Quantum vectorial Boolean function Algorithm

Waffa faeik keidan

Diyala university Mathematic department

Abstract

We shall study the problem

Input :A computable vectorial Boolean function

$$f: \{0,1\}^n \to \{o,1\}^m,\ m \geq n$$

That is either $1-to-1$ or $2-to-1$ with mask, i.e.

$$(\exists s \neq o^n)(\forall x) f(x \oplus s) = f(x)$$

Output: Distinguish between the two eases, and in the second case produce S.

To solve this problem exactly or with high probability, for every such f, a classical (probabilistic) computer needs to evaluate f an exponential number of times.

- However, this problem can be solved with high probability, by a quantum algorithm with only $O(n)$ quantum evaluation of f.

Keyword: quantum algorithm, quantum computation, Hilbert space, qubit, vector, Walsh – Hadamard

الخلاصة

في بحثنا هذا تم مناقشة المشكلة الاتية:

Input: حساب وتقدير دالة الدالة الاتجاهية Boolean

$$f:\{0,1\}^n \to \{o,1\}^m,\ m \geq n$$

وذلك اما 1الى 1 او 2 الى 1, بلاتفاق , بمعنى اخر

$$(\exists s \neq o^n)(\forall x) f(x \oplus s) = f(x)$$

Output: يصف او يميز بين الاثنين بسهولة , وفي الحالة الثانية يكون الناتج S.

ان حل هذه المشكلة يحتاج الى درجة تعقيد من النوع الاسي عند استخدامنا الى الخوارزمية الكمية ثم تقليل درجة التعقيد الى النوع الخطي o(n) .

الكلمات الدليلية: الخوارزمية الكمية, الحساب الكمي, فضاء هلبرت, الموجه,qubit ,والش,هادامارد

Introduction

In the early 1980s, Manin (1980)and Feynman (1982) in-dependently observed that computers built from quantum mechanical components would be ideally suited to simulating quantum mechanics. Whereas brute-force classical simulation of a system of *n* quantum particles(say, tow-level atoms) requires storing 2^n complex amplitudes, and hence exponentially many bits of information, a quantum computer can naturally represent those amplitudes using only *n* quantum bits. Thus, it is natural to expect a quantum mechanical computer to outperform a classical one at quantum simulation. [1,2]

The perspective of quantum systems as abstract information processing devices subsequently led to the identification of concrete tasks, apparently unrelated to quantum mechanics, for which quantum computers have a quantifiable advantage. Deutsch (1985) gave the first such example, a black box problem that requires tow queries to solve on a classical computer, but that can be solved with only one quantum query.[2]

Quantum vectorial Boolean function Algorithm

Waffa faeik keidan

Quantum computers achieve speedup over classical computation by taking advantage of interference between quantum amplitudes. Of course, interference occurs, in classical wave mechanics as well, but quantum mechanics is distinguished by the ability to efficiently represent a large number of amplitudes with only a few quantum bits. In Shor's algorithm and its predecessors, the "exponential interference" leading to quantum speedup is orchestrated using a unitary operation called the *quantum Fourier transform* (QFT), an algebraic operation. In this article, we review the state of the art in quantum algorithms for *algebraic problems,* which can be viewed as continuations of the line of work leading from Deutsch to Shor. Many, though not all, of these algorithms make use of the QFT in some capacity.

Before beginning our exploration of quantum algorithms for algebraic problems, we briefly summarize the development of quantum algorithms more generally. It has sometimes been said that there are really only tow quantum algorithms: Shor. And Grover's. we hope that this article will, in some small way, help to dispel this pernicious myth. While it is difficult to compete with the impact of Shor's algorithms (a dramatic speedup for a problem profoundly relevant to modern electronic commerce) or the broad applicability of Grover's algorithm (a modest yet surprising speedup for the most basic of search problems), recent years have seen a steady stream of new quantum algorithms, both for artificial problems that shed light on the power of quantum computation, and for problems of genuine practical interest.[3,4]

