Approximation of U by Hadamard and T gates

Remember: $E(R_{\hat{n}}(\alpha), R_{\hat{n}}(\theta)^{\wedge}) < \varepsilon/3$

where $\hat{n} = (\cos\frac{\pi}{8}, \sin\frac{\pi}{8}, \cos\frac{\pi}{8})$

observe: $H R_{\hat{n}}(\alpha) H = R_{\hat{m}}(\alpha)$, where $\hat{m} = (\cos\frac{\pi}{8}, -\sin\frac{\pi}{8}, \cos\frac{\pi}{8})$

$\Rightarrow E(R_{\hat{m}}(\alpha), R_{\hat{m}}(\theta)^{\wedge}) < \frac{\varepsilon}{3}.$

But, an arbitrary unitary U can be written,

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

$\Rightarrow$

$$E(U, R_{\hat{n}}(\theta)^{\wedge_1} H R_{\hat{n}}(\theta)^{\wedge_2} H R_{\hat{n}}(\theta)^{\wedge_3}) < \varepsilon.$$

Universality of Hadamard, T gate, and CNOT

CNOT and single qubit gate are universal.

Hadamard and T gate can approximate any single qubit gate

$\Rightarrow$

Hadamard, T gate and CNOT are universal.

Accuracy of ε for m-gate circuit by approximating each single qubit unitary to within ε/m.

Efficiency of Circuit Approximation

Roughly, the sequence of angles θ_k "fills in" the interval $[0, 2\pi)$ more or less uniformly.

Therefore approximating an arbitrary single qubit gate takes $\Theta(\frac{1}{\epsilon})$ gates from the discrete set.

Therefore the number of discrete-set gates required to approximate an n gate circuit to accuracy becomes $\tilde{\Theta}(n^2/\epsilon)$.

- a quadratic increase over original circuit.

The True Rate of Convergence is Faster

Solovay - Kitaev theorem:

An arbitrary single qubit gate may be approximated to accuracy ε using

$$O(\log^c(1/\varepsilon))$$ gates from the discrete set,

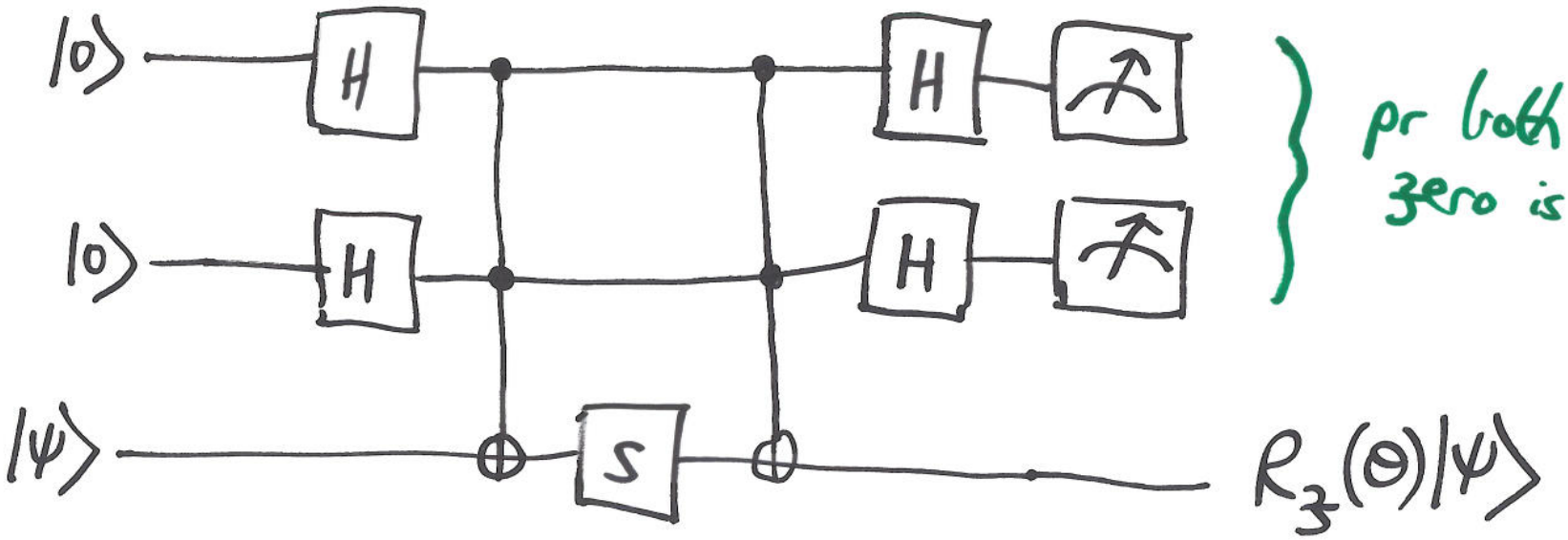
where $c \simeq 2$.

