Algorithm Design XXI

Quantum Algorithms

Guoqiang Li
School of Computer Science

Shanghai Jiao Tong University

Qubits, Superpositions, and Measurement

A Quote from Richard Feynman

I think I can safely say that no one understands quantum physics.

Chips

In ordinary computer chips, bits are physically represented by low and high voltages on wires.

Chips

In ordinary computer chips, bits are physically represented by low and high voltages on wires.

But there are many other ways a bit could be stored, for instance, in the state of a hydrogen atom. The single electron in this atom can

Chips

In ordinary computer chips, bits are physically represented by low and high voltages on wires.

But there are many other ways a bit could be stored, for instance, in the state of a hydrogen atom. The single electron in this atom can

- either be in the ground state (the lowest energy configuration),
- or it can be in an excited state(a high energy configuration).

In ordinary computer chips, bits are physically represented by low and high voltages on wires.

But there are many other ways a bit could be stored, for instance, in the state of a hydrogen atom. The single electron in this atom can

- either be in the ground state (the lowest energy configuration),
- or it can be in an excited state(a high energy configuration).

We can use these two states to encode for bit values 0 and 1, respectively.

Notation

Ground state: $|0\rangle$

Excited state: $|1\rangle$

Superpositions

If a quantum system can be in one of two states, then it can also be in any linear superposition of those two states.

Superpositions

If a quantum system can be in one of two states, then it can also be in any linear superposition of those two states.

For instance,

$$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \text{ or } \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

Superpositions

If a quantum system can be in one of two states, then it can also be in any linear superposition of those two states.

For instance,

$$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \text{ or } \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

or an infinite number of other combination of the form

$$\alpha_0|0\rangle + \alpha_1|1\rangle$$

Superpositions

If a quantum system can be in one of two states, then it can also be in any linear superposition of those two states.

For instance,

$$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \text{ or } \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

or an infinite number of other combination of the form

$$\alpha_0|0\rangle + \alpha_1|1\rangle$$

The α's can be even complex numbers, provided

$$|\alpha_0|^2 + |\alpha_1|^2 = 1$$

Superpositions

If a quantum system can be in one of two states, then it can also be in any linear superposition of those two states.

For instance,

$$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \text{ or } \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

or an infinite number of other combination of the form

$$\alpha_0|0\rangle + \alpha_1|1\rangle$$

The α's can be even complex numbers, provided

$$|\alpha_0|^2 + |\alpha_1|^2 = 1$$

i.e., they are normalized.

Superpositions

The whole concept of a superposition suggests that the electron does not make up its mind about whether it is in the ground or excited state,

Superpositions

The whole concept of a superposition suggests that the electron does not make up its mind about whether it is in the ground or excited state, and the amplitude α_0 is a measure of its inclination toward the ground state.

Superpositions

The whole concept of a superposition suggests that the electron does not make up its mind about whether it is in the ground or excited state, and the amplitude α_0 is a measure of its inclination toward the ground state.

Continuing along this line of thought, it is tempting to think of α_0 as the probability that the electron is in the ground state.

Superpositions

The whole concept of a superposition suggests that the electron does not make up its mind about whether it is in the ground or excited state, and the amplitude α_0 is a measure of its inclination toward the ground state.

Continuing along this line of thought, it is tempting to think of α_0 as the probability that the electron is in the ground state.

But then how are we to make sense of the fact that α_0 can be negative, or even worse, imaginary?

Superpositions

The whole concept of a superposition suggests that the electron does not make up its mind about whether it is in the ground or excited state, and the amplitude α_0 is a measure of its inclination toward the ground state.

Continuing along this line of thought, it is tempting to think of α_0 as the probability that the electron is in the ground state.

But then how are we to make sense of the fact that α_0 can be negative, or even worse, imaginary?

WE DON'T UNDERSTAND THIS, BUT GET USED TO IT.

Measurement

This linear superposition is the private world of the electron.

Measurement

This linear superposition is the private world of the electron.

For us to get a glimpse of the electron's state we must make a measurement to get a single bit of information - 0 or 1.

