PREMIUM
...SERIES...

SCHOLAR MATE

In every walk in with nature one receives far more than he seeks. ...

Flowers

PREMIUM QUALITY NOTEBOOK
* Bright and Fine Quality Paper
* Smooth Writing Paper
* 'A' Grade Paper For Long Lasting

KING SIZE

soorajss1729@gmail.com / +91-9400635788

INDEX (5)

NAME : SOORAJ S.

STD : ..... SEC: .....

ROLL No.: ..... SUB: .....

S.No.	Date	Title	Page No.	Teacher's Sign/ Comment
		QUANTUM COMPUTATION		
		& QUANTUM INFORMATION		
		- Nielsen & Chuang		

Ex: 4.37 Provide a decomposition of the transform

$$\frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{bmatrix}$$

$w = i$

into a product of two-level unitaries. This is a special case of the quantum Fourier transform.

Ans: $$V_1 = \begin{bmatrix} \frac{a^*}{\sqrt{|a|^2+|b|^2}} & \frac{+b^*}{\sqrt{|a|^2+|b|^2}} & 0 & 0 \\ \frac{b}{\sqrt{|a|^2+|b|^2}} & \frac{-a}{\sqrt{|a|^2+|b|^2}} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

given $$U = \begin{bmatrix} a & e & i & m \\ b & f & j & n \\ c & g & k & o \\ d & h & l & p \end{bmatrix}$$

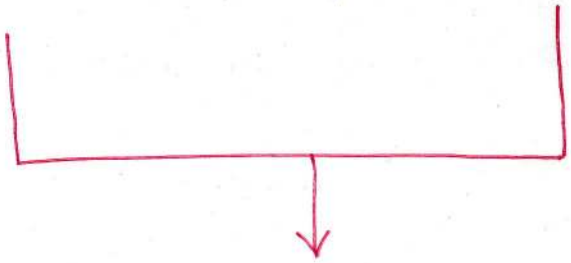
$$V_1 U = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 & 0 \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{bmatrix}$$

$$= \frac{1}{2} \begin{bmatrix} \sqrt{2} & \frac{1+i}{\sqrt{2}} & 0 & \frac{1-i}{\sqrt{2}} \\ 0 & \frac{1-i}{\sqrt{2}} & \sqrt{2} & \frac{1+i}{\sqrt{2}} \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{bmatrix}$$

(13) Single qubit & CNOT gates are universal.

- an arbitrary unitary matrix on a d-D Hilbert space may be written as a product of two-level unitary matrices.

- Single qubit and CNOT gates together can be used to implement an arbitrary two-level unitary operation on the state-space of n qubits.



Single qubit & CNOT gates can be used to implement an arbitrary unitary operation on n qubits. & therefore are universal for quantum computation.

Suppose,

U is a two-level unitary matrix on an n-qubit quantum computer.

Suppose,

U acts non-trivially on the space spanned by the computational basis states $|s\rangle$ and $|t\rangle$, where $s = s_1 \cdots s_n$ and $t = t_1 \cdots t_n$ are the binary expansions for s and t.

Let $\tilde{U}$ be the non-trivial 2×2 unitary submatrix of U.

i.e., $\tilde{U}$ can be thought of as a unitary operator on a single qubit.

We need to construct a circuit implementing U built from single qubit and CNOT gates.

↓

Gray codes.

A Gray code connecting s and t is a sequence of binary numbers, starting with s and concluding with t, such that adjacent numbers of the list differ in exactly one bit.

For instance, with $s = 101001$ & $t = 110011$

Gray code:

$g_1 = 101001$
$g_2 = 101011$
$g_3 = 100011$
$g_4 = 110011$

g_1 thro' g_m be the elements of a Gray code connecting s and t

Basic idea: The quantum circuit implementing U is to perform a sequence of gates effecting the state changes $|g_1\rangle \to |g_2\rangle \to \cdots \to |g_{m-1}\rangle$, then to perform a controlled-$\tilde{U}$ operation, with the target qubit located at the single bit where g_{m-1} and g_m differ, and then to undo the 1st stage, transforming $|g_{m-1}\rangle \to |g_{m-2}\rangle \to \cdots \to |g_1\rangle$.

The 1st step is to swap the states $|g_1\rangle$ and $|g_2\rangle$. Suppose g_1 and g_2 differ at the i^{th} digit. Then we accomplish the swap by performing a controlled bit flip on the i^{th} qubit, conditioned on the values of the other qubits being identical to those in both g_1 and g_2. Next, we use a controlled operation to swap $|g_2\rangle$ and $|g_3\rangle$. We continue in this fashion until we swap $|g_{m-2}\rangle$ with $|g_{m-1}\rangle$. The effect of this sequence of $(m-2)$ operations is to achieve the operation,

$$|g_1\rangle \longrightarrow |g_{m-1}\rangle$$

$$|g_2\rangle \longrightarrow |g_1\rangle$$

$$|g_3\rangle \longrightarrow |g_2\rangle$$

. . . . . .

$$|g_{m-1}\rangle \longrightarrow |g_{m-2}\rangle$$

All other computational basis states are left unchanged by this sequence of operations.

Next,

Suppose g_{m-1} and g_m differ in the j^{th} bit. We apply a controlled-$\tilde{U}$ operation with the j^{th} qubit as target, conditional on the other qubits having the same values as appear in both g_m and g_{m-1}.

Finally,

we complete the U operation by undoing the swap operations: we swap $|g_{m-1}\rangle$ with $|g_{m-2}\rangle$ then $|g_{m-2}\rangle$ with $|g_{m-3}\rangle$ and so on, until we swap $|g_2\rangle$ with $|g_1\rangle$.

Ex:-

$$U = \begin{bmatrix} a & 0 & 0 & 0 & 0 & 0 & 0 & c \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ b & 0 & 0 & 0 & 0 & 0 & 0 & d \end{bmatrix}$$

$\tilde{U} = \begin{bmatrix} a & c \\ b & d \end{bmatrix}$ is a unitary matrix where $a, b, c, d \in \mathbb{C}$.

Qm: U acts non-trivially only on two basis states $|s\rangle = |000\rangle$ and $|t\rangle = |111\rangle$. and the operation on these states gives.

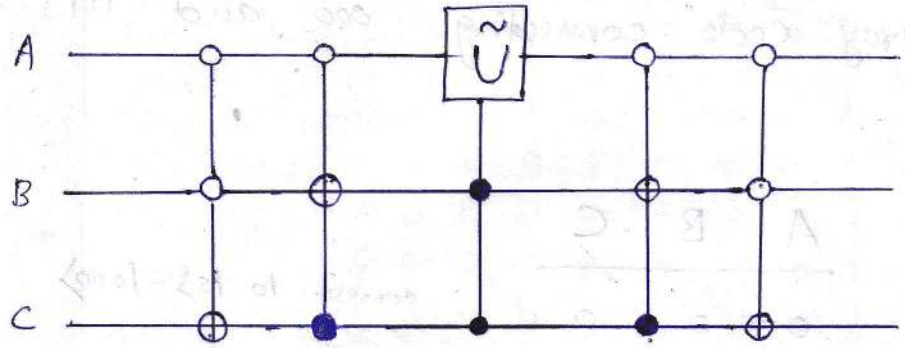
$$U|s\rangle = a|s\rangle + b|t\rangle$$

$$U|t\rangle = c|s\rangle + d|t\rangle$$

A Gray code connecting 000 and 111:

	A	B	C	
g_1	0	0	0	corresp. to $\|s\rangle = \|000\rangle$
	0	0	1	
	0	1	1	
g_m	1	1	1	corresp. to $\|t\rangle = \|111\rangle$

For qubit states, the transformation b/w two adjacent elements in the Gray code is a swap b/w 2 computational basis states.



Step 1:

The 1st two gates shuffle the states so that $|000\rangle$ gets swapped with $|011\rangle$, but $|111\rangle$ remains $|111\rangle$.

$$S = \underbrace{|011\rangle\langle 000| + |000\rangle\langle 001| + |001\rangle\langle 011| +}_{\text{permutation of Gray codes.}}$$

$$+ |010\rangle\langle 010| + |100\rangle\langle 100| + |101\rangle\langle 101| + |110\rangle\langle 110| + |111\rangle\langle 111|$$

trivial action.

This is just a permutation of the computational basis states. Its main purpose is to ensure that $|000\rangle$ becomes $|110\rangle$ but $|111\rangle$ remains $|111\rangle$.

