ON APPROXIMATING UNIVERSAL QUANTUM COMPUTATION

A REPORT
submitted in fulfillment of the summer project

in
PHYSICS
by
SWADHIN AGRAWAL
(15223)
under
Dr.R.SRIKANTH

DEPARTMENT OF PHYSICS
INDIAN INSTITUTE OF SCIENCE EDUCATION AND RESEARCH BHOPAL
BHOPAL–462 066

August 2017

1. INTRODUCTION

Quantum Computers are thought of as the very near future device to make computations easier and faster. The principle on which it will work is the principle of superposition of quantum states. So, multiple operations can be done simultaneously. There are certain Algorithms as there are in classical computers, designed to solve problems that are nearly impossible to solve over thousands of years in remarkably short time spans.

Certain quantum Algorithms and their applications are :

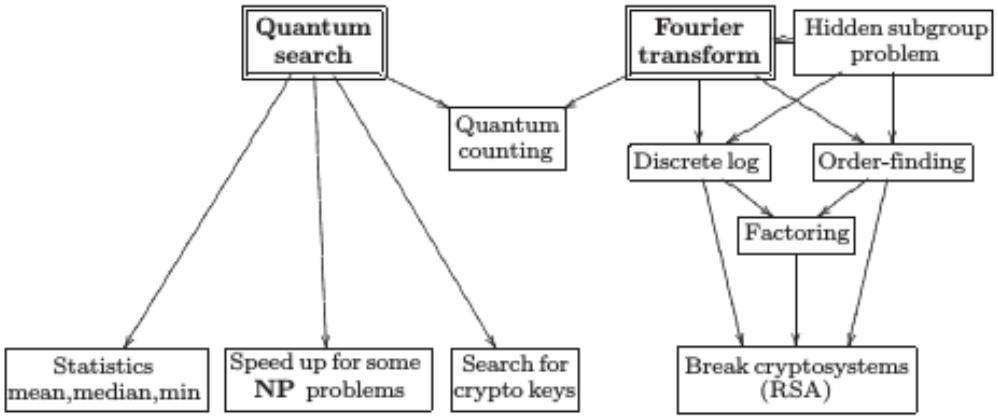


Image source : Quantum Computation and Quantum Information (Nielsen & Chuang).

Such Algorithms can be described using language of Quantum Circuits. Quantum Circuits are assembly of discrete components which can describe computational procedures. This will bring algorithms into phisical existance, techniques can be found to simplify circuits further.

2. Quantum Circuits

Quantum Circuits are built using single and multiple qubit gates.The most useful gates are Pauli matrices , Hadamard gate, S Gate, $\pi/8$ Gate.

$$\mathcal{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \mathcal{Y} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad \mathcal{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad \mathcal{S} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

$$\mathcal{H} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad \mathcal{T} = \begin{pmatrix} 1 & 0 \\ 0 & \frac{1+i}{\sqrt{2}} \end{pmatrix} \qquad \mathcal{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Rotation operators are operators that rotate $|\psi\rangle$ vector along the respective axes. These operators are produced by exponentiating pauli matrices.

$$R_x(\theta) \equiv (e)^{(-i\theta X/2)} = (\cos(\theta/2))\, I - i(\sin(\theta/2))\, X$$

$$= \begin{pmatrix} \cos(\theta/2) & -i(\sin(\theta/2)) \\ -i(\sin(\theta/2)) & \cos(\theta/2) \end{pmatrix}$$

$$R_y(\theta) \equiv (e)^{(-i\theta Y/2)} = (\cos(\theta/2))\, I - i(\sin(\theta/2))\, Y$$

$$= \begin{pmatrix} \cos(\theta/2) & -\sin(\theta/2) \\ \sin(\theta/2) & \cos(\theta/2) \end{pmatrix}$$

$$R_z(\theta) \equiv (e)^{(-i\theta Z/2)} = (\cos(\theta/2))\, I - i(\sin(\theta/2))\, Z$$

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

$$e^{iAx} = \cos(x)\, I + i \sin(x)\, A$$

$$R_{\hat{n}}(\theta) \equiv (e)^{(-i\theta\, \hat{n}.\vec{\sigma}/2)} = (\cos(\theta/2))\, I - i(\sin(\theta/2))\, (n_x X + n_y Y + n_z Z)$$

here $\hat{n} = (n_x, n_y, n_z)$ is a real unit vector in 3 D. Its a general rotation operator along an axes ' n '.
Every Quantum State can be represented through Bloch Sphere in 3 D, also the operation of gates can be visualised through these representation.
And thus arbitrary unitary operator can be decomposed as :

$$U = e^{i\alpha}\, R_{\hat{n}}(\beta)\, R_{\hat{m}}(\gamma)\, R_{\hat{n}}(\delta) \quad [\text{in general}]$$

where β, γ and δ are angles from respective axes to the state vector and α is global phase of rotation.

