

Quantum Computing

Sam Daitch

January 24, 2005

Outline

- Quantum Computing Model
- Deutsch-Josza Algorithm
- Shor's Algorithm

Quantum Computing Model

Quantum Computing Model

qubit: $|0\rangle$ or $|1\rangle$

or superposition $\alpha|0\rangle + \beta|1\rangle$

where $\alpha, \beta \in \mathbb{C}$, $|\alpha|^2 + |\beta|^2 = 1$.

measure qubit:

probability α^2 of observing $|0\rangle$

probability β^2 of observing $|1\rangle$

all future measurements yield same result

quantum register: group of qubits

e.g. $|9\rangle = |1001\rangle = |1\rangle|0\rangle|0\rangle|1\rangle$

Quantum Computing Model

quantum gate: performs multiplication by unitary matrix

note: unitary matrices are invertible,

so all quantum gate operations must be invertible

e.g. Hadamard gate $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

$$|0\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \xrightarrow{H} |0\rangle$$

applying H to each bit of an n -bit register creates an equal superposition of all n -bit values:

e.g. $|000\rangle \xrightarrow{H}$

$$2^{-3/2}(|0\rangle + |1\rangle)(|0\rangle + |1\rangle)(|0\rangle + |1\rangle) =$$

$$2^{-3/2}(|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle)$$

Quantum Computing Model

note: measuring a qubit in the state $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ forces the qubit to *collapse* to one of the states $|0\rangle$ or $|1\rangle$

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \xrightarrow{H} |0\rangle$$

but

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \xrightarrow{\text{measure}} |0\rangle \text{ or } |1\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$$

STRANGE BEHAVIOR #1:

measuring a qubit affects its state

STRANGE BEHAVIOR #2:

an unmeasured qubit can simultaneously exhibit the behavior of multiple superimposed states

Quantum Computing Model

quantum gate can act on multiple qubits

n -qubit gate is represented by $2^n \times 2^n$ unitary matrix

e.g. a two-qubit gate $U =$

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

$$\begin{array}{l} |00\rangle \xrightarrow[\text{qubit 1}]{H} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \\ \xrightarrow{U} \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \end{array}$$

STRANGE BEHAVIOR #3:

entanglement - measuring one qubit affects another
(e.g. above, other qubit collapses to same value)

Quantum Computing Model

any function $f : \{0, 1\}^n \rightarrow \{0, 1\}^m$ can be computed on a quantum computer in the form of a gate that acts on two registers of size n and m , performing the following invertible transformation:

$$|x\rangle|y\rangle \rightarrow |x\rangle|f(x) \oplus y\rangle$$

to find $f(x)$, do $|x\rangle|00 \cdots 0\rangle \rightarrow |x\rangle|f(x)\rangle$

BQP: class of problems that can be solved with polynomial size family of quantum circuits, with error probability $< 1/3$ for any input

we know $P \subseteq BPP \subseteq BQP$

we believe $BQP \cap NP\text{-complete} = \emptyset$

Deutsch-Josza Algorithm

Deutsch-Josza Algorithm

Problem: given black box that computes a function

$f : \{0, 1\}^n \rightarrow \{0, 1\}$ known either to be constant or balanced (takes value 0 on precisely half the input values), determine whether f is constant or balanced

any deterministic algorithm requires $2^{n-1} + 1$ evaluations of f in the worst-case

Deutsch-Josza algorithm (1992) solves this problem with certainty in a quantum computing model, using only a single function evaluation

Deutsch-Josza Algorithm

we are given a quantum circuit that performs the following transformation on an n -qubit and 1-qubit register:

$$|x\rangle|y\rangle \xrightarrow{f} |x\rangle|f(x) \oplus y\rangle$$

note that for any $x \in \{0, 1\}^n$:

$$|x\rangle(|0\rangle - |1\rangle) \xrightarrow{f} (-1)^{f(x)}|x\rangle(|0\rangle - |1\rangle)$$

recall the effect of applying the Hadamard gate to each bit of an n -qubit register:

$$|x\rangle \xrightarrow{H} \frac{1}{\sqrt{2^n}} \sum_{y \in \{0,1\}^n} (-1)^{x \cdot y} |y\rangle$$