Therefore a circuit containing m CNOTs and single qubit gates requires $O(m \log^c(m/\varepsilon))$ gates from the discrete set to obtain an accuracy of ε....

... a polylogarithmic increase over the original ...

The Hadamard, phase, CNOT and Toffoli gates are universal

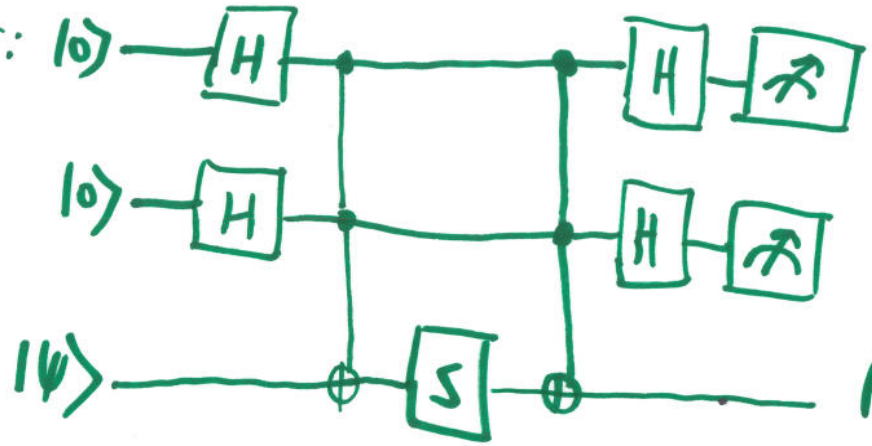
Consider,



If both measurement outcomes are 0,
then circuit applies $R_3(\theta)$, where $\cos(\theta) = \frac{3}{5}$
otherwise Z is applied.

$R_z(\theta)$ Approximated

Remember:



$\Rightarrow R_z(\theta)|\psi\rangle$

$$\begin{cases} pr(R_z(\theta)) = 5/8 \\ pr(Z) = 3/8 \end{cases}$$

... repeated use of above circuit and $Z = S^2$ gates will result in $R_z(\theta)$ with $pr \to 1$.

Moreover, $\cos\theta = \frac{3}{5} \Rightarrow \theta$ is irrational

$\Rightarrow R_z(\alpha)$ can be approximated for any α.

... using H's, $R_m(\phi)$ can then be approximated.

$\Rightarrow$ Hadamard, phase, CNOT and Toffoli are universal.

Approximating Arbitrary Unitaries is Generically Hard

Efficiency?

Given a unitary, U, on n qubits, does there always exist a circuit of size polynomial in n approximating U?

No - most unitaries can only be implemented very inefficiently.

How many gates does it take to generate an arbitrary state of n qubits?

... exponentially many, in general...

... therefore most unitaries are inefficiently implemented.

Counting Argument

Suppose g different gate types, each working on at most f qubits.

Now consider quantum circuit containing m gates, starting from $|0\rangle^{\otimes n}$.

Any particular gate can be chosen from

$$\binom{n}{f}^g = O(n^{fg}) \text{ choices.}$$

$\Rightarrow$ at most $O(n^{fgm})$ different states may be computed using m gates.

We now wish to approximate $|\psi\rangle$ to within ϵ.

... cover the set of all possible states with regions, each of radius ϵ.

... then show that the number of regions rises doubly exponentially in n....

.. comparing with the exponential number of states that may be computed using m gates implies the result..

Observe:

the state space of vectors of n qubits is on the unit $(2^{n+1}-1)$-sphere.

Observe:

The surface area of radius ϵ near $|\psi\rangle$ is approximately the same as the volume of a $(2^{n+1}-2)$-sphere of radius ϵ.

