Seminar 3

Quantum Computations

Schedule

- 1. Introduction to Quantum Computing
- 2. Formalisms in QM & Computing
- 3. Quantum Circuits – Today
- 4. Fourier Analysis & Search Algorithms
- 5. Realisations of Quantum Computers
- More to come…
- I rescheduled the overall syllabus as now we require more time to explain concepts.

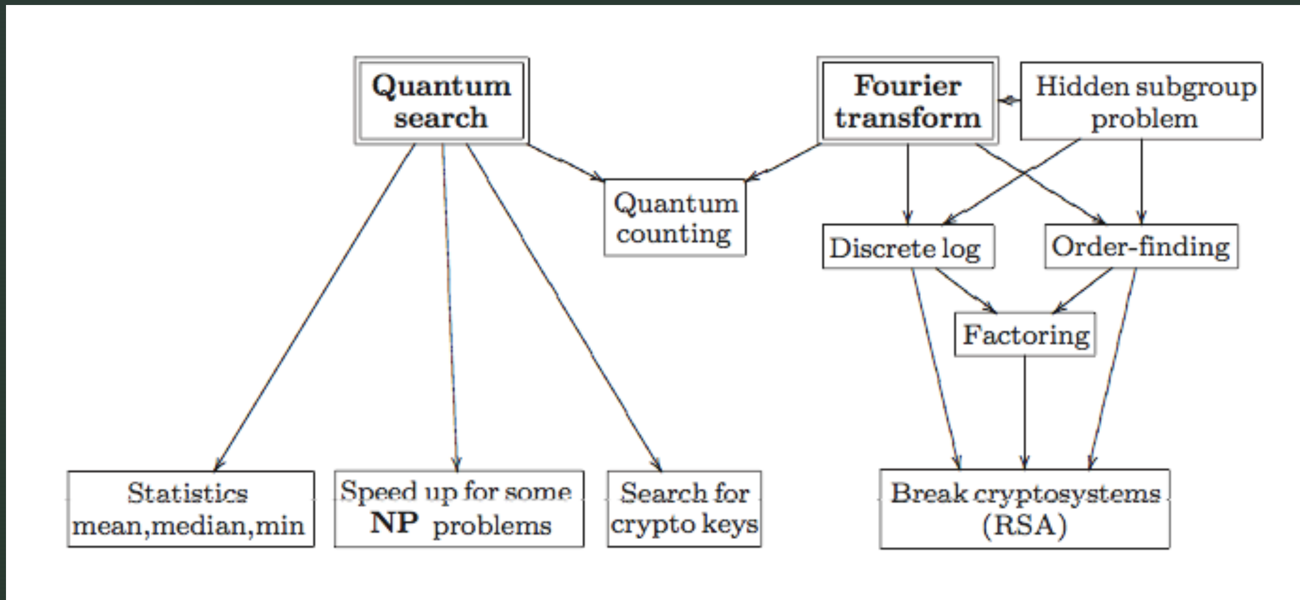
Before going in…

- From now, we are entering the ‘real’ Quantum Computing.
- Recall our first seminar? We shall prove many theorems and elaborate further on the topics I introduced at then.
- It shall be little more technical and hard than before, but I think it will be transmittable.

Before going in…

- Today, our content is based on chapters 4 on Nielsen & Chuang.
- First, we go through algorithms and little more on Quantum Circuits.
- I tried to incorporate some exercises. Harder exercises are explained, you must solve the easier ones.

An Overview


Quantum search
Fourier transform
Hidden subgroup problem
Quantum counting
Discrete log
Order-finding
Factoring
Statistics mean,median,min
Speed up for some NP problems
Search for crypto keys
Break cryptosystems (RSA)

Some Extra Gates

- $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
- Think of the Pauli Spin Matrices.
- Hadamard Gate $H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
- Phase Gate $S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$
- $\pi/8$ Gate $T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix} = e^{i\pi/8} \begin{bmatrix} e^{-i\pi/8} & 0 \\ 0 & e^{i\pi/8} \end{bmatrix}$

