Quantum Computation

Πατμανίδης Σπύρος
ΣΗΜΜΥ

Quantum Computation

The only difference between a probabilistic classical world and the equations of the quantum world is that somehow or other it appears as if the possibilities would have to go negative.

-Richard Feynman, in “Simulating Physics with Computers”, 1982

Quantum Computation

Introduction

- Quantum computing is an new computational model that **<u>may</u>** be physically realizable and **<u>may</u>** provide an exponential advantage over “classical” computational models such as probabilistic and deterministic Turing machines.
- Quantum computers pose a serious challenge to the strong Church-Turing thesis – if quantum computers are physically realizable, then the strong Church-Turing thesis is wrong.

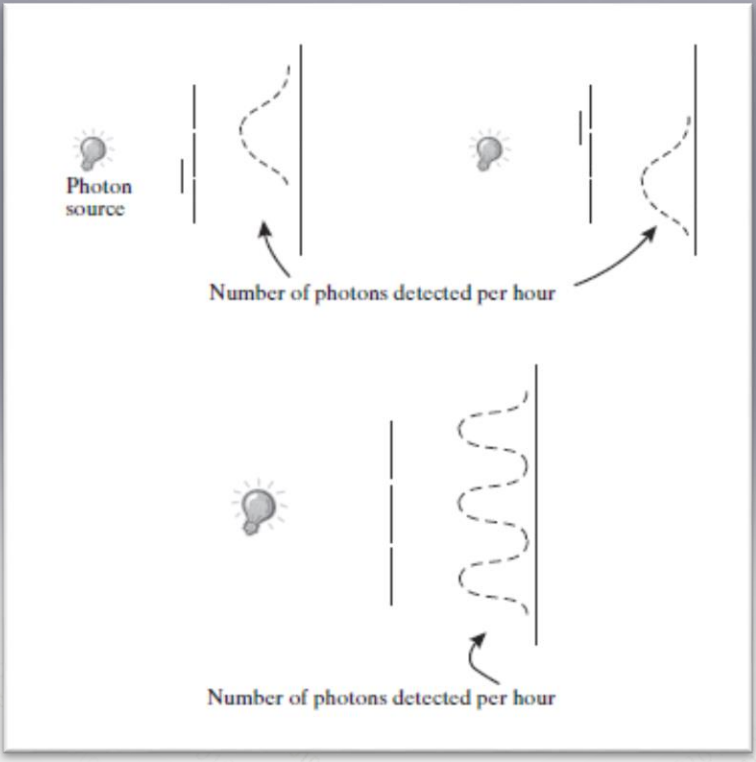
Quantum Computation

Introduction

- The physical parameters (energy, momentum, spic, etc.) of elementary particle such as an electron are *quantized* and can only take values in a discrete set.
- The value of a physical parameter of a particle (including location, energy, etc.) at any moment in time is not a single number. Rather the parameter has a kind of *probability wave* associated with it, involving a "*smearing*" or "*superposition*" over all possible values. The parameter only achieves a definite value when it is measured by an observer, at which point we say that the probability wave *collapses* to a single value.

Quantum Computation

Quantum Weirdness: The Two-Slit Experiment



Quantum Computation

Quantum Superposition and Qubits

- The unit of storage in quantum computing is a *qubit*.
- Elementary particle, which can be *simultaneously* in both basic states.
- The state of a qubit at any time is called a *superposition* of these basic states.
- We denote the basic states $|0\rangle$ and $|1\rangle$.
- We allow a qubit to be in any state of the form

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

where α_o, α_1 are called *amplitudes* and are *complex* numbers satisfying

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

- When the qubit is observed, with probability $|\alpha_o|^2$, it is revealed to be in state zero and with probability $|\alpha_1|^2$, it is revealed to be in state one.
- After observation the amplitude wave *collapses*, and the values of the amplitudes are *irretrievably* lost.

