

Grover Algorithm Applied to Four Qubits System

Z. Sakhi (Corresponding author)

Laboratory of Information Technology and Modelisation, and Laboratory of Information processing
Ben M'sik Faculty of Sciences, Hassan II-mohamedia University
PO box 7955, Casablanca, Morocco
Tel: 212-0522-754-670 E-mail: zb.sakhi@yahoo.fr

A. Tragha

Laboratory of Information Technology and Modelisation
Ben M'sik Faculty of Sciences, Hassan II-mohamedia University
PO box 7955, Casablanca, Morocco
Tel: 212-0522-754-670 E-mail: atragha@yahoo.fr

R. Kabil

Laboratory of Information processing
Ben M'sik Faculty of Sciences, Hassan II-mohamedia University
PO box 7955, Casablanca, Morocco
Tel: 212-0522-754-670 E-mail: relkabil@yahoo.fr

M. Bennai

Laboratory of Condensed Matter Physics
Ben M'sik Faculty of Sciences, Hassan II-mohamedia University
PO box 7955, Casablanca, Morocco
Tel: 212-0522-754-670 E-mail: mdbennai@yahoo.fr

Received: January 8, 2011

Accepted: February 25, 2011

doi:10.5539/cis.v4n3p125

Abstract

We present some applications of quantum algorithm on many qubits system. We focus in particular on Grover algorithm which we apply to four qubits case. We give definition of some quantum gates used in the context of Grover algorithm as Hadamard gate. We consider specially the case of four qubits system and show that Grover algorithm allows as obtaining a maximal probability to get the result.

Keywords: Qubits, Grover algorithm, Probability

1. Introduction

Quantum information processing has emerged recently as a new information science combining physic, informatics and electronic. The mean idea behind quantum information computing is the use the fundamental laws of quantum physics in information processing. Feynman (R. P. Feynman, 1982) in early 1980 years, has proposed to use the power of quantum mechanics to simulate quantum phenomena. Thus, the information can be encoded in a superposition of states of photons, atoms, or ions which were defined as qubits. On the other hand, the increasing miniaturization of electronic circuits will be certainly limited by quantum effects at nanometer scale. This observation was first pointed out by Moore (D. Deutsch, 1985).

Recently, a renewed interest in the subject was seen, since the seminal work of Shor (P. W. Shor, 1994) and Grover (L. K. Grover, 1997). This make possible to solve many problems which can't be reach in classical computing. In this perspective, Grover algorithm has showed an increasing capacity to solve many problems and

was applied in many context: quantum cryptography (Li-Yi-Hsu, 2003), charge Josephson junction qubits system (Xiao-Hu Zheng, Ping Dong, Zheng-Yuan Xue, Zhuo-Liang Cao, 2007). Note that Josephson junction qubits are one of the strongest candidates for quantum computing physical systems. In practice, many difficult are in order to realize a concrete and a real physical quantum information system, especially in the case of many qubits circuits introducing various coupling scheme. Thus, the study of many qubits algorithms has become very important. We signal that four qubits case is very special and entanglement of four qubits systems was studied by many authors and in different context (F. Verstraete, J. Dehaene, B. De Moor, H. Verschelde, 2002).

In the present work, we are interested on Grover algorithm which we apply in the case of four qubits system. We begin, in the next section, by recalling some basic quantum gates and circuits which are fundamental in defining quantum algorithms. Some features of Grover algorithm are presented in section 3. The last two sections are devoted to our work and to a conclusion. We show specially that Grover algorithm allows as to obtain a maximal probability to get the result.

2. Quantum Circuits and logic Gates

2.1 One qubit gate

We begin by presenting some interesting examples of one-qubit and two-qubits gates. Recall that a qubit is any state which is a linear combination of states $|0\rangle$ and $|1\rangle$: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. This state is a vector in a two dimensional complex vector space. In order to construct an adequate quantum algorithm, one has to introduce a quantum logical gates similar to the classical ones. The most known quantum gates are: Hadamard and CNOT gates. The first one which is used in the context of Grover algorithm, is a one qubit gate. This gate is very important because it allows as constructing a superposed state from individual qubits. In matrix representation, the Hadamard gate, is a one-qubit rotation, mapping the qubit-basis states $|0\rangle$ and $|1\rangle$ to two superposition states with equal weight of the computational basis states $|0\rangle$ and $|1\rangle$. This corresponds to the transformation matrix given by:

$$H_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

in the $\{|0\rangle, |1\rangle\}$ basis.