Surface area of a k-sphere of radius r:

$$S_k(r) = 2\pi^{(k+1)/2} r^k / \Gamma((k+1)/2)$$

Volume of a k-sphere of radius r:

$$V_k(r) = 2\pi^{(k+1)/2} r^{k+1} / [(k+1)\Gamma((k+1)/2)]$$

$\Rightarrow$ Number of regions needed to cover state space goes like

$$\frac{S_{2^{n+1}-1}(1)}{V_{2^{n+1}-2}(\epsilon)} = \frac{\sqrt{\pi}\,\Gamma(2^n - \frac{1}{2})(2^{n+1}-1)}{\Gamma(2^n)\epsilon^{2^{n+1}-1}}$$

Using $\Gamma(2^n + 1/2) \geq \Gamma(2^n)/2^n$,

#regions required to cover the space is at least

$$\Omega\left(\frac{1}{\epsilon^{2^{n+1}-1}}\right).$$

... but number of regions reachable by m gates is $O(n^{fgm})$.

$\Rightarrow$ to reach all ϵ-regions, we require,

$$O(n^{fgm}) \geq \Omega\left(\frac{1}{\epsilon^{2^{n+1}-1}}\right)$$

$\Rightarrow$ $$m = \Omega\left(\frac{2^n \log(1/\epsilon)}{\log(n)}\right)$$

... i.e. there are n-qubit states which take $\Omega(2^n \log(1/\epsilon)/\log(n))$ operations to approximate to within distance ϵ. ... exponential in n.

Exponential Approximation Complexity

Remember: $m = \Omega\left(\frac{2^n \log\left(\frac{1}{\epsilon}\right)}{\log(n)}\right)$.

$\Rightarrow$ there are unitary transformations, U, on n qubits requiring $\Omega(2^n \log(1/\epsilon)/\log(n))$ operations to approximate by V, where $E(U,V) \leq \epsilon$.

In contrast, using Solovay-Kitaev, an arbitrary U on n qubits may be approximated to within ϵ using,

$$O(n^2 4^n \log^c(n^2 4^n/\epsilon)) \text{ gates.}$$

$\Rightarrow$ to within a polynomial factor, the construction given is optimal.

..... but which families of unitaries may be computed efficiently?

Quantum Computational Complexity

PSPACE - class of decision problems which can be solved on a Turing machine using space polynomial in problem size arbitrary amount of time.

BQP - class of decision problems that can be solved on a quantum computer using bounded probability of error on a polynomial size quantum circuit.

A language L is in BQP if there is a family of polynomial size quantum circuits which decides the language, accepting strings in the language with pr $\geq 3/4$, and rejecting strings outside the language with pr $\geq 3/4$.

... in other words...

the quantum circuit takes binary strings as input..

it tries to determine whether they are elements of the language or not...

at the conclusion of the circuit, one qubit is measured,

0 indicates that the string has been accepted.

1 indicates rejection.

repeated testing determines whether the string is in L or not with high probability..

Why a family of Circuits?

... a quantum circuit is a fixed entity..

... it can only decide on strings up to some finite length..

... so we use a family of circuits ...

... for every possible input length there is a different circuit in the family.

Two additional restrictions:

1. Circuit size should only grow polynomially with size of input string

2. The circuits should be uniformly generated

i.e there is a Turing machine capable of efficiently outputting a description of the quantum circuit.

Results

$$BQP \subseteq PSPACE$$

moreover,

$$BPP \subseteq BQP \subseteq PSPACE$$

where BPP is class of decision problems that can be solved with bounded probability of error using poly time on a classical Turing machine.

If $BQP \neq BPP$ (ie. quantum computers more powerful than classical computers)

then

$BPP \neq PSPACE$ – not known... would be a major breakthrough!

BQP ⊆ PSPACE

Proof outline:

We have an n-qubit quantum computer.

A computation involves a sequence of $p(n)$ gates,

$p(n)$ a polynomial in n.

Suppose the QC starts in state $|0\rangle$. We explain how to evaluate in poly space on a classical computer the probability that it ends in state $|y\rangle$.

prob. ending in state $|y\rangle$ is,

$$\langle y | U_{p(n)} \dots U_2 U_1 |0\rangle \dots$$

... using the completeness relation... $\sum_x |x\rangle\langle x| = I$,

$$\langle y|U_{p(n)}\ldots U_2U_1|0\rangle = \sum_{x_1\ldots x_{p(n)-1}} \langle y|U_{p(n)}|x_{p(n)-1}\rangle\langle x_{p(n)-1}|U_{p(n)-2}\ldots U_2|x_1\rangle\langle x_1|U_1|0\rangle$$

... the individual unitaries will be Hadamard, CNOT .... etc..