Quantum Computation

Quantum Superposition and Qubits

- A system of two qubits can be in four states $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$ and the state of a two-qubit system at any time is described by a superposition of the type

$$a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle$$

where $\sum_{b1,b2}|a_{b1b2}|^2 = 1$. When this system is observed, its state is revealed to be $|b1b2\rangle$ with probability $|a_{b1b2}|^2$.

Quantum Computation

Quantum Superposition and Qubits - Examples

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

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

- If the qubit is measured, what is the possibility it contains 0?
- If the qubit is measured, what is the possibility it contains 1?

Quantum Computation

Quantum Superposition and Qubits - Examples

We call the state where all the coefficients are equal the *uniform* state.

$|0\rangle + |1\rangle$ denotes the state $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$

$|0\rangle - |1\rangle$ denotes the state $\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$

The uniform state for a two-qubit system is

$$|00\rangle + |01\rangle + |10\rangle + |11\rangle$$

What is the normalization factor for a two-qubit system?

Quantum Computation

Quantum Superposition and Qubits

- We will sometimes denote the state $|xy\rangle$ as $|x\rangle|y\rangle$.
- Using this notation, we can write the uniform state of a two-qubit system as

$$(|0\rangle + |1\rangle)(|0\rangle + |1\rangle)$$

  which shows that this state just consists of two one-qubit systems in uniform state.

Quantum Computation

Some necessary Linear Algebra

- If $z = a + ib$ is a complex number (where $i = \sqrt{-1}$), then $\bar{z} = a - ib$ denotes complex *conjugate* of z. Note that $z\bar{z} = a^2 + b^2 = |z|^2$.
- The *inner* product of two vectors $\mathbf{u}, \mathbf{v} \in \mathbb{C}^M$,denoted by $\langle \mathbf{u}, \mathbf{v} \rangle$, is equal to $\sum_{x \in [M]} \mathbf{u}_x \bar{\mathbf{v}}_x$.
- The *norm* of a vector $\mathbf{u}$, denoted by $\|\mathbf{u}\|_2$, is equal to $\sqrt{\langle \mathbf{u}, \boldsymbol{u} \rangle} = \sqrt{\sum_{x \in [M]} |\mathbf{u}_x|^2}$.
- If $\langle \mathbf{u}, \mathbf{v} \rangle = 0$ we say that $\mathbf{u}$ and $\mathbf{v}$ are *orthogonal*.
- A set $\{\mathbf{v}^i\}_{i \in [M]}$ of vectors in $\mathbb{C}^M$ is an *orthonormal* basis of $\mathbb{C}^M$ if for every $i, j \in [M]$, $\langle \mathbf{v}^i, \mathbf{v}^j \rangle$ is equal to 1 if $i = j$ and equal to 0 if $i \neq j$.
- If A is an MxM matrix, then A^* denotes the *conjugate transpose* of A. That is $A^*_{x,y} = \bar{A}_{y,x}$ for every $x, y \in [M]$.
- An MxM matrix A is *unitary* if $AA^* = I$, where I is the MxM identity matrix.

Quantum Computation

Some necessary Linear Algebra

Claim 10.5 For every MxM complex matrix A, the following conditions are equivalent:

1. A is unitary (i.e. $AA^* = I$)
2. For every vector $\mathbf{v} \in \mathbb{C}^M$, $\|A\mathbf{v}\|_2 = \|\mathbf{v}\|_2$.
3. For every orthonormal basis $\{\mathbf{v}^i\}_{i\in[M]}$ of $\mathbb{C}^M$, the set $\{A\mathbf{v}^i\}_{i\in[M]}$ is a orthonormal basis of $\mathbb{C}^M$.
4. The columns of A form an orthonormal basis of $\mathbb{C}^M$.
5. The rows of A form an orthonormal basis of $\mathbb{C}^M$.