Proof :

Consider an arbitrary transform :

$U = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ **Since** U **is unitary,**

$$U^\dagger U = I \quad \text{or} \quad \begin{pmatrix} a^* & c^* \\ b^* & d^* \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

this implies :

$$a^* a + c^* c = 1$$
$$b^* b + d^* d = 1$$
$$a^* b + c^* d = 0$$
$$b^* a + d^* c = 0$$

Assuming an arbitrary form for $a = e^{-ia'} \cos(\gamma/2)$ **then** $a^* = e^{ia'} \cos(\gamma/2)$
and –

$$1 - e^{ia'} \cos(\gamma/2)\, e^{-ia'} \cos(\gamma/2) = c^* c$$

$$\Rightarrow c^* c = 1 - \cos^2(\gamma/2)$$

So $c = e^{-ic'} \sin(\gamma/2)$ and our unitary equation becomes –

$$\cos^2(\gamma/2) + \sin^2(\gamma/2) = 1$$

$$b^* b + d^* d = 1$$

$$e^{ia'} \cos(\gamma/2).b + e^{ic'} \sin(\gamma/2).d = 0$$

$$b^*.e^{-ia'} \cos(\gamma/2) + d^*.e^{-ic'} \sin(\gamma/2) = 0$$

from last two equations it should be clear that $b = -e^{-ib'} \sin(\gamma/2)$ and $d = e^{-id'} \cos(\gamma/2)$

Now focusing on last two equations – $a' - b' - c' = -d'$

There are so many solutions with three free variables, but for our purpose

$$a = (-\delta - \beta)/2 - \alpha$$

$$b = (\delta - \beta)/2 - \alpha$$

$$c = (-\delta + \beta)/2 - \alpha$$

$$d = (\delta + \beta)/2 - \alpha$$

This makes :

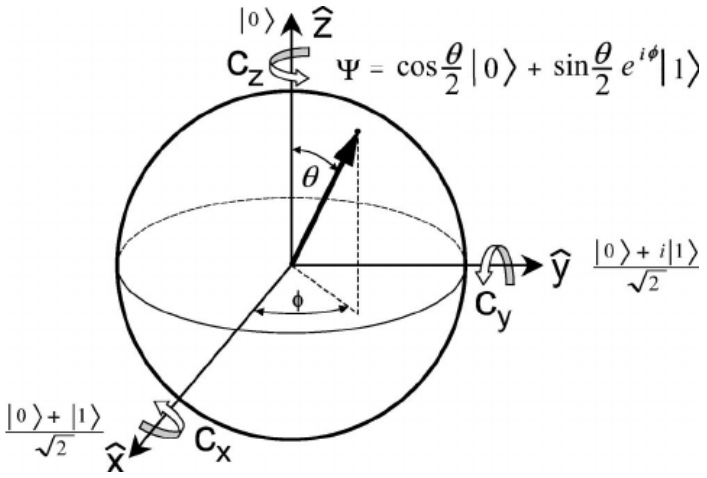
$$U = \begin{pmatrix} \left(e^{-i\alpha}\, e^{-i\delta/2}\, e^{-i\beta/2} \cos(\gamma/2)\right) & \left(-e^{-i\alpha}\, e^{i\delta/2}\, e^{-i\beta/2} \sin(\gamma/2)\right) \\ \left(e^{-i\alpha}\, e^{-i\delta/2}\, e^{i\beta/2} \sin(\gamma/2)\right) & \left(e^{-i\alpha}\, e^{i\delta/2}\, e^{i\beta/2} \cos(\gamma/2)\right) \end{pmatrix}$$

$$= e^{-i\alpha} \left[\begin{pmatrix} \left(e^{-i\delta/2}\, e^{-i\beta/2} \cos(\gamma/2)\right) & \left(-e^{i\delta/2}\, e^{-i\beta/2} \sin(\gamma/2)\right) \\ \left(e^{-i\delta/2}\, e^{i\beta/2} \sin(\gamma/2)\right) & \left(e^{i\delta/2}\, e^{i\beta/2} \cos(\gamma/2)\right) \end{pmatrix} \right]$$

