In this lecture, I'd like to talk about

"What is a quantum computer?" Dave Bacon

This may seem like a silly question to ask, but I'd like to argue that it is an extremely relevant question. The two reasons which I believe make this an important question are

(1) We are unsure of what a future quantum computer will look like. There are lots of people who think they have a good plan for building a quantum computer, and we have all these different proposals for a quantum computing architecture (ion traps, optical lattices, NMR quantum dots, etc.). But this early in the game it is hard to see a clear winner: we talk about 20-50 years for building one!

The outlook must have looked pretty dreadful too when Alan Turing wrote his famous paper in 1936 which founded computer science and people began to think about physical realizations of Turing's abstract ideas. And remember we built these vacuum tube machines along until the transistor was invented and Moore's incredible guess began to take over.

So I ask: do we really know what a future quantum computer will look like? And I'd have to be unbiased and say, in terms of physical realization, no. But if I showed Turing a modern computer, he'd certainly recognize how its operation fit in with the notion of a computer as he understood it (no slouch that Turing: he programmed primitive code in a base 32 notation others had to convert to decimal to understand).

So as we try to build a quantum computer, its important to understand exactly what is required to be a quantum computer

(2) Rolf Laundaur's ghost shouts at us that "information is physical!" Thus we'd better know what we mean by a quantum computer so when we examine different physical systems, if we find something which we cannot call a quantum computer, we'd better be able to point and say → "that's different!" These are the kind of deep questions that people like Fields medalist Michael Freedman and all-round-genius Alexi Kitaev ask - questions like "do topological field theories represent quantum computers?" I'm not so deep so I won't say any more about this - but I think its a healthy program to carry out and something that you might ponder on Sundays.

So lets jump in: what do we think is a quantum computer? I'm going to approach this question by first telling you of an example quantum computer and then working our way outward into more and more generality so that we can hopefully pen down what we mean by a quantum computer.

Introducing the Simpleton's quantum computer...

Consider a quantum system consisting of n two level systems.

system's Hilbert space $\equiv \mathcal{H} = \bigotimes_{i=1}^{n} \mathbb{C}^2$

This is an assumption of the subsystem nature of the

quantum system (more on this later!) Lets put these qubits on a linear array and give the qubits a standard basis $|0\rangle, |1\rangle$.

quantum circuit on n qubits (procedure)

(1) Preparation of an input state $|i\rangle$

$|i\rangle = |i_1\rangle \otimes |i_2\rangle \otimes \cdots \otimes |i_n\rangle \quad i_j \in \{0,1\}$ $|0\rangle, |1\rangle$ = computational basis

i.e. we feed in some "classical" information.

(2) Unitary evolution due to some quantum gates $\equiv U$
~for right now just think quantum gate $\equiv$ unitary evolution of k of n qubits.

(3) Measurement of the state of the n qubits in the computational basis. Output is measured state $|j\rangle$. Probability of output $|j\rangle$ is simply $P(j) = |\langle j|U|i\rangle|^2$

A quantum circuit on n qubits is just the above manipulation of quantum information: it doesn't yet embody the notion of a quantum computer!

(Think of the classical case. We input some information and get some output. At the current state any possible output is attainable. In fact any conceivable input-output relationship is acheivable. But nothing has been said about some mechanical recipe for ending up in this state of affairs.)

The notion of a quantum algorithm is embedded in the concept of a consistent uniform quantum circuit family.

quantum circuit family is a set of quantum circuits. The elements of this set are labeled by an integer n. n is the number of qubits in the quantum circuit on n qubits of which the circuit labeled by n is a member of.

quantum circuit family: set $\mathcal{C}$ of circuits $\mathcal{C} = \{C_1, C_2, C_3, \ldots\}$ where C_n is a quantum circuit on n qubits.

A quantum circuit family is called consistent if a circuit on n qubits C_n acting on an m qubit input ($m < n$) padded by $|0\rangle$'s gives the same output as C_m gives.

consistent: Let $C_n(|i\rangle)$ denote the output of circuit C_n on input $|i\rangle$. A circuit family $\mathcal{C} = \{C_1, C_2, C_3, \ldots\}$ is called consistent if

$$C_n(|i\rangle_m \otimes |0\rangle_{n-m}) = C_m(|i\rangle_m)$$

$|i\rangle_m \equiv$ m qubit input

$|0\rangle_{n-m} \equiv \underbrace{|0\rangle \otimes \cdots \otimes |0\rangle}_{n-m \text{ } |0\rangle\text{'s}}$

A quantum circuit family is called uniform if there is a classical algorithm for constructing the quantum circuit C_n given the input n describing the length of the input to C_n.

uniform: Given n there is a classical algorithm to construct C_n.

We brush some stuff under the rug when we say classical algorithm, but lets just assume you're all happy with what exactly a classical algorithm is! Also note the classical algorithm to construct the circuit is a place where we can hide some computational power! Beware!)

OK so now we have a notion of what a quantum algorithm is...
... its a consistent uniform quantum circuit family!

If this was the end of the story, we would be in a wicked state of affairs: for every quantum algorithm we would have to redesign our hardware (the quantum gates) each time we wanted to run a different quantum algorithm.

Luckily we aren't in such a pickle! Define:

A set of quantum gates $\mathcal{G}$ is a fully universal gate set if, for any $\epsilon > 0$, a sequence of gates from $\mathcal{G}$ can be used to produce a quantum circuit on n qubits to an accuracy of ϵ.

Well here we've gone and used a concept - accuracy - which we have even defined. So lets fix that:

The accuracy of two unitary evolutions, U and V, is

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

Why is this a good measure of accuracy?

1. Start in $|\psi\rangle$
2. perform U or V
3. measure $P_i = |i\rangle\langle i|$ ← doesn't matter that its a projection, lets just assume it.