Rotations of Quantum Gates

- $R_x(\theta) \equiv e^{-\frac{i\theta X}{2}} = \cos\frac{\theta}{2} I - i\sin\frac{\theta}{2} X = \begin{bmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2} \\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix}$
- $R_y(\theta) \equiv e^{-\frac{i\theta Y}{2}} = \cos\frac{\theta}{2} I - i\sin\frac{\theta}{2} Y = \begin{bmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix}$
- $R_z(\theta) \equiv e^{-\frac{i\theta Z}{2}} = \cos\frac{\theta}{2} I - i\sin\frac{\theta}{2} Z = \begin{bmatrix} e^{-\frac{i\theta}{2}} & 0 \\ 0 & e^{\frac{i\theta}{2}} \end{bmatrix}$
- The Rotation operators rotate the state ket on the Bloch sphere. Check it!

Z-Y Decomposition for a Single Qubit

- Theorem. Suppose U is a unitary operation on a single qubit. Then there exist real numbers α, β, γ and δ such that U = exp(iα)Rz(β)Ry(γ)Rz(δ).
- Proof. The right hand side can be expressed as

$$U = \begin{bmatrix} e^{i(\alpha-\frac{\beta}{2}-\frac{\delta}{2})}\cos\frac{\gamma}{2} & -e^{i(\alpha-\frac{\beta}{2}+\frac{\delta}{2})}\sin\frac{\gamma}{2} \\ e^{i(\alpha+\frac{\beta}{2}-\frac{\delta}{2})}\sin\frac{\gamma}{2} & e^{i(\alpha+\frac{\beta}{2}+\frac{\delta}{2})}\cos\frac{\gamma}{2} \end{bmatrix}$$

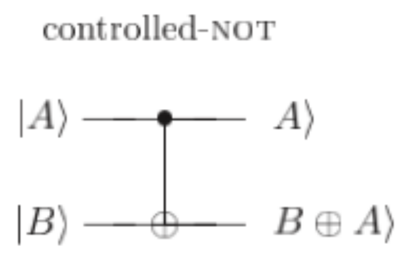
- Since U is unitary and therefore the rows and columns are orthonormal, we can decide the four variables.
- Should it be just Z & Y?

A Little Generalisation

- We can generalise the axes and state that:
- Suppose m and n are non-parallel real unit vectors in three dimensions.
- $U = \exp(i\alpha)R_n(\beta)R_m(\gamma)R_n(\delta)$.
- Corollary : Suppose U is a unitary gate on a single qubit. Then there exist unitary operators A, B, C on a single qubit such that $ABC = I$ and $U = \exp(i\alpha)AXBXC$, where α is some overall phase factor.

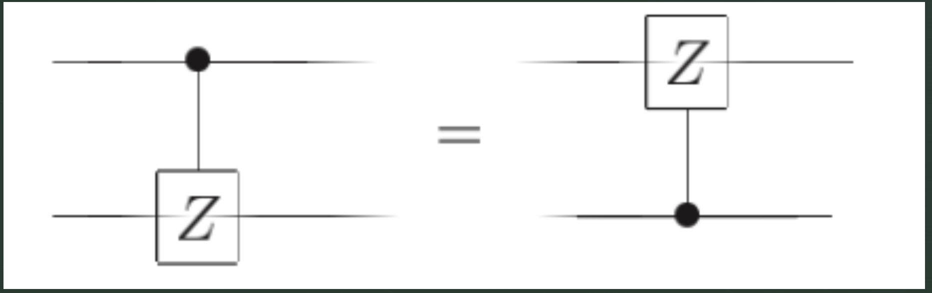
Controlled Operations

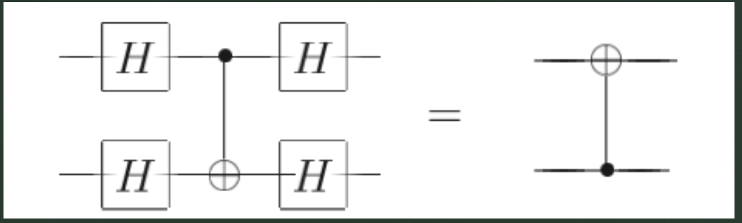
- Matrix Representations: Remember this?
- If the control qubit is set then U is applied to the target qubit, otherwise the target qubit is left alone; that is, $|c\rangle|t\rangle \rightarrow |c\rangle U^c|t\rangle$
- (Generalisation)



