Today's outline - February 23, 2023

- Period-finding and factoring strategy
- Shor's factoring algorithm
- The quantum core, and period extraction
- An example of Shor's algorithm
- Review problems

Reading Assignment: Reiffel: 9.1–9.2 Wong: 7.6

Exam #1 Tuesday, February 28, 2023
Covers Chapters HW 01–04

Homework Assignment #05:
due Thursday, March 09, 2023

Classical period-finding

In 1994 Shor developed an algorithm for factoring integers which coupled with the quantum Fourier transform threatened to crack the standard encryption algorithms of the time

The factoring algorithm relies finding the period of a function $f(k)$

The order of an integer $a \bmod M$ is the smallest integer r such that $r > 0$ and $a^r = 1 \bmod M$

If the two integers a and M are relatively prime (i.e. they share no prime factors) then r exists and the order of a is finite

Consider the function $f(k)$
Since $a^r = 1 \bmod M$ we can write and r is the period of $f(k)$

$$f(k) = a^k \bmod M = a^{k+r} \bmod M$$

For example, take $a = 5$ and $M = 13$

Thus $r = 4$ is the period of the function
$f(k) = a^k = 5^k$

r	a^r	$a^r \bmod M$
1	5	5
2	25	12
3	125	8
4	625	1

Factoring strategy

If $a^r = 1 \mod M$ and r is even then $$(a^{r/2}+1)(a^{r/2}-1) \equiv 0 \mod M$$

In our example $r = 4$ so we have $$(5^2+1)(5^2-1) = 26 \cdot 24 = 13 \cdot 48$$

If neither $a^{r/2} \pm 1$ is a multiple of M then they both likely have common factors with M and so suggest a method for factoring M

1. Randomly choose an integer a and determine the period r of $f(k) = a^k \mod M$
2. If r is even use the Euclidean algorithm to compute the greatest common divisor of $a^{r/2} \pm 1$ and M
3. Repeat as necessary

Given that an encryption key, M, is generally a large number, this is still a computationally expensive operation for a classical computer, however Shor's quantum algorithm makes it possible efficiently perform step 2.

Shor's factoring algorithm

The implementation of Shor's algorithm can be summarized in a few steps

1. Randomly choose an integer a such that $0 < a < M$ and apply the Euclidean algorithm
   a. If a and M have a common factor, this is a factor of M, save and start over at step 1
   b. If a and M are relatively prime, continue to 2.
2. Use quantum parallelism to compute $f(x) = a^x \bmod M$ on the superposition of $n : M^2 \leq 2^n < 2M^2$ inputs and apply a quantum Fourier transform to the result
3. Measure. With high probability, a value v close to a multiple of $\frac{2^n}{r}$ will be obtained
4. Use classical methods to obtain a possible period q from v
5. For q even, use the Euclidean algorithm to find any common factors of M and $a^{q/2} \pm 1$
6. Start over with step 1 if more factors are needed

Only steps 2 and 3 require a quantum computer since the other steps are efficiently performed with a classical computer

The quantum core

Start by preparing a uniform superposition state of an n-qubit register

$$W|0\cdots0\rangle = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle$$

The function $f(x) = a^x \bmod M$ can be computed with an efficiently implemented transformation U_f

$$U_f : |x\rangle|0\rangle \rightarrow |x\rangle|f(x)\rangle$$

This requires a second m-qubit register such that

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

The second register is now measured randomly and this returns a value u for $f(x)$ so that the two registers are no longer entangled and the state is

$$C\sum_{x=0}^{N-1}g(x)|x\rangle|u\rangle, \quad g(x) = \begin{cases} 1 & \text{if } f(x) = u \\ 0 & \text{otherwise} \end{cases}$$

C is the normalization constant and $g(x)$ must, by definition, have the same period as $f(x)$ but is sparse and only has non-zero values at intervals of the period