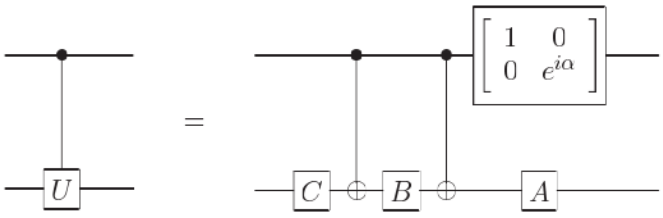
$$= e^{-i\alpha} \begin{pmatrix} e^{-i\beta/2} & 0 \\ 0 & e^{i\beta/2} \end{pmatrix} \begin{pmatrix} \left(e^{-i\delta/2} \cos(\gamma/2)\right) & \left(-e^{i\delta/2} \sin(\gamma/2)\right) \\ \left(e^{-i\delta/2} \sin(\gamma/2)\right) & \left(e^{i\delta/2} \cos(\gamma/2)\right) \end{pmatrix}$$

$$= e^{-i\alpha} \begin{pmatrix} e^{-i\beta/2} & 0 \\ 0 & e^{i\beta/2} \end{pmatrix} \begin{pmatrix} \cos(\gamma/2) & -\sin(\gamma/2) \\ \sin(\gamma/2) & \cos(\gamma/2) \end{pmatrix} \begin{pmatrix} e^{-i\delta/2} & 0 \\ 0 & e^{i\delta/2} \end{pmatrix}$$

$$= e^{-i\alpha}\, R_z(\beta)\, R_y(\gamma)\, R_z(\delta)$$



Also $U = e^{i\alpha} A \chi B \chi C$ and $ABC = \mathcal{I}$ as shown below :



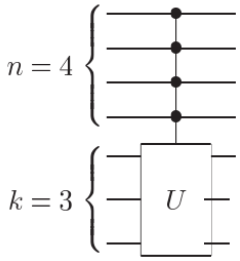
There is also Controlled operations where operation of a gate on qubits is controlled by one or more other qubits.And there are two qubits one is control bit and other one is target bit. And the operation of gate will effect either controll bit or target bit.This depends on the basis in which the state is present.

For mor than one control and target qubits :

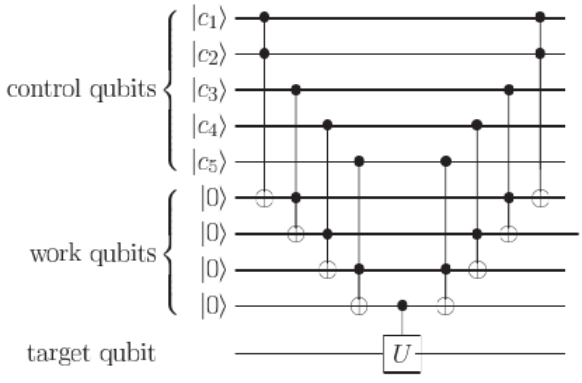
say n + k qubits we have and U is a k qubit unitary operator then controlled operation $C^n[U]$ is given by -

$$C^n[U] \; |x_1 x_2 \ldots x_n\rangle \; |\psi\rangle = |x_1 x_2 \ldots x_n\rangle \, U^{x_1 x_2 \ldots x_n} \; |\psi\rangle$$

if all $x_1 x_2 x_3 \ldots x_n$ are control qubits and U will be applied to k qubits only if all x_i ' s are 1 if set so or 0 if set so depending upon the choice.

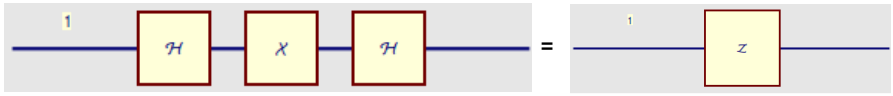


the other way to implement this is -

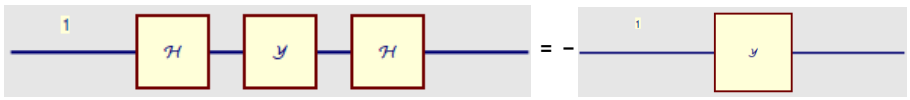


Circuit identities

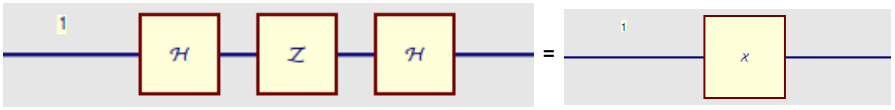
$\mathcal{H}_{\hat{1}} \otimes \mathcal{X}_{\hat{1}} \otimes \mathcal{H}_{\hat{1}} \equiv \mathcal{Z}_{\hat{1}}$



