# Quantum algorithm

ANIMESH DATAA

2015 年 7 月 19 日

## 1 classical computational models

**SINGLE BIT GATES**

1. Turing Machine
2. Circuit Model: bits, gates

1.Identity : I: $a \longrightarrow a$

2.NOT :

3.FANOUT(copy):

**TWO BIT GATES**

1:SWAP:

2:AND:

3:XOR:

4:NAND:

5:NOR:

6:OR:

That is already quite a lot of gates,so what can we do with these things?

Question :What do we want to do ?

Ansumer: Evaluate function $f : 0, 1^N \to 0, 1^N$

The simplest case is $M = 1$.Such Boolean function are called DECISION problems.

In fact there are $2^N$ Boolean funtions on N bits.Single and two-bit gates are $N = 1 and N = 2$ Boolean functions.

Most(or many)functions(or problems) can be cast to decision problems .

Example: Factoring

$$f(x) = \begin{cases} 1, & \text{if x has a ? y} \\ 0, & o.w. \end{cases} \tag{1}$$

EXAMPLE: Add $x = x_2x_1x_0$and $y = y_2y_1y_0$.needs a half-adder(HA) and full-adder(FA).

HAFFADDER:

**

FULL ADDER:

**

Putting it all together:

**

Computing any Boolean function :

The computation proceed by ? the matriced induction.Assume there is a circuit for any Boolean function N bits.

Say , f is a (N+1) bit function.

Now define N-bit function $f_0$ and $f_1$ as :

$$f_0(x_1, ...x_N) \equiv f(0, x_1, ..., x_N)$$

$$f_1(x_1, ...x_N) \equiv f(1, x_1, ..., x_N)$$

That is :

$$f_{x_0}(x_1, ...x_N) \equiv f(x_0, x_1, ..., x_N) OR (1 \oplus x_0) f_0(x_1, ..., x_N) \oplus x_0 f_1(x_1, ...x_N)$$

Thus:

**

The induction two needs AND,NOT,XOR,and FANOUT.

Furthermore,

***

NAND is a universal gate with ancilla bits of FANOUT.

The NAND gate is also irreversible.This is because the 2 input bits and one output bit;and it is not possible to recover the inputs by ? the output bits

This leads to energy dissipution:Lauduer principle.

Here is an illustration: A molecule of gas can be put into box with a partion.We can put the gas in the left or right .Say on the R.

**

Now, erasure means ? it in one of the sides irrespect of where it started.This can be done by removing the partition and then compressing the partition to one side.

**

This reduces the ? by $\Delta S = Kln2$

At isothermal temperature T,$\Delta w = KTln2$,which has to be provided.Thus,erasure of information leads to an energy bill.At room temperature $(20^oC)$,this is about :

$$\Delta \approx 2FSJ \sim 10^{-24} J$$

.

Modern computations are at about $10^{-6}$times this .

**Reversible classical computation**

Any irreversible function $f : 0, 1^N \to 0, 1^N$can be embedded in a function $\widetilde{f} : 0, 1^{N+M} \to 0.1^{N+M}$ such the

$$\widetilde{f}(x, o^N) = (x, f(x))$$

$\widetilde{f}$can be extended to a 1-1 function,e.g:

$$\widetilde{f}(x, y) = (x, y \oplus f(x))$$

This is not a unique extension,but we will ues it as the reversible function.
Question: Does this work for reversible gates as well
Number of N-bit gates :(N inputs,N outputs):$(2^N)^{2^N} : (N_i)$
Number of N-bit reversible gates : :$(2^N)! : (N_i)$
Let us study this in some detail for N=2 bits. A general 2 bit gate is :

As we can see ,the irreversibly ? in the nonlinear term ,2-bit reversible gates are all linear,with reversible M.
Exercise: Show that no 2-bit gate can lead to a universal set.
so we need 3 bit reversible gets for a universal set.
FREDKIN GATE:
**

TOFFOLI GATE :
**
EXERCISE:1.Show that the CNOT GATE is reversible .
2. Obtain the SWAP gate using only CNOT .
3. What is the least ??