Many quantum algorithms use the Hadamard transform as an initial step, since it maps n qubits initialized with $|0\rangle$ to a superposition of all 2^n orthogonal states in the $|0\rangle, |1\rangle$ basis with equal weight. This is a general feature, valid also for two or more qubits.

2.2 Two qubits gate: Controlled note

In the two qubits A and B case, the Hilbert space is a tensor product of the one qubit ones:

$$H^{AB} = H^A \otimes H^B$$

The corresponding basis is $\{|00\rangle; |01\rangle; |10\rangle; |11\rangle\}$, where:

$$|11\rangle = |1\rangle \otimes |1\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \quad |00\rangle = |0\rangle \otimes |0\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad |01\rangle = |0\rangle \otimes |1\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \quad |10\rangle = |1\rangle \otimes |0\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

Another important 2-qubits quantum gate is the CNOT gate, which is the quantum generalization of the classical gate described earlier. It has two input qubits, the control and the target qubit, respectively. The target qubit is flipped only if the control qubit is set to 1. On the other hand, the output of the CNOT gate can be entangled while the input is non-entangled. For more details on quantum circuits see (Yang Liu, Gui Lu Long and Yang Sun, 2008). The Controlled NOT gate (or CNOT) is a quantum gate that is an essential component in the construction of a various quantum algorithms. The matrix representation of this gate is

$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

It was shown by Barenco et al. (A. Barenco, C.H. Bennett, R. Cleve, D.P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J.A. Smolin, and H. Weinfurter, 1995), that the CNOT gate and any one qubit gates can be considered as an universal set for quantum computing. In other word, any unitary transformation for an n qubits system can be decomposed in one qubit gate and a CNOT gate.

Note that there exist also many other quantum gates, but the above cited ones are the most used in the realization of quantum circuits and quantum algorithms.

3. Grover algorithm

In this section, we recall the essential feature or Grover algorithm. Suppose we have an unstructured database with N elements which are numbered from 0 to N-1, and the elements are not ordered. Classically, we would test each element at a time, until we get the one searched for. In Grover algorithm, only $O(\sqrt{N})$ trials are needed (M. A. Nielsen, I. L. Chuang, 2000).

Grover's algorithm has two registers: n qubits in the first and one qubit in the second. The first step is to create a superposition of all $2n$ computational basis states. This is achieved by initializing the first register in the state and apply the operator H_n . Then we define a function f which recognizes the solution as: f:

$$\{0, \dots, N-1\} \rightarrow \{0, 1\}, f(k) = 1 \text{ if } k \text{ is the searched element, } f=0 \text{ otherwise.}$$

Thus we can resume the Grover algorithm as consisting of the following steps:

- 1) Consider an initial state: $|0\rangle^{\otimes n}$,
- 2) We apply the Hadamard gate on the first n qubits to get a uniform superposition of all possible f arguments,
- 3) Apply the oracle f. Note that the information on f are included in the $(n+1)^{\text{th}}$ qubit,
- 4) Apply against the Hadamard gate,
- 5) Do an observation.

Note that the above algorithm can be illustrated in the fooling diagram:

Figure 1

In this figure, note that we have a succession of a one Grover iteration (G) and the states of the first register correspond to the first iteration. In the next section, we apply this algorithm to the case of four qubits system.

4. Four qubits system case

Consider now the particular case of four qubits system for which we apply the above procedure. We begin by affecting to the first and the second register four qubits and one qubit respectively. Then we initialize the first register to be in state $|0000\rangle$ and the second register in the state $|1\rangle$.

Apply now the Hadamard operator to the first register. We obtain:

$$|\psi\rangle = H|0\rangle^{\otimes 4} = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle$$

Thus

$$|\psi\rangle = \frac{1}{\sqrt{16}} \sum_{i=0}^{15} |i\rangle$$

On the other hand, we apply Hadamard gate to the second register to get entangled following state

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

Now, to apply the Grover operator G, one must to calculate the iteration number given by [10]

$k_0 = \text{round}\left(\frac{\pi}{4}\sqrt{N}\right)$. In our case, where $N=16$, we have $k_0=3$.