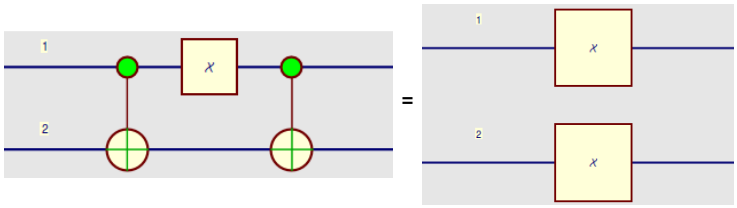
$\mathcal{H}_{\hat{1}} \otimes \mathcal{Y}_{\hat{1}} \otimes \mathcal{H}_{\hat{1}} \equiv -\mathcal{Y}_{\hat{1}}$



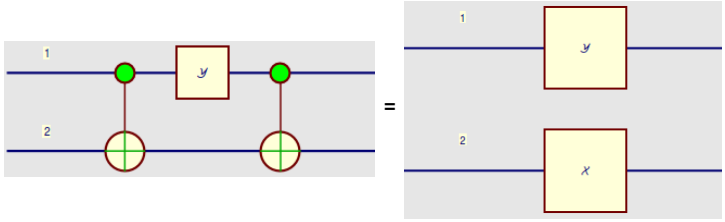
$\mathcal{H}_{\hat{1}} \otimes \mathcal{Z}_{\hat{1}} \otimes \mathcal{H}_{\hat{1}} \equiv \mathcal{X}_{\hat{1}}$



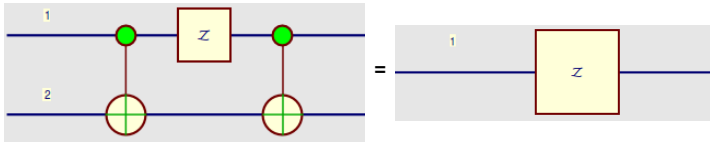
$C^{\{\hat{1}\}}[\mathcal{NOT}_{\hat{2}}] \bigotimes \mathcal{X}_{\hat{1}} \bigotimes C^{\{\hat{1}\}}[\mathcal{NOT}_{\hat{2}}] = \mathcal{X}_{\hat{1}} \otimes \mathcal{X}_{\hat{2}}$



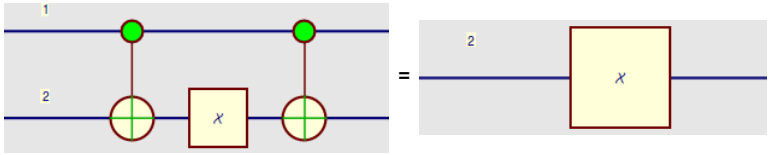
$C^{\{\hat{1}\}}[\mathcal{NOT}_{\hat{2}}] \bigotimes \mathcal{Y}_{\hat{1}} \bigotimes C^{\{\hat{1}\}}[\mathcal{NOT}_{\hat{2}}] = \mathcal{Y}_{\hat{1}} \bigotimes \mathcal{X}_{\hat{2}}$



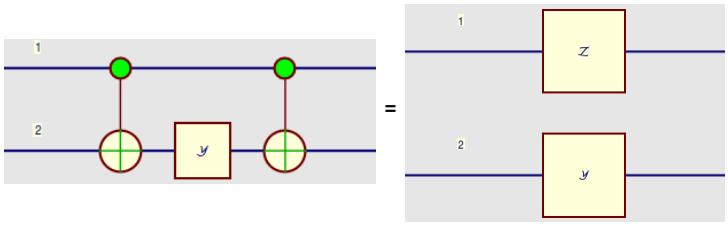
$C^{\{\hat{1}\}}[\mathcal{NOT}_{\hat{2}}] \otimes \mathcal{Z}_{\hat{1}} \otimes C^{\{\hat{1}\}}[\mathcal{NOT}_{\hat{2}}] = \mathcal{Z}_{\hat{1}}$