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

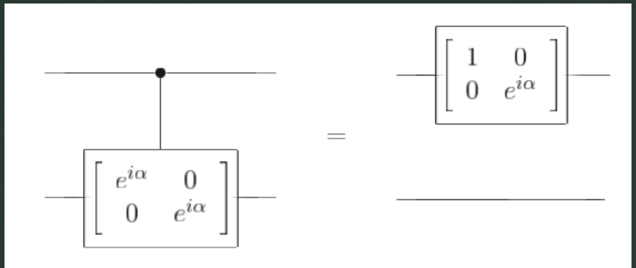
Exercises

- 1. Construct a gate from one controlled-Z gate, that is, the gate whose action in the computational basis is specified by the unitary matrix and two Hadamard gates.
- 2. Show 

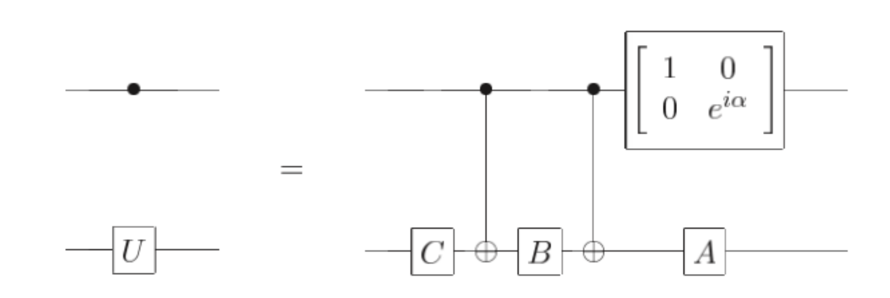
- 3. Flip of CNOT basis: 

Construction of the Controlled-U Opeartions

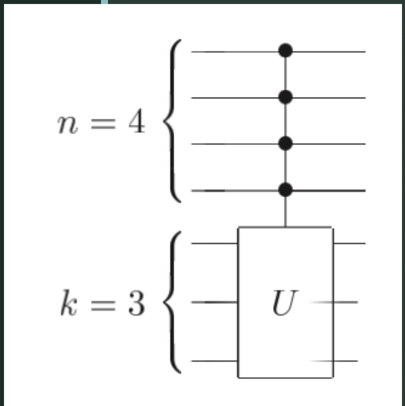
- Recall ABC = I and U = exp(iα)AXBXC
- Also, we have to give the phase, which is not very hard as



- From this,



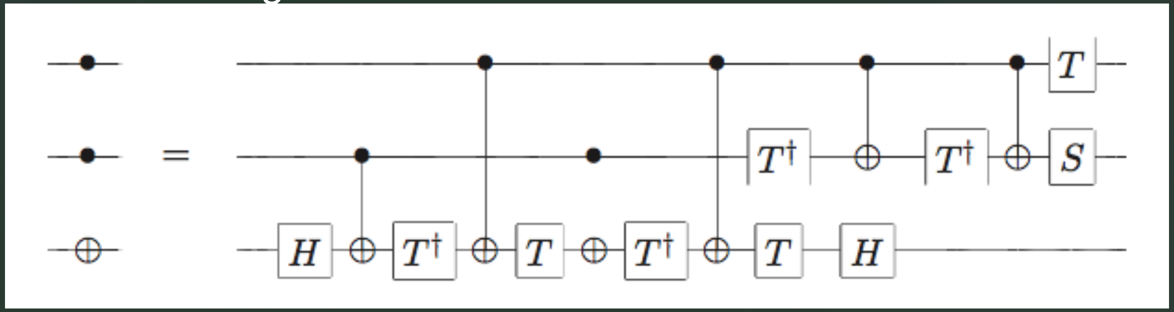
Conditioning of Multiple Qubits



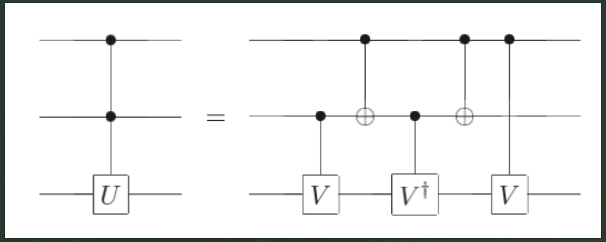
- $C^n(U)|x_1x_2x_3 \ldots x_n\rangle|\psi\rangle = |x_1x_2x_3 \ldots x_n\rangle U^{x_1x_2x_3\ldots x_n}|\psi\rangle$
- (More generally, suppose we have n + k qubits, and U is a k qubit unitary operator.)
- For U to operate in the k target qubits, all slots in $x_1x_2x_3 \ldots x_n$ should be 1!