Deutsch-Josza Algorithm

using an n -qubit register and a 1-qubit register:

$$\begin{aligned} |00 \cdots 0\rangle |1\rangle &\xrightarrow{H} 2^{-n/2} \sum_x |x\rangle (|0\rangle - |1\rangle) \\ &\xrightarrow{f} 2^{-n/2} \sum_x (-1)^{f(x)} |x\rangle (|0\rangle - |1\rangle) \\ &\xrightarrow{H} 2^{-n} \sum_x \sum_y (-1)^{f(x) + x \cdot y} |y\rangle |1\rangle \end{aligned}$$

measure all qubits of the first register

probability of measuring $|00 \cdots 0\rangle$ is $(2^{-n} \sum_x (-1)^{f(x)})^2$

which equals 1 if f is constant and 0 if f is balanced

so, if all qubits are $|0\rangle$, f is definitely constant,

otherwise f is definitely balanced

Shor's Algorithm

Shor's Algorithm

Problem: given composite integer N , find a factor of N

this problem is in NP but not NP -complete

Shor found BQP algorithm in 1994

algorithm was performed in 2001 on 7-qubit computer,
factoring $15 = 3 \cdot 5$

if it were possible to construct a quantum computer that performs
this algorithm efficiently, it would not bode well
for cryptography

Shor's Algorithm

- randomly choose a positive integer a such that $\gcd(a, N) = 1$
this means there is an r such that $a^r \pmod N \equiv 1$
in other words r is the period of $f(x) = a^x \pmod N$
- find r using quantum computer
- if r is odd, restart from top
- if $a^{r/2} = \pm 1$, restart from top
- we now have $(a^{r/2} - 1)(a^{r/2} + 1) \equiv 0 \pmod N$
these factors must contain nontrivial factors of N
- calculate $\gcd(a^{r/2} - 1, N)$ and $\gcd(a^{r/2} + 1, N)$
to obtain factors of N

all that remains is to give quantum algorithm to find period the of
a function

Shor's Algorithm

we will use the quantum gate that performs the *quantum Fourier transform*, which is defined as follows:

$$|x\rangle \xrightarrow{QFT} \frac{1}{\sqrt{2^n}} \sum_y e^{2\pi i \frac{xy}{2^n}} |y\rangle$$

Shor's Algorithm

to find period r of $f : \mathbb{Z}_{2^n} \rightarrow \mathbb{Z}_{2^m}$, where $n > 2m > 2 \log_2 r$:

$$\begin{array}{lcl}
 |00 \dots 0\rangle |00 \dots 0\rangle & \xrightarrow[\text{reg 1}]{H} & 2^{-n/2} \sum_x |x\rangle |00 \dots 0\rangle \\
 & \xrightarrow{f} & 2^{-n/2} \sum_x |x\rangle |f(x)\rangle \\
 & \xrightarrow[\text{reg 1}]{QFT} & 2^{-n} \sum_x \sum_y e^{2\pi i \frac{xy}{2^n}} |y\rangle |f(x)\rangle
 \end{array}$$

measure 2nd register; value will be $f(x_0)$ for some $x_0 < r$

let $S = \{x : f(x) = f(x_0)\} = \{x_0 + kr : 0 \leq k < \lfloor \frac{2^n - x_0}{r} \rfloor\}$

1st register collapses to:

$$\frac{1}{\sqrt{|S|2^n}} \sum_{x \in S} \sum_y e^{2\pi i \frac{xy}{2^n}} |y\rangle = \frac{1}{\sqrt{|S|2^n}} \sum_{k=0}^{|S|-1} \sum_y e^{2\pi i \frac{(x_0 + kr)y}{2^n}} |y\rangle$$

so probability of observing y is $|S|^{-1} 2^{-n} \left| \sum_{k=0}^{|S|-1} e^{2\pi i \frac{(x_0 + kr)y}{2^n}} \right|^2$

Shor's Algorithm

probability of observing y is $|S|^{-1}2^{-n} \left| \sum_{k=0}^{|S|-1} e^{2\pi i \frac{(x_0+kr)y}{2^n}} \right|^2$

this value is higher the closer $ry/2^n$ is to an integer,

so it is likely that $y/2^n$ is an integer multiple of $1/r$,
which allows us to generate a candidate value for r

check if r is indeed the period of f ;

if not, retry the algorithm, generating another y
and calculating another candidate value for r

the period of r will be found quickly with high probability