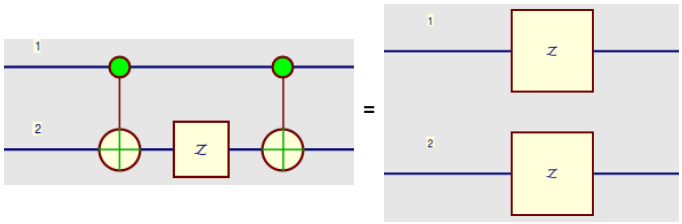
$C^{\{\hat{1}\}}[\mathcal{NOT}_{\hat{2}}] \otimes \mathcal{X}_{\hat{2}} \otimes C^{\{\hat{1}\}}[\mathcal{NOT}_{\hat{2}}] = \mathcal{X}_{\hat{2}}$



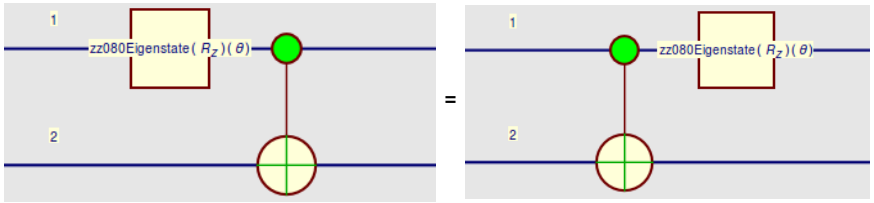
$C^{\{\hat{1}\}}[\mathcal{NOT}_{\hat{2}}] \bigotimes \mathcal{Y}_{\hat{2}} \bigotimes C^{\{\hat{1}\}}[\mathcal{NOT}_{\hat{2}}] = \mathcal{Z}_{\hat{1}} \bigotimes \mathcal{Y}_{\hat{2}}$



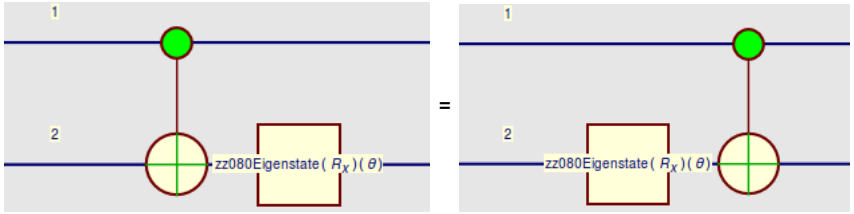
$C^{\{\hat{1}\}}[NOT_{\hat{2}}] \otimes Z_{\hat{2}} \otimes C^{\{\hat{1}\}}[NOT_{\hat{2}}] = Z_{\hat{1}} \otimes Z_{\hat{2}}$



$R_{z_{\hat{1}}}[\theta] \otimes C^{\{\hat{1}\}}[NOT_{\hat{2}}] = C^{\{\hat{1}\}}[NOT_{\hat{2}}] \otimes R_{z_{\hat{1}}}[\theta]$



$R_{x_{\hat{2}}}[\theta] \otimes C^{\{\hat{1}\}}[NOT_{\hat{2}}] = C^{\{\hat{1}\}}[NOT_{\hat{2}}] \otimes R_{x_{\hat{2}}}[\theta]$



There can be many more !

3. Measurements

In Circuits it is denoted by a ' meter ' symbol, and it is the final element of the quantum circuits.Quantum systems are in superposition states.Any measurement on system leads to the collapse of superposition state into a specific state which makes the probability of finding resulting state in further measurement 1.
There are 2 principles of quantum circuits –

Principle of deferred measurement : Measurements can always be moved from an intermediate stage of a quantum circuit to the end of the circuit.If measurement results are used at any stage of the circuit then classically

controlled operations can be replaced by conditional quantum operations.

Principle of implicit measurement : Without loss of generality, any unterminated quantum wires (qubits that are not measured) at the end of a quantum circuit may be assumed to be measured.

The second principle can be verified by seeing that reduced density matrix for 1 st qubit in a two qubit system is not affected by measurement i.e.

$$\mathrm{Tr}_2[\rho] = \mathrm{Tr}_2\left[\rho'\right]$$

where $\rho' = P_0 \rho P_0 + P_1 \rho P_1$ and ρ is a density matrix of two qubit system.