There are also transitions $|001\rangle \rightarrow |000\rangle$ and $|011\rangle \rightarrow |001\rangle$ which I think only serve the purpose of more efficient circuit design because they allow an implementation which uses only CNOT gates without any working qubits.

Step 2: The operation $\tilde{U}$ is applied to the 1st qubit of the states $|011\rangle$ and $|111\rangle$, conditional on the 2nd and 3rd qubits being in the state $|11\rangle$.

Action of the single qubit operation $\tilde{U}$ on the 1st qubit on the states $|011\rangle$ & $|111\rangle$ are:

$$|011\rangle \xrightarrow{\tilde{U}} (a|0\rangle + b|1\rangle)|11\rangle = a|011\rangle + b|111\rangle$$

$$|111\rangle \xrightarrow{\tilde{U}} (c|0\rangle + d|1\rangle)|11\rangle = c|011\rangle + d|111\rangle$$

All other states are left alone

$$\tilde{U} = \underbrace{(a|011\rangle + b|111\rangle)\langle 011| + (c|011\rangle + d|111\rangle)\langle 111|}_{\text{action of single qubit gate}}$$

$$+ |000\rangle\langle 000| + |001\rangle\langle 001| + |010\rangle\langle 010| + |100\rangle\langle 100| + |101\rangle\langle 101| + |110\rangle\langle 110|$$

trivial action.

Step: 3. We unshuffle the states, ensuring that $|011\rangle$ gets swapped back with the state $|000\rangle$.

$$S^{\dagger} = \underbrace{|000\rangle\langle 011| + |001\rangle\langle 000| + |011\rangle\langle 001|}_{\text{undoing permutation of Gray codes.}} +$$

$$+ |010\rangle\langle 010| + |100\rangle\langle 100| + |101\rangle\langle 101| + |110\rangle\langle 110| + |111\rangle\langle 111|$$

trivial action.

Verify

$$\tilde{U}S = (a|011\rangle + b|111\rangle)\langle 000| + (c|011\rangle + d|111\rangle)\langle 111|$$

$$+ |000\rangle\langle 001| + |001\rangle\langle 011| + |010\rangle\langle 010| + |100\rangle\langle 100| +$$

$$|101\rangle\langle 101| + |110\rangle\langle 110|$$

$$S^{\dagger}\tilde{U}S = \underbrace{a|000\rangle\langle 000| + b|111\rangle\langle 000| + c|000\rangle\langle 111| + d|111\rangle\langle 111|}_{\text{non-trivial action}}$$

$$+ |001\rangle\langle 001| + |010\rangle\langle 010| + |011\rangle\langle 011| + |100\rangle\langle 100| + |101\rangle\langle 101|$$

$$+ |110\rangle\langle 110|$$

trivial action.

$$U = \begin{bmatrix} a & 0 & 0 & 0 & 0 & 0 & 0 & c \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ b & 0 & 0 & 0 & 0 & 0 & 0 & d \end{bmatrix}$$

$|s\rangle = |s\rangle = |000\rangle$ & $|t\rangle = |111\rangle$

$|g_1\rangle = |001\rangle$

$|g_2\rangle = |011\rangle$

$|g_3\rangle = |111\rangle$

$U(\alpha|000\rangle + \beta|111\rangle) = U \begin{bmatrix} \alpha \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ \beta \end{bmatrix} = \begin{bmatrix} \alpha' \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ \beta' \end{bmatrix}$

$|011\rangle = |0\rangle \otimes |11\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$

$|111\rangle = |1\rangle \otimes |11\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$

$U(\alpha|011\rangle + \beta|111\rangle) = U(0\,0\,0\,\alpha\,0\,0\,0\,\beta) = \begin{bmatrix} 0 \\ 0 \\ 0 \\ \alpha' \\ 0 \\ 0 \\ 0 \\ \beta' \end{bmatrix}$

$\tilde{U} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \tilde{U}(\alpha|0\rangle + \beta|1\rangle) = \begin{bmatrix} \alpha' \\ \beta' \end{bmatrix}$

$\tilde{U} \otimes I_2 \otimes I_3 (\alpha|011\rangle + \beta|111\rangle) = \alpha \tilde{U}|0\rangle \otimes |11\rangle + \beta \tilde{U}|1\rangle \otimes |11\rangle$

$= \tilde{U}(\alpha|0\rangle + \beta|1\rangle) \otimes |11\rangle = \tilde{U} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} \alpha' \\ \beta' \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$

$= \begin{bmatrix} 0 \\ 0 \\ 0 \\ \alpha' \\ 0 \\ 0 \\ 0 \\ \beta' \end{bmatrix} = U(\alpha|011\rangle + \beta|111\rangle)$

⇒ Implementing the two-level unitary operation U requires at most $2(n-1)$ controlled operations to swap $|g_i\rangle$ with $|g_{m-1}\rangle$ and then back again.

Each of these controlled operations can be realized using $O(n)$ single qubit and CNOT gates.

The controlled-U operation also requires $O(n)$ gates.

⇒ Implementing U requires $O(n^2)$ single qubit and CNOT gates.

An arbitrary unitary matrix on the 2^n-D state space of n qubits may be written as a product of $O(2^{2n}) = O(4^n)$ two-level unitary operations.

$\therefore$

An arbitrary unitary operation on n qubits can be implemented using a circuit containing $O(n^2 4^n)$ single qubit and CNOT gates.

⇒ This construction does not provide terribly efficient quantum circuits.

Ex: 4.39 Find a quantum circuit using single qubit operations and CNOT to implement the transformation.

$$U = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & a & 0 & 0 & 0 & 0 & c \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & b & 0 & 0 & 0 & 0 & d \end{bmatrix}$$

where $\tilde{U} = \begin{bmatrix} a & c \\ b & d \end{bmatrix}$ is an arbitrary 2×2 unitary matrix.

Ans: The unitary matrix U acts non-trivially only on the states $|010\rangle$ and $|111\rangle$.

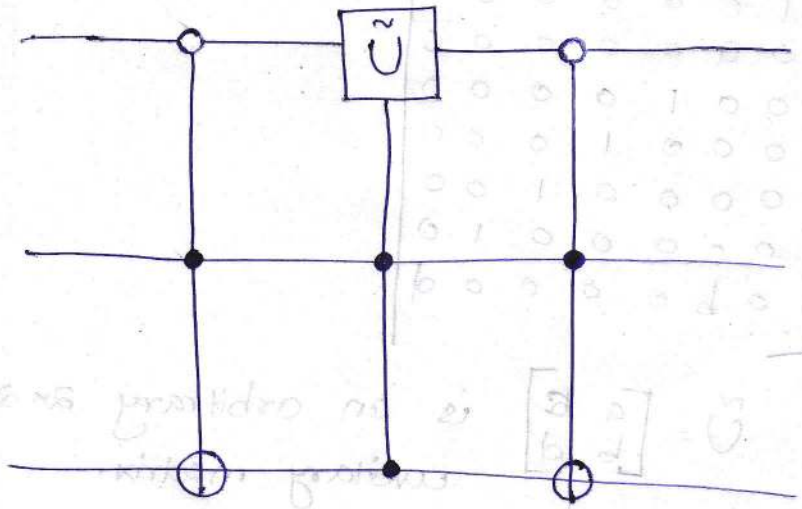
$$U|010\rangle = a|010\rangle + b|111\rangle$$

$$U|111\rangle = c|010\rangle + d|111\rangle$$

Gray code connecting $|010\rangle$ and $|111\rangle$:

A	B	C
0	1	0
0	1	1
1	1	1

The quantum circuit that implements the transformation is:



© A discrete set of universal operations

We proved that the CNOT and single qubit unitaries together form a universal set for quantum computation. Unfortunately, no straightforward method is known to implement all these gates in a fashion which is resistant to errors.

We can find a discrete set of gates which can be used to perform universal quantum computation, and in Chapter 10, we'll show how to perform these gates in an error-resistant fashion, using quantum error correcting codes.

Approximating unitary operators

A discrete set of gates can't be used to implement an arbitrary unitary operation exactly, since the set of unitary operations is continuous. Rather it turns out that a discrete set can be used to approximate any unitary operation.

What it means to approximate a unitary operation ?

Suppose U and V are 2 unitary operators on the same state space.

U is the target unitary operator that we wish to implement, and V is the unitary operator that is actually implemented in practice.