The probability of outcome i is then either

$$p_i^U = \langle\psi| U^\dagger P_i U |\psi\rangle \quad \text{or} \quad p_i^V = \langle\psi| V^\dagger P_i V |\psi\rangle$$

The absolute value of the difference of these measurements is a good measure of accuracy

$$\begin{aligned} dP_i = |p_i^U - p_i^V| &= |\langle\psi| U^\dagger P_i U|\psi\rangle - \langle\psi| V^\dagger P_i V|\psi\rangle| \\ &\le |\langle\psi| U^\dagger P_i |\delta\rangle| + |\langle\delta| P_i V|\psi\rangle| \qquad |\delta\rangle = (U-V)|\psi\rangle \\ &\le \| P_i U|\psi\rangle \| \, \||\delta\rangle\| + \| P_i V_i |\psi\rangle\| \, \||\delta\rangle\| \\ &\le 2 \||\delta\rangle\| \end{aligned}$$

Thus

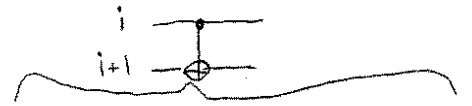
$$dP_i \le 2 \max_{|\psi\rangle} \|(U-V)|\psi\rangle\| \qquad dP_i \le 2E(U,V)$$

Lets look at a simple example to show that these things exist:

universal gate sets

Consider the set of quantum gates:

$$\mathcal{G} = \{ \exp[i\alpha \sigma_x^{(i)}],\ \exp[i\beta \sigma_z^{(i)}],\ \tfrac{1}{2}(\mathbb{I}+\sigma_z^{(i)}) + \tfrac{1}{2}(\mathbb{I}-\sigma_z^{(i)})\sigma_x^{(i+1)} \}$$



controlled (on i^{th} qubit) - not (on $(i+1)^{th}$ qubit)
$C(i)X^{(i+1)}$

α, β = irrational multiples of π.

steps towards showing universality:

(1) single qubit gates densely fill all possible single qubit operations:

$(\exp[i\alpha\sigma_x^{(i)}])^n = \exp[in\alpha\sigma_x^{(i)}]$ $\quad n\alpha \bmod 2\pi$ densely fills $[0, 2\pi)$ as n grows.

Thus we can generate $\exp[i\theta\sigma_x^{(i)}]$ and $\exp[i\phi\sigma_z^{(i)}]$ to any accuracy $\epsilon > 0$.

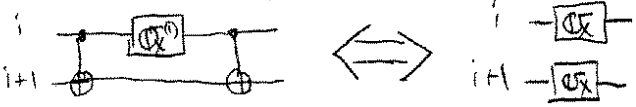
Recall Euler angle construction

$$\exp[i\vec{n}\cdot\vec{\sigma}^{(i)}] = \exp[i\theta_1\sigma_x^{(i)}]\exp[i\theta_2\sigma_z^{(i)}]\exp[i\theta_3\sigma_x^{(i)}]$$

so we can generate any $\exp[i\vec{n}\cdot\vec{\sigma}^{(i)}]$ to an accuracy $\epsilon > 0$.

(2) two qubit gates and SU(4) on two qubits

recall identity



$$[C(i)X^{(i+1)}]\,\sigma_x^{(i)}\,[C(i)X^{(i+1)}] = \sigma_x^{(i)}\sigma_x^{(i+1)}$$

sandwhich the controlled nots around a $\exp[i\theta\sigma_x^{(i)}]$ gate

$$[C(i)X^{(i+1)}]\exp[i\theta\sigma_x^{(i)}][C(i)X^{(i+1)}] = \exp[i\theta\sigma_x^{(i)}\sigma_x^{(i+1)}]$$

Now we can use the single qubit gates to rotate $\exp[i\theta\sigma_x^{(i)}\sigma_x^{(i+1)}]$ to $\exp[i\theta\sigma_\alpha^{(i)}\otimes\sigma_\beta^{(i+1)}]$; we can choose $\vec{n}_1$ and $\vec{n}_2$ such that.

$$\exp[i\vec{n}_1\cdot\vec{\sigma}^{(i)}]\exp[i\vec{n}_2\cdot\vec{\sigma}^{(i+1)}]\left(\exp[i\theta\sigma_x^{(i)}\sigma_x^{(i+1)}]\right)\exp[-i\vec{n}_1\cdot\vec{\sigma}^{(1)}]\exp[-i\vec{n}_2\cdot\vec{\sigma}^{(2)}]$$
$$= \exp[i\theta\sigma_\alpha^{(i)}\sigma_\beta^{(i+1)}]$$

(example $\frac{1}{\sqrt{2}}\begin{pmatrix}1&1\\1&-1\end{pmatrix}\begin{pmatrix}0&1\\1&0\end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix}1&1\\1&-1\end{pmatrix} = \begin{pmatrix}1&0\\0&-1\end{pmatrix}$)

This provides a prescription for densely generating

$$\exp[i\vec{n}\cdot\vec{\sigma}^{(i)}],\quad \exp[i\theta_{\alpha\beta}\sigma_\alpha^{(i)}\sigma_\beta^{(i+1)}]$$

The the Trotter formula

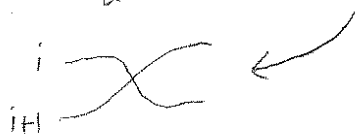
$$\left(\exp[iA\tfrac{t}{n}]\exp[iB\tfrac{t}{n}]\right)^n = \exp[i(A+B)t] + O\left(\tfrac{1}{n}\right)$$

then implies that between neighboring qubits we can perform to a desired accuracy

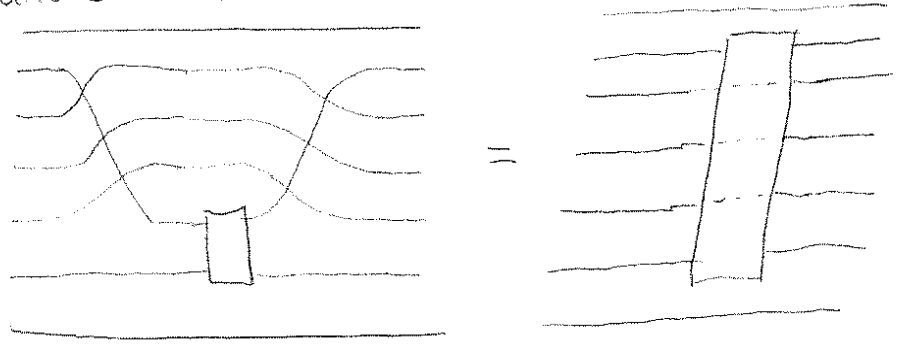
$$\exp\Big[i\sum_{\alpha,\beta=1}^{3}\theta_{\alpha\beta}\sigma_\alpha^{(i)}\sigma_\beta^{(i+1)} + \sum_{\alpha=1}^{3}(v_\alpha\sigma_\alpha^{(i)} + w_\alpha\sigma_\alpha^{(i+1)})\Big]$$