Applying the quantum Fourier transform

The second register can be thrown away as it is no longer entangled with the first

$$|\psi\rangle = C\sum_{x=0}^{N-1} g(x)|x\rangle$$

Now apply the quantum Fourier transform, U_F, to the first register to get

$$U_F|\psi\rangle = C'\sum_{c=0}^{N-1} G(c)|c\rangle$$

Where $G(c)$ is given by

$$G(c) = \sum_{x=0}^{N-1} g(x)e^{2\pi icx/2^n}$$

Recalling the properties of the quantum Fourier transform, if the period, r, of the function $g(x)$ is a power of two, $G(c) \equiv 0$ except when c is a multiple of $\frac{2^n}{r}$

When the period is not a power of two, the quantum Fourier transform approximates the exact case and yields a value v close to a multiple of $\frac{2^n}{r}$

Continued fraction expansion

In the case where r is a power of 2,the measured output $v = j\frac{2^n}{r}$ and the period is straightforward to extract

It is more challenging when the Fourier transform produces values which are only approximate multiples of the scaled frequency

In this case, a good guess for the period is obtained by the continued fraction expansion of $\frac{v}{2^n}$

Define $[x] = trunc(x)$ as the greatest integer less than x and define the quantities

$$a_0 = \left[\frac{v}{2^n}\right], \quad \epsilon_0 = \frac{v}{2^n} - a_0, \quad a_i = \left[\frac{1}{\epsilon_{i-1}}\right], \quad \epsilon_i = \frac{1}{\epsilon_{i-1}} - a_i$$

$$p_0 = a_0, \quad p_1 = a_1 a_0 + 1, \quad p_i = a_i p_{i-1} + p_{i-2}, \quad q_0 = 1, \quad q_1 = a_1, \quad q_i = a_i q_{i-1} + q_{i-2}$$

Compute the first fraction $\frac{p_i}{q_i}$ such that $q_i < M \leq q_{i+1}$

This is the unique fraction with denominator less than M that is within $\frac{1}{M^2}$ of $\frac{v}{2^n}$

Shor showed that this fraction is within $\frac{1}{2}$ of a multiple of $\frac{2^n}{r}$

Period extraction

Recall that we chose the size of the qubit register to be $n : M^2 \leq 2^n < 2M^2$

According to Shor, in the high probability case that

$$\left| v - j\frac{2^n}{r} \right| < \frac{1}{2}$$

For some j, $M^2 \leq 2^n$ so that

$$\left| \frac{v}{2^n} - \frac{j}{r} \right| < \frac{1}{2 \cdot 2^n} \leq \frac{1}{2M^2}$$

The difference between two fractions $\frac{p}{q}$ and $\frac{p'}{q'}$ with denominators less than M is bounded

$$\left| \frac{p}{q} - \frac{p'}{q'} \right| = \left| \frac{pq' - p'q}{qq'} \right| > \frac{1}{M^2}$$

There is at most one fraction $\frac{p}{q}$ with denominator $q < M$ such that

$$\left| \frac{v}{2^n} - \frac{p}{q} \right| < \frac{1}{M^2}$$

This fraction, computed by fraction expansion will likely be equal to $\frac{j}{r}$ so the denominator q is the guess for the period r which will be correct if r and j are relatively prime

Shor's algorithm example

In order to factor $M = 21$, note that $M^2 = 441$ so that $2^9 = 512$ is the power of 2 between M^2 and $2M^2$

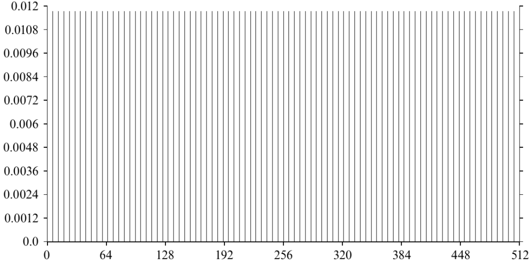
With $n = 9$ as the size of the first register, the size of the second is set by the ceiling $\lceil \ln M \rceil + 1 = m = 5$