We define the error when V is implemented instead of U by,

$$E(U,V) = \max_{|\psi\rangle} \|(U-V)|\psi\rangle\|$$

where the maximum is over all normalized quantum states $|\psi\rangle$ in the state space.

If $E(U,V)$ is small, then any measurement performed on the state $V|\psi\rangle$ will give approximately the same measurement statistics as a measurement of $U|\psi\rangle$, for any initial state $|\psi\rangle$.

$$|P_U - P_V| \leq 2E(U,V) \qquad 4.62$$

Proof

where, $E(U,V) = \|U-V\| = \max_{|\psi\rangle \neq 0} \|(U-V)|\psi\rangle\|$

Suppose a quantum system starts in the state $|\psi\rangle$, and we perform either the unitary operation U, or the unitary operation V. Following this, we perform a measurement.

Let M be a POVM element associated with the measurement, and let P_U (or P_V) be the probability of obtaining the corresp. measurement outcome if the operation U (or V) was performed. Then,

$$|P_U - P_V| = |\langle\psi|U^\dagger M U|\psi\rangle - \langle\psi|V^\dagger M V|\psi\rangle|$$

$$= |\langle\psi|U^\dagger M U|\psi\rangle - \langle\psi|U^\dagger M V|\psi\rangle + \langle\psi|U^\dagger M V|\psi\rangle - \langle\psi|V^\dagger M V|\psi\rangle|$$

$$= |\langle\psi|U^\dagger M (U-V)|\psi\rangle + \langle\psi|(U-V)^\dagger M V|\psi\rangle|$$

Let $|\Delta\rangle = (U-V)|\psi\rangle$, then

$$E(U,V) \geq |(U-V)|\psi\rangle|$$
$$E(U,V) \geq \||\Delta\rangle\|$$

$$|P_U - P_V| = |\langle\psi|U^\dagger M|\Delta\rangle + \langle\Delta|MV|\psi\rangle|$$

$$\leq |\langle\psi|U^\dagger M|\Delta\rangle| + |\langle\Delta|MV|\psi\rangle|$$

- Cauchy Schwarz inequality,

$$|\langle u|v\rangle| \leq \||u\rangle\| \cdot \||v\rangle\|$$

- $\|A\| = \max_{|\alpha\rangle \neq 0} \frac{\|A|\alpha\rangle\|}{\||\alpha\rangle\|} = \sigma_1$, largest singular value of the matrix A

$$\|A\| \geq \frac{\|A|\alpha\rangle\|}{\||\alpha\rangle\|} \longrightarrow \|A|\alpha\rangle\| \leq \|A\| \cdot \||\alpha\rangle\|$$

ILA (10)

M is an element of a POVM.

$\Rightarrow M$ is positive definite.

$$\sum M = \underline{I} \quad \& \quad \lambda_i^M \geq 0$$

Starke
13/10/2021

$\Rightarrow I - M$ is positive definite

I & M are simultaneously diagonalizable.

$$\lambda^{I-M} = 1 - \lambda^M \geq 0.$$

$$\Rightarrow \lambda^M \leq 1 \quad \& \quad \lambda^M \geq 0.$$

$$\therefore 0 \leq \lambda^M \leq 1$$

$$\lambda_{max}^{M} = \|M\| \leq 1$$

$$|\langle\psi|U^{\dagger}M|\Delta\rangle| \leq \|\langle\psi|U^{\dagger}\| \cdot \|M|\Delta\rangle\| = \|M|\Delta\rangle\|$$

$$\leq \|M\| \cdot \||\Delta\rangle\| \leq \||\Delta\rangle\|$$

$$|\langle\Delta|MV|\psi\rangle| \leq \|\langle\Delta|M\| \cdot \|V|\psi\rangle\| = \|\langle\Delta|M\|$$

$$= \|M|\Delta\rangle\| \leq \||\Delta\rangle\|.$$

$\therefore$

$$|P_U - P_V| = |\langle\psi|U^{\dagger}M|\Delta\rangle + \langle\Delta|MV|\psi\rangle|$$

$$\leq |\langle\psi|U^{\dagger}M|\Delta\rangle| + |\langle\Delta|MV|\psi\rangle|$$

$$\leq \|M|\Delta\rangle\| + \|M|\Delta\rangle\|$$

$$\leq \||\Delta\rangle\| + \||\Delta\rangle\| = 2\||\Delta\rangle\| \leq 2E(U,V)$$

$\Rightarrow$ When the error $E(U,V)$ is small, the difference in probabilities b/w measurement outcomes is small.

Suppose we perform a sequence $V_1, V_2, \ldots, V_m$ of gates intended to approximate some other sequence of gates $U_1, U_2, \ldots, U_m$.

Then it turns out that the error caused by the entire sequence of imperfect gates is at most the sum of the errors in the individual gates.

$$E(U_m U_{m-1} \cdots U_1, V_m V_{m-1} \cdots V_1) \leq \sum_{j=1}^{m} E(U_j, V_j) \qquad 4.63$$

i.e., the errors add at most linearly.

Proof.

For $m = 2$, for some state $|\psi\rangle$ we have

$$E(U_2 U_1, V_2 V_1) = \|(U_2 U_1 - V_2 V_1)|\psi\rangle\|$$
$$= \|(U_2 U_1 - V_2 U_1)|\psi\rangle + (V_2 U_1 - V_2 V_1)|\psi\rangle\|$$

Triangle inequality,

$$\| |a\rangle + |b\rangle \| \leq \| |a\rangle \| + \| |b\rangle \|$$

$$E(U_2 U_1, V_2 V_1) \leq \| (U_2 - V_2) U_1 |\psi\rangle \| + \| V_2 (U_1 - V_1) |\psi\rangle \|$$

$$\leq E(U_2, V_2) + E(U_1, V_1)$$

Apply induction.

If M is a POVM element in an arbitrary POVM, and P_U (or P_V) is the probability of obtaining this outcome if U (or V) were performed with a starting state $|\psi\rangle$, then

$$|P_U - P_V| \leq 2E(U,V)$$

where,

$$E(U,V) = \max_{|\psi\rangle \neq 0} \|(U-V)|\psi\rangle\| = \|U-V\|$$

is the error when V is implemented instead of U.

If we perform a sequence of gates $V_1, \ldots, V_m$ intended to approximate some other sequence of gates $U_1, \ldots, U_m$, then the errors add at most linearly.

$$E(U_m \cdots U_1, V_m \cdots V_1) \leq \sum_{j=1}^{m} E(U_j, V_j)$$

⟹ Suppose we wish to perform a quantum circuit containing m gates, U_1 through U_m. Unfortunately, we are only able to approximate the gate U_j by the gate V_j. In order that the probabilities of different measurement outcomes obtained from the approximate circuit be within a tolerance $\Delta > 0$ of the correct probabilities, it suffices that

$$E(U_j, V_j) \leq \Delta / 2m$$

$$E(U_3 \cdots U_1, V_3 \cdots V_1) \leq \sum_{j=1}^{3} E(U_j, V_j) \leq \frac{\Delta}{2}$$

$$\left| P_{U_1 \cdots U_3} - P_{V_1 \cdots V_3} \right| \leq 2E\left(U_3 \cdots U_1, V_3 \cdots V_1\right) \leq \Delta$$

☐ Universality of Hadamard + phase + CNOT + $\pi/8$ gates.

two discrete sets of gates which are universal

Standard set of universal gates.

consists of the

Hadamard, Phase, CNOT, $\pi/8$ gates

- Fault-tolerant constructions for these gates in Chapter 10.

Hadamard, phase, CNOT, Toffoli gates

Hadamard

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \frac{X+Z}{\sqrt{2}}$$

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

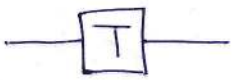
Phase gate

$$S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$$

$$S|0\rangle = |0\rangle$$

$$S|1\rangle = i|1\rangle = e^{i\pi/2}|1\rangle$$

$\pi/8$ gate (T gate)



$$T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$$

$$T|0\rangle = |0\rangle$$

$$T|1\rangle = e^{i\pi/4}|1\rangle$$

CNOT gate

$$U_{cN} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X$$

$$= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

- Hadamard & $\pi/8$ gates can be used to approximate any single qubit unitary operation to arbitrary accuracy.

Proof.

