqrt{2/N} + O(1/N) = 2^{(1-n)/2} + O(2^{-n})$ . Thus, it is not until  $m \gtrsim n/2$ , that one can obtain nontrivial estimates of  $\theta/2\pi$ .