The state, after applying U_f is therefore, a 14-qubit state with 9 qubits in the first register and 5 in the second

$$|\psi\rangle = \frac{1}{\sqrt{2^9}} \sum_{x=0}^{2^9-1} |x\rangle |f(x)\rangle$$

If the randomly selected integer $a = 11$ and the measurement of the second register gives $u = 8$

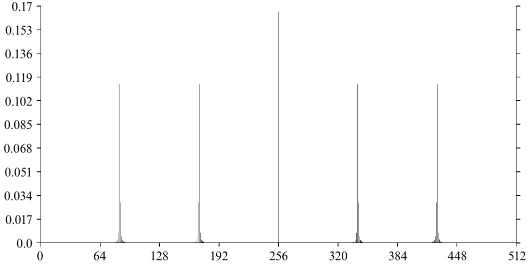
The state of the first register after the measurement shows the periodicity of $f(x)$



Shor's algorithm example

The result of the Fourier transform U_F is applied to $|\psi\rangle$ clearly shows that the period of $f(x)$ is not a multiple of 2

Measurement of $|\psi\rangle$ now returns a value $v = 427$ which is relative prime to 2^n



The continued fraction algorithm is then applied, giving

i	a_i	p_i	q_i	ϵ_i
0	0	0	1	0.8339844
1	1	1	1	0.1990632
2	5	5	6	0.02352941
3	42	211	253	0.5

The computation is terminated when $6 = q_2 < M \leq q_3 = 253$ since $M = 21$

$q = 6$ is thus the guess for the period of $f(x)$

Shor's algorithm example

With $q = 6$ being even we can now find the greatest common factor of $a^{q/2} \pm 1$ and M where $M = 21$ and $a = 11$ by applying the Euclidean algorithm

$$a^{q/2} + 1 = 11^3 + 1 = 1332$$

	M	n	m
1332	21		63
9	21	2	
9	3		3
0			

$$a^{q/2} - 1 = 11^3 + 1 = 1330$$

	M	n	m
1330	21		63
7	21	3	
	0		

With a single Fourier transform application we have factored $M = 21$ into 3 and 7

Clearly this is a trivial example but the potential efficiency of the algorithm is evident

https://tinyurl.com/9p3cyz6s

Problem 3.7

Write the following states in terms of the Bell basis

(a) $|00\rangle$ (b) $|+\rangle|-\rangle$ (c) $\frac{1}{\sqrt{3}}\left(|00\rangle + |01\rangle + |10\rangle\right)$

Starting with the definition of the Bell states

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right), \qquad |\Phi^-\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right)$$
$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right), \qquad |\Psi^-\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right)$$

(a) $|00\rangle = \frac{1}{\sqrt{2}}\left(|\Phi^+\rangle + |\Phi^-\rangle\right)$

(b) $|+\rangle|-\rangle = \frac{1}{2}\left(|00\rangle - |01\rangle + |10\rangle - |11\rangle\right) = \frac{1}{\sqrt{2}}\left(|\Phi^-\rangle - |\Psi^-\rangle\right)$

(c) $\frac{1}{\sqrt{3}}\left(|00\rangle + |01\rangle + |10\rangle\right) = \frac{1}{\sqrt{6}}\left(|\Phi^+\rangle + |\Phi^-\rangle + 2|\Psi^+\rangle\right)$

Problem 3.13

(a) Show that the four-qubit state $|\psi\rangle = \frac{1}{2}(|00\rangle + |11\rangle + |11\rangle + |33\rangle)$ is entangled with respect to the decomposition into two two-qubit subsystems consisting of the first and second qubits and the third and fourth qubits

(b) For the four decompositions into two subsystems consisting of one and three qubits, say whether $|\psi\rangle$ is entangled or unentangled with respect to each of these decompositions