Note that the calculation is done in the following working basis

$$\{|0000\rangle, |0001\rangle, |0010\rangle, |0011\rangle, |0100\rangle, |0101\rangle, |0110\rangle, |0111\rangle, \\ |1000\rangle, |1001\rangle, |1010\rangle, |1011\rangle, |1100\rangle, |1101\rangle, |1110\rangle, |1111\rangle\}$$

If we assume that the unknown element is $|1011\rangle = |11\rangle$, thus one can deduce

$$|\psi\rangle = \frac{1}{\sqrt{16}} \left(\sum_{\substack{i=0 \\ i \neq 11}}^{15} |i\rangle + |1011\rangle \right) \\ = \frac{1}{\sqrt{16}} (\sqrt{15}|\xi\rangle + |1011\rangle)$$

Where: $|\xi\rangle = \frac{1}{\sqrt{15}} \sum_{\substack{i=0 \\ i \neq 11}}^{15} |i\rangle$

The next step of Grover algorithm consist of applying the oracle U_f , as:

$$U_f(|i\rangle|-\rangle) = (-1)^{f(i)}|i\rangle|-\rangle \\ |\psi_1\rangle|-\rangle = U_f(|\psi\rangle|-\rangle) \\ = \frac{\sqrt{15}}{4} U_f(|\xi\rangle|-\rangle) + \frac{1}{4} U_f(|1011\rangle|-\rangle) \\ = \frac{\sqrt{15}}{4} |\xi\rangle|-\rangle - \frac{1}{4} |1011\rangle|-\rangle$$

Introduce

$$|\psi_1\rangle = \frac{\sqrt{15}}{4} |\xi\rangle - \frac{1}{4} |1011\rangle \\ |\psi_1\rangle = \frac{1}{4} \sum_{\substack{i=0 \\ i \neq 11}}^{15} |i\rangle - \frac{1}{4} |1011\rangle$$

Now, if we apply the inversion operator about the mean, one can easily obtain

$$|\psi_2\rangle = (2|\psi\rangle\langle\psi| - I)|\psi_1\rangle \\ |\psi_2\rangle = \frac{3}{4} |\psi\rangle + \frac{1}{2} |1011\rangle$$

$$|\psi_2\rangle = \frac{3}{16} \sum_{\substack{i=0 \\ i \neq 11}}^{15} |i\rangle + \frac{11}{16} |1011\rangle$$

The second iteration (oracle) in Grover algorithm leads to

$$|\psi_3\rangle|-\rangle = U_f(|\psi_2\rangle|-\rangle)$$

$$|\psi_3\rangle = \frac{3}{4}|\psi\rangle - \frac{7}{8}|1011\rangle$$

$$|\psi_3\rangle = \frac{3}{16} \sum_{\substack{i=0 \\ i \neq 11}}^{15} |i\rangle - \frac{11}{16}|1011\rangle$$

Inversion operator about the mean leads to

$$|\psi_4\rangle = (2|\psi\rangle\langle\psi| - I)|\psi_3\rangle$$

$$|\psi_4\rangle = \frac{5}{64} \sum_{\substack{i=0 \\ i \neq 11}}^{15} |i\rangle + \frac{19}{64}|1011\rangle$$

By applying the 3th iteration, one can obtain easily

$$|\psi_5\rangle|-\rangle = U_f(|\psi_4\rangle|-\rangle)$$

$$|\psi_5\rangle = \frac{5}{16}|\psi\rangle - \frac{33}{32}|1011\rangle$$

Apply again the inversion operator about the mean, on get

$$|\psi_f\rangle = (2|\psi\rangle\langle\psi| - I)|\psi_5\rangle$$

$$|\psi_f\rangle = -\frac{13}{256} \sum_{\substack{i=0 \\ i \neq 11}}^{15} |i\rangle + \frac{251}{256}|1011\rangle$$

Finally, to test Grover algorithm, we calculate the probability to find the state $|1011\rangle$. We find:

$$P = \left| \frac{251}{256} \right|^2 \cong 0.96$$

Thus, the probability of getting the result $|1011\rangle$ is around 96%.