Quantum Computation

The quantum register and its state vector

- In a standard digital computer, by taking *m* physical objects (every object has two states) together we have an *m*-bit *register* whose state can be described by a string in $\{0,1\}^m$.
- A quantum *register* is composed of *m* qubits, and its state is a superposition of all 2^m basic states: a vector $\mathbf{v} = \langle \mathbf{v}_{0^m}, \mathbf{v}_{0^{m-1}1}, \dots, \mathbf{v}_{1^m} \rangle \in \mathbb{C}^{2m}$, where $\sum_x |\mathbf{v}_x|^2 = 1$.

Quantum Computation

Quantum Operations

Definition 10.6 (*Quantum Operation*) A quantum operation for an *m*-qubit register is a function $F: \mathbb{C}^{2m} \to \mathbb{C}^{2m}$ that maps its previous state to the new state and satisfies the following conditions:

Linearity: F is a linear function. That is, for every $\mathbf{v} \in \mathbb{C}^{2m}$,

$$F(\mathbf{v}) = \sum_x |\mathbf{v}_x|^2 F(|x\rangle).$$

Norm preservation: F maps unit vectors to unit vectors. That is, for every $\mathbf{v}$ with $\|\mathbf{v}\|_2 = 1$, $\|F(\mathbf{v})\|_2 = 1$.

Lemma 10.7 (*Composition of quantum operations*) If A_1, A_2 are matrices representing any quantum operations, then their composition (i.e. applying A_1 followed by applying A_2) is also a quantum operation whose matrix is $A_2 A_1$.

Quantum Computation

Some examples of Quantum Operations

- Flipping qubits
- Reordering qubits
- Copying qubits
- Rotation on single qubit
- AND of two qubits – Toffoli Gate
- The Hadamard operation

Quantum Computation

Quantum Computation and BQP

Definition 10.8 (*Elementary quantum operations or quantum gates*) A quantum operation is called *elementary*, or sometimes *quantum gate*, if it acts on three or less qubits of the register.

Quantum Computation

Quantum Computation and BQP

Definition 10.9 (*Quantum Computation and the class **BQP***) Let $f: \{0,1\}^* \to \{0,1\}$ and $T: \mathbb{N} \to \mathbb{N}$ be some functions. We say that f is computable in quantum $T(n)$-time if there is a polynomial-time classical TM that on input $\left(1^n, 1^{T(n)}\right)$ for any $n \in \mathbb{N}$ outputs the description of quantum gates $F_1, \ldots, F_T$ such that for every $x \in \{0,1\}^n$, we can compute $f(x)$ by the following process with probability at least ${}^2/_3$:

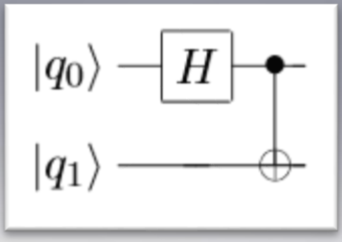
1. Initialize an m qubit quantum register to state $|x0^{n-m}\rangle$ (i.e., x padded with zeros), when $m \leq T(n)$.
2. Apply one after the other $T(n)$ elementary quantum operations $F_1, \ldots, F_T$ to the register.
3. Measure the register and let Y denote the obtained value. (That is, if $\mathbf{v}$ is the final state of the register, then Y is a random variable that takes the value y with probability $\left|\mathbf{v}_y\right|^2$ for every $y \in \{0,1\}^m$.)
4. Output Y_1.

A Boolean function $f: \{0,1\}^* \to \{0,1\}$ is in ***BQP*** if there is some polynomial $p: \mathbb{N} \to \mathbb{N}$ such as that f is computable in quantum $p(n)$-time.

Quantum Computation

Quantum Circuits

Quantum circuits are similar to Boolean circuits: These are directed acyclic graphs with sources (vertices with in-degree zero) denoting the inputs, sinks (vertices with out-degree zero) denoting the outputs and internal nodes denoting the gates.