(a) Start by expressing the state in individual qubit pairs and assume that it can be decomposed into a product state for qubits 12 and 34

$$\begin{aligned} |\psi\rangle &= \frac{1}{2}(|0\rangle_{12}|0\rangle_{34} + |1\rangle_{12}|1\rangle_{34} + |2\rangle_{12}|2\rangle_{34} + |3\rangle_{12}|3\rangle_{34}) \\ &= (a_0|0\rangle_{12} + a_1|1\rangle_{12} + a_2|2\rangle_{12} + a_3|3\rangle_{12}) \otimes (b_0|0\rangle_{34} + b_1|1\rangle_{34} + b_2|2\rangle_{34} + b_3|3\rangle_{34}) \end{aligned}$$

looking at the two equations, we see that $a_0 b_0 = \frac{1}{2}$ and $a_1 b_1 = \frac{1}{2}$ but $a_0 b_1 = a_1 b_0 = 0$ which is an inconstency that leads to the conclusion that $|\psi\rangle$ must be entangled in this decomposition

Problem 3.13 (cont.)

(b) Start by expressing the state in individual qubits and assume that it can be decomposed into a product state for qubits 1 and 234

$$\begin{aligned}
|\psi\rangle &= \tfrac{1}{2}\left(|0\rangle|000\rangle + |0\rangle|101\rangle + |1\rangle|010\rangle + |1\rangle|111\rangle\right) \\
&= \left(a_0|0\rangle + a_1|1\rangle\right) \otimes \\
&\qquad \left(b_0|000\rangle + b_1|001\rangle + b_2|010\rangle + b_3|011\rangle + b_4|100\rangle + b_5|101\rangle + b_6|110\rangle + b_7|111\rangle\right)
\end{aligned}$$

looking at the two equations, we see that $a_0 b_0 = \frac{1}{2}$ and $a_1 b_2 = \frac{1}{2}$ but $a_0 b_2 = 0$ which is an inconstency that leads to the conclusion that $|\psi\rangle$ must be entangled in this decomposition and the same reasoning will hold for the other three possible 1:3 decompositions

Problem 4.9

Design a measurement on a three-qubit system that distinguishes between states in which all bit values are equal and those in which they are not, and gives no further information.

The following measurement operator will give 1 when the three bits are all the same and 0 when they are not

$$M = 1 \cdot \big(|000\rangle\langle 000| + |111\rangle\langle 111| \big)$$

Problem 4.11

Design a measurement on a three-qubit system that distinguishes between states with different numbers of 1 bits and gives no further information.

The following measurement operator will return the number of 1 bits

$$\begin{aligned} M = \; & 1 \cdot \big(|001\rangle\langle 001| + |010\rangle\langle 010| + |001\rangle\langle 001| \big) + \\ & 2 \cdot \big(|110\rangle\langle 110| + |101\rangle\langle 101| + |011\rangle\langle 011| \big) + \\ & 3 \cdot |111\rangle\langle 111| \end{aligned}$$

Problem 1.6

In 1992 Bennett proposed the B92 quantum key distribution protocol. Instead of encoding each bit in either the standard basis or the Hadamard basis as is done in the BB84 protocol, Alice encodes her random string x as follows

$$0 \mapsto |0\rangle, \quad 1 \mapsto |+\rangle$$

and sends them to Bob. Bob generates a random bit string y. If $y_i = 0$ he measures the i-th qubit in the Hadamard basis $\{|+\rangle, |-\rangle\}$, if $y_i = 1$ he measures in the standard basis $\{|0\rangle, |1\rangle\}$. In this protocol, instead of telling Alice over the public classical channel which basis he used to measure each qubit, he tells her the results of his measurements. If his measurement resulted in $|+\rangle$ or $|0\rangle$ Bob sends 0, if his measurement indicates the state is $|1\rangle$ or $|-\rangle$, he sends 1. Alice and Bob discard all bits from strings x and y for which Bob's bit value from measurement yielded 0, obtaining strings x' and y'. Alice uses x' as the secret key and Bob uses y'. Then, depending on the security level they desire, they compare a number of bits to detect tampering. They discard these check bits from their key.