Consider the gates T and HTH.

$$T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix} = e^{i\pi/8} \begin{bmatrix} e^{-i\pi/8} & 0 \\ 0 & e^{i\pi/8} \end{bmatrix} = e^{i\pi/8} R_z(\pi/4)$$

Ex: 4.3

Q.C (3) M

Ex: 4.14

$\Rightarrow$ T is, up to an unimportant global phase, a rotation by $\pi/4$ radians around the $\hat{z}$-axis on the Bloch sphere.

$$HTH = H e^{i\pi/8} R_z(\pi/4) H$$

$$= e^{i\pi/8} \cdot H R_z(\pi/4) H$$

$$= e^{i\pi/8} H e^{-i\pi/8 Z} H$$

$$= e^{i\pi/8} H \left[I - \frac{i\pi}{8} Z - \frac{1}{2!}\left(\frac{\pi Z}{8}\right)^2 + \cdots \right] H$$

$$= e^{i\pi/8} \left[H^2 - \frac{i\pi}{8} HZH - \frac{1}{2!}\left(\frac{\pi}{8}\right)^2 HZ^2H + \cdots \right]$$

Q.C (3) / M

$HXH = Z$; $HYH = -Y$; $HZH = X$

$HZ^2H = X^2$

Ex. 4.14

$$HTH = e^{i\pi/8} \left[I - i\frac{\pi}{8} X - \frac{1}{2!}\left(\frac{\pi}{8}\right)^2 X^2 + \cdots \right]$$

$$= e^{i\pi/8} \cdot e^{-i\frac{\pi}{8}X} = e^{i\pi/8} R_x(\pi/4)$$

$\Longrightarrow$ HTH is a rotation by $\pi/4$ radians around the $\hat{x}$-axis on the Bloch sphere.

$$R_z(\pi/4)\,R_x(\pi/4) = \exp\left[-i\frac{\pi}{8}Z\right]\times\exp\left[-i\frac{\pi}{8}X\right]$$

$$= \left(\cos\frac{\pi}{8}I - i\sin\frac{\pi}{8}Z\right)\left(\cos\frac{\pi}{8}I - i\sin\frac{\pi}{8}X\right)$$

$$= \cos^2\frac{\pi}{8}I - i\left[\cos\frac{\pi}{8}(X+Z)\right]\sin\frac{\pi}{8} - \sin^2\frac{\pi}{8}\underbrace{ZX}_{iY}$$

$$= \cos^2\frac{\pi}{8}I - i\left[\cos\frac{\pi}{8}(X+Z) + \sin\frac{\pi}{8}Y\right]\sin\frac{\pi}{8}$$

$$= \cos^2\frac{\pi}{8}I - i\left[\cos\frac{\pi}{8}X + \sin\frac{\pi}{8}Y + \cos\frac{\pi}{8}Z\right]\sin\frac{\pi}{8}$$

$$= \cos^2\frac{\pi}{8}I - i(\vec{n}\cdot\vec{\sigma})\sin\pi/8$$

where $\vec{n} = \left(\cos\pi/8, \sin\pi/8, \cos\pi/8\right)$ & $\vec{\sigma} = (X, Y, Z)$

$$|\vec{n}| = \sqrt{1+\cos^2\pi/8} \quad\Longrightarrow\quad \hat{n} = \frac{\left(\cos\pi/8, \sin\pi/8, \cos\pi/8\right)}{\sqrt{1+\cos^2\pi/8}}$$

$$\cos\theta/2 \equiv \cos^2\pi/8 \quad\Longrightarrow\quad \sin\theta/2 = \sqrt{1-\left(\cos^2\theta/2\right)^2} = \sqrt{1-\cos^4\pi/8}$$

$$= \sqrt{\left(1-\cos^2\pi/8\right)\left(1+\cos^2\pi/8\right)}$$

$$= \sin\pi/8\sqrt{1+\cos^2\pi/8}$$

$$R_{\hat{z}}(\pi/4)\, R_{\hat{x}}(\pi/4) = \cos^2\pi/8\, I - i\, \frac{(\cos\pi/8\, X + \sin\pi/8\, Y + \cos\pi/8\, Z)}{\sqrt{1+\cos^2\pi/8}} \times \sin\pi/8\sqrt{1+\cos^2\pi/8}$$

$$= \cos^2\theta/2\, I - i(\hat{n}\cdot\vec{\sigma})\sin\theta/2. \quad = R_{\hat{n}}(\theta)$$

This is a rotation of the Bloch sphere about an axis along $\vec{n} = (\cos\pi/8, \sin\pi/8, \cos\pi/8)$ with corresp. unit vector $\hat{n}$, and thro' an angle θ defined by $\cos(\theta/2) \equiv \cos^2\pi/8$.

$$T = e^{i\pi/8} R_{\hat{z}}(\pi/4) \quad \& \quad HTH = e^{i\pi/8} R_{\hat{x}}(\pi/4)$$

$\Rightarrow$ Using only the Hadamard and $\pi/8$ gates we can construct $R_{\hat{n}}(\theta)$. such that $\cos\theta/2 \equiv \cos^2\pi/8$.

* θ is an irrational multiple of 2π given

$\cos\theta/2 \equiv \cos^2(\pi/8)$

Stated 16/10/2021

Proof required 16/10/2021

Repeated iteration of $R_{\hat{n}}(\theta)$ can be used approximate to arbitrary accuracy any rotation $R_{\hat{n}}(\alpha)$.

Part 1: Achieving arbitrarily fine approximations of all angles.

- one can achieve arbitrarily fine approximations of all angles using a rotation by an irrational multiple of π

Let $\delta > 0$ be the desired accuracy &
let N be an integer larger than $2\pi/\delta$.

i.e., $\frac{2\pi}{N} < \delta$

Define θ_k so that $\theta_k = (k\theta) \bmod 2\pi$

$\theta_k = (k\theta) \operatorname{div} (2\pi) \iff$

$$\begin{array}{r|l} & t_k \\ \hline 2\pi & k\theta \\ \hline & \theta_k \end{array}$$

$$k\theta = 2\pi t_k + \theta_k$$

θ is an irrational multiple of 2π

$$\theta = 2\pi t_1 + \theta_1$$
$$2\theta = 2\pi t_2 + \theta_2$$
$$3\theta = 2\pi t_3 + \theta_3$$
$$\vdots$$
$$k\theta = 2\pi t_k + \theta_k$$

$\Big\}$ $\theta_k \in [0, 2\pi)$

$$(j+1)\theta = j\theta + \theta = 2\pi(t_j + t_1) + (\theta_j + \theta_1)$$

~~$\theta_{j+1} = \theta_j + \theta_1 = 2\pi(t_j + t_1) + (\theta_j + \theta_1)$~~

What if θ_k exceeds $2\pi k$,

$n\theta_1 = 2\pi t + k\theta_1$

$\theta_1(n-k) = 2\pi t \Rightarrow$ Not possible as θ_1 is irrational

$n\theta_k = 2\pi t + \theta_k \Rightarrow (n-1)\theta_k = 2\pi t$

Not possible

θ is an irrational multiple of 2π

$\Rightarrow \theta_k$ is irrational.

$\therefore \theta_k \neq 2\pi$ & there will be no repeats in the θ_k values.

Stack
17/10/2021

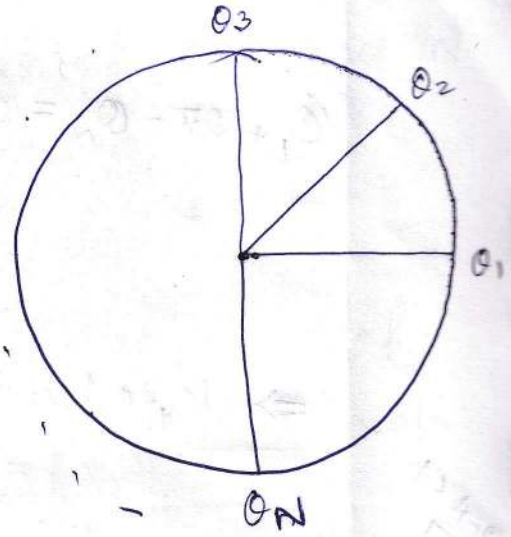
By pigeonhole principle, the θ_k split the unit circle into N subintervals whose boundaries are the θ_j values.

They are most spread apart when they are equally distributed on the circle.

∴

At least 2 θ_i, θ_j are at most $2\pi/N$ radians apart in absolute difference

(OR)



Assume that θ_k are sorted & assume that $\theta_1 = 0$ because we can rotate (i.e., subtract) all points on the circle without changing distance.