So we see that with $\mathcal{G}$ we can generate any element to a desired accuracy in $SU(4)$ between neighboring qubits. Among the $SU(4)$'s we can obtain the exchange gate between neighboring qubits (we have to goto $U(4)$, but this isn't a problem)

$$E_i = \tfrac{1}{2}(\mathbb{I} + \sigma_x^{(i)}\sigma_x^{(i+1)} + \sigma_y^{(i)}\sigma_y^{(i+1)} + \sigma_z^{(i)}\sigma_z^{(i+1)})$$



This allows us to create $SU(4)$ between any two qubits



(3) We've shown how to perform any unitary operator which can be generated by a two qubit "Hamiltonian", between any two qubits. Notice that the trick that we've used for permuting qubits is very powerful. It means that if we can perform $SU(2^k)$ on k qubits out of n, we can perform $SU(2^k)$ on any k of the n qubits.

This means that if we can show the lemma below, then we can perform all of $SU(2^n)$:

lemma: Given the ability to perform $SU(2^{K-1})$ on any $(K-1)$ of K qubits, the combined action of these operators can perform any $SU(2^K)$ on the K qubits

proof: Along with the Trotter formula,

$$\left(\exp\left[iA\tfrac{1}{n}\right]\exp\left[iB\tfrac{1}{n}\right]\right)^n = \exp[i(A+B)] + O\left(\tfrac{1}{n}\right)$$

the Lie product formula

$$\left(\exp\left[i\tfrac{A}{\sqrt{n}}\right]\exp\left[i\tfrac{B}{\sqrt{n}}\right]\exp\left[-i\tfrac{A}{\sqrt{n}}\right]\exp\left[-i\tfrac{B}{\sqrt{n}}\right]\right)^n$$

$$= \exp([B,A]) + O\left(\tfrac{1}{n^{3/2}}\right)$$

is also useful. These two formula tell us how to get elements of the Lie Algebra from elements of a Lie group. To the proof at hand:

(a) Using two elements of $SU(2^{K-1})$ we can construct Lie product evolutions with $A = \sum_{i=1}^{K-1} \sigma_x^{(i)} \sigma_z^{(K-1)}$, $B = \sum \sigma_y^{(K-1)} \sigma_x^{(K)}$, such that we obtain

$$\exp\left[[B,A]\right] + O\left(\tfrac{1}{n^{3/2}}\right) = \exp\left[it \prod_{i=1}^{K} \sigma_x^{(i)}\right] + O\left(\tfrac{1}{n^{3/2}}\right)$$

(b) Conjugating $\exp[it \prod_{i=1}^{K} \sigma_x^{(i)}]$ by elements of $SU(2)$ on single qubits we can rotate this to any Pauli basis on K qubits

$$\exp[i\vec{n}_1\cdot\vec{\sigma}^{(1)}]\cdots\exp[i\vec{n}_K\vec{\sigma}^{(K)}]\left(\exp\left[it\prod_{i=1}^{K}\sigma_x^{(i)}\right]\right)\exp[-i\vec{n}_1\cdot\vec{\sigma}]\cdots\exp[-i\vec{n}_K\cdot\vec{\sigma}^{(K)}]$$

$$= \exp[it\,\sigma_{\alpha_1}^{(1)}\sigma_{\alpha_2}^{(2)}\cdots\sigma_{\alpha_K}^{(K)}]$$

(c) Using Trotter, we can therefore obtain any

$$\exp\Big[\sum_{\alpha_1,\ldots,\alpha_K=0}^{3} h_{\alpha_1\alpha_2\cdots\alpha_K}\,\sigma_{\alpha_1}^{(1)}\sigma_{\alpha_2}^{(2)}\cdots\sigma_{\alpha_K}^{(K)}\Big] \qquad (\sigma_0^{(i)} = \mathbb{I})$$

$\alpha_1\neq 0$ and $\alpha_2\neq 0\cdots$ and $\alpha_K\neq 0$

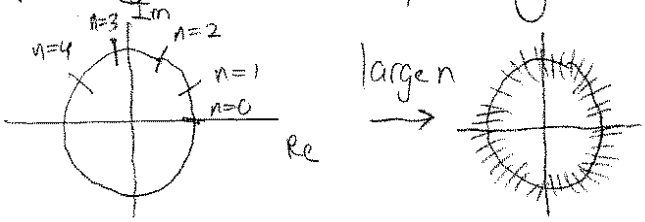
Thus we see how $\mathcal{G}$ can densely produce any $SU(2^n)$ acting on n qubits.

In discussing universal quantum gates, we haven't worried much about the efficiency of our constructions. Lets now worry about the efficiency.

Lets look at our first step in our demonstration of the universality above. We recall we used

$$(\exp[i\alpha\sigma_x^{(i)}])^n = \exp[in\sigma_x^{(i)}] \qquad \alpha \text{ irrational multiple of } \pi.$$

Diagramatically, we think about this going around the circle, never repeating and densely filling the circle



If we assume this filling is rather uniform, then we expect the *maximum* distance of any point from one of the elements to go like $O(\frac{1}{n})$. (Think if it was completely symmetric, then the distance between points is $O(\frac{1}{n})$. For large n, and uniform filling we thus get $\sim O(\frac{1}{n})$.)

Thus the first step in our construction produces gates to an accuracy $\epsilon = \frac{1}{n}$ if approximately n gates are used.