# 2 quantum computational models

Chunch-Turing thesis: is a hypothesis about the nature of computable functions.
The heuristic agreement is that all algorithmically computable functions are Turing-computable .
Generally speaking,this is a classical computes with unlimited memory.
But it addresses and suggests connection to the space and time requirements for computations.It asks fundamental question such as
1. what is physical computation?
2. What is the potential and limitation of physical computation ?
3. What is mean by the universality of computation?
The long-standing open question is its derivation from the lows of physics.A modern,stronger

?:

Church-Turing-Deutsdu Principle:

Every physical pocess can be simulated efficiently by a universal computation device.

So, nature is a massive computation device.

The laws of physic(including the undiscovered theories of the future) according the notion of universal computation .

Correct status of observation: classical computers do not seem to be able to simulate system efficiently.

Possible resolution: 1: A quantum Turing machine should be a universal computing model. 2: An efficient classical simulation of quantum system is indeed possible.

The following models are throwing to be universal computation device/system.

Quantum Turing machine

Quantum circuit model$\longrightarrow$quamtum cellular automachine,Topological computation,Holonomic computation.

Quantum adiabatic computation.

Quantum random walk

Measurement based quantum computation $\longrightarrow$ teleportation-based.$\longrightarrow$entanglement-based

Quantum circuits:

bit strings $\leftrightarrow$state vectors

gates $\leftrightarrow$state unitary operations

measurement$\leftrightarrow$state Born rule possible

Since vectors and operation need a basis, we will use the eigenstate of a Pauli-Z operation ,$|0> and |1>$

**

So what is going on?

1. An arbitrary classical gate M because linear operator

$$A|x>=|M_X>, <y|A|x>=\sigma_{y,Mx}$$

2. A reversible classical gate becomes a permutation unitary.
3. There are many more unitaries than reversible classical gates.
4. Born rule to measurements

Function evaluation in quantum circuits:

If f is a Boolean function, $U_f$ is a controlled bit flip op.

The control qubits are $|x>=|x_1,...x_N$,the value of the control is determined by $f(x)$

If $f(x)=0$,the target qubit remain unchanged.

If $f(x)=1$,the target qubit flips.

Quantum parallelism: f on an N-bit Boolean function .

**

Any classical algorithm to determin the partly of f, or whether f is constant or balanced, needs two runs.Deutsch does it in one.

Deutsch-Jossa algorithm :
To determine ?

$$f : 0, 1^N \to 0, 1$$

is constant or balanced.
**

# 3 universal quantum gates

Established in 3 steps.
1. Any $D \times D$ unitary matrix U can be written as a product of at most $D(D-1)/2$ two-level unitary tran? machine[Note that this is not efficient,now of $D = 2^N$,for N.
2. Any two-level transition can be reduced to CNOTs and simple-qubit ?
3. Any simple qubit ?can be appoximated by a sequence of ? drawn from a finite set,for example ,Hand T.Moreover,the approximation can be efficient in the new ? in a ? with M gates (CNOTs or simple-qubit ?),the approximation can be performed with 0(Mlog(M/$\varepsilon$)) gates ,where $\varepsilon$ is the ?? of the approximation

Step:1, Let $T^{JK}$ denote a translation matrix between levels $|J >< ||k >$

$$[T^{JK}]_{jk} = \begin{cases} \delta_{jk}, & j \neq J, K, k \neq J, K \\ \alpha, & j = J, k = J \\ \beta, & j = J, k = K \\ \gamma & j = K, k = J \\ \sigma & j = K, k = K \end{cases} \tag{2}$$

Suppose that $U' = UT^{JK}$.All matrix elements of $U^{'}$are the same as these in U,expect those in columns J and K, for which we have

$$U^{'}_{jJ} = U_{jK}T^{JK}_{KL} = \alpha U_{jJ} + \gamma U_{jk}$$

$$U'_{jk} = U_{jk}T^{JK}_{kK} = \beta U_{jJ} + \sigma U jK$$

In each row,$T^{JK}$mixes the elements in columns J and K to set new elements for columns J and K.
Let us now suppose that U has the structure :
**
Now that :
There is a transition matrix $T^{JK}$ such that $U' = UT^{JK}$ has the same structure as $U_1$ with(?),$U^{'}_{jk} =$ 0and $U'_{Jj}$ ?