Construction of the Toffoli Gate

- Doesn't the content in the last slide REALLY imply that we can make Toffoli gates?

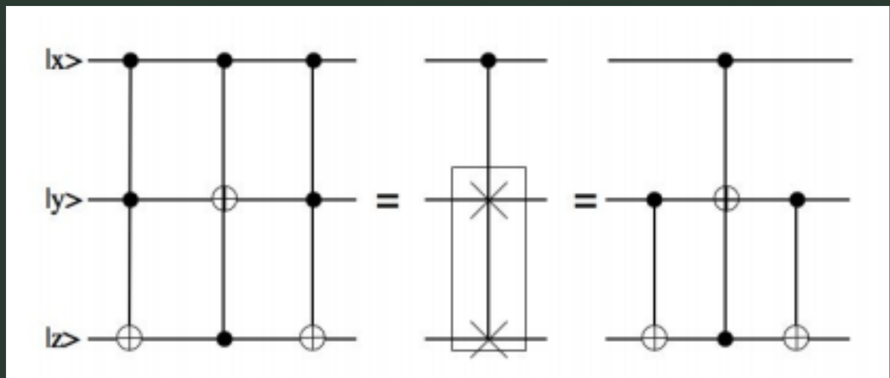


- Actually, we can create all CCU Gates with just CNOT and single Qubit operations.
- (You know what to do from here.)



Fredkin Gates

- Known as the CSWAP gate
- 1. Construct the Fredkin Gate using THREE Toffoli gates.
- 2. Actually, the first and third Toffoli can be replaced with CNOT.
- 3. More simply, we can just make this with 5 two-qubit operations.

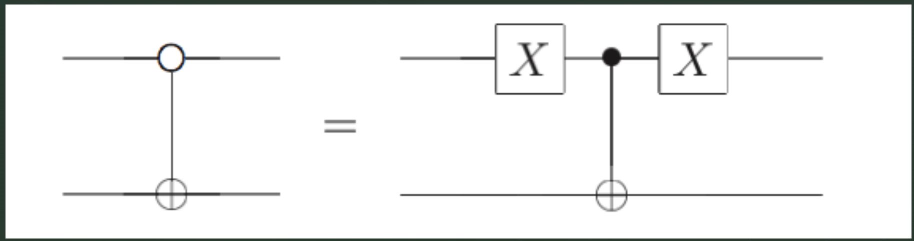


INPUT			OUTPUT		
C	I_1	I_2	C	O_1	O_2
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	1	0
1	1	0	1	0	1
1	1	1	1	1	1

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

Conditional Dynamics when control qubit is 0

- Until now, all the controlled operations were made only if the controlled qubits are 1.
- Constructing the gates which operates if the conrolled qubits are 0 is quite useful!
- Construction is easy:



Two Useful Theorems for Measurement

- **Principle of deferred measurement**: Measurements can always be moved from an intermediate stage of a quantum circuit to the end of the circuit; if the measurement results are used at any stage of the circuit then the classically controlled operations can be replaced by conditional quantum operations.

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

Universality

- Recall seminar 1 and 2?
- Some set of gates can create all algorithms by combination of their elements.
- Our goal: CNOT gates and single qubit gates can create all quantum computer algorithms.

Two-Level Unitary Gates

- Consider a unitary matrix U which acts on a d-dimensional Hilbert space.
- U may be decomposed into a product of two-level unitary matrices; that is, unitary matrices which act non-trivially only on two-or-fewer vector components.
- Considering for d=3 shall suffice the overall logic.