5. Conclusion

In this paper, we have presented an introduction to quantum algorithm in relation to many qubits system. We have in particular, considered the Grover algorithm which we have applied to the special case of four qubits and calculated the Grover probability in this case. In a perspective, one must use the same procedure to analyze a realistic case of physical system like Josephson junction qubits. In this context, it will be interesting to consider various coupling types of qubits effect on Grover algorithm. Further more general and concrete realization of Grover algorithm must be realized on a real quantum system such as many bodies Josephson qubits.

References

- A. Barenco, C.H. Bennett, R. Cleve, D.P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J.A. Smolin, and H. Weinfurter. (1995). Elementary gates for quantum computation, *Phys. Rev. A* 52, 3457–3467.
- D. Deutsch. (1985). *Int. J. theor. Phys.* 24 (1985) 1.
- F. Verstraete, J. Dehaene, B. De Moor, H. Verschelde. (2002). Four qubits can be entangled in nine different ways, *Phys. Rev. A*, 65 (2002) 052112.
- L. K. Grover. (1997). *Phys. Rev. Lett.* 79 (1997) 325.
- Li-Yi-Hsu. (2003). Quantum secret-sharing protocol based on Grover's algorithm, *Phys. Rev. A* 68 (2003) 022306.
- M. A. Nielsen, I. L. Chuang. (2000). *Quantum Computation and Quantum Information*, (Cambridge University Press, Cambridge, 2000).
- P. W. Shor. (1994). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, in Proceedings of the 35th Annual Symposium on the Foundations of Computer Science, edited by S. Goldwasser, page 124, Los Alamitos, CA, (1994), IEEE Computer Society.

R. P. Feynman. (1982). Simulating physics with computers, *Int. J. Theor. Phys.* 21 (1982) 467-488.

Xiao-Hu Zheng, Ping Dong, Zheng-Yuan Xue, Zhuo-Liang Cao. (2007). Implementation of Grover search algorithm with Josephson charge qubits, *Physica C*. 453 (2007) 76-79.

Yang Liu, Gui Lu Long and Yang Sun. (2008). Analytic one-bit and CNOT gate constructions of general n-qubit controlled gates, *International Journal of Quantum Information (IJQI)*. Volume: 6, Issue: 3 (2008) 447-462.

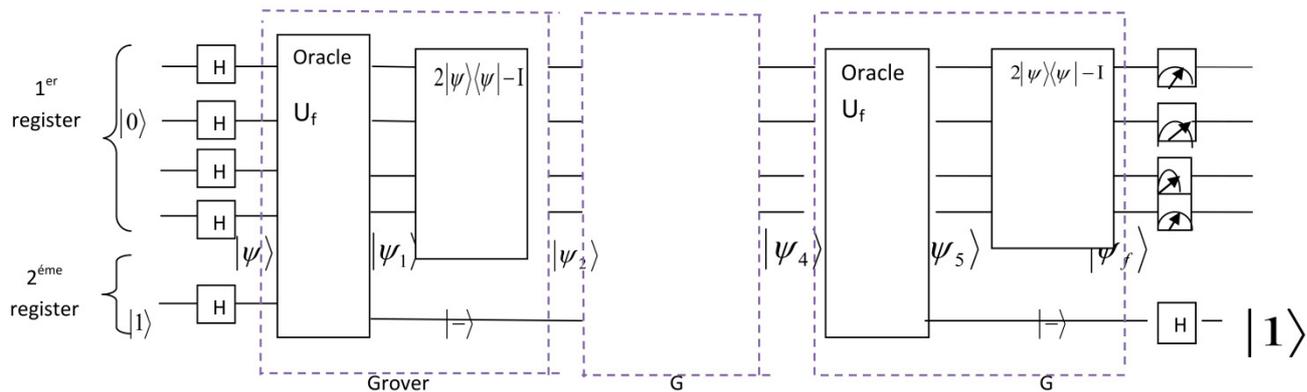


Figure 1.