This is bad! To see why this is bad, we first need to show how accuracies "add" when we apply multiple gates. Previously we have seen how $\max_{|\psi\rangle} \|(U-V)|\psi\rangle\|$ is a good distance measure ($E(U,V)$)

Suppose we wish to execute T gates U_i, $i=1$ to T: $U_T U_{T-1} \cdots U_1$, but we use gates $\tilde{U}_i$ where $E(\tilde{U}_i, U_i) = \epsilon_i$. If we start in $|\psi_0\rangle$, and define the ideal state after t gates as

$$|\psi_t\rangle = U_t |\psi_{t-1}\rangle$$

Then we can trace the non ideal gates:

$\tilde{U}_t |e_{t-1}\rangle = |e_t\rangle + |E_t\rangle$ where $|E_t\rangle = (\tilde{U}_t - U_t)|e_{t-1}\rangle$ $\| |E_t\rangle \| \leq \epsilon_t$

So we find that if $|\tilde{e}_t\rangle = \tilde{U}_t \tilde{U}_{t-1} \cdots \tilde{U}_1 |e_0\rangle$,

$$|\tilde{e}_1\rangle = \tilde{U}_1 |e_0\rangle = |e_1\rangle + |E_1\rangle$$

$$|\tilde{e}_2\rangle = \tilde{U}_2 |\tilde{e}_1\rangle = |e_2\rangle + |E_2\rangle + \tilde{U}_2 |E_1\rangle$$

$$\vdots$$

$$|\tilde{e}_T\rangle = \tilde{U}_T |\tilde{e}_{T-1}\rangle = |e_T\rangle + |E_T\rangle + \tilde{U}_T |E_{T-1}\rangle + \cdots + \tilde{U}_T \tilde{U}_{T-1} \cdots \tilde{U}_2 |E_1\rangle$$

Thus

$$(U - \tilde{U})|e_0\rangle = |e_T\rangle - |\tilde{e}_T\rangle = |E_T\rangle + \tilde{U}_T |E_{T-1}\rangle + \cdots + \tilde{U}_T \tilde{U}_{T-1} \cdots \tilde{U}_2 |E_1\rangle$$

So the total error is

$$E(U, \tilde{U}) = \max_{|e_0\rangle} \| |E_T\rangle + \tilde{U}_T |E_{T-1}\rangle + \cdots + \tilde{U}_T \tilde{U}_{T-1} \cdots \tilde{U}_2 |E_1\rangle \|$$

$$\leq \sum_{i=1}^{T} E(U_i, \tilde{U}_i)$$

What is the significance of this for quantum circuits?

First this tells us about how accurate gates in a circuit family need to be in order to produce an ϵ accurate computation. If a circuit has T gates implemented with individual accuracy ϵ, the total accuracy is $T\epsilon$. To obtain a constant error, then an accuracy of $\epsilon = O(\frac{1}{T})$ is needed.

Second this tells us about efficiency for universal gate sets. Suppose we have a circuit family C_n which requires $f(n)$ gates from a gate set $\mathcal{G}$. To produce this circuit family with a universal gate set one approximates each of these $f(n)$ gates with a set of gates from the universal gate set. To produce an accuracy ϵ simulation of the quantum circuit each gate should be simulated to an accuracy $\frac{\epsilon}{f(n)}$.

Now we saw above how our simulation technique produced $O(\frac{1}{n})$ accuracy with n gates from the universal gate set. Thus to obtain total accuracy ϵ, each gate will be replaced by $f(n)/\epsilon$ universal gates [We want $O(\frac{\epsilon}{f(n)}) = O(\frac{1}{n}) \Rightarrow n = O(f(n)/\epsilon)$]. Thus a circuit family C_n with $f(n)$ gates from one gate set will take

$$O(f(n)^2/\epsilon) \text{ gates}$$

to simulate this circuit to order ϵ.

Now this isn't too good: it shows that different gate sets lead to different quantification of the number of gates needed depending on which gate set is used.

$$O(n^{10}) \longrightarrow O(\frac{n^{20}}{\epsilon}.) \quad \text{ouch!}$$

What is <u>really</u> bad about this is that every degree of precision we increase ϵ implies an order of magnitude increase in the number of gates needed

ϵ	ϵ^{-1}
10^{-1}	10
10^{-2}	10^2
10^{-3}	10^3

↓ ack!

Luckily we can do better than this due to an important theorem due to Kitaev and Solovay.

Kitaev-Solovay Theorem: Let the unitary operators $U_1, \ldots U_p$ generate a dense subset of $SU(n)$. Then any matrix $U \in SU(n)$ can be approximated to within ϵ by $\log^c(\frac{1}{\epsilon})$ elements of $U_1, \ldots, U_p$ and the inverses $U_1^+, \ldots U_p^+$ (c is constant)

We won't prove this here, but we can get some idea of how it works. In our arguement above, we took one $\exp[i a \sigma_q^{(i)}]$ and showed how repeated application produced n different gates. Now suppose we have two non-commuting operators U_a and U_b. The order of the application of the gates now matters.

n	possible gates
1	$U_a, U_b,$
2	$U_a U_b, U_b U_a, U_a^2, U_b^2$
3	$U_a^3, U_a^2 U_b, U_a U_b U_a, U_b U_a^2, U_b^2 U_a, U_b U_a U_b, U_a U_b^2, U_b^3$
⋮	

In general there are 2^n such combinations. If we assume these gates uniformly fill $SU(d)$, then if the gates don't "overlap" too much (i.e. same gate via different gate orders) we thus expect to obtain accuracy $\epsilon = O(\frac{1}{2^n})$ n gates. In general, we thus expect $\epsilon = O(\frac{1}{c^n})$ under the conditions of the Kitaev-Solovay Theorem.

For a circuit family with $f(n)$ gates, the Kitaev-Solovay Theorem implies a universal gate set can execute this circuit family with $O(f(n) \log^c(\frac{f(n)}{\epsilon}))$ elements to accuracy ϵ.

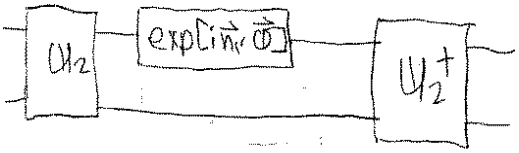
The Kitaev-Solovay theorem guarantees (to some limits) that different universal gate sets are basically the same in terms of efficiency.

The gate set

$$\mathcal{G} = \{\exp[i\alpha\sigma_x^{(1)}], \exp[i\beta\sigma_z^{(1)}], \text{CNOT}^{(1,2)}\}$$

is called the controlled-not plus single qubit gates for obvious reasons. What other gates can we combine with single qubit gates to obtain a universal gate set?