A quantum computer is a device for performing calculations using a quantum mechanical representation of information. Data are stored using quantum bits, or *qubits,* the states of which can be represented by ℓ_2 - normalized vectors in a complex vector space For example, we can write the state of n qubits as $|\psi\rangle = \sum_{x\in\{0,1\}^n} a_x|\psi\rangle$, Where the $a_x \in \mathbb{C}$ satisfy $\sum_{x\in\{0,1\}^n}|a_x|^2 = 1$. we refer to the basis of states $|x\rangle$ as the *computational basis.*

Although we can always suppose that our data is represented using qubits, it is often useful to think of quantum states as storing data more abstractly. For example, given a group G , we write $|g\rangle$ for a computational basis state corresponding to the group element $g \in G$, and

$|\phi\rangle = \sum_{g\in G} b_g |g\rangle$, (where $b_g \in \mathbb{C}$ with $\sum_{g\in G} b_g |b_g|^2 = 1$)for an arbitrary superposition over the group. We often implicitly assume that there is some canonical way of concisely representing group elements using bit strings; it is usually unnecessary to make this representation explicit. We use the convention that for any finite set *S*, the state $|S\rangle$ denotes the normalized uniform superposition of its elements, i.e., $|S\rangle := \frac{1}{\sqrt{|S|}} \sum_{s\in S} |S\rangle$.

If a quantum computer stores the state $|\psi\rangle$ in one register and the state $|\phi\rangle$ in another, the overall state is given by the tensor product of those states. This may variously be denoted $|\psi\rangle\otimes|\phi\rangle$, $|\psi\rangle|\phi\rangle$, or $|\psi, \phi\rangle$.[5]

Preliminaries

Elements of Quantum Mechanics

A quantum state is a mathematical description of a physical system at a given time.For example , it can consist of positions, momentums, polarizations, spins, etc., of various particles in the system. It is reaper sented as a ray in a Hilbert space of wave functions: a ray is an equivalence class of all vectors that differ by a multiplicative non Zero complex scalar.

A Hilbert space is a vector space over the complex numbers C: vectors are denoted $|\psi\rangle$ (Dirac's ket notation). It has a complex – valued inner product $\langle\psi|\varphi\rangle$ with properties

- Positivity: $\langle\psi|\psi\rangle \geq 0$ with equality iff $\psi = 0$
- Linearity: $\langle\varphi(a|\psi\rangle + b|\xi\rangle) = a\langle\varphi|\psi) + b < \varphi|\xi)$
- Skew symmetry: $\langle\psi|\varphi\rangle = \langle\varphi|\psi\rangle^*$

Complete in the corresponding norm (square root of $\langle\psi|\varphi\rangle$) Vectors can be normalized to have unit norm, i.e., $\langle\psi|\psi\rangle = 1$. A self –adjoin operator A is linear operator in a Hilbert space (mapping vectors to vectors)that is equal to this adjoint operator, .e., $A = A^*$. In a finite-dimensions Hilbert space, vectors are ne column matrices. Linear operators are matrices, and A^* is conjugate transpose of A. In an n-dimensional column vector whose component are coordinates with respect to the canonical basis. In Dirac's bar notation, $\langle\varphi|$ denotes conjugate transpose of $|\varphi\rangle$ and the inner product $\langle\varphi|\psi\rangle$ is defined as the scalar corresponding to the matrix product $\langle\varphi \mid |\psi\rangle$. Two vectors are orthogonal if their inner product is zero A is a matrix and A^* is its conjugate transpose. Time evolution of a closed quantum system is defined by the Schrödinger equation $h\frac{d}{dt}|\psi(t)\rangle = -t\,H|\psi(t)\rangle$

where the (time- dependent) Hamiltonian H is a self – adjoint operator It follows that

$$|\psi(t)\rangle = U(t)|\psi(0)\rangle$$

Where the time- dependent U is the corresponding linear and reversible evolution operator which is Unitary, i.e., $UU^* = U^*U = 1$ (preserves orthogonality)

Thus, the evolution is deterministic, linear, and reversible; for any unitary U there exists a physical Hamiltonian to implement it.