Two-Level Unitary Gates are Universal

- Claim. We can construct U_1, U_2, U_3 such that $I = U_3U_2U_1U$.
- Proof. Set $U = \begin{bmatrix} a & d & g \\ b & e & h \\ c & f & i \end{bmatrix}$
- If b=0, U1=I, else, $U_1 = \begin{bmatrix} \frac{a^*}{\sqrt{|a|^2+|b|^2}} & \frac{b^*}{\sqrt{|a|^2+|b|^2}} & 0 \\ \frac{b}{\sqrt{|a|^2+|b|^2}} & \frac{-a}{\sqrt{|a|^2+|b|^2}} & 0 \\ 0 & 0 & 1 \end{bmatrix}$
- $U_1U = \begin{bmatrix} a' & d' & g' \\ 0 & e' & h' \\ c' & f' & i' \end{bmatrix}$

Two-Level Unitary Gates are Universal

- If c'=0, $U_2 = \begin{bmatrix} a'^* & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$, else, $U_2 = \begin{bmatrix} \frac{a'}{\sqrt{|a'|^2+|c'|^2}} & 0 & \frac{c'}{\sqrt{|a'|^2+|c'|^2}} \\ 0 & 1 & 0 \\ \frac{c'}{\sqrt{|a'|^2+|c'|^2}} & 0 & \frac{-a'}{\sqrt{|a'|^2+|c'|^2}} \end{bmatrix}$
- $U_2 U_1 U = \begin{bmatrix} 1 & 0 & 0 \\ 0 & e'' & h'' \\ 0 & f'' & i'' \end{bmatrix}$
- I think it is now quite straightforward how to construct U_3.

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 members of the list differ in exactly one bit.
- For instance, with s = 101001 and t = 110011 we have the Gray code 101001 101011 100011 110011.

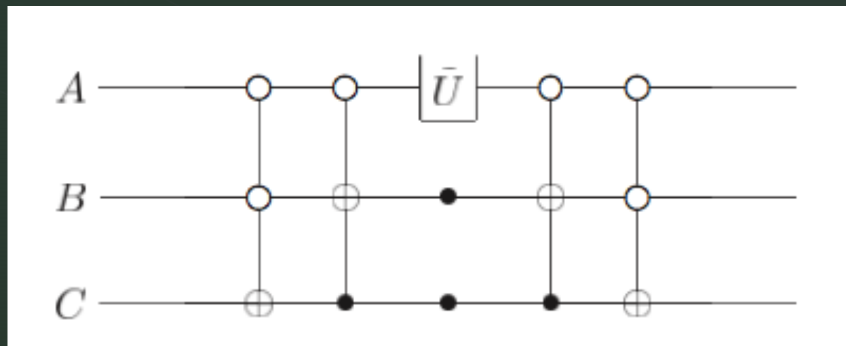
Shortening the Unitary operator to Two-Level Unitary Gates

- Implementing each step of the Gray code is easy: Use the controlled bit flip.
- Stop just before the final step: By now, the remaining operation is a controlled one-qubit gate. We know that this can be implemented using CNOT and single qubit operations.
- Then, just do the inverse process, and we are done.

Example

- Implement U.
- $\widetilde{U} = \begin{bmatrix} a & c \\ b & d \end{bmatrix}$
- Note that only 000 and 111 gives non-trivial terms.

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



Approximation of 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.
- A discrete set CAN be used to approximate any unitary operation.
- Definition of *Error*: $E(U,V) = \max_{|\psi\rangle} \|(U-V)|\psi\rangle\|$, where U is the real operator and V is the approximated one.

Approximation of Unitary Operators

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 corresponding measurement outcome if the operation U (or V) was performed. Then

$$|P_U - P_V| = \left|\langle\psi|U^\dagger M U|\psi\rangle - \langle\psi|V^\dagger M V|\psi\rangle\right|. \tag{4.64}$$

Let $|\Delta\rangle \equiv (U - V)|\psi\rangle$. Simple algebra and the Cauchy–Schwarz inequality show that

$$\begin{aligned} |P_U - P_V| &= \left|\langle\psi|U^\dagger M|\Delta\rangle + \langle\Delta|MV|\psi\rangle\right|. && (4.65)\\ &\leq |\langle\psi|U^\dagger M|\Delta\rangle| + |\langle\Delta|MV|\psi\rangle| && (4.66)\\ &\leq \||\Delta\rangle\| + \||\Delta\rangle\| && (4.67)\\ &\leq 2E(U,V). && (4.68)\end{aligned}$$

What does this inequality mean?
Ans: If the error is small, the difference of probabilities in measurement outcomes are also small.