Then,

assume that, $\theta_{k+1} - \theta_k > \frac{2\pi}{N}$

for all $1 \leq k \leq N$

Then,

$$\theta_N > (N-1)\frac{2\pi}{N}$$

$$-\theta_N < -(N-1)\frac{2\pi}{N}$$

$$\theta_1 + 2\pi - \theta_N = 2\pi - \theta_N < 2\pi - (N-1)\frac{2\pi}{N}$$

$$= 2\pi\left(\frac{N-(N-1)}{N}\right) = \frac{2\pi}{N}$$

$$\Rightarrow |\theta_N - \theta_1| < \frac{2\pi}{N}$$

(OR) θ is an irrational multiple of 2π and k be an integer. $\theta_k = (k\theta) \bmod 2\pi$

Define θ_k so that $k\theta = \theta_k \pmod{2\pi}$

$\therefore \quad k\theta = 2\pi t_k + \theta_k \quad \forall \quad k = 0, 1, \ldots, N$

where $t_k \in \mathbb{Z}$ and $\theta_k \in [0, 2\pi)$

We can divide the interval $[0, 2\pi)$ into N smaller intervals of measure $2\pi/N$.

$\therefore$ We have $(N+1)$ number of θ_k and N intervals.

The Pigeonhole principle $\Rightarrow$ At least two of θ_k's are in the same interval.
say, θ_i & θ_j with $i \neq j$

$$|\theta_i - \theta_j| < \frac{2\pi}{N}$$

$\Rightarrow$ There are distinct j and k in the range $1, \ldots, N$ such that

$$|\theta_k - \theta_j| \leq \frac{2\pi}{N} < \delta.$$

Without loss of generality assume that $k > j$.

$$\left.\begin{aligned} k\theta &= 2\pi t_k + \theta_k \\ j\theta &= 2\pi t_j + \theta_j \end{aligned}\right\} \quad \theta(k-j) = 2\pi(t_k - t_j) + (\theta_k - \theta_j)$$
$$= 2\pi t_{k-j} + \theta_{k-j}$$

$$\Longrightarrow |\theta_k - \theta_j| = |\theta_{k-j}| < \delta$$

Since $j \neq k$ and θ is an irrational multiple of 2π we must have $\theta_{k-j} \neq 0$.

$k\theta = 2\pi t_k + \theta_k$ & $j\theta = 2\pi t_j + \theta_j = 2\pi t + \theta_k$.

where, $\theta_j = 2\pi t' + \theta_k$

$\theta_j - \theta_k = 2\pi t$! Not possible since θ_j, θ_k are irrational.

Stack-QC
20/10/2021.

→ $(k-j)\theta = 2\pi t_{k-j} + \theta_{k-j}$

$l(k-j)\theta = 2\pi t_{l(k-j)} + \theta_{l(k-j)} = l\left[2\pi t_{k-j} + \theta_{k-j}\right]$

$l\theta_{k-j} = 2\pi\left(t_{l(k-j)} - lt_{k-j}\right) + \theta_{l(k-j)}$

$l\theta_{k-j} = 2\pi t + \theta_{l(k-j)}$

$$(l+1)\theta_{k-j} = 2\pi t + \theta_{(l+1)(k-j)}$$

$$l\theta_{k-j} = 2\pi t + \theta_{l(k-j)}$$

$$\theta_{k-j} = \theta_{(l+1)(k-j)} - \theta_{l(k-j)} < \delta$$

$\Rightarrow$ the sequence $\theta_{l(k-j)}$ fills up the interval $[0, 2\pi)$ as l is varied, so that adjacent members of the sequence are no more than δ apart.

ie.,

the elements of the sequence $\theta_{l(k-j)}$ are less than δ apart and end up filling the interval $[0, 2\pi)$ with density at least one element every δ.

Briefly ↓

The set $\Theta = \{\theta_k : \theta_k = (k\theta) \bmod 2\pi\}$

of angles of rotations around $\hat{n}$ attainable by $\left(R_{\hat{n}}(\theta)\right)^k = R_{\hat{n}}(k\theta)$ for $k \in \mathbb{Z}$ fills up the interval $[0, 2\pi)$ in the sense that for any rotation angle α and any desired accuracy $\delta > 0$ there exists $\tilde{\theta} \in \Theta$ such that $|\alpha - \tilde{\theta}| < \delta$.

i.e., the set of attainable angles Θ contains arbitrarily fine approximations of all angles.

Part 2: Reducing gate approximation to angle approximation

- reduces the problem of approximating the rotation gate $R_{\hat{n}}(\alpha)$ to the problem of approximating the rotation angle α.

It is defined that the error when V is implemented instead of U is:

$$E(U,V) = \max_{|\psi\rangle \neq 0} \|(U-V)|\psi\rangle\| = \|U-V\|$$

i.e., $E(U,V) = \|(U-V)|\phi\rangle\|$ for some $|\phi\rangle$.

$$E\left(R_{\hat{n}}(\alpha), R_{\hat{n}}(\alpha+\beta)\right) = \|(R_{\hat{n}}(\alpha) - R_{\hat{n}}(\alpha+\beta))|\phi\rangle\| \quad \text{for some } |\phi\rangle$$

$$= \|(R_{\hat{n}}(\alpha) - R_{\hat{n}}(\alpha) R_{\hat{n}}(\beta))|\phi\rangle\|$$

$$= \|R_{\hat{n}}(\alpha)(1 - R_{\hat{n}}(\beta))|\phi\rangle\|$$

$$= \sqrt{\langle\phi| \left[1 - R_{\hat{n}}(\beta)\right]^{\dagger} R_{\hat{n}}^{\dagger}(\alpha) R_{\hat{n}}(\alpha) \left[1 - R_{\hat{n}}(\beta)\right] |\phi\rangle}$$

$$= \sqrt{\langle\phi| \left[1 - R_{\hat{n}}^{\dagger}(\beta)\right]\left[1 - R_{\hat{n}}(\beta)\right] |\phi\rangle}$$

$$= \sqrt{\langle\phi| \left[1 - R_{\hat{n}}(-\beta)\right]\left[1 - R_{\hat{n}}(\beta)\right] |\phi\rangle}$$

$$= \sqrt{\langle\phi| 1 - R_{\hat{n}}(\beta) - R_{\hat{n}}(-\beta) + 1 |\phi\rangle}$$

$$= \sqrt{2 - 2\cos(\beta/2)}$$

$$= \left|1 - \exp\left(i\beta/2\right)\right|$$

$$\left|1 - \exp(i\beta/2)\right| = \left|1 - \cos\beta/2 - i\sin\beta/2\right| = \sqrt{1 - 2\cos\beta/2 + \cos^2\beta/2 + \sin^2\beta/2}$$

$$= \sqrt{2 - 2\cos\beta/2}$$

$$E\left(R_{\hat{n}}(\alpha), R_{\hat{n}}(\alpha+\beta)\right) = \left|1 - \exp\left(i\beta/2\right)\right| \quad \text{— Eq}^{n}.\ 4.77$$

$$\lim_{\beta \to 0} E\left(R_{\hat{n}}(\alpha), R_{\hat{n}}(\alpha+\beta)\right) = \lim_{\beta \to 0} \left|1 - \exp\left(i\beta/2\right)\right| = 0$$

$\Rightarrow$ If we can apply a rotation around $\hat{n}$ by an angle that approximates the rotation angle α to arbitrary accuracy then we can approximate $R_{\hat{n}}(\alpha)$ to arbitrarily small error E.

⟹ Part 1 proves that we can indeed approximate the rotation angle α arbitrarily well using repeated applications of $R_{\hat{n}}(\theta)$, as long as θ is an irrational multiple of π.

Part 2 proves if we can approximate the rotation angle α arbitrarily well then we can approximate $R_{\hat{n}}(\alpha)$ to arbitrarily small error E.

∴ For any $\epsilon > 0$ there exists an n such that

$$E\left(R_{\hat{n}}(\alpha), R^{n}_{\hat{n}}(\theta)\right) < \epsilon/3$$

— 4.76

i.e.,

Since we can approximate any angle α with arbitrary accuracy δ, then we can execute $R_{\hat{n}}(\alpha)$ with arbitrary accuracy by choosing δ to be so small that $E\left(R_{\hat{n}}(\alpha), R^{n}_{\hat{n}}(\theta)\right) < \epsilon/3$. This is possible because $\lim_{\gamma \to \alpha} E\left(R_{\hat{n}}(\alpha), R_{\hat{n}}(\gamma)\right) = 0$.