However, the process of measure ement always has a probabilistic outcome This is the dual nature of quantum mechanics deterministic dynamics of quantum systems and uncertain, probabilistic measurements[7]

Quantum Bits – Qubits

A quantum bit – qubit is a quantum analog of a classical information bit taking only two values: 0 and 1.Qubit is a quantum system with two-dimensional state: it is a unit vector in the two dimensional Hilbert space C^2 , If $|0\rangle$ and $|1\rangle$ denote two orthogonal unit vectors, i.e., an orthonormal basis, them a qubit is a linear superposition

$$a|0\rangle + b|1\rangle$$

where a and b are complex numbers such tat $|a|^2 + |b|^2 = 1$

In matrix notation, with respect to the assumed basis

$$|0\rangle = \binom{1}{0} = (1,0)^T,\ |1\rangle = \binom{0}{1} = (0,1)^T$$

$a|0\rangle + b|1\rangle - \binom{a}{b} - (a,b)^T$ Conjugate transpose of $|q\rangle - a|0\rangle + b|1\rangle$

$$|q\rangle = \binom{a^*}{b^*}^T = (a^*, b^*)$$ Lnner product

$$\langle q_1|q_2\rangle = \langle q_1||q_2\rangle = (a_1^*, b_1^*)\binom{a_2}{b_2} = a_1^* a_2 + b_1^* a_2$$

Qubit measurement

If aqubit $a|0\rangle + b|1\rangle$ is measured with respect to basis $\{|0\rangle, |1\rangle\}$ then the measured outcome is $|0\rangle$ with probability $|a|^2$ and $|1\rangle$ with probability $|b|^2$

A qubit contains the same amount of information as a classical bit, i.e., it is only possible to encode a single bit in each quantum bit, as information can only be extracted by measurements and any measurement has only two possible outcomes

As measurement changes the state and cloning of quantum states is impossible, it is impossible to measure first in one basis and them into another

Consider a new orthonormal (conjugate) basis

$$|\acute{0}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}$$

$$|\acute{1}\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}$$

Then

$$|q\rangle = a|0\rangle + b|1\rangle = \acute{a}|\acute{0}\rangle + \acute{b}|\acute{1}\rangle$$

$$\acute{a} = \langle\acute{0}|q\rangle = \frac{1}{\sqrt{2}}(a+b), \acute{b} = \langle\acute{1}|q\rangle = \frac{1}{\sqrt{2}}(a-b)$$

If the same qubit is measured with respect to new basis, then the measured outcome is $|\acute{0}\rangle$ with probability $|\acute{a}|^2$ and $|\acute{1}\rangle$ with probability $|\acute{b}|^2$.[8,9]

Example

Measuring the first qubit in tow – qubit state vector

$$|\psi\rangle = \sum_{i_1=0}^{1}\sum_{i_1=0}^{1} c_{i_1 i_2}|i_1\rangle\otimes|i_2\rangle$$

gives outcome $|0\rangle$ and $|1\rangle$ with probabilities

$|c_{00}|^2 + |c_{01}|^2$ and $|c_{10}|^2 + |c_{11}|^2$, respectively

If the outcome is $|0\rangle$ then the resulting state will be

$$\frac{1}{\sqrt{|c_{00}|^2 + |c_{10}|^2}}(c_{00}|00\rangle + c_{10}|01\rangle)$$

Tf the outcome $|1\rangle$ then the resulting state will be

$$\frac{1}{\sqrt{|c_{10}|^2+|c_{11}|^2}}(c_{10}|10\rangle + c_{11}|11\rangle)$$

A quantum state is not entangled if and only if the partial measurements of all individual qubits are statistically independent, i.e., if and only if measurements of other qubits.

In the example, the state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ is entangled s that partial measurements of individual bits have equally likely outcomes, while partial measurements of remaining bits have outcomes with probability 1.