4. Universal Quantum Gates

A. Two level unitary gates are universal. Two level unitary matrices are those that acts non - trivially only on two or fewer vector components.

Let U is of the form -

$$U = \begin{pmatrix} a & d & g \\ b & e & h \\ c & f & j \end{pmatrix}$$

Two level Unitary matrices $U_1, \ldots, U_3$ are such that,

$$U_3 U_2 U_1 U = \mathcal{I}$$

so, $$U = U_1^\dagger U_2^\dagger U_3^\dagger$$

To Construct U_1 : if $b = 0$ then,

$$U_1 \equiv \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

if $b \neq 0$ then,

$$U_1 \equiv \begin{pmatrix} \left(a^* / \sqrt{\left(|a|^2 + |b|^2\right)}\right) & \left(b^* / \sqrt{\left(|a|^2 + |b|^2\right)}\right) & 0 \\ \left(b / \sqrt{\left(|a|^2 + |b|^2\right)}\right) & \left(-a / \sqrt{\left(|a|^2 + |b|^2\right)}\right) & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

so

$$U_1 U = \begin{pmatrix} a' & d' & g' \\ 0 & e' & h' \\ c' & f' & j' \end{pmatrix}$$

Now, if $c' = 0$ then ,

$$U_2 \equiv \begin{pmatrix} a'^* & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

if $c' \neq 0$ then,

$$U_2 \equiv \begin{pmatrix} \left(a'^* / \sqrt{\left(|a'|^2 + |c'|^2\right)}\right) & 0 & \left(c'^* / \sqrt{\left(|a'|^2 + |c'|^2\right)}\right) \\ 0 & 1 & 0 \\ \left(c' / \sqrt{\left(|a'|^2 + |c'|^2\right)}\right) & 0 & \left(-a' / \sqrt{\left(|a'|^2 + |c'|^2\right)}\right) \end{pmatrix}$$

so

$$U_2\,U_1\,U = \begin{pmatrix} 1 & d'' & g'' \\ 0 & e'' & h'' \\ 0 & f'' & j'' \end{pmatrix}$$

Since U_2, U_1, U are unitary, $\Rightarrow U_2\,U_1\,U$ is also Unitary, thus $d''=g'' = 0$, since the first row of $U_2\,U_1\,U$ must have norm 1. Finally, set

$$U_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & e'' * & h'' * \\ 0 & f'' * & j'' * \end{pmatrix}$$

In general, this way an arbitrary dXd unitary matrix may be written as:

$$U = V_1 \ldots V_k$$

where V_i are two level unitary matrices, and $(d-1) \le k \le (d-1) + .. + 1 = d\,(d-1)/2$ and d is dimension of the space.

B. Single qubit and CNOT gates are universal. Suppose U is a two level unitary matrix on an n qubit quantum computer. Say U acts non-trivially on space spanned by computational basis states $|s\rangle$ and $|t\rangle$ and here $s = s_1 \ldots s_n$ and $t = t_1 \ldots t_n$ are binary expansions for s & t. $\tilde{U}$ is nontrivial submatrix of U; $\tilde{U}$ can be thought of as a unitary operator on a single qubit.

Gray codes are used to construct circuit implementing U build from single qubit and CNOT gates. A Gray code connecting s and t is a sequence of binary numbers, starting with s and concluding with t such that adjacent members of the list differ in exactly one bit.

example:

s : 101 010 t : 110 010

Gray code =

1 0 1 0 1 0
1 0 0 0 1 0
1 1 0 0 1 0

Let g_1 to g_m be the elements of Gray code connecting s & t, with $g_1 = s$, $g_m = t$. $m \le n+1$ since s & t can differ atmost at n locations.

The basic idea is to apply gates to change states as $|g_1\rangle \to |g_2\rangle \to \ldots \to |g_{m-1}\rangle$ then to perform Controlled - $\tilde{U}$ operation with target qubit located at the single bit where g_{m-1} & g_m differ and then undo the first stage transforming $|g_{m-1}\rangle \to |g_{m-2}\rangle \to \ldots \to |g_1\rangle$ thus final result is implementation of U.