... so each term can be calculated to high accuracy using poly space on a classical computer..

... therefore complete sum only requires poly space.

..... a similar procedure can be used to simulate an arbitrary quantum computation on a classical computer, irrespective of the length of the quantum computation.

Church-Turing thesis

Quantum computers do not violate the Church-Turing thesis that any algorithmic process can be simulated efficiently using a Turing machine.

Strong Church-Turing thesis

Quantum computers may be more efficient than their classical counterparts....

... challenges the strong Church-Turing thesis:

any algorithmic process can be simulated efficiently using a probabilistic Turing machine.

Summary of Quantum Circuit model

1. Classical resources:

   In principle, classical part not necessary, but certain tasks are easier if done classically.

2. Suitable state space:

   n qubits: 2^n-dimensional complex Hilbert space.

   computational basis states: $|x_1, \ldots x_n\rangle$.

3. Ability to prepare computational basis states:

   ... any such state can be prepared in n steps.

4. Ability to perform gates:

   ... a universal family can be implemented.

5. Ability to perform measurements in computational basis:

The Quantum Circuit Model is equivalent to many other models

e.g.

do three-level quantum systems have any advantage over two-level systems?

.... negligible from a theoretical point of view.

the "quantum Turing model" has been shown to be equivalent to the quantum circuit model.

.... possible criticisms/modifications of quantum circuit model..

what about infinite dimensional state space?

Use highly entangled states as starting states, instead of computational basis (product) states?

Use "entangling measurements" in multi-qubit bases?

Simulation of Quantum Systems

General goal of simulation is:

given an initial system state, what is the state at some other time and/or position?

Solutions obtained by approximating state with digital representation, then discretizing the differential equation in time and space. An iterative procedure then carries the state from initial to final conditions.

the error is bounded, and grows no faster than some small power of the number of iterations.

But . . . .

... but..

not all dynamical systems can be simulated efficiently - only (typically) those systems which can be described efficiently can be simulated efficiently.

Dynamical behaviour of simple quantum systems governed by Schrödinger's equation:

$$i\hbar \frac{d}{dt}|\psi\rangle = H|\psi\rangle$$

For a typical Hamiltonian, dealing with real particles in space (rather than abstract qubits), Schrödinger's equation reduces to,

$$i\frac{\partial}{\partial t}\psi(x) = \left[-\frac{1}{2m}\frac{\partial^2}{\partial x^2} + V(x)\right]\psi(x)$$

.... using the position representation,

$$\langle x|\psi\rangle = \psi(x).$$

This is an elliptical equation.

What's the Problem?

The challenge in simulating quantum systems is the exponential number of differential equations to be solved.

One qubit evolving according to Schrödinger's equation requires the solution of two differential equations.

n qubits .... requires the solution of 2^n differential equations.

... sometimes simplifications can be made but not usually....

Exponential complexity growth of quantum systems

Let ρ be a density matrix describing the state of n qubits.

Then ρ requires $4^n - 1$ independent real numbers.

Quantum computers can efficiently simulate quantum systems for which there is no known efficient classical simulation.

.... same reasoning as for the constructability of any quantum circuit from a universal set of quantum gates.

... but just as it is possible that there are unitaries which cannot be efficiently approximated...

... so there exist Hamiltonians without efficient simulation on a quantum computer.

Quantum Simulation Algorithm

For classical simulation of $\frac{dy}{dt} = f(y)$,

we have the first order approximation,

$$y(t+\Delta t) \approx y(t) + f(y)\Delta t.$$

Similarly, for quantum simulation of $i\,d|\psi\rangle/dt = H|\psi\rangle$,

the solution is,

$$|\psi(t)\rangle = e^{-iHt}|\psi(0)\rangle,$$

with first order solution,

$$|\psi(t+\Delta t)\rangle \approx (I - iH\Delta t)|\psi(t)\rangle.$$

Remember: $|\psi(t+\Delta t)\rangle \approx (I - iH\Delta t)|\psi(t)\rangle$.

For many Hamiltonians H it is straightforward to efficiently approximate $I - iH\Delta t$...

... but, in general, such solutions are unsatisfactory.

Sometimes high order approximations are possible.

Often the Hamiltonian can be written as a sum,

$$H = \sum_{k=1}^{L} H_k,$$

where each H_k acts on $\leq$ a constant c number of systems, and L is polynomial in the number of particles, n.