Almost any! The reason is due to the fact that we can use the conjugacy trick. Let U_2 be a two qubit gate which we combine with a gate set which is dense on $SU(2)$ for individual qubits. Then



will in general not be a member of $SU(2)$ on either qubit. The only gates which take $\exp[i\vec{n}_1\cdot\vec{\sigma}]$ to $SU(2)$ on either qubit are

1. SWAP GATE: $\$|i\rangle|j\rangle = |j\rangle|i\rangle$
2. Single qubit gates
   or combinations of (1) and (2)

Thus if U_2 is not in this set, then we produce

$$U_2 \exp[i\vec{n}_1\cdot\vec{\sigma}^{(1)}] U_2^\dagger = \exp\left[i\left(\sum_{\alpha,\beta=1}^{3}\theta_{\alpha\beta}\sigma_\alpha^{(1)}\sigma_\beta^{(2)} + \sum_{\alpha=1}^{3} v_\alpha\sigma_\alpha^{(1)} + w_\alpha\sigma_\alpha^{(2)}\right)t\right]$$

with $\theta_{\alpha\beta} \neq 0$ for at least one choice of α, β. Using the Trotter formula, we can subtract off the single qubit terms and produce

$$\exp\left[it\sum_{\alpha,\beta=1}^{3}\theta_{\alpha\beta}\sigma_\alpha^{(1)}\sigma_\beta^{(2)}\right]$$

Pick a $\theta_{\alpha\beta} \neq 0$. Then one can use the Lie Product to produce

$$\exp[it\,\theta_{\alpha\beta}\sigma_\alpha^{(1)}\sigma_\beta^{(2)}]$$

To see this note:

$$[\sigma_{\alpha_1}^{(1)}, [\sigma_{\alpha_2}^{(1)}, [\sigma_{\beta_1}^{(2)}, [\sigma_{\beta_2}^{(2)}, \sigma_{\alpha}^{(1)}\sigma_{\beta}^{(2)}]]]] =$$

$$\epsilon_{\alpha_1\eta\eta'}\,\epsilon_{\alpha_2\alpha\eta}\,\epsilon_{\beta_1\gamma\gamma'}\,\epsilon_{\beta_2\beta\gamma}\,\sigma_{\eta'}^{(1)}\sigma_{\gamma}^{(2)}$$

From which we can see every $\sigma_{\alpha}^{(1)}\sigma_{\beta}^{(2)}$ can be obtained from appropriate commutation.

Now starting from

$$\exp[it\,\theta_{\alpha\beta}\sigma_{\alpha'}^{(1)}\sigma_{\beta'}^{(2)}]$$

we can apply the arguements of the controlled not plus single qubit universality construction.

Board Plan

What is a quantum computer?

important cus:

(1) Unsure of future quantum computer!

(2) Information is physical ← beyond our current models??

The Simpleton's Quantum Computer

n qubits $\mathcal{H} = \bigotimes_{i=1}^{n} \mathbb{C}^2$ on a linear array

↑ subsystems structure

computational basis: $|i\rangle = |i_1\rangle \otimes |i_2\rangle \otimes \cdots \otimes |i_n\rangle \quad i_j \in \{0,1\}$

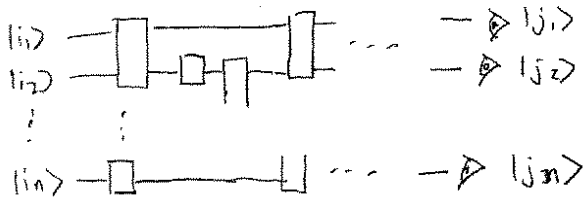
quantum circuit on n qubits (procedure)

(1) Preparation of input $|i\rangle$ in computational basis

(2) Unitary evolution (quantum gates) $\equiv U$

(3) Measurement in computational basis. Output is $|j\rangle$

$$\text{Prob}(j) = |\langle j|U|i\rangle|^2$$



quantum circuit NOT synonymous with quantum computation.

quantum circuit family: set $\mathcal{C}$ of circuits, $\mathcal{C} = \{C_1, C_2, \ldots\}$

where C_n is a quantum circuit on n qubits

consistent: $C_n(|i\rangle)$ denote output of circuit C_n on input $|i\rangle$ (n qubits)

$$C_n(|i\rangle_m \otimes |0\rangle_{n-m}) = C_m(|i\rangle_m) \quad n > m$$

uniform: Given n there is a classical algorithm to describe construction of C_n.

quantum algorithm = consistent uniform quantum circuit family

Universal gate set: A set of quantum gates $\mathcal{G}$ is universal if, for any $\epsilon > 0$, a sequence of gates from $\mathcal{G}$ can be used to produce a quantum circuit on n qubits to an accuracy of ϵ.

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

start in $|\psi\rangle$, perform U or V, measure $P_i = |i\rangle\langle i|$ (generally could be POVM.)

$$p_i^U = \langle\psi|U^\dagger P_i U|\psi\rangle \qquad p_i^V = \langle\psi|V^\dagger P_i V|\psi\rangle$$

$$dP_i = |p_i^U - p_i^V| = |\langle\psi|U^\dagger P_i U|\psi\rangle - \langle\psi|V^\dagger P_i V|\psi\rangle|$$

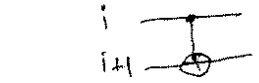
$$= |\langle\psi|U^\dagger P_i|\delta\rangle + \langle\delta|P_i V|\psi\rangle| \qquad |\delta\rangle = (U-V)|\psi\rangle$$

$$\le |\langle\psi|U^\dagger P_i|\delta\rangle| + |\langle\delta|P_i V|\psi\rangle|$$

$$\le \|P_i U|\psi\rangle\| \cdot \||\delta\rangle\| + \|P_i V|\psi\rangle\| \cdot \||\delta\rangle\| \le 2\||\delta\rangle\|$$

Thus

$$dP_i \le 2 \max_{|\psi\rangle} \|(U-V)|\psi\rangle\| \quad \text{or} \quad \boxed{dP_i \le 2E(U,V)}$$



example: $\mathcal{G} = \{\exp[i\alpha\sigma_x^{(i)}], \exp[i\beta\sigma_z^{(i)}], \frac{1}{2}(I+\sigma_z^{(i)}) + \frac{1}{2}(I-\sigma_z^{(i)})\sigma_x^{(i+1)} \equiv C^{(i)}X^{(i+1)}\}$

α, β irrational multiples of π.

controlled-not on i^{th} qubit, on $(i+1)^{th}$ qubit

1. single qubit gates

$(\exp[i\alpha\sigma_x^{(i)}])^n = \exp[in\alpha\sigma_x^{(i)}]$ $\quad n\alpha \bmod 2\pi$ densely fills $[0, 2\pi)$

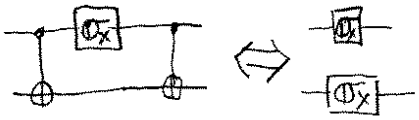
$\Rightarrow$ ability to generate $\exp[i\theta\sigma_x^{(i)}]$ and $\exp[i\phi\sigma_z^{(i)}]$ to any accuracy $\epsilon > 0$.