This linear superposition is the private world of the electron.

For us to get a glimpse of the electron's state we must make a measurement to get a single bit of information - 0 or 1.

If the state of the electron is $\alpha_0 |0\rangle + \alpha_1 |1\rangle$, then the outcome of the measurement is 0 with probability $|\alpha_0|^2$ and 1 with probability $|\alpha_1|^2$.

This linear superposition is the private world of the electron.

For us to get a glimpse of the electron's state we must make a measurement to get a single bit of information - 0 or 1.

If the state of the electron is $\alpha_0 |0\rangle + \alpha_1 |1\rangle$, then the outcome of the measurement is 0 with probability $|\alpha_0|^2$ and 1 with probability $|\alpha_1|^2$.

Moreover, the act of measurement causes the system to change its state:

if the outcome of the measurement is 0, then the new state of the system is $|0\rangle$ (the ground state), and if the outcome is 1, the new state is $|1\rangle$ (the excited state).

k-level systems

The superposition principle holds not just for 2-level systems, but in general for k-level systems.

k-level systems

The superposition principle holds not just for 2-level systems, but in general for k-level systems.

In reality the electron in the hydrogen atom can be in one of many energy levels, starting with the ground state, the first excited state, the second excited state, and so on.

k-level systems

The superposition principle holds not just for 2-level systems, but in general for k-level systems.

In reality the electron in the hydrogen atom can be in one of many energy levels, starting with the ground state, the first excited state, the second excited state, and so on.

A k-level systems consists of the ground state and the first $k-1$ excited states denoted by

$$|0\rangle, |1\rangle, |2\rangle, \ldots, |k-1\rangle$$

k-level systems

The general quantum state of the system is

$$\alpha_0 |0\rangle + \alpha_1 |1\rangle + \alpha_{k-1} |k-1\rangle$$

where $\sum_{j=0}^{k-1} |\alpha_j|^2 = 1$

$\mathtt{k}$-level systems

The general quantum state of the system is

$$\alpha_0 |0\rangle + \alpha_1 |1\rangle + \alpha_{\mathtt{k}-1} |\mathtt{k}-1\rangle$$

where $\sum_{j=0}^{k-1} |\alpha_j|^2 = 1$

Measuring the state of the system would now reveal a number between 0 and $\mathtt{k}-1$, and outcome j would occur with probability $|\alpha_j|^2$.

k-level systems

The general quantum state of the system is

$$\alpha_0 |0\rangle + \alpha_1 |1\rangle + \alpha_{k-1} |k-1\rangle$$

where $\sum_{j=0}^{k-1} |\alpha_j|^2 = 1$

Measuring the state of the system would now reveal a number between 0 and $k-1$, and outcome j would occur with probability $|\alpha_j|^2$.

The measurement would disturb the system, and the new state would actually become $|j\rangle$ or the jth excited state.

Encoding n bits

We could choose $\mathtt{k} = 2^n$ levels of the hydrogen atoms.

Encoding n bits

We could choose $\mathbf{k} = 2^n$ levels of the hydrogen atoms.Or it is more promising to use n qubits.

Encoding n bits

We could choose $\mathtt{k} = 2^n$ levels of the hydrogen atoms.Or it is more promising to use n qubits.

Considering two qubits, that is, the state of the electrons of two hydrogen atoms.

Since each electron can be in either the ground or excited state, in classical physics the two electrons have a total of four possible states 00, 01, 10, or 11, and are therefore suitable for storing 2 bits of information.

Encoding n bits

SHANGHAI JIAO TONG UNIVERSITY

We could choose $\mathtt{k} = 2^n$ levels of the hydrogen atoms.Or it is more promising to use n qubits.

Considering two qubits, that is, the state of the electrons of two hydrogen atoms.

Since each electron can be in either the ground or excited state, in classical physics the two electrons have a total of four possible states 00, 01, 10, or 11, and are therefore suitable for storing 2 bits of information.