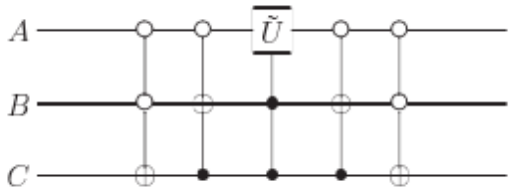
example :

$$\text{Let } U = \begin{pmatrix} a & 0 & 0 & 0 & 0 & 0 & 0 & c \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ b & 0 & 0 & 0 & 0 & 0 & 0 & d \end{pmatrix}, \ (a, b, c, d) \in \text{complex number set}$$

$\tilde{U} \equiv \begin{pmatrix} a & c \\ b & d \end{pmatrix}$, Notice that U acts non-trivially only on $|000\rangle$ & $|111\rangle$

So, Gray code connecting 000 and 111 =

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



1 st two gates shuffle the states so, $|000\rangle$ gets swapped with $|011\rangle$. $\tilde{U}$ gets applied to 1 st qubit of $|011\rangle$ and $|111\rangle$, conditional on the second and third qubits being in the state $|11\rangle$.Finnaly, we unshuffle the states, ensuring that $|011\rangle$ gets swapped back with the state $|000\rangle$.

So, Such U requires at most $2(n-1)$ controlled operations to swap $|g_1\rangle$ with $|g_{m-1}\rangle$ and then back again.These controlled operations can be realized using $O(n)$ single qubit and CNOT gates.Controlled $\tilde{U}$ also requires $O(n)$ gates.So U requires $O(n^2)$ single qubit and CNOT gates.According to A point arbitrary unitary matrix on 2^n-dimensional state space of n qubits may be written as a product of $O(2^{2n}) = O(4^n)$ two level unitary operations.

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

5. Approximating Arbitrary Unitary Gates

Unitary operations are continuous , so arbitrary unitary operation cannot be implemented using discrete set of gates.Suppose U and V are two 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.So, error when V is implement instead of U -

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

where the maximum is over all normalized quantum states $|\psi\rangle$ in the state space. This measure of error has interpretation that 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 $|\psi\rangle$ i.e. 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

$$|P_u - P_v| \leq 2 E(U, V) \qquad \{1\}$$

Proof :

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

Let $|\triangle\rangle \equiv (U - V) \; |\psi\rangle$, using simple algebra and Cauchy - Schwarz inequality

$$\begin{aligned} |P_u - P_v| &= |\langle\psi| U^\dagger M |\triangle\rangle + \langle\triangle| M V |\psi\rangle| \\ &\leq |\langle\psi| U^\dagger M |\triangle\rangle| + |\langle\triangle| M V |\psi\rangle| \\ &\leq \| |\triangle\rangle \| + \| |\triangle\rangle \| \\ &\leq 2 E(U, V) \end{aligned}$$

If $E(U, V)$ becomes significantly small then outcome occures with similar probabilities regardless of whether U or V were performed.Also if we perform sequence of gates $V_1, \ldots, V_m$ intended to approximate $U_1, \ldots, U_m$, then the errors add at most linearly :

$$E(U_m U_{m-1} \ldots U_1, V_m V_{m-1} \ldots V_1) \leq \sum_{j=1}^{m} E(U_j, V_j) \qquad \{2\}$$

Proof :

Let $m = 2$ (through induction can be proved for general m.)

$$\begin{aligned} E(U_2 U_1, V_2 V_1) &= || (U_2 U_1 - V_2 V_1) \; |\psi\rangle || \\ &= || (U_2 U_1 - V_2 U_1) \; |\psi\rangle + (V_2 U_1 - V_2 V_1) \; |\psi\rangle || \end{aligned}$$

using triangle inequality :

$$\begin{aligned} E(U_2 U_1, V_2 V_1) &\leq || (U_2 - V_2) U_1 \; |\psi\rangle || + || V_2 (U_1 - V_1) \; |\psi\rangle || \\ &\leq E(U_2 U_1) + E(V_2 V_1) \end{aligned}$$

$\{1\}$ & $\{2\}$ are useful as if suppose we wish to perform a quantum circuit m gates but unfortunately we are only able to approximate jth gate.In order that the probabilities of different measurement outcomes obtained from the approximate circuit be within a tolerance $\triangle > 0$ of the correct probabilities $E(U_j, V_j) \leq \triangle / (2 m)$ from $\{1\}$ & $\{2\}$.

Universality of Hadamard + Phase + CNOT + $\pi/8$ gates :

2 sets of universal gates -

1 st is standard set - Hadamard + Phase + CNOT + $\pi/8$ gates

2 nd is - Hadamard + Phase + CNOT + Toffoli gates

$R_{\hat{n}}(\theta)$ can be created using just Hadamard gate and $\pi/8$ gate i.e. $HTH = R_{\hat{x}}(\pi/4)$, while T only does $R_{\hat{z}}(\pi/4)$. (Refer exercise 4.14 Neilsen & Chuang).