$HXH = Z$, $HYH = -Y$, $HZH = X$, $H^2 = I$

$$H R_{\hat{n}}(\alpha) H = H\left[\cos\frac{\alpha}{2} I - i(\hat{n}\cdot\vec{\sigma}) \sin\frac{\alpha}{2}\right] H$$

where $\vec{n} = (\cos\pi/8, \sin\pi/8, \cos\pi/4)$ & $\hat{n} = \frac{\vec{n}}{|\vec{n}|}$ and

$\vec{\sigma} = (X, Y, Z)$

$$= H\left[\cos\frac{\alpha}{2} I - \frac{i}{|\vec{n}|}\left(X\cos\pi/8 + Y\sin\pi/8 + Z\cos\pi/8\right)\sin\frac{\alpha}{2}\right] H$$

$$= \cos\frac{\alpha}{2} H^2 - \frac{i}{|\vec{n}|}\left(HXH\cos\frac{\pi}{8} + HYH\sin\pi/8 + HZH\cos\pi/8\right)\sin\frac{\alpha}{2}$$

$$= \cos\frac{\alpha}{2} I - \frac{i}{|\vec{n}|}\left(Z\cos\pi/8 - Y\sin\pi/8 + X\cos\pi/8\right)\sin\alpha/2$$

$$= \cos\frac{\alpha}{2} I - \frac{i}{|\vec{n}|}\left(X\cos\pi/8 - Y(-\sin\pi/8) + Z\cos\pi/8\right)\sin\alpha/2$$

$$= \cos\frac{\alpha}{2} I - i\frac{(\vec{m}\cdot\vec{\sigma})}{|\vec{m}|}\sin\frac{\alpha}{2}$$

$$= \cos\frac{\alpha}{2} I - i(\hat{m}\cdot\vec{\sigma})\sin\frac{\alpha}{2} = R_{\hat{m}}(\alpha)$$

where $\vec{m} = (\cos\pi/8, -\sin\pi/8, \cos\pi/8)$ & $|\vec{m}| = |\vec{n}|$.

$\Rightarrow$ For any α,

$$H R_{\hat{n}}(\alpha) H = R_{\hat{m}}(\alpha)$$

where $\hat{m}$ is a unit vector in the direction $\vec{m} = (\cos\pi/8, -\sin\pi/8, \cos\pi/8)$.

$$E\left(R_{\hat{m}}(\alpha), R_{\hat{m}}(\alpha+\beta)\right) = \sqrt{2 - 2\cos(\beta/2)} = \left|1 - \exp\left(i\beta/2\right)\right|$$

$$= E\left(R_{\hat{n}}(\alpha), R_{\hat{n}}(\alpha+\beta)\right)$$

&

From part 1, we can approximate the rotation angle α arbitrarily well using repeated applications of $R_{\hat{m}}(\theta) = H R_{\hat{n}}(\theta) H$ as long as θ is an irrational multiple of π.

$$\Longrightarrow \quad E\left(R_{\hat{m}}(\alpha),\ R_{\hat{m}}(\theta)^{n}\right) < \epsilon/3$$

4.79

From Ex: 4.11, an arbitrary unitary U on a single qubit may be written as:

$$U = R_{\hat{n}}(\beta)\, R_{\hat{m}}(\gamma)\, R_{\hat{n}}(\delta)$$

upto an unimportant global phase shift.

$$\Rightarrow \quad E\left(R_{\hat{m}}(\alpha),\ R_{\hat{m}}(\theta)^n\right) < \epsilon/3$$

4.79

From Ex: 4.11, an arbitrary unitary U on a single qubit may be written as:

$$U = R_{\hat{n}}(\beta)\, R_{\hat{m}}(\gamma)\, R_{\hat{n}}(\delta)$$

upto an unimportant global phase shift.

Eq. 4.63 says,

$$E(U_m U_{m-1} \cdots U_1, V_m V_{m-1} \cdots V_1) \leq \sum_{j=1}^{m} E(U_j, V_j)$$

& Together with Eq. 4.76 and 4.79.

$$E\left(R_{\hat{n}}(\alpha), R_{\hat{n}}(\theta)\right) < \epsilon/3 \quad \& \quad E\left(R_{\hat{m}}(\alpha), R_{\hat{m}}(\hat{\theta})\right) < \epsilon/3$$

& $U = R_{\hat{n}}(\beta)\, R_{\hat{m}}(\gamma)\, R_{\hat{n}}(\delta)$

$$E(U,V) = E\left(U, R_{\hat{n}}(\theta)^{n_1} R_{\hat{m}}(\theta)^{n_2} R_{\hat{n}}(\theta)^{n_3}\right)$$

$$= E\left(R_{\hat{n}}(\beta) R_{\hat{m}}(\gamma) R_{\hat{n}}(\delta), R_{\hat{n}}(\theta)^{n_1} R_{\hat{m}}(\theta)^{n_2} R_{\hat{n}}(\theta)^{n_3}\right)$$

$$\leq E\left(R_{\hat{n}}(\beta), R_{\hat{n}}(\theta)^{n_1}\right) + E\left(R_{\hat{m}}(\gamma), R_{\hat{m}}(\theta)^{n_2}\right) + E\left(R_{\hat{n}}(\delta), R_{\hat{n}}(\theta)^{n_3}\right)$$

$$= \epsilon/3 + \epsilon/3 + \epsilon/3 = \epsilon$$

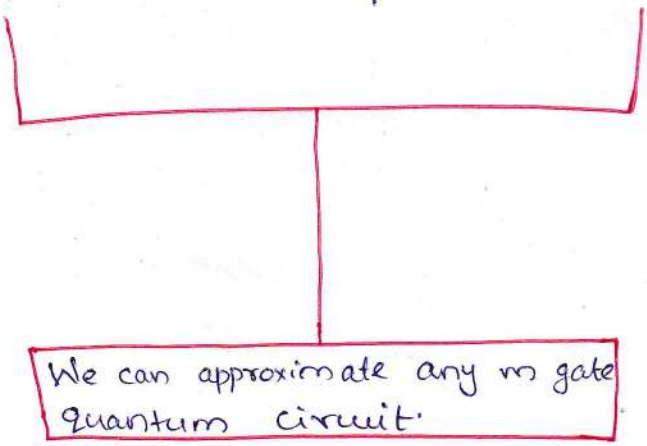
$\Rightarrow$ For suitable positive integers n_1, n_2, n_3

$$E\left(U, R_{\hat{n}}(\theta)^{n_1} H R_{\hat{n}}(\theta)^{n_2} H R_{\hat{n}}(\theta)^{n_3}\right) < \epsilon$$

$\therefore$ Given any single qubit unitary operator U & any $\epsilon > 0$, it is possible to approximate U to within ϵ using a circuit composed of Hadamard gates and $\pi/8$ gates alone.

- Single qubit & CNOT gates can be used to implement an arbitrary unitary operation on n-qubits

- $\pi/8$ and Hadamard gates allow us to approximate any single qubit unitary operator.



- Given a quantum circuit containing m gates, either CNOTs or single qubit unitary gates, we may approximate it using Hadamard, controlled-NOT and $\pi/8$ gates.

Later, we'll find that phase gates make it possible to do the approximation fault-tolerantly, But for the present universality argument they are not strictly necessary.

If we desire an accuracy of ϵ for the entire circuit, then this may be achieved by approximating each single qubit unitary using the above procedure to within ϵ/m & applying the chaining inequality (4.63) to obtain an accuracy of ϵ for the entire circuit.

□ Hadamard + phase + CNOT + Toffoli gates are universal.