Remember: $H = \sum_{k=1}^{L} H_k$.

Often the H_k are two-body interactions, such as $X_i X_j$, or one-body Hamiltonians such as X_i.

(e.g. Hubbard and Ising models).

This type of locality is physically reasonable, as, often, interactions fall off with increasing distance, or difference in energy.

Although e^{-iHt} is difficult to compute,

$e^{-iH_k t}$ acts on a much smaller subsystem,

and can therefore be approximated using quantum circuits.

But, as $[H_j, H_k] \neq 0$ in general,

then $e^{-iHt} \neq \prod_k e^{-iH_k t}$.

... so how can $e^{-iH_k t}$ be useful in constructing e^{-iHt}?

Observe:

For $H = \sum_k^L H_k$,

one can show that,

$$e^{-iHt} = e^{-iH_1 t} e^{-iH_2 t} \cdots e^{-iH_L t}, \quad \forall t,$$

if $[H_j, H_k] = 0, \quad \forall j, k.$

Trotter Formula

Let A and B be Hermitian operators.

Then, for t real,

$$\lim_{n\to\infty} \left(e^{iAt/n} e^{iBt/n} \right)^n = e^{i(A+B)t}$$

..... this is true even if A and B do not commute.

Proof of the Trotter formula

Remember: $\lim_{n\to\infty}\left(e^{iAt/n}e^{iBt/n}\right)^n = e^{i(A+B)t}$.

By definition,

$$e^{iAt/n} = I + \frac{1}{n}iAt + O\left(\frac{1}{n^2}\right),$$

$$\Rightarrow \quad e^{iAt/n}e^{iBt/n} = I + \frac{1}{n}i(A+B)t + O\left(\frac{1}{n^2}\right).$$

$$\Rightarrow \left(e^{iAt/n}e^{iBt/n}\right)^n = I + \sum_{k=1}^{n}\binom{n}{k}\frac{1}{n^k}\left[i(A+B)t\right]^k + O\left(\frac{1}{n}\right)$$

... but $\binom{n}{k}\frac{1}{n^k} = \left(1 + O\left(\frac{1}{n}\right)\right)/k!$ ...

$$\Rightarrow \lim_{n\to\infty}\left(e^{iAt/n}e^{iBt/n}\right)^n = \lim_{n\to\infty}\sum_{k=0}^{n}\frac{\left(i(A+B)t\right)^k}{k!}\left(1 + O\left(\frac{1}{n}\right)\right) + O\left(\frac{1}{n}\right) = e^{i(A+B)t}.$$

Similarly...

$$e^{i(A+B)\Delta t} = e^{iA\Delta t} e^{iB\Delta t} + O(\Delta t^2),$$

$$e^{i(A+B)\Delta t} = e^{iA\Delta t/2} e^{iB\Delta t} e^{iA\Delta t/2} + O(\Delta t^3).$$

.... and so on...

Quantum Simulation Algorithm

Inputs: (1) Hamiltonian $H = \sum_k H_k$, where each H_k acts on a small subsystem of constant size.

(2) Initial state, $|\psi_0\rangle$, at $t = 0$.

(3) Positive, non-zero accuracy, δ

(4) Time t_f of desired evolved state.

Outputs: State $|\tilde{\psi}(t_f)\rangle$, where,

$$|\langle\tilde{\psi}(t_f)| e^{-iHt_f} |\psi_0\rangle|^2 \geq 1 - \delta.$$

Runtime: $O(\text{poly}(1/\delta))$ operations.

Procedure:

For an N-dimensional system, choose a representation for $|\tilde{\psi}\rangle$ of $n = \text{poly}(\log N)$ qubits, and where the operators $e^{-iH_k \Delta t}$ have efficient quantum circuit approximations.

Select approximation method and acceptable Δt.

Let $j\Delta t = t_f$, j integer.

Construct quantum circuit $U_{\Delta t}$.

Do:

1. $|\tilde{\psi}_0\rangle \leftarrow |\psi_0\rangle$; $j = 0$ — init. state
2. $\rightarrow |\tilde{\psi}_{j+1}\rangle = U_{\Delta t} |\tilde{\psi}_j\rangle$ — iterative update
3. $\rightarrow j = j+1$; goto 2 until $j\Delta t \geq t_f$ — loop
4. $\rightarrow |\tilde{\psi}(t_f)\rangle = |\tilde{\psi}_j\rangle$ — final result.