On the other hand, the state

$\frac{1}{\sqrt{2}}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|10\rangle + |1\rangle \otimes \frac{1}{\sqrt{2}}(|10\rangle + |1\rangle)$ is not entangled and the outcomes of all the partial measurements of individual qubits are equiprobable.

Quantum Transformations

Time evolution of a multiple qubits system is defined by a unitary transformations which is linear, reversible, and preserves inner products and hence orthogoality , Such a transformations can be regarded as rotation in Hilbert space. It is described by a unitary matrix, which for n qubits has dimension 2^n .Tensor product of unitary transformations (unitary)

$$A|\psi\rangle \otimes B|\varphi\rangle = (A \otimes B)(|\psi\rangle \otimes |\varphi\rangle)$$

Here $A \otimes B$ is the tensor product of matrices, which is defined as the right kronecker product.

$$A \otimes B = (a_{ij})_{m\times m} \otimes B = (a_{ij}B)_{m\times n}$$

More general property $(A \otimes B)(C \otimes D) = AC \otimes BD$

Tensor product describes combined action of transformations on parts of a quantum state.

Multiplying a matrix by a unit. Complex number $e^{i\varphi}$ does not affect quantum state vectors.

For bass vectors, the outer matrix product $|i\rangle\langle j|$ is a linear transformation that map $|i\rangle$ into $\langle j|$ and all other vectors to the zero vector.It is not unitary, but can be used to express unitary transformations.

For any matrix U

$$U = (u_{ij})_{2^n \times 2^n} = \sum_{i=0}^{2^n-1} \sum_{i=0}^{2^n-1} u_{ij} |i\rangle\langle j|$$

Action of unitary transformation

$$U\left(\sum_j a_j |j\rangle\right) = \sum_j a_j |j\rangle$$

So $U|j\rangle$ is in fact the j- th column of U. [10,11]

Thus, because of linearity, a unitary transformation is completely determined by its action on the basis vectors.

Product of unitary transformations is unitary (composition, matrix product).

Example:

Some single – qubit unitary transformations

$1 = |0\rangle\langle 0| + |1\rangle\langle 1| = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ identity.

$X = |1\rangle\langle 0| + |0\rangle\langle 1| = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ bit - flip

$Z = |0\rangle\langle 0| - |1\rangle\langle 1| = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ phase – flip

$Y = XZ = |1\rangle\langle 0| - |0\rangle\langle 1| = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ phase – bit-flip

Square root of not transform

$$\sqrt{Not} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1-i & 1+i \\ 1+i & 1-i \end{pmatrix} = \frac{e^{i\pi/4}}{\sqrt{2}}\begin{pmatrix} -i & 1 \\ 1 & -i \end{pmatrix}$$

Note: $\sqrt{Not}\sqrt{Not} = X$

Headmard transform (on a single qubit)

$$H = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\langle 0| + \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\langle 1|$$

$$= \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Basic tool for creating quantum parallelism

Their actions (directly or through matrix products)

$$I(a|0\rangle + b|1\rangle) = a|0\rangle + b|1\rangle$$

$$X(a|0\rangle + b|1\rangle) = b|0\rangle + a|1\rangle$$

$$Z(a|0\rangle + b|1\rangle) = a|0\rangle - b|1\rangle$$

$$Y(a|0\rangle + b|1\rangle) = -b|0\rangle + a|1\rangle$$

$$\sqrt{Not}(a|0\rangle + b|1\rangle) = \frac{1}{\sqrt{2}}(a + b + i(b-a)|0\rangle + \frac{1}{\sqrt{2}}(a + b + i(a-b))|1\rangle$$

$$H(a|0\rangle + b|1\rangle) = \frac{1}{\sqrt{2}}(a+b)|0\rangle + \frac{1}{\sqrt{2}}(a-b)|1\rangle$$

Controlled – NOT transform on two qubits:

$$C_{not} = |00\rangle\langle 00| + |01\rangle\{01\rangle + |11\rangle\langle 10| + |10\rangle\langle 11|$$