Ex: 4.41

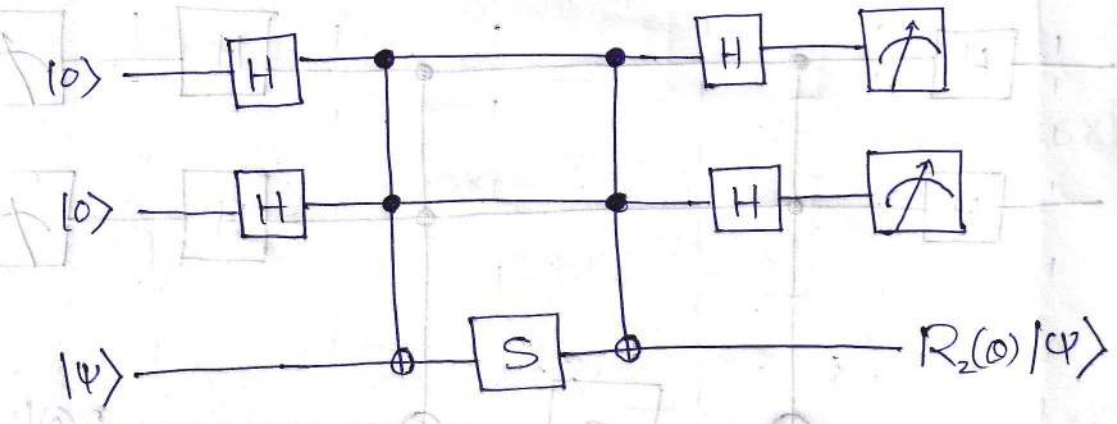
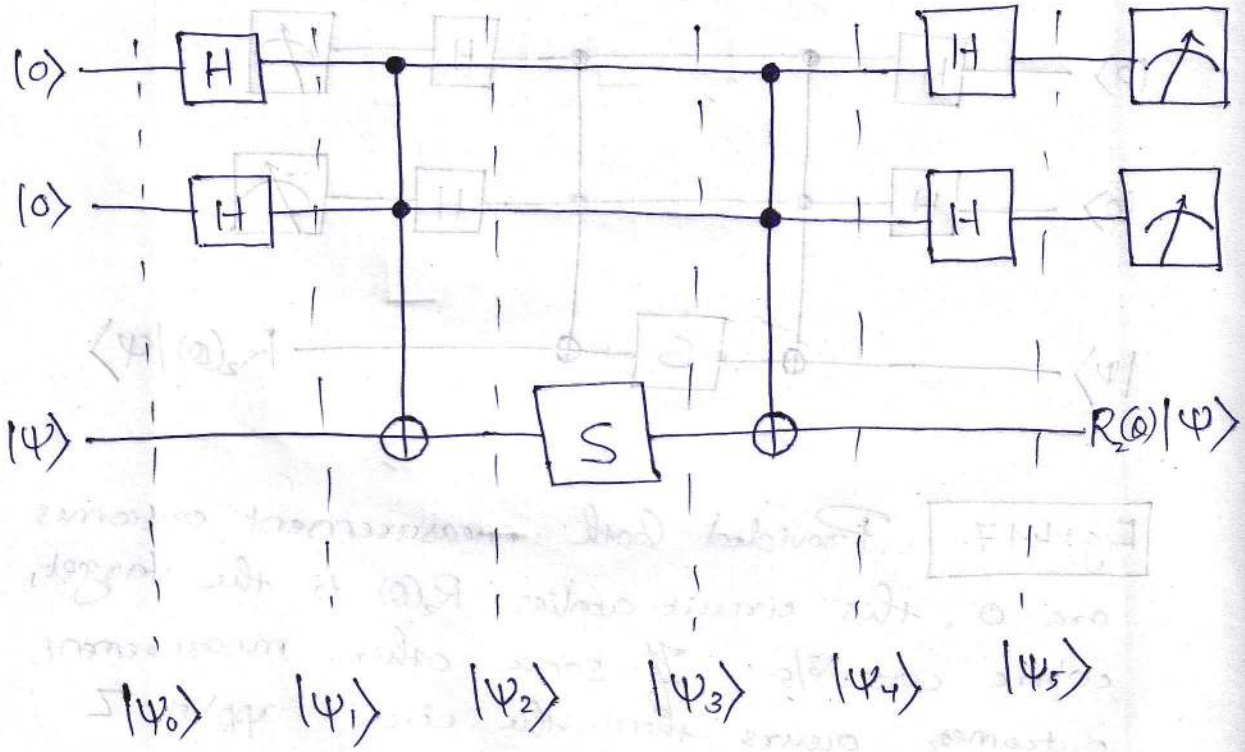


Fig: 4.17 Provided both measurement outcomes are 0, this circuit applies $R_z(\theta)$ to the target, where $\cos\theta = 3/5$. If some other measurement outcomes occurs then the circuit applies Z to the target.

— Proof.

Show that the probability of both measurement outcomes being 0 is 5/8, and explain how repeated use of this circuit and $Z = S^2$ gates may be used to apply a $R_z(\theta)$ gate with probability approaching 1.

Ans:



$$|\psi_0\rangle = |0\rangle \otimes |0\rangle \otimes |\psi\rangle$$

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |\psi\rangle$$

$$= \frac{1}{2}(|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) \otimes |\psi\rangle$$

$$|\psi_2\rangle = \frac{1}{2}\left[|0\rangle \otimes (|0\rangle + |1\rangle) \otimes |\psi\rangle + |1\rangle \otimes |0\rangle \otimes |\psi\rangle + |1\rangle \otimes |1\rangle \otimes X|\psi\rangle\right]$$

$$|\psi_3\rangle = \frac{1}{2}\left[|0\rangle \otimes (|0\rangle + |1\rangle) \otimes S|\psi\rangle + |1\rangle \otimes |0\rangle \otimes S|\psi\rangle + |1\rangle \otimes |1\rangle \otimes SX|\psi\rangle\right]$$

$$|\psi_4\rangle = \frac{1}{2}\left[|0\rangle \otimes (|0\rangle + |1\rangle) \otimes S|\psi\rangle + |1\rangle \otimes |0\rangle \otimes S|\psi\rangle + |1\rangle \otimes |1\rangle \otimes XSX|\psi\rangle\right]$$

$$|\psi_5\rangle = \frac{1}{4}\left[(|0\rangle + |1\rangle) \otimes |0\rangle \otimes S|\psi\rangle + (|0\rangle - |1\rangle) \otimes (|0\rangle + |1\rangle) \otimes S|\psi\rangle + (|0\rangle - |1\rangle) \otimes (|0\rangle - |1\rangle) \otimes XSX|\psi\rangle\right]$$

$$= \frac{1}{4}\left[|00\rangle(3S + XSX)|\psi\rangle + |01\rangle(S - XSX)|\psi\rangle + |10\rangle(S - XSX)|\psi\rangle + |11\rangle(-S + XSX)|\psi\rangle\right]$$

$\cos\theta = 3/5, \sin\theta = 4/5$

If the measurement outcomes are both 0, the 3rd qubit is:

$$(3S + XSX)|\psi\rangle = \left(3\begin{bmatrix}1 & 0\\ 0 & i\end{bmatrix} + \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\begin{bmatrix}1 & 0\\ 0 & i\end{bmatrix}\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\right)|\psi\rangle$$

$$= \left(\begin{bmatrix}3 & 0\\ 0 & 3i\end{bmatrix} + \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\begin{bmatrix}0 & 1\\ i & 0\end{bmatrix}\right)|\psi\rangle$$

$$= \left(\begin{bmatrix}3 & 0\\ 0 & 3i\end{bmatrix} + \begin{bmatrix}i & 0\\ 0 & 1\end{bmatrix}\right)|\psi\rangle$$

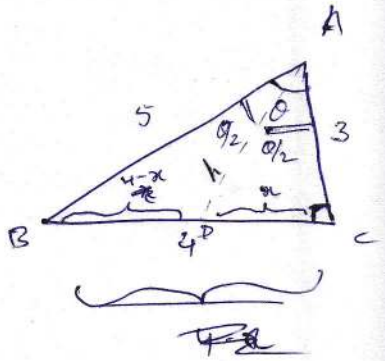
$$= \begin{bmatrix}3+i & 0\\ 0 & 1+3i\end{bmatrix}|\psi\rangle$$

$$= \sqrt{10}\begin{bmatrix}\frac{3+i}{\sqrt{10}} & 0\\ 0 & \frac{1+3i}{\sqrt{10}}\end{bmatrix}|\psi\rangle$$

$$R_z(\theta) = \begin{bmatrix}e^{-i\theta/2} & 0\\ 0 & e^{i\theta/2}\end{bmatrix}$$