Problem 1.6 (cont.)

(a) Show that if Bob receives exactly the states Alice sends, then the strings x' and y' are identical strings.

Case 1: Alice encodes a $0 \mapsto |0\rangle$. If Bob generates a $y_i = 0$, he measures in the Hadamard basis and has a 50% chance of measuring $|+\rangle$, which will be discarded, and 50% chance of measuring $|-\rangle$, which will be kept. If he generates $y_i = 1$, he measures in the Standard basis and has a 100% chance of measuring $|0\rangle$ so this will always be discarded. In this case, the remaining bits satisfy $x' \equiv y'$.

Case 2: Alice encodes a $1 \mapsto |+\rangle$. If Bob generates a $y_i = 0$, he measures in the Hadamard basis and has a 100% chance of measuring $|+\rangle$, which will always be discarded. If he generates a $y_i = 1$, he measures in the Standard basis and has a 50% chance of measuring $|0\rangle$ and 50% chance of measuring $|1\rangle$. He keeps only the y_i where he measured $|1\rangle$ again ensuring that $x' \equiv y'$. Thus in all cases, the strings that Bob and Alice have at the en are identical.

Problem 1.6 (cont.)

(b) Why didn't Alice and Bob decide to keep the bits of x and y for which Bob's bit value from measurement was 0?

The cases where Bob measures a 0 are all the ones in which he has generated a bit that is different than Alice's and half the cases in which he has generated the same bit as Alice. When Bob measured a 1, he has 100% chance of having generated $y_i \equiv x_i$.

Problem 1.6 (cont.)

(c) What if an eavesdropper Eve measures each bit in either the standard basis or the Hadamard basis to obtain a bit string z and forwards the measured qubits to Bob. On average, how many bits of Alice and Bob's key does she know for sure after listening in on the public classical? If Alice and Bob compare s bit values of their strings x' and y', how likely are they to detect Eve's presence?

Eve's best case is if she knows that Alice and Bob are using the B92 protocol, she can follow the same protocol as Bob, and discard all bits measured as $|0\rangle$ or $|+\rangle$ when she measures $|-\rangle$ and $|1\rangle$, she knows what the bit encoded by Alice is.

When Eve interferes however, there is a 25% chance for errors for each bit in Bob's resulting string y'. The likelihood that Alice and Bob will detect Eve's presence as a function of the number of compared bits s, is then: $1 - \left(\frac{3}{4}\right)^s$

Problem 2.6

This exercise analyzes the effectiveness of some simple attacks an eavesdropper Eve could make on Ekert's entangled state based QKD protocol.

(a) Say Eve can measure Bob's half of each of the EPR pairs before it reaches him. Say she always measures in the standard basis. Describe a method by which Alice and Bob can determine that there is only a 2^{-s} chance that this sort of interference by Eve has gone undetected. What happens if Eve instead measures each qubit randomly in either the standard basis of the Hadamard basis? What happens if she uniformly at random chooses a basis from all possible bases?

(b) Say Eve can pose as the entity sending the purported EPR pairs. Say instead of sending EPR pairs she sends a random mixture of qubit pairs in the states $|00\rangle$, $|11\rangle$, $|++\rangle$, and $|--\rangle$. After Alice and Bob perform the protocol of Section 3.4, on how many bits on average do their purported shared secret keys agree? On average, how many of these bits does Eve know?

Problem 2.6 (cont.)

(a) Once Alice and Bob have determined a bit string by comparing the bases they measured and keeping only the results where they agree, they should compare s bits of the string to ensure that they agree.