But in quantum physics, the superposition principle tells us that the quantum state of the two electrons is a linear combination of the four classical states,

$$|\alpha\rangle = \alpha_{00}\,|00\rangle + \alpha_{01}\,|01\rangle + \alpha_{10}\,|10\rangle + \alpha_{11}\,|11\rangle$$

where $\sum_{x\in\{0,1\}^2} |\alpha_x|^2 = 1$.

Measuring 2 qubits

Measuring the state of the system now reveals 2 bits of information, and the probability of outcome $x \in \{0,1\}^2$ is $|\alpha_x|^2$.

Measuring 2 qubits

Shanghai Jiao Tong University

Measuring the state of the system now reveals 2 bits of information, and the probability of outcome $x \in \{0,1\}^2$ is $|\alpha_x|^2$.

If the outcome of measurement is jk, then the new state of the system is $|jk\rangle$.

Measuring 2 qubits

Measuring the state of the system now reveals 2 bits of information, and the probability of outcome $x \in \{0,1\}^2$ is $|\alpha_x|^2$.

If the outcome of measurement is jk, then the new state of the system is $|jk\rangle$.

What if we make a partial measurement?

Measuring 2 qubits

Shanghai Jiao Tong University

Measuring the state of the system now reveals 2 bits of information, and the probability of outcome $x \in \{0,1\}^2$ is $|\alpha_x|^2$.

If the outcome of measurement is jk, then the new state of the system is $|jk\rangle$.

What if we make a partial measurement?

If we measure just the first qubit, what is the probability that the outcome is 0?

Measuring 2 qubits

Measuring the state of the system now reveals 2 bits of information, and the probability of outcome $x \in \{0,1\}^2$ is $|\alpha_x|^2$.

If the outcome of measurement is jk, then the new state of the system is $|jk\rangle$.

What if we make a partial measurement?

If we measure just the first qubit, what is the probability that the outcome is 0?

$$\text{Prob}\{1stbit = 0\} = \text{Prob}\{00\} + \text{Prob}\{01\} = |\alpha_{00}|^2 + |\alpha_{01}|^2$$

Partial measurements

How much does this partial measurement disturb the state of the system?

Partial measurements

How much does this partial measurement disturb the state of the system?

If the outcome of measuring the first qubit is 0, then the new superposition is obtained by crossing out all terms of $|\alpha\rangle$ that are inconsistent with this outcome (that is, whose first bit is 1).

Partial measurements

How much does this partial measurement disturb the state of the system?

If the outcome of measuring the first qubit is 0, then the new superposition is obtained by crossing out all terms of $|\alpha\rangle$ that are inconsistent with this outcome (that is, whose first bit is 1).

The new state would be

$$|\alpha_{new}\rangle = \frac{\alpha_{00}}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}} |00\rangle + \frac{\alpha_{01}}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}} |01\rangle$$

n hydrogen atoms

Classically the states of the n electrons could be used to store n bits of information in the obvious way.

n hydrogen atoms

Classically the states of the n electrons could be used to store n bits of information in the obvious way.

But the quantum state of the n qubits is a linear superposition of all 2^n possible classical states:

$$\sum_{x \in \{0,1\}^n} \alpha_x |x\rangle$$

n hydrogen atoms

Classically the states of the n electrons could be used to store n bits of information in the obvious way.

But the quantum state of the n qubits is a linear superposition of all 2^n possible classical states:

$$\sum_{x \in \{0,1\}^n} \alpha_x |x\rangle$$

For $n = 500$, the number 2^n s much larger than estimates of the number of elementary particles in the universe.

n hydrogen atoms

Classically the states of the n electrons could be used to store n bits of information in the obvious way.

But the quantum state of the n qubits is a linear superposition of all 2^n possible classical states:

$$\sum_{x \in \{0,1\}^n} \alpha_x |x\rangle$$

For $n = 500$, the number 2^n s much larger than estimates of the number of elementary particles in the universe.

- Where does Nature store this information?

n hydrogen atoms

Classically the states of the n electrons could be used to store n bits of information in the obvious way.