angle

$$\frac{\theta}{2} = \frac{AB}{AC} = \frac{BD}{CD}$$



$$\frac{5}{3} = \frac{4-x}{x} \Longrightarrow 5x = 12 - 3x$$

$$8x = 12 \Longrightarrow \boxed{x = \frac{3}{2}}$$

$$h = \sqrt{\frac{9}{4} + 9} = \sqrt{\frac{45}{4}} = \frac{3}{2}\sqrt{5}$$

$$\cos\theta/2 = \frac{3 \times 2}{3\sqrt{5}} = \frac{2}{\sqrt{5}} \quad \& \quad \sin\theta/2 = \frac{3}{2} \times \frac{2}{3\sqrt{5}} = \frac{1}{\sqrt{5}}$$

$$(a+ib)(2+i) = 3+i \quad = (2a+b) + i(a+2b)$$

$$(a+ib)(2+i) = 1+3i \quad = (2a-b) + i(-a+2b)$$

$$4+4i = 4a + 4bi$$

$$\boxed{a=1,\ b=1}$$

$$\Longrightarrow (3S+XSX)|\psi\rangle = \sqrt{10} \begin{bmatrix} \frac{(a+ib)}{\sqrt{2}}\frac{(2+i)}{\sqrt{5}} & 0 \\ 0 & \frac{(a+ib)}{\sqrt{2}}\frac{(2+i)}{\sqrt{5}} \end{bmatrix}$$

$$= \sqrt{10} \begin{bmatrix} \left(\frac{1}{\sqrt{2}} + i\frac{1}{\sqrt{2}}\right)\left(\frac{2}{\sqrt{5}} + i\frac{1}{\sqrt{5}}\right) & 0 \\ 0 & \left(\frac{1}{\sqrt{2}} + i\frac{1}{\sqrt{2}}\right)\left(\frac{2}{\sqrt{5}} + i\frac{1}{\sqrt{5}}\right) \end{bmatrix}$$

$$= \sqrt{10} \begin{bmatrix} e^{i\pi/4} \times e^{-i\theta/2} & 0 \\ 0 & e^{-i\pi/4} \, e^{+i\theta/2} \end{bmatrix}$$

$$(ZS+XSX)|\psi\rangle = \sqrt{10}\, e^{i\pi/4} \begin{bmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{bmatrix}$$

$$= \sqrt{10}\, e^{i\pi/4} R_z(\theta)\,|\psi\rangle$$

$$P(00) = \left| \frac{\sqrt{10}\, e^{i\pi/4}}{4} \right|^2 = \left| \frac{\sqrt{10}\left(\frac{1}{\sqrt{2}} + i\,\frac{1}{\sqrt{2}}\right)}{4} \right|^2$$

$$= \cos^2\frac{1}{16} = \frac{5}{8}$$

If one of the measurement outcome is 1 & the other is 0 then the 3rd qubit is,

$$(S - XSX)|\psi\rangle = \left(\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} - \begin{bmatrix} i & 0 \\ 0 & 1 \end{bmatrix} \right) |\psi\rangle$$

$$= \begin{bmatrix} 1-i & 0 \\ 0 & -1+i \end{bmatrix} |\psi\rangle$$

$$= \begin{bmatrix} \frac{1-i}{\sqrt{2}}\sqrt{2} & 0 \\ 0 & -\left(\frac{1}{\sqrt{2}} - \frac{i}{\sqrt{2}}\right) \end{bmatrix} |\psi\rangle$$

$$= e^{-i\pi/4} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} |\psi\rangle = e^{-i\pi/4} Z |\psi\rangle$$

$$|\psi_5\rangle = \frac{1}{4}|00\rangle(3S+XSX)|\psi\rangle + \frac{1}{4}(|01\rangle+|10\rangle-|11\rangle)(S-XSX)|\psi\rangle$$

$$= |00\rangle\frac{\sqrt{10}}{4}e^{i\pi/4}R_z(\theta)|\psi\rangle +$$

$$(|01\rangle+|10\rangle-|11\rangle)\frac{1}{4}e^{-i\pi/4}Z|\psi\rangle$$

where, $\cos\theta = 3/5$

If we get any of the measurement results 01, 10, or 11, the output state is $Z|\psi\rangle$. If that happens, you apply Z and your state is back to the one you started with and repeat the circuit.

If we get 00 in the measurement, we have accomplished the process.

Each repetition succeeds with probability $p = 5/8$.

∴ After k repetitions the probability of success is,

$$p + qp + q^2p + q^3p + \cdots = \sum_{n=1}^{k} q^{n-1} p$$

succes in 1st trial

1st fail & success in 2nd trial

$$= \sum_{n=1}^{k} \left(\frac{3}{8}\right)^{n-1} \left(\frac{5}{8}\right)$$

$$= \frac{\frac{5}{8}\left(\left(\frac{3}{8}\right)^k - 1\right)}{\frac{3}{8} - 1}$$

$$= \frac{5\left(\left(\frac{3}{8}\right)^k - 1\right)}{-5}$$

$$= 1 - \left(\frac{3}{8}\right)^k$$

which tends to 1 as k becomes large.

Ex: 4.42 . **Irrationality of θ**

Suppose $\cos\theta = 3/5$, then θ is an irrational multiple of 2π

– Proof by contradiction

(1) Using the fact that $e^{i\theta} = \frac{3+4i}{5}$, show that if θ is rational, then there must exist a +ve integer m such that $(3+4i)^m = 5^m$.

Ans: If θ is rational then there exists an integer m such that

$$e^{i\theta m} = (e^{i\theta})^m = e^{i(2\pi j)} = 1 \quad \text{where } j \in \mathbb{Z}$$

Using m,

$$e^{mi\theta} = (e^{i\theta})^m = \frac{(3+4i)^m}{5^m} = 1$$

$$\Rightarrow (3+4i)^m = 5^m \;//$$

(2) Show that $(3+4i)^m = 3+4i \pmod 5$ for all $m>0$ and conclude that no m such that $(3+4i)^m = 5^m$ can exist.

Ans: $m=1$: $3+4i = 3+4i \pmod 5$

$m=2$: $(3+4i)^2 = (9-16) + 24i = -7+24i$

$= (-10+20i) + (3+4i)$

$= 5(-2+4i) + 3+4i$

$\therefore (3+4i)^2 = 3+4i \pmod 5$

Let, $(3+4i)^k = 3+4i \pmod 5$

$(3+4i)^k - (3+4i) = 5t$

$(3+4i)^{k+1} - (3+4i)^2 + (3+4i) - (3+4i) = 5t(3+4i)$

$(3+4i)^{k+1} - (3+4i) = 5t'' = 5t'''$

$(3+4i)^{k+1} - (3+4i) = 5t_1$

$(3+4i)^{k+1} = 3+4i \pmod 5$

$\Rightarrow (3+4i)^m = 3+4i \pmod 5$ for all $m>0$

Since $5^m = 0 \pmod 5$, there is no m such that $(3+4i)^m = 5^m$.

Ex: 4.43 . Hadamard + Phase + CNOT + Toffoli gates are universal.

θ which satisfies $\cos\theta = 3/5$ is an irrational multiple of 2π.

* Arbitrarily fine approximations of all angles can be achieved using rotations by an irrational multiple of 2π

$\therefore$ We can approximate $R_z(\theta)$ to arbitrarily small error E.

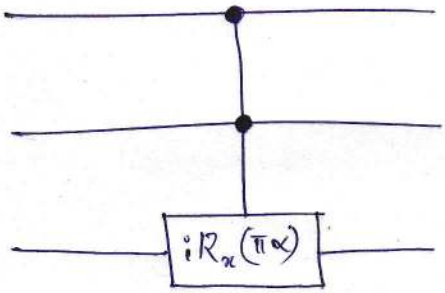
- $HZH = X$

$HR_z(\theta)H = R_x(\theta)$

$\Longrightarrow$

$\therefore$ Hadamard, phase, CNOT, Toffoli gates are universal.

Ex: 4.44 Show that the 3 qubit gate G_1 defined by the circuit:



is universal for quantum computation whenever α is irrational.

Ans:

Quantum Circuit model of computation

The key elements of the quantum circuit mode of computation:

① Classical resources :

A quantum computer consists of 2 parts - a classical part & a quantum part.

In principle, there is no need for the classical part of the computer, but in practice certain tasks may be made much easier if parts of the computation can be done classically. Ex:- many schemes for quantum error correction are likely to involve classical computations in order to maximize efficiency.

While classical computations can always be done, in principle, on a quantum computer, it may be more convenient to perform the calculations on a classical computer.

⑤ Ability to perform measurements in the computational basis:

Measurements may be performed in the computational basis of one or more of the qubits in the computer.