Euler angle:

$$\exp[i\vec{n}\cdot\vec{\sigma}^{(i)}] = \exp[i\theta_1\sigma_x^{(i)}]\exp[i\theta_2\sigma_z^{(i)}]\exp[i\theta_3\sigma_x^{(i)}]$$

$\Rightarrow$ single qubit gates ($SU(2)$) $e^{i\vec{n}\cdot\vec{\sigma}^{(i)}}$ to accuracy ϵ

2. two qubit gates

identity: 

$$C(i)X^{(i+1)}\,\sigma_x^{(i)}\,C(i)X^{(i+1)} = \sigma_x^{(i)}\,\sigma_x^{(i+1)}$$

This works "upstairs" too: downstairs $\rightarrow \{\ e^{iH}$ ← upstairs

$$C(i)X^{(i+1)}\exp[i\theta\sigma_x^{(i)}]\,C(i)X^{(i+1)} = \exp[i\theta\sigma_x^{(i)}\sigma_x^{(i+1)}]$$

Thus we can densely generate using $\mathcal{U}$

$$\exp[i\theta\,\sigma_x^{(i)}\sigma_x^{(i+1)}]$$

Further we can use the single qubits from (1) to produce

$$\exp[i\vec{n}_1\cdot\vec{\sigma}^{(i)}]\exp[i\vec{n}_2\cdot\vec{\sigma}^{(i+1)}]\,\sigma_x^{(i)}\sigma_x^{(i+1)}\exp[-i\vec{n}_1\cdot\vec{\sigma}^{(i)}]\exp[-i\vec{n}_2\cdot\vec{\sigma}^{(i+1)}]$$
$$= \sigma_\alpha^{(i)}\sigma_\beta^{(i+1)}$$

so that using this we can densely produce any

$$\exp[i\theta\,\sigma_\alpha^{(i)}\sigma_\beta^{(i+1)}]$$

$$\Rightarrow \{\exp[i\vec{m}_1\cdot\vec{\sigma}^{(i)}],\ \exp[i\vec{m}_2\cdot\vec{\sigma}^{(i+1)}],\ \exp[i\theta_{\alpha\beta}\sigma_\alpha^{(i)}\sigma_\beta^{(i+1)}]\} = \mathcal{U}$$

which is SU(4) on two qubits

Trotter formula

$$\left(\exp[i\tfrac{At}{n}]\exp[i\tfrac{Bt}{n}]\right)^n = \exp[i(A+B)t] + O(\tfrac{1}{n})$$

$$\left[\left(\mathbb{I}+i\tfrac{At}{n}\right)\left(\mathbb{I}+i\tfrac{Bt}{n}\right)\right]^n = \left[\mathbb{I}+i\left(\tfrac{At}{n}+\tfrac{Bt}{n}\right)+O(\tfrac{1}{n^2})\right]^n = \exp[i\tfrac{(A+B)t}{n}]+O($$

Using $\mathcal{U}$ Trotter ⇒

$$\exp\left[i\left(\left(\sum_{\alpha,\beta=1}^{3}\theta_{\alpha\beta}\sigma_\alpha^{(i)}\sigma_\beta^{(i+1)}\right)+\sum_\alpha v_\alpha\sigma_\alpha^{(i)}+w_\alpha\sigma_\alpha^{(i+1)}\right)\right]$$

But these are all the elements of SU(4)

SU(4) = unitary matrices $U^\dagger U=\mathbb{I}$ with $\det U=1$

$U=\exp[iH]$, $U^\dagger=U^{-1}\Rightarrow H$ is hermitian.

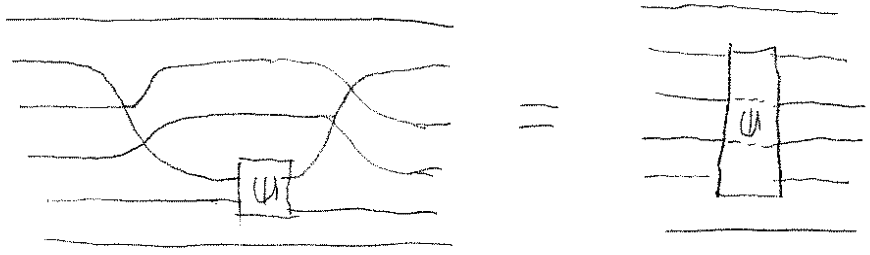
Any Hermitian on two qubits

$$H=\sum_{\alpha\beta=1}^{3}\theta_{\alpha\beta}\sigma_\alpha^{(i)}\sigma_\beta^{(i+1)}+\sum_{\alpha=1}^{3}v_\alpha\sigma_\alpha^{(i)}+w_\alpha\sigma_\alpha^{(i+1)}$$

Important gate in $U(4)$ = exchange gate = SWAP gate.