But the quantum state of the n qubits is a linear superposition of all 2^n possible classical states:

$$\sum_{x \in \{0,1\}^n} \alpha_x |x\rangle$$

For $n = 500$, the number 2^n s much larger than estimates of the number of elementary particles in the universe.

- Where does Nature store this information?
- How could microscopic quantum systems of a few hundred atoms contain more information than we can possibly store in the entire classical universe?

n hydrogen atoms

Classically the states of the n electrons could be used to store n bits of information in the obvious way.

But the quantum state of the n qubits is a linear superposition of all 2^n possible classical states:

$$\sum_{x \in \{0,1\}^n} \alpha_x |x\rangle$$

For $n = 500$, the number 2^n s much larger than estimates of the number of elementary particles in the universe.

- Where does Nature store this information?
- How could microscopic quantum systems of a few hundred atoms contain more information than we can possibly store in the entire classical universe?

WE DON'T UNDERSTAND THIS, BUT GET USED TO IT.

Basic motivation

In this phenomenon lies the basic motivation for quantum computation. Why not tap into this massive amount of effort being expended at the quantum level?

Basic motivation

In this phenomenon lies the basic motivation for quantum computation. Why not tap into this massive amount of effort being expended at the quantum level?

There is a fundamental problem: this exponentially large linear superposition is the private world of the electrons.

Basic motivation

In this phenomenon lies the basic motivation for quantum computation. Why not tap into this massive amount of effort being expended at the quantum level?

There is a fundamental problem: this exponentially large linear superposition is the private world of the electrons.

Measuring the system only reveals n bits of information. The probability that the outcome is a particular n-bit string x is $|\alpha_x|^2$. And the new state after measurement is just $|x\rangle$.

The Plan

The structure of a quantum algorithm

The structure of quantum algorithm reflects the tension between

- The exponential private workspace of an n-qubit system
- and the mere n bits that can be obtained through measurement.

The structure of a quantum algorithm

The structure of quantum algorithm reflects the tension between

- The exponential private workspace of an n-qubit system
- and the mere n bits that can be obtained through measurement.

The input to a quantum algorithm consists of n classical bits, and the output also consists of n classical bits.

The structure of a quantum algorithm

The structure of quantum algorithm reflects the tension between

- The exponential private workspace of an n-qubit system
- and the mere n bits that can be obtained through measurement.

The input to a quantum algorithm consists of n classical bits, and the output also consists of n classical bits.

It is while the quantum system is not being watched that the quantum effects take over and we have the benefit of Nature working exponentially hard on our behalf.

The structure of a quantum algorithm

If the input is an n-bit string x, then the quantum computer takes as input n qubits in state $|x\rangle$.

The structure of a quantum algorithm

If the input is an n-bit string x, then the quantum computer takes as input n qubits in state $|x\rangle$.

Then a series of quantum operations are performed, by the end of which the state of the n qubits has been transformed to some superposition

$$\sum_y \alpha_y |y\rangle$$

The structure of a quantum algorithm

If the input is an n-bit string x, then the quantum computer takes as input n qubits in state $|x\rangle$.

Then a series of quantum operations are performed, by the end of which the state of the n qubits has been transformed to some superposition

$$\sum_y \alpha_y |y\rangle$$

Finally, a measurement is made, and the output is the n-bit string y with probability $|\alpha_y|^2$.

The structure of a quantum algorithm

If the input is an n-bit string x, then the quantum computer takes as input n qubits in state $|x\rangle$.

Then a series of quantum operations are performed, by the end of which the state of the n qubits has been transformed to some superposition

$$\sum_y \alpha_y |y\rangle$$

Finally, a measurement is made, and the output is the n-bit string y with probability $|\alpha_y|^2$.

Observe that this output is random. As long as y corresponds to the right answer with high enough probability, we can repeat the whole process a few times to make the chance of failure miniscule.

Quantum factoring algorithm

The algorithm to factor a large integer N can be viewed as a sequence of reductions:

Quantum factoring algorithm

The algorithm to factor a large integer N can be viewed as a sequence of reductions:

- Factoring is reduced to finding a nontrivial square root of $1 \text{ modulo } N$.