When Eve measures Bob's qubit, she collapses Alice's qubit to a specific value and the qubit Eve sends on to Bob is not entangled with Alice's any longer. We need to examine the possibilities when Alice and Bob have measured in the same basis

Case 1: If Alice and Bob measure in the standard basis then they will always get the same value because Alice's qubit has been collapsed to the same state and the qubit that Eve sends to Bob

Case 2: If Alice and Bob measure in the Hadamard basis, then their measurements are uncorrelated and 50% of the time they will obtain the same result

Assuming that Alice and Bob choose each of the two bases with equal probability, the chance that they will obtain the same value and not detect Eve's presence is $\frac{1}{2} \cdot 1 + \frac{1}{2} \cdot \frac{1}{2} = \frac{3}{4}$

Problem 2.6 (cont.)

The probability that Eve's interference is undetected is thus $\frac{3}{4}^n$ when n bits of the key are compared. If this is to be equal to 2^{-s} then we have

$$\frac{3}{4}^n = 2^{-s} \quad \longrightarrow \quad -s = n \ln\left(\frac{3}{4}\right) \quad \longrightarrow \quad n = \frac{s}{\ln(\frac{4}{3})} \approx 8s$$

If Eve chooses randomly either in the standard or Hadamard basis, there are 4 cases with the probability of Eve escaping detection is the same as before

$$\frac{1}{2}\left(\frac{1}{2}\cdot 1 + \frac{1}{2}\cdot\frac{1}{2}\right) + \frac{1}{2}\left(\frac{1}{2}\cdot 1 + \frac{1}{2}\cdot\frac{1}{2}\right) = \frac{3}{4}$$

If Eve chooses from any of the three orthogonal bases, the probility of escaping detection drops

$$2\cdot\frac{1}{3}\left(\frac{1}{2}\cdot 1 + \frac{1}{2}\cdot\frac{1}{2}\right) + \frac{1}{3}\left(\frac{1}{2}\cdot\frac{1}{2} + \frac{1}{2}\cdot\frac{1}{2}\right) = \frac{7}{12} \quad \longrightarrow \quad n = \frac{s}{\ln(\frac{12}{7})} \approx 4.3s$$

Problem 2.6 (cont.)

(b) When Alice and Bob measure an unentangled state, they have a 100% chance of measuring the same value when they choose the same basis as Eve sent and a 50% chance when they choose the other basis. If they choose each basis 50% of the time, then the probability of their measured bit agreeing for each of the two bases that Eve uses is the same

$$2 \cdot \frac{1}{2}\left(\frac{1}{2} \cdot 1 + \frac{1}{2} \cdot \frac{1}{2}\right) = \frac{3}{4}$$

Eve will know all the values for which Alice and Bob choose the same basis as she sent and on average 25% of those where they choose a different basis

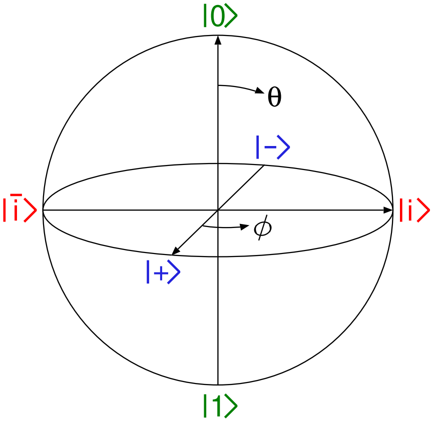
If we assume that on average Alice and Bob choose the same basis as Eve 50% of the time then Eve will know $\frac{3}{4}$ of the bits

Problem 4.2

(a) Show that $R(\alpha)$ is a rotation of 2α about the y-axis of the Bloch sphere

(b) Show that $T(\beta)$ is a rotation of 2β about the z-axis of the Bloch sphere

(c) Find a family of single-qubit transformations that correspond to rotations of 2γ about the x-axis



(a) Recall the spherical representation of a general qubit

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + \sin\left(\frac{\theta}{2}\right)e^{i\phi}|1\rangle$$

Start by applying $R(\alpha)$ to $|0\rangle$ and $|1\rangle$ to see what the transformation does to these two polar vectors

Problem 4.2 (cont.)