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

Proof :

Let $\delta > 0$ be the desired accuracy , $N \in$ integer $> 2\pi/\delta$

Define θ_k so that $\theta_k \in [0, 2\pi)$ & $\theta_k = (k\theta) \bmod 2\pi$.

Then pigeon hole principle implies that there are distinct j & k in range 1, ..., N such that

$$|\theta_k - \theta_j| \leq 2\pi/N < \delta.$$

Without loss of generality assume that $k > j$, so $|\theta_{k-j}| < \delta$. Since $j \neq k$ & θ is an irrational multiple of 2π we must have $\theta_{k-j} \neq 0$. So $\theta_{l(k-j)}$ fills up the interval $[0, 2\pi)$ as l is varied, so that adjacent members of the sequence are no more than δ apart.

It follows that for any $\epsilon > 0$ there exists an n such that

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

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

n_1, n_2, n_3 are positive integers.

i.e. Given U & ϵ it is possible to approximate U within $\epsilon > 0$ circuit using Hadamard and $\pi/8$ gates alone. if there are m gates then, whole circuit can be approximated to ϵ accuracy by approximating each gate to ϵ/m accuracy by chaining inequality {2}.

How efficient is this to approximate quantum circuits useing discrete set of gates? Approximating an arbitrary single qubit unitary to within a distance ϵ requires $\Omega(2^{1/\epsilon})$ gates from discrete set. To approximate m gates require $\Omega(m2^{m/\epsilon})$ gates (exponential increase). But the sequence of angles θ_k fills in the interval $[0, 2\pi)$ in more or less uniform fashion. So it takes $\Theta(1/\epsilon)$ gates from discrete set. For approximating m gate circuit requires $\Theta(m^2/\epsilon)$ gates to get accuracy of ϵ. Sufficient for many applications !

The Solovay Ketaev theorem implies that arbitrary single qubit gate may be approximated to an accuracy ϵ using $O(\log^c(1/\epsilon))$ gates from our discrete set, c is approximately equal to 2. For m CNOTs and single qubit unitaries to an accuracy ϵ requires $O(m\log^c(m/\epsilon))$ gates from discrete set.

(Polylogarithemic increase, acceptable for virtually all applications).

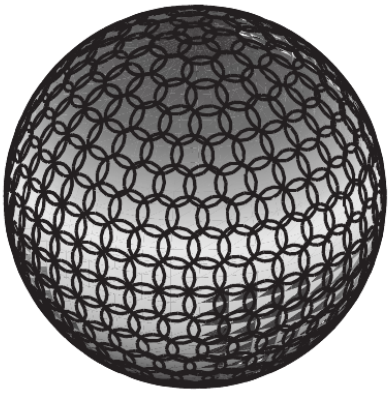
It is hard to approximate any arbitrary unitary operation in general. There are unitary operations that require exponentially many operations.

Say we have g different types of gates and each gate works at most f input qubits $(f \& g$ fixed by the computer hardware$)$, suppose our quantum circuit has m gates starting from computational basis state $|0\rangle^{\otimes n}$. For any particular gate in circuit, at most possible choices -

$$\begin{bmatrix} n \\ f \end{bmatrix}^g = O\left(n^{fg}\right)$$

i.e at most $O\left(n^{fgm}\right)$ different states can be computed using m gates.

We have to optimise this i.e. finding a way to approximate that arbitrary Unitary operation using minimum number of gates and with higher accuracy.



From Solovay - Kitaev theorem and our universality constructions, an arbitrary unitary opoeration U on n qubits may be approximated to within a distance ϵ using $O\left(n^2\, 4^n \log^c\left(n^2\, 4^n / \epsilon\right)\right)$ gates. This is optimal but unfortunately, it does not address the problem of determining which families of unitary operations can be computed efficiently in the quantum circuits model.

5. New ideas and thoughts to work on

1. Doing operations in some other dimention and converting the result back to the dimension we are working on can lead to the reduced number of operations & gates significantly. (As a sphere in 2 D becomes a circle.) But it seems little unclear that to do that we need quantum gates in that dimension which is not that easy.

6. Bibliography

Nielsen and Chuang [Quantum Computation and Quantum information - pg 170 to pg 200]