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

Acts on basis vector as a vectorial Boolean faction: first bit unchanged, second bit changed if and only if first bit equal to 1 (reversible)

Action on a general two-qubit vector:

$$C_{not}(a\langle 00| + b\langle 01\rangle + c\langle 10| + d\langle 11|) = a\langle 00| + b\langle 01\rangle + d\langle 10| + c\langle 11|$$

Cannot be decomposed in to tensor product of two single – qubit transformations, but

$$C_{not} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X$$

Creating entangled stat from disentangle led state

$$C_{not}(H \otimes I)(|0\rangle \otimes \langle 0|) = C_{not}(H|0\rangle \otimes \langle 0|)$$

$$= C_{not}\left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle\right)$$

$$= C_{not}\left(\frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)\right)$$

$$= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Walsh-Handmard transform (on n qubits)

$$H_n = H \otimes H \otimes \dots \otimes H$$

$$H_n|j\rangle = (H \otimes \dots \otimes H)(|j_1\rangle \otimes \dots \otimes |j_n\rangle)$$

$$= \frac{1}{\sqrt{2^n}}\left(|0\rangle + (-1)^{j_1}|1\rangle\right) \otimes \dots \otimes \left(|0\rangle + (-1)^{j_n}|1\rangle\right)$$

$$= \frac{1}{\sqrt{2^n}}\sum_{i_1 \dots i_n}(-1)^{\sum_{k=0}^{n} j_k i_k}|i_1 \dots i_n\rangle = \frac{1}{\sqrt{2^n}}\sum_{i=0}^{2^n-1}(-1)^{j.i}|i\rangle$$

H_n is the well – known walsh – Hadamard matrix ($i.j$ is the inner product of i and j modulo 2)[3]

The main Result Algorithm

Operates on two quantum registers of length *n* and *m* qubits with initial state $|0^n\rangle\otimes|0^m\rangle$

1) Apply walsh – Hadamard transform to first register

$$(H_n\otimes I_m)(|0^n\rangle\otimes|0^m\rangle) = \frac{1}{\sqrt{2^n}}\sum_{i=0}^{2^n-1}|i\rangle\otimes|0^m\rangle$$

2) Evaluate function

$$U_f\left(\frac{1}{\sqrt{2^n}}\sum_{i=0}^{2^n-1}|i\rangle\otimes|0^m\rangle\right) = \frac{1}{\sqrt{2^n}}\sum_{i=0}^{2^n-1}|i\rangle\otimes|f(i)\rangle$$

3) Apply walsh – Hadamard transform to first register

$$(H_n\otimes I_m)\left(\frac{1}{\sqrt{2^n}}\sum_{i=0}^{2^n-1}|i\rangle\otimes|f(i)\rangle\right) = \frac{1}{\sqrt{2^n}}\sum_{i=0}^{2^n-1}((H_n\otimes I_m)|i\rangle\otimes|f(i)\rangle)$$

$$= \frac{1}{\sqrt{2^n}}\sum_{i=0}^{2^n-1}H_n|i\rangle\otimes|f(i)\rangle$$

$$= \frac{1}{2^n}\sum_{i=0}^{2^n-1}\left(\sum_{i=0}^{2^n-1}(-1)^{i.j}|i\rangle\right)\otimes|f(i)\rangle$$

$$= \frac{1}{2^n}\sum_{i=0}^{2^n-1}\sum_{i=0}^{2^n-1}(-1)^{i.j}|i\rangle\otimes|f(i)\rangle$$

$$= \sum_{i=0}^{2^n-1}|i\rangle\otimes\left(\frac{1}{2^n}\sum_{i=0}^{2^n-1}(-1)^{i.j}|f(i)\rangle\right)$$

4) Measure first register (standard basis) to get outcome $|j_1\rangle$

5) Repeat steps (1)-(4) cn times to get outcome $j_1, \dots j_{cn}$

6) Classical post-processing: solve the system of linear equations over the binary field (mod 2), by Gaussian elimination,

$$j_1.s = 0$$

$$\vdots$$

$$j_{cn}.s = 0$$

If a nontrivial solution $(s \neq o^n)$ exists, output 2- to -1 and s

If not, output 1- to -1.