$\mathbb{E}_i |\psi\rangle_i |\phi\rangle_{i+1} = |\phi\rangle_i |\psi\rangle_{i+1}$

$\mathbb{E}_i$ allows for $SU(4)$ between any qubits



(3) Combining subsystems

$\exp[iHt]$ $H = \sum$ $\underbrace{\sigma_{q_1}^{(B_1)} \cdots \sigma_{q_{K-1}}^{(B_{K-1})}}_{(K-1)\text{ Pauli matrices}}$

lemma: The ability to perform $SU(2^{K-1})$ on any $(K-1)$ of K qubits $\Rightarrow$ the combined action of these operators can perform $SU(2^K)$ on all K qubits.

proof: Trotter: $\left(\exp[i\frac{A}{n}]\exp[i\frac{B}{n}]\right)^n = \exp[i(A+B)] + O(\frac{1}{n})$

Lie Product:

$$\left(\exp[i\tfrac{A}{n}]\exp[i\tfrac{B}{n}]\exp[-i\tfrac{A}{n}]\exp[-i\tfrac{B}{n}]\right)^n = \exp([B,A]) + O(\tfrac{1}{n^2})$$

(a) Let $A = \sqrt{t}\left(\prod_{i=1}^{K-2}\sigma_x^{(i)}\right)\sigma_z^{(K-1)}$ and $B = \sqrt{t}\,\sigma_y^{(K-1)}\sigma_x^{(K)}$

Now $\exp[i\frac{A}{n}]$ and $\exp[i\frac{B}{n}]$ are both in $SU(2^{K-1})$'s.

Lie Product $\Rightarrow$

$\exp[\,[B,A]\,]$ $\rightarrow [A,B] = \left[\sqrt{t}\left(\prod_{i=1}^{K-2}\sigma_x^{(i)}\right)\sigma_z^{(K-1)}, \sqrt{t}\,\sigma_y^{(K-1)}\sigma_x^{(K)}\right]$

$= -it\prod_{i=1}^{K}\sigma_x^{(i)}$.

$\exp[[B,A]] = \exp[it\prod_{i=1}^{K}\sigma_x^{(i)}]$

(b) conjugation trick

$$\exp[i\vec{n}_1\cdot\vec{\sigma}^{(1)}]\cdots\exp[i\vec{n}_K\vec{\sigma}^{(K)}]\left(\prod_{i=1}^{K}\sigma_x^{(i)}\right)\exp[i\vec{n}_1\cdot\vec{\sigma}^{(1)}]\cdots\exp[-i\vec{n}_K\cdot\vec{\sigma}^{(K)}]$$

$$= \sigma_{a_1}^{(1)}\sigma_{a_2}^{(2)}\cdots\sigma_{a_K}^{(K)}$$

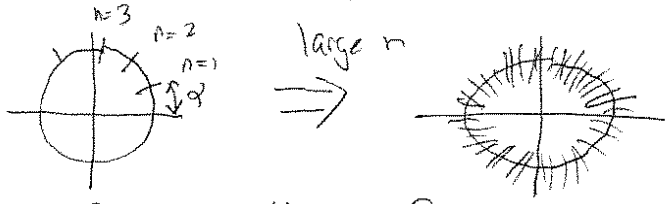
$\Rightarrow \exp[it\,\sigma_{a_1}^{(1)}\sigma_{a_2}^{(2)}\cdots\sigma_{a_K}^{(K)}]$

(c) Trotter $\Rightarrow$

$$\exp[i\sum_{\substack{a_1,\ldots,a_K=0 \\ a_1\neq 0 \text{ and } a_2\neq 0 \cdots \text{ and } a_K=0}}^{3} h_{a_1 a_2\cdots a_K}\,\sigma_{a_1}^{(1)}\sigma_{a_2}^{(2)}\cdots\sigma_{a_K}^{(K)}] \qquad (\sigma_0^{(i)} = \mathbb{I})$$

accuracy:

$(\exp[i\alpha\sigma_x^{(j)}])^n = \exp[i\alpha n \sigma_x^{(j)}]$



Assume filling is rather uniform.

distance between elements $\sim O(\frac{1}{n})$ (Think evenly divided pi)

$\Rightarrow$ accuracy of gate $\sim O(\frac{1}{n})$.

use n gates, get arbitrary gate to accuracy $O(\frac{1}{n})$

BAD! Why?...

multiple gate accuracy

$U_T U_{T-1} \cdots U_2 U_1 \equiv U$ desired

$\tilde{U}_T \tilde{U}_{T-1} \cdots \tilde{U}_2 \tilde{U}_1 \equiv \tilde{U}$ actual

start with $|\varphi_0\rangle$

$|\varphi_t\rangle = U_t |\varphi_{t-1}\rangle$, $|\tilde{\varphi}_t\rangle = \tilde{U}_t |\tilde{\varphi}_{t-1}\rangle$

define $|E_t\rangle$:

$\tilde{U}_t |\varphi_{t-1}\rangle = |\varphi_t\rangle + |E_t\rangle \quad |E_0\rangle = (\tilde{U}_t - U_t)|\varphi_{t-1}\rangle$

see...

$|\tilde{\varphi}_1\rangle = \tilde{U}_1 |\varphi_0\rangle = |\varphi_1\rangle + |E_1\rangle$

$|\tilde{\varphi}_2\rangle = \tilde{U}_2 |\tilde{\varphi}_1\rangle = U_2|\varphi_1\rangle + \tilde{U}_2|E_1\rangle = |\varphi_2\rangle + |E_2\rangle + \tilde{U}_2|E_1\rangle$

$\vdots$

$|\tilde{\varphi}_T\rangle = \tilde{U}_T |\tilde{\varphi}_{T-1}\rangle = |\varphi_T\rangle + |E_T\rangle + \tilde{U}_T|E_{T-1}\rangle + \cdots + \tilde{U}_T \tilde{U}_{T-1} \cdots \tilde{U}_2 |E_1\rangle$

Total error

$E(U, \tilde{U}) = \max_{|\psi\rangle} \|(U - \tilde{U})|\psi\rangle\| = \max_{|\varphi_0\rangle} \| |\varphi_T\rangle - |\tilde{\varphi}_T\rangle \|$

$= \max_{|\varphi_0\rangle} \| |E_T\rangle + \tilde{U}_T|E_{T-1}\rangle + \cdots + \tilde{U}_T \tilde{U}_{T-1} \cdots \tilde{U}_2 |E_1\rangle \|$

$\leq \| |E_T\rangle \| + \| \tilde{U}_T |E_{T-1}\rangle \| + \cdots + \| \tilde{U}_T \tilde{U}_{T-1} \cdots \tilde{U}_2 |E_1\rangle \|$

$E(U, \tilde{U}) \leq \sum_{T=1}^{T} E(U_T, \tilde{U}_T)$

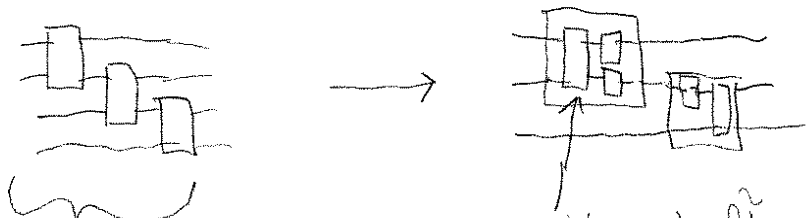
Circuit with T gates, individual accuracy $\epsilon \Rightarrow$ total accuracy $= T\epsilon$.