Quantum factoring algorithm

The algorithm to factor a large integer N can be viewed as a sequence of reductions:

- Factoring is reduced to finding a nontrivial square root of $1 \mod N$.
- Finding such a root is reduced to computing the order of a random integer modulo N.

Quantum factoring algorithm

The algorithm to factor a large integer N can be viewed as a sequence of reductions:

- Factoring is reduced to finding a nontrivial square root of $1 \mod N$.
- Finding such a root is reduced to computing the order of a random integer modulo N.
- The order of an integer is precisely the period of a particular periodic superposition.

Quantum factoring algorithm

The algorithm to factor a large integer N can be viewed as a sequence of reductions:

- Factoring is reduced to finding a nontrivial square root of $1 \text{ modulo } N$.
- Finding such a root is reduced to computing the order of a random integer modulo N.
- The order of an integer is precisely the period of a particular periodic superposition.
- Finally, periods of superpositions can be found by the quantum FFT.

The Quantum Fourier Transform

Interpolation resolved

FFT takes as input an M-dimensional, complex-valued vector α (where $M = 2^m$), and outputs an M-dimensional complex-valued vector β:

$$\begin{bmatrix} \beta_0 \\ \beta_1 \\ \vdots \\ \beta_{M-1} \end{bmatrix} = \frac{1}{\sqrt{M}} \begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \omega & \omega^2 & \dots & \omega^{n-1} \\ & & \vdots & & \\ 1 & \omega^j & \omega^{2j} & \dots & \omega^{(n-1)j} \\ & & \vdots & & \\ 1 & \omega^{n-1} & \omega^{2(n-1)} & \dots & x^{(n-1)(n-1)} \end{bmatrix} \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{M-1} \end{bmatrix}$$

Interpolation resolved

FFT takes as input an M-dimensional, complex-valued vector α (where $M = 2^m$), and outputs an M-dimensional complex-valued vector β:

$$\begin{bmatrix} \beta_0 \\ \beta_1 \\ \vdots \\ \beta_{M-1} \end{bmatrix} = \frac{1}{\sqrt{M}} \begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \omega & \omega^2 & \dots & \omega^{n-1} \\ & & \vdots & & \\ 1 & \omega^j & \omega^{2j} & \dots & \omega^{(n-1)j} \\ & & \vdots & & \\ 1 & \omega^{n-1} & \omega^{2(n-1)} & \dots & x^{(n-1)(n-1)} \end{bmatrix} \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{M-1} \end{bmatrix}$$

The new factor $\sqrt{M}$ is to ensure that if the $|\alpha_i|^2$ add up to 1, then so do the $|\beta_i|^2$.

The quantum fast Fourier transform

Input: A superposition of $m = \log M$ qubits, $|\alpha\rangle = \sum_{j=1}^{M-1} \alpha_j |r\rangle$

The quantum fast Fourier transform

Input: A superposition of $m = \log M$ qubits, $|\alpha\rangle = \sum_{j=1}^{M-1} \alpha_j |r\rangle$

Method: Using $O(m^2) = O(\log^2 M)$ quantum operation perform the quantum FFT to obtain the superposition $|\beta\rangle = \sum_{j=1}^{M-1} \beta_j |r\rangle$.

The quantum fast Fourier transform

Input: A superposition of $m = \log M$ qubits, $|\alpha\rangle = \sum_{j=1}^{M-1} \alpha_j |r\rangle$

Method: Using $O(m^2) = O(\log^2 M)$ quantum operation perform the quantum FFT to obtain the superposition $|\beta\rangle = \sum_{j=1}^{M-1} \beta_j |r\rangle$.

Output: A random m-bit number j (i.e., $0 \leq j < M$) from the probability distribution $\mathrm{Prob}[j] = |\beta_2|^2$.