Apply Hadamard operation on $|q_0\rangle$

Apply the mapping $|q_0 q_1\rangle \mapsto |q_0 (q_0 \oplus q_1)\rangle$

Quantum Computation

Classical Computation as a subcase of Quantum Computation

Lemma 10.10 (*Boolean circuits as a subcase of quantum circuits*) If $f: \{0,1\}^n \to \{0,1\}^m$ is computable by a Boolean circuit of size S then there is a sequence of $2S + m + n$ quantum operations computing the mapping $|x\rangle|0^{2m+S}\rangle \mapsto |x\rangle|f(x)\rangle|0^{S+m}\rangle$.

Corollary 10.11 BPP$\subseteq$BQP

Quantum Computation

Universal Operations

Theorem 10.12 (*Universal basis for quantum operations* [Deu89, Kit97]) For every $D \geq 3$ and $\varepsilon > 0$, there is $l \leq 100(D\log {}^1/_\varepsilon)^3$ such that the following is true. Every $D\text{x}D$ unitary matrix U can be approximated as a product of unitary matrices $U_1, \ldots, U_l$ in the sense that its (i, j) the entry for each $i, j \leq D$ satisfies

$$\left|U_{i,j} - (U_l \cdots U_1)_{i,j}\right| < \varepsilon$$

and each U_r corresponds to applying either the Hadamard gate $\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$, the Toffoli gate $|abc\rangle \mapsto |ab(c \oplus a \wedge b)\rangle$, or the phase shift gate $\begin{pmatrix}1 & 0\\ 0 & i\end{pmatrix}$, on at most three qubits.

Quantum Computation

Shor’s Algorithm: Integer Factorization using Quantum Computers

- The *integer factorization* problem is to find , given an integer N, the set of all *prime factors* of N.
- The best classical algorithm takes roughly $2^{(logN)^{1/3}}$ steps to factor N [LLMP90].

Theorem 10.15 Shor’s algorithm: Factoring in BQP [Sho97]

There is a quantum algorithm that given a number N, runs in $poly(\log(N))$ and outputs the prime factorization of N.

Quantum Computation

Shor's Algorithm: Integer Factorization using Quantum Computers

1. Since N has at most $logN$ factors, it clearly suffices to show how to find a *single* factor of N in $poly(\log N)$ time because we can then repeat the algorithm with N divided by that factor, and thus find all factors
2. It is a well-known fact that in order to find a single factor, it suffices to be able to find the *order* of a random number $A\,(mod\ N)$, in other words, the smallest r such that $A^r \equiv 1\ (mod\ N)$. With good probability, the order r of A will be even and $A^{r/2} - 1$ will have a nontrivial common factor with N, which we can find using a GCD computation.
3. The mapping $A \mapsto A^x\ (mod\ N)$ is computable in $poly(\log N)$ time even on classical TMs.

Using those observations we can come up with a simple $poly(\log N)$ time quantum algorithm that transforms a quantum register initialized to all zeros into the state that is the uniform superposition of all states of the type $|x\rangle$, where $x \leq N$ and satisfies $A^x \equiv y_0\ (mod\ N)$ for some randomly chosen $y_0 \leq N - 1$. By elementary number theory, the set of x's form an arithmetic progression of the type $x_0 + ri$ for $i = 1,2, \ldots$ where $A^{x_0} \equiv y_0\ (mod\ N)$ is the order of A.

Quantum Computation

Shor's Algorithm: Integer Factorization using Quantum Computers

- We created a quantum state involving strong periodicity (namely an arithmetic progression) and we are interested in determining its period.
- The Quantum Fourier Transform (QFT) allows us to detect periods in quantum state. This is a quantum algorithm that takes a register from some arbitrary state $f \in \mathbb{C}^M$ into a state whose vectors is the Fourier transform $\hat{f}$ of f.
- The QFT takes only $O(log^2 M)$ elementary steps and is thus very sufficient.

Quantum Computation

Thank You