Proof:

If f is 1- to -1,then for each state $|j\rangle$ all different states $|f(i)\rangle$ appear in the superposition before the measurement, so that the probability to get outcome j ,is, independently of j, equal to

$$\sum_{i=0}^{2^n-1} \left|\frac{(-1)^{i.j}}{2^n}\right|^2 = \frac{1}{2^n}$$

If f is 2- to –L, then for each stat $|j\rangle$ exactly 2^{n-1} different state $|f(i)\rangle$ appear in the superposition before the measurement, because the state $|f(i\oplus s)\rangle$ and $|f(i)\rangle$ are identical.

Hence, the probability to get outcome j is equal to

$$\frac{1}{2}\sum_{i=0}^{2^n-1} \left|\frac{(-1)^{i.j}+(-1)^{(i\oplus s).j}}{2^n}\right|^2 = \begin{cases} 2^{-(n-1)} & if\ j.s=0 \\ 0 & if\ j.s=1 \end{cases}$$

Because $(i\oplus s).j = i.j + j.s$

Thus, only j orthogonal to s are possible.

If the process is repeated cn times,in the 1- to -1 case we will get cn random vectors j, and in the 2- to -1 case we will get cn random vectors j that are orthogonal to s.

The tow cases can probabilistically be distinguished by looking for a non-trivial solution to the considered system of linear equations(in $o(n^3)$ time) namely, if C is sufficiently (moderately) large, then in the 1-to-1 case the vectors will with high probability span the whole n- dimensional space (full – ran k matrix) and in the 2-to -1 case the matrix will with high probability have (maximal) rank $n-1$.

as $\propto$ consequence, th system will have exactly one nontrivial solution in the 2- t0 -1 case and no nontrivial solution in the 1- to -1 case

References

1. Aharonov, D., and I. Arad, 2006,The BQP-hardness of approximating the Jones polynomial, eprint quant-ph/0605181.
2. Aharonov, D., I. Arad, E. Eban, and Z. Landau, 2007a, polynomial quantum algorithms for additive approximations of the Potts model and other points of the Tutte plane, eprint quant ph/0702008.
3. Ambainis, A., 2007, Quantum walk algorithm for element distinctness, *SIAM Journal on Computing* 37(1), pp. 210-239, preliminary version in FOCS 2004, eprint quant - ph/0311001.
4. Arad, I., and Z. Landau, 2008, Quantum computation and the evaluation of tensor networks, eprint arXiv:0805.0040.
5. Bacon, D., 2008, How a Clebsch -Gordan transform helps to solve the Heisenberg hidden subgroup problem, *Quantum Information & Computation 8(5), pp. 438-467,* eprint quant- ph/0612107.
6. Bernstein, E., and U. Vazirani, 1997, Quantum complexity theory, *SIAM Journal on Computing* 26(5), pp. 1411-1473, preliminary version in STOC 1993.
7. Childs, A. M., and W. van Dam, 2007, Quantum algorithm for a generalized hidden shift problem , *Proceedings of the 18th ACMSIAM Symposium on Discrete Algorithms,* pp. 1225-1234, eprint quant- ph/0507190.
8. Hallgren, S., 2007, Polynomial-time q quantum algorithms for Pell's equation and the principal idea problem, *Journal of the ACM* 54(1), preliminary version in STOC 2002.
9. Manin, Y., 1980, Computable and uncomputable, Sovetskoye Radio.
10. Sen, P., 2006, Random measurement bases, quantum state distinction and applications to the hidden subgroup problem,*Proceedings of the 21st IEEE Conference on Computational Complexity,* pp. 274-287, eprint quant- ph/0512085.
11. P. Wocjan and J. Yard, "The Jones Polynomial: quantum algorithms and applications in quantum complexity theory", Quantum Information and Computation, 147-180, (2008).