Periodicity

Periodicity

Periodicity

Suppose $|\alpha\rangle = (\alpha_0, \ldots, \alpha_{M-1})$ is such that

$$\alpha_i = \alpha_j \qquad \text{if } i \equiv j \mod k$$

Periodicity

Suppose $|\alpha\rangle = (\alpha_0, \ldots, \alpha_{M-1})$ is such that

$$\alpha_i = \alpha_j \qquad \text{if } i \equiv j \mod k$$

Moreover, suppose that exactly one of the $\mathtt{k}$ numbers $\alpha_0, \ldots, \alpha_{\mathtt{k}-1}$ is nonzero, say α_j. Then we say that $|\alpha\rangle$ is periodic with period $\mathtt{k}$ and offset j.

Quantum FFT for periodicity

SHANGHAI JIAO TONG UNIVERSITY

Theorem

Suppose the input to quantum Fourier sampling is periodic with period $\mathtt{k}$*, for some* $\mathtt{k}$ *that divides* M*. Then the output will be a multiple of* $M/\mathtt{k}$*, and it is equally likely to be any of the* $\mathtt{k}$ *multiples of* $M/\mathtt{k}$*.*

Computing $M/\mathtt{k}$

SHANGHAI JIAO TONG UNIVERSITY

Lemma

Suppose s independent samples are drawn uniformly from

$$0, \frac{M}{\mathtt{k}}, \frac{2M}{\mathtt{k}}, \ldots, \frac{(k-1)M}{\mathtt{k}}$$

with probability at least $1 - k/2^s$, the greatest common divisor of these samples is $M/\mathtt{k}$.

Factoring as Periodicity

Nontrivial square root

Nontrivial square root

Fix an integer N. A nontrivial square root of $1 \mod N$ is any integer $x \not\equiv \pm 1 \mod N$ such that $x^2 \equiv 1 \mod N$.

Nontrivial square root

Fix an integer N. A nontrivial square root of $1 \mod N$ is any integer $x \not\equiv \pm 1 \mod N$ such that $x^2 \equiv 1 \mod N$.

Lemma

If x is a nontrivial square root of $1 \mod N$, then $\gcd(x+1, N)$ is a nontrivial factor of N.

Order

Order

The order of $x \mod N$ is the smallest positive integer r such that $x^r \equiv 1 \mod N$.

Order

The order of $x \mod N$ is the smallest positive integer r such that $x^r \equiv 1 \mod N$.

Lemma

Let N be an odd composite, with at least two distinct prime factors, and let x be chosen uniformly at random between 0 and $N-1$. If $\gcd(x, N) = 1$, then with probability at least $1/2$, the order r of $x \mod N$ is even, and moreover $x^{r/2}$ is a nontrivial square root of $1 \mod N$.

The Quantum Algorithm for Factoring

The algorithm

1. Choose x uniformly at random in the range $1 \leq x \leq N-1$.
2. Let M be a power of 2 near N.
3. Repeat $s = 2 \log N$ times:
   - 3.1. Start with two quantum registers, both initially 0, the first large enough to store a number $\text{modulo } M$ and the second $\text{modulo } N$.
   - 3.2. Use the periodic function $f(a) \equiv x^a \mod N$ to create a periodic superposition $|\alpha\rangle$ of length M as follows:
     - 3.2.1. Apply the QFT to the first register to obtain the superposition $\sum_{a=0}^{M-1} \frac{1}{\sqrt{M}} |a, 0\rangle$
     - 3.2.2. Compute $f(a) = x^a \mod N$ using a quantum circuit, to get the $\sum_{a=0}^{M-1} \frac{1}{\sqrt{M}} |a, x^a \mod N\rangle$
     - 3.2.3. Measure the second register. Now the first register contains the periodic superposition $|\alpha\rangle = \sum_{j=0}^{M/r-1} \sqrt{\frac{r}{M}} |jr + k\rangle$ where k is a random offset between 0 and $r-1$ (recall that r is the order of $x \mod N$).
   - 3.3. Fourier sample the superposition $|\alpha\rangle$ to obtain an index between 0 and $M-1$.

   Let g be the $\gcd$ of the resulting indices $j_1, \ldots, j_s$.
4. If M/g is even, then compute $\gcd(N, x^{M/2g} + 1)$ and output it if it is a nontrivial factor of N; otherwise return to 1.