- We CAN generalise this to n operators, and the result is:
- $E(U_m U_{m-1} \dots U_1, V_m V_{m-1} \dots V_1) \leq \sum_{j=1}^{m} E(U_j, V_j)$

Some Additional Theorems

- 1. The *standard set of gates*, comprised of Hadamard, Phase, CNOT, and $\frac{\pi}{8}$ gates are universal.
- Proof is made by picturing those gates at the Bloch sphere, which turns the gates into a rotation operators. We then use some $\epsilon - \delta$ technique to prove the theorem.

Some Additional Theorems

- Solovay-Kitaev Theorem: An arbitrary single qubit gate can be approximated to an accuracy ϵ requires $O(\log^{c}(1/\varepsilon))$ gates from our discrete set, where c is a constant approximately equal to 2.
- This is a polylogarithmic increase over the size of the original circuit, which is likely to be acceptable for virtually all applications.

Simulation of Quantum Systems

- Of course, this is possible in classical computers, albeit very inefficiently.
- Schrodinger's Equation: $i\frac{\partial}{\partial t}\psi(x) = (-\frac{1}{2m}\frac{\partial^2}{\partial x^2} + V(x))\psi(x)$
- This means we have to solve exponential amounts of equations for many-particle systems…

Quantum Simulation Algorithm

- $i\frac{\partial}{\partial t}|\psi\rangle = H|\psi\rangle$ ->$|\psi(t)\rangle = e^{-iHt}|\psi(0)\rangle$
- Yeah..of course we can just approximate to the first order. But srsly, do you really think this will be accurate?
- What we should do?: Let's class Hamiltonians to many local interactions. $H = \sum_{k=1}^{L} H_k$
- Each H_k shall work on finite numbers (actually, usually two) of particles and therefore be quite easy to evaluate using Quantum Circuits. (i.e. $e^{-iH_k t}$ is much easier to evaluate than e^{-iHt}.)

Quantum Simulation Algorithm

- Okay, but we do have some problems.
- If $[H_i, H_k]$ is NOT zero (which is the default), $e^{-iHt} \neq \prod_{k=1}^{L} e^{-iH_k t}$
- *Trotter's Formula:* Let A and B be Hermitian operators. Then for any real t, $\lim_{n\to\infty} (e^{iAt/n} e^{iBt/n})^n = e^{i(A+B)t}$
- I will not state the proof since it is little complicated, but one important consequence is $e^{i(A+B)\Delta t} = e^{iA\Delta t} e^{iB\Delta t} + O(\Delta t^2)$

Quantum Simulation Algorithm

Algorithm: Quantum simulation

Inputs: (1) A Hamiltonian $H = \sum_k H_k$ acting on an N-dimensional system, where each H_k acts on a small subsystem of size independent of N, (2) an initial state $|\psi_0\rangle$, of the system at $t = 0$, (3) a positive, non-zero accuracy δ, and (3) a time t_f at which the evolved state is desired.

Outputs: A state $|\tilde{\psi}(t_f)\rangle$ such that $|\langle\tilde{\psi}(t_f)|e^{-iHt_f}|\psi_0\rangle|^2 \geq 1 - \delta$.

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

Procedure: Choose a representation such that the state $|\tilde{\psi}\rangle$ of $n = \text{poly}(\log N)$ qubits approximates the system and the operators $e^{-iH_k\Delta t}$ have efficient quantum circuit approximations. Select an approximation method (see for example Equations (4.103)–(4.105)) and Δt such that the expected error is acceptable (and $j\Delta t = t_f$ for an integer j), construct the corresponding quantum circuit $U_{\Delta t}$ for the iterative step, and do:

1.	$|\tilde{\psi}_0\rangle \leftarrow |\psi_0\rangle$; $j = 0$	initialize 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