$$R(\alpha)|0\rangle = \begin{pmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \cos\alpha \\ -\sin\alpha \end{pmatrix} = \cos\alpha|0\rangle - \sin\alpha|1\rangle$$

$$= \cos\left(\frac{\theta}{2}\right)|0\rangle + \sin\left(\frac{\theta}{2}\right)e^{i\phi}|1\rangle \quad \longrightarrow \quad \theta = 2\alpha, \phi = \pi$$

This is a rotation of 2α from the z-axis in the direction of the negative x-axis, a pure rotation about the y-axis

$$R(\alpha)|1\rangle = \begin{pmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \sin\alpha|0\rangle + \cos\alpha|1\rangle = \cos\left(\frac{\pi}{2} - \alpha\right)|0\rangle + \sin\left(\frac{\pi}{2} - \alpha\right)|1\rangle$$

$$= \cos\left(\frac{\theta}{2}\right)|0\rangle + \sin\left(\frac{\theta}{2}\right)e^{i\phi}|1\rangle \quad \longrightarrow \quad \theta = \pi - 2\alpha, \phi = 0$$

This is a rotation of 2α from the negative z-axis toward the positive x-axis, again a pure rotation about the y-axis

Since both $|0\rangle$ and $|1\rangle$ are rotated by 2α about the y-axis then any superposition will be also

Problem 4.2 (cont.)

(b) We can do the same for the $T(\beta)$ rotation but with the $\{|+\rangle, |-\rangle\}$ basis

$$T(\beta)|+\rangle = \begin{pmatrix} e^{+i\beta} & 0 \\ 0 & e^{-i\beta} \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} e^{+i\beta}|0\rangle + \frac{1}{\sqrt{2}} e^{-i\beta}|1\rangle$$

$$= e^{i\beta}\left(\frac{1}{\sqrt{2}}|0\rangle + e^{-i2\beta}\frac{1}{\sqrt{2}}|1\rangle\right) \longrightarrow \theta = \frac{\pi}{2}, \phi = -2\beta$$

$$T(\beta)|-\rangle = \begin{pmatrix} e^{+i\beta} & 0 \\ 0 & e^{-i\beta} \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \frac{1}{\sqrt{2}} e^{+i\beta}|0\rangle - \frac{1}{\sqrt{2}} e^{-i\beta}|1\rangle$$

$$= e^{i\beta}\left(\frac{1}{\sqrt{2}}|0\rangle - e^{-i2\beta}\frac{1}{\sqrt{2}}|1\rangle\right) \longrightarrow \theta = \frac{\pi}{2}, \phi = \pi - 2\beta$$

This is clearly a pure rotation about the z-axis of -2β in the clockwise direction (as viewed from above for both $|+\rangle$ and $|-\rangle$ so any vector will be rotated accordingly

(c) A rotation of 2γ about the x-axis can be achieved by rotating the x-axis to the z-axis, applying a z-axis rotation, and then rotating back to the original orientation

$$R\left(+\tfrac{\pi}{2}\right) T(\gamma) R\left(-\tfrac{\pi}{2}\right)$$

Problem 4.2 – alternative solution

The problem is relatively straightforward if you know a few identities

The first are the Pauli matrices

$$\hat{\sigma}_x = X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \hat{\sigma}_y = iY = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \hat{\sigma}_z = Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

The second important identity is that in three dimensional space, a rotation by an angle 2θ about an arbitrary unit vector, $\hat{n}$ can be expressed as $e^{i\theta(\hat{n}\cdot\vec{\sigma})}$

In terms of matrix operators this becomes

$$e^{i\theta(\hat{n}\cdot\vec{\sigma})} = I\cos\theta + i(\hat{n}\cdot\vec{\sigma})\sin\theta$$

(a) For $\hat{n} = \hat{y}$ and $\theta = \alpha$ a rotation of 2α is

$$I\cos\alpha + i\hat{\sigma}_y\sin\alpha = \begin{pmatrix} \cos\alpha & 0 \\ 0 & \cos\alpha \end{pmatrix} + i\begin{pmatrix} 0 & -i\sin\alpha \\ i\sin\alpha & 0 \end{pmatrix} = \begin{pmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{pmatrix} = R(\alpha)$$