Clearly,the way $T^{JK}$ acts,it does not disturb the structure of 1's and 0's in U.

$$U'_{JK} = \beta U_{JJ} + \sigma U_{JK}, U'_{JJ} = \alpha U_{JJ} + \gamma U_{JK}$$

if $U_{Jj} = U_{jk} = 0$,any unitary choice of $\mathfrak{T}$ will do ,even the identity.If not, then choose :

$$\beta = \frac{U_{JK}}{\sqrt{|U_{JJ}|^2 + |U_{JU}|^2}}$$

So, can now start with a unitary matrix of the form
**
and convert it ,by application of transition ?,to one where the $J^{th}$ now has all news expect a need,nonnegative entry on the diagonal . **
So,we set a matrix $U^{T+1}$:

$$U^{J+1} = U^J T^{J,J+1} T^{J,J+2} ... T^{JD}$$

Finally,then

We have this shoeing that the two-level transitions are universal.
STEP2:
Show that any two-level transition $T^{JK}$ are N qubits can be converted to a controlled unitary $e^{N-1}(T)$,which can be reduced to CNOTs and 1-qubit rotation.
This is as 2-level transition;to convert any 2-level transition to this ,we shut the ?? the 2 important level are $|1>^{\otimes N-1} |0>$ and $|1>^{\otimes N-1} |1>$,do a $C^{N-1}(\widetilde{T})$,and then shuttle the level back.
Convert s to t,though a sequence of strings $s = g_0, g_1, ...g_m$
at each step the last differing bit is switched.
Each of these is a controlled operation with (N+1) ? (the showed) bits as 1 target (differing) bit flip ?,target ? on the ? bits. Each is a 2-level translation that ? the needs.

Appraised: Any n qubits unitary can be decomposed into $O(D^2) = O^{2^{2N}}$ 2 level transition,each of which can be decomposed into $O(NlogN)$ CNOTs to 1-qubit ?
Thus: CNOT of 1-qubit rotation are a universal set for quantum computation .The total resouce requirement is $O(N4^N logN)$gates.
(This is nearly optimed for a ? unitary .)
STEP3: see the textbook.
? unitaries: Any 2-level transition can be efficiently ? using $O(NlogN)$ CNOTs and 1-qubit rotation.A 1-qubit rotation U cannot be efficiently implemented using 2-level translations.
It takes $2^{N-1}$ ? transitions to implement a single bit ratation U,to compared to $O(2^{2N})$ for a generic unitary.
N qubits,g gates to chose from,each ? om $f <= N/2$ qubits.

If we allowed all 2-level translations at reflection $\varepsilon$ at each step?

# 4 Clusler state quantum computation

1. Qubit state in $|0>$
2. Hadamard on each qubit(all qubits in $|+>$)
3. CSIGN between neighbor in school

EXAMPLES;
**

Step3: teleportation
If the standard circuit work for $|\psi>=|0>$,then step 2 show that it works for all $|\psi>$.This because choose U in step 2 such that $U|\psi>=|0>$.then the end result is $U^{+}|0>=|\psi>$.
Thus,all we need to show is that the standard circuit can teleport $|0>$
**

Note the ? structure of the circuit in the middle step,where this ? depend on the outcome of measurements not yet performed.This is not a problem.Why?
Machine for Clucker State Quantum computation:
The standard teleportation circuit is as follows :
The aim of the lecture would be to show that this is indeed the teleportation circuit,without reserting to algebra.The purpose is to become familiar with the manipulation of quantum gates and circuits.
Graph States:
For any graph(nodes with edges),the correspond graph state is obtained by all qubits(nodes) in the state $|+>$ and applying a C-SIGN between all qubits connected by edges.
? a graph state: Hamiltonian for CSIGN:
So, For all CSIGN in a graph state ,use the hamiltonian
**

Aside:
Relation to stabiliser formulation: A graph state is the unique simultaneous eigenstate of the stabiliser generators.
For a 2D cluster state,if there are 3 or more ? and columns,one can fold the grid into a ?,so that every qubits has 4 neighbours.The hamiltonian then becomes $H = -1/2N + \Sigma_T Z_j - 1/4\Sigma_{j<n} B_{jk} Z_j Z_K$
Cluster state Qe:
Initialization: Make Z-measurement to lay out the circuit.
The measured qubit is discarded.Remaining qubits have an initial H,CSIGNs between neighbors and z errors.
Why not make this directly and avoid the Z errors?