$\Rightarrow$ To obtain constant error $\epsilon = O(\frac{1}{T})$.

BAD? why?...

Circuit family C_n which uses $f(n)$ gates (n is input size) from $\tilde{\mathcal{G}}$

Suppose we use our universal gate set $\mathcal{G}$



$f(n)$ gates from $\tilde{\mathcal{G}}$

simulate each $\tilde{\mathcal{G}}$ gate with $\mathcal{G}$ gates.

total accuracy $= \epsilon$

gates from $\mathcal{G}$ to accuracy $= \frac{\epsilon}{f(n)}$

our universality construction $\Rightarrow$ accuracy $\epsilon = O(\frac{1}{n})$ where n is number of gates from $\mathcal{G}$.

$\frac{\epsilon}{f(n)} = \frac{1}{n} \Rightarrow n = \frac{f(n)}{\epsilon}$ gates to simulate gates in $\mathcal{G}$ to accuracy $\frac{\epsilon}{f(n)}$.

total gates from $\mathcal{G}$

$= f(n) \times n = \frac{f(n)^2}{\epsilon}$

$f(n)$ gates from $\tilde{\mathcal{G}}$ to obtain C_n

$\uparrow$

$\frac{f(n)^2}{\epsilon}$ gates from $\mathcal{G}$ to approximate C_n to accuracy ϵ

Ack: $f(n) \to f(n)^2$ and $\frac{1}{\epsilon} \Rightarrow$ each bit of precision $\Rightarrow$ multiplicative more work.

Kitaev-Sdovay: Let the unitary operators $U_1, \ldots, U_p$ generate a dense subset of $SU(n)$. Then any matrix $U \in SU(n)$ can be approximated to within ϵ by $\log^c\left(\frac{1}{\epsilon}\right)$ elements of $U_1, \ldots, U_p$ and the inverses $U_1^\dagger \ldots U_p^\dagger$ (c is constant)

Basic idea:

above we used one U to produce U^n. For fixed n, only n different U^n's. n, # possible gates $= n$

one of two $\{U_1, U_2\}$ where U_1, U_2 do not commute.

n	possible gates
1	U_1, U_2, I
2	U_1^2, U_1U_2, U_2U_1, U_2^2 + $n=1$ gates
3	U_1^3, $U_1^2U_2$, $U_1U_2U_1$, $U_2U_1^2$, $U_2^2U_1$, $U_2U_1U_2$, $U_1U_2^2$, U_2^3 + $n=2$ gates
⋮	
n	2^n possible combinations + $n-1$ gates

exponential growth

Universality: circuit family with $f(n)$ gates.
to $\frac{\epsilon}{f(n)}$ with $\log^c\left(\frac{f(n)}{\epsilon}\right)$

$\Rightarrow O\left(f(n)\log\left(\frac{f(n)}{\epsilon}\right)\right)$ gates from $\mathcal{G}$ need to produce circuit families in $\mathcal{G}$

Kitaev-Sdovay $\Rightarrow$ many different gate sets essentially equivalent.

expand... qutrits, qudits
subsystem structure

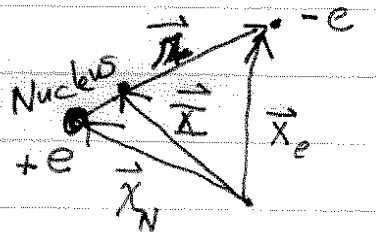
example load XX
$ZI + IZ = 0$
$-IZ + ZI = 0$

Ivan Deutsch

SQuInT Student Summer Retreat 6/25 - 6/29/01

Lecture #2: Optical Lattices

- Interaction of E+M field with atom:



Single electron in conduction shell (Alkali)

$$\vec{x} = \vec{x}_e - \vec{x}_N \qquad \vec{X} = \frac{m_e \vec{x}_e - m_N \vec{x}_N}{M}$$

$$\vec{p}_\mu = \frac{\vec{p}_e}{m_e} - \frac{\vec{p}_N}{m_N} \qquad \vec{P} = \vec{p}_e + \vec{p}_N$$

Interaction energy

$$H_{int} = \frac{e}{c m_e} \vec{p}_e \cdot \frac{\vec{A}}{c}(\vec{x}_e, t) - \frac{e}{c m_N} \vec{p}_N \cdot \frac{\vec{A}}{c}(\vec{x}_N, t)$$

$$- \vec{\mu}_e \cdot \vec{B}(\vec{x}_e, t) - \vec{\mu}_N \cdot \vec{B}(\vec{x}_N, t) + \sum q_i V(\vec{x}_i, t)$$

$V \to 0$ (Not static $\vec{E}$)

Plane wave (laser) $\vec{A}(\vec{x}, t) = \mathrm{Re}\left(\vec{\epsilon}\, A_0(\vec{x})\, e^{i(\vec{k}_L \cdot \vec{x} - \omega_L t)}\right)$

$$\vec{x}_e = \vec{X} + \frac{m_N}{m_e + m_N}\vec{r} \approx \vec{X} + \vec{r}$$

$$\vec{x}_N = \vec{X} - \frac{m_e}{m_e + m_N}\vec{r} \approx \vec{X}$$

$$\Rightarrow H_{int}^{(Field)} = \mathrm{Re}\left[\frac{e}{c}\left(\frac{\vec{p}_e}{m_e} e^{i\vec{k}_L \cdot \vec{r}} A_0(\vec{X} + \vec{r}) - \frac{\vec{p}_N}{m_N} A_0(\vec{X})\right) e^{i\vec{k}\cdot\vec{X}} e^{-i\omega_L t}\right]$$

Electric dipole approximation $\lambda_L \gg a_0 = |\vec{r}|$

$k_L a_0 \ll 1 \Rightarrow$ set $\vec{r} = 0$