Problem 4.2 – alternative solution

$$e^{i\theta(\hat{n}\cdot\vec{\sigma})} = I\cos\theta + i(\hat{n}\cdot\vec{\sigma})\sin\theta$$

(b) For $\hat{n} = \hat{z}$ and $\theta = \beta$ a rotation of 2β is

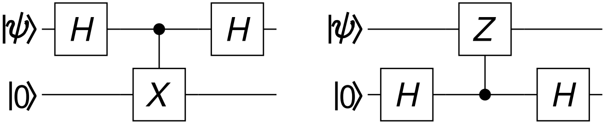
$$\begin{aligned} I\cos\beta + i\hat{\sigma}_z\sin\beta &= \begin{pmatrix} \cos\beta & 0 \\ 0 & \cos\beta \end{pmatrix} + i\begin{pmatrix} \sin\beta & 0 \\ 0 & -\sin\beta \end{pmatrix} \\ &= \begin{pmatrix} \cos\beta + i\sin\beta & 0 \\ 0 & \cos\beta - i\sin\beta \end{pmatrix} = \begin{pmatrix} e^{+i\beta} & 0 \\ 0 & e^{-i\beta} \end{pmatrix} = T(\beta) \end{aligned}$$

(c) For $\hat{n} = \hat{x}$ and $\theta = \gamma$ a rotation of 2γ is

$$I\cos\gamma + i\hat{\sigma}_x\sin\gamma = \begin{pmatrix} \cos\gamma & 0 \\ 0 & \cos\gamma \end{pmatrix} + i\begin{pmatrix} 0 & \sin\gamma \\ \sin\gamma & 0 \end{pmatrix} = \begin{pmatrix} \cos\gamma & i\sin\gamma \\ i\sin\gamma & \cos\gamma \end{pmatrix}$$

Problem 4.6

Compare the effect of the following two circuits

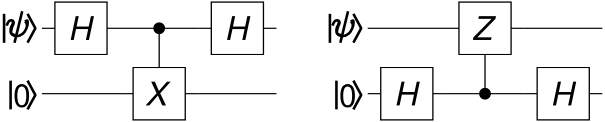


Start with a general state $|\psi\rangle = a|0\rangle + b|1\rangle$ and apply the left side circuit

$$|\psi\rangle|0\rangle \xrightarrow{H\otimes I} \frac{a}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle + \frac{b}{\sqrt{2}}(|0\rangle - |1\rangle) \otimes |0\rangle$$

$$\xrightarrow{C_{not}} \frac{a+b}{\sqrt{2}}|00\rangle + \frac{a-b}{\sqrt{2}}|11\rangle \xrightarrow{H\otimes I} \frac{a+b}{2}(|00\rangle + |10\rangle) + \frac{a-b}{2}(|01\rangle - |11\rangle)$$

Problem 4.6 (cont.)



Now the right side circuit

$$|\psi\rangle|0\rangle \xrightarrow{I\otimes H} (a|0\rangle + b|1\rangle)\otimes\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle) = \frac{1}{\sqrt{2}}\big[a(|00\rangle+|01\rangle)+b(|10\rangle+|11\rangle)\big]$$

$$\xrightarrow{\wedge^{1}_{01} Z} \frac{1}{\sqrt{2}}\big[a(|00\rangle+|01\rangle)+b(|10\rangle-|11\rangle)\big]$$

$$\xrightarrow{I\otimes H} \tfrac{1}{2}\big[a|00\rangle + \cancel{a|01\rangle} + a|00\rangle - \cancel{a|01\rangle} + \cancel{b|10\rangle} + b|11\rangle - \cancel{b|10\rangle} + b|11\rangle = a|00\rangle + b|11\rangle$$

Problem 4.6 (cont.)

Problem 4.6 (cont.)