Single -qubit gates:

1. Measuring X applies a H gate.
2. Arbitrary $U = Z(\alpha)X(\beta)Z(y) = H \cdot HZ(\alpha)HX(\beta) \cdot H \cdot HZ(\gamma) = H \cdot HZ(\alpha)HZ(\beta)HZ(\gamma)$
3. Only need measurements in the ? place of ?
4. measurement on the leftmost qubits have the initial H's,so the unitary performed on the neighbor qubits is $HZ(\theta)H = X(\theta)$

Two qubit gate :CSIGN

# 5 quantum Fourier transform

D-dimention Hilbert space:

Orthogonal 'position' basis:$|q_i >= |e_i >= |i > j = 0, 1, ...D-1, q_i = i/D$

Conjugate momentum basis: $|p_u, k = 0, 1...D-1, p_u = k/D$

**

The quantum Forier transform is then defined as:

**

This shows that Fn can be implemented by seperate (controled)operations on each qubit,giving an $O(n^2)$algorithm.

The total ? count for the full circuit is $O(n^2)$

Phase estimation

**

The controlled unitaries prepare a momentous stste

To determine $\phi$, we need to determin the period $2\pi k/p_\phi$,which can be obtained by a measurement in the momentous bisis.As we may not know how to do that,we perform a FT which puts the phase information into the standard basis.

2. What happens when $\phi = \phi_1\phi_2...$ has move ? t digits?

Now det $|\phi >$ denote the state that is input into the converse FT:

**

TO get to the result ,look at the state after the Hadamard.The controlled leads to

**

So,if $|\varphi >$ is a superposition of multiple eigenstates of U,the output measurement will yield one of the eigenvalues with the probability from the superposition.

Two source of error:

1. $\delta 2^{-t}$ is the error in determination of $\phi$ bacause of $\phi$ having more than t bits.
2. $e2^{-t}$ is the error in determination of $\phi$ because the measurement doesn't yield b.

# 6 Power of one qubit model

Thus,we have reduced our problem to that of counting the number of zeros of a cubic polynomial over $Z_2$

It is known, in computational algebraic geometry, that counting the number of zeros of a general cubic polynomial over any finite field is #P complete.This is ? the complexily of exact trace evaluation of a general unitary is hand ,Since#P is exponential.In other words ,if there were ,#P would collapse to an efficient class.

Of course, we are interested in the approximate value of the normalised trace

$$\frac{tr(U)}{2^N} = 1/2^{2n+h}\Sigma_x 2^{n/2}(-1)^{\phi(x)}$$

which ? between +1 and -1.It is an average of $2^{2n+h}$ quantities,whose ? $2^{n/2}$ is exp in the number of Hadamard.

Estimation the average with a fixed ? (say e) requires a number of sample that goes as $2^{n/2}$,implying that there is an efficient method of estimation the normalised trace.

Note that there is the reason the problem is hard. If we were adding probabilities, all the terms in the san will be true,and Stockmayer's theories says it can be approximated efficiently in a efficient ? of sample.

Thus ,this algorithm provides an exponentially faster algorithm.That's good!

But it is better because it is a mixed state algorithm with a very small probability.

Exercise:Show that the purity of the state in this model is $1/2^n$,which goes to 0 as $n \to \infty$.

So the system is very easy to produce in the ?.

Only one pure qubit is necessary .But when is the entanglement is the previous version with 1 eigen vector.

Note that this is a multipation state and in fact there is as little bit of entanglement.

So,why is entanglement so important ?What do we know about the role of entanglement in quantum computational advantages of sppedup

1. Entanglement is not sufficient (Gottesman-Knill theorem) show that stabiliser state can be simulated exactly in a classical ? efficiently.

2. IS entanglement necessary?

TO answer that, we study a classic result by Jozsa and Linden.

What will this result show?

It will show that if the amount of entanglement in a quantum algorithm is in some ? 'small' or 'bounded',the algorithm can be simulated efficiently classically.In other words, if there is a lot of entanglement the classically.In other words,if there is a lot of entanglement, the classical simulation will be hard,and the quantum algorithm will show a quantum speedup .

Definition 1:

A quantum algorithm with running time T(n) is defined as follows: For each fixed position integer n(input size),we have a sequence of triples