Annals of DAAAM for 2010 & Proceedings of the 21st International DAAAM Symposium, Volume 21, No. 1, ISSN 1726-9679
ISBN 978-3-901509-73-5, Editor B. Katalinic, Published by DAAAM International, Vienna, Austria, EU, 2010
Make Harmony Between Technology and Nature, and Your Mind will Fly Free as a Bird
Annals of DAAAM International

ELEMENTARY GATES FOR FAULT-TOLERANT QUANTUM COMPUTING

DRAGNE, L[ucian]

Abstract: *A novel proof on the universality of the fault-tolerant Shor's basis is provided. Such a set of elementary quantum gates is necessary for the approximation of the generic unitary operators, on any number of qubits. The basis considered here contains the following quantum gates: Hadamard, phase, CNOT and Toffoli. Since the proof is made by construction, a couple of circuits necessary for implementing some elementary unitary operators on one qubit are also provided.*

Key words: *Quantum circuits approximations, Universal gates, Toffoli gate*

1. INTRODUCTION

The model of computation based on the laws of quantum mechanics is already known to provide superior efficiency in solving some problems, than the standard (i.e. classical) computational model. But in order to use the quantum computing model in practice, a few problems must be solved first. Most important, especially because the processes at quantum level are extremely susceptible to noisy interferences, the model must provide for fault-tolerant implementations.

Therefore, it is mandatory that the unitary operators (which are used for modelling quantum computations) are proved to have implementations that are based only on fault tolerant quantum gates. There are several well-established results on the universality of quantum bases (Barenco, 1995), which rest primarily on using a non-elementary gate, i.e. a gate that performs a single qubit rotation by an irrational multiple of 2π. However, a direct, fault tolerant realization of such gate is not really possible, therefore they can't be easily used in noisy quantum environments.

There are quantum codes that can be used to show that a small sub-set of elementary quantum gates: Hadamard, phase, CNOT, called the normalizer group, can be implemented in a fault-tolerant manner. But this set of gates it is not enough for universality as it doesn't spawn the whole set of unitary operators. This fact led to the suggestion of adding of a new elementary gate to the normalizer group: Toffoli, a gate which can be also implemented fault-tolerantly (Shor, 1997). But a direct proof of the universality of the new set was not provided.

There are some indirect proofs (Boykin et al., 1999) which follow an indirect approach by demonstrating the direct equivalence between the Shor's basis and other universal bases. That is, these bases provide simple and accurate circuits that implement the operators in Shor's basis. There are also other categories of bases which were proved to not be directly equivalent to Shor's basis; that is, they can only be approximated by gates in the Shor's basis, and not implemented exactly.

2. IMPLEMENTING A BASIC ROTATION

2.1 Basic circuit for the non-elementary rotation

The quantum circuit below (Fig. 1.) implements a basic rotation operator, around the z axis, with a specific angle: $R_z(\theta)$, where $\cos\theta = 3/5$. This angle θ was chosen so that it is an irrational multiple of 2π. To prove the circuit, we use the definitions of the gates involved: Hadamard, phase and Toffoli.

$$|00\psi\rangle \xrightarrow{Hadamard} \tfrac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)|\psi\rangle \quad (1)$$

$$\xrightarrow{Toffoli} \frac{1}{2}[(|00\rangle + |01\rangle + |10\rangle)|\psi\rangle + |11\rangle X|\psi\rangle]$$

$$\xrightarrow{phase} \frac{1}{2}[(|00\rangle + |01\rangle + |10\rangle)S|\psi\rangle + |11\rangle SX|\psi\rangle]$$

$$\xrightarrow{Toffoli} \frac{1}{2}[(|00\rangle + |01\rangle + |10\rangle)S|\psi\rangle + |11\rangle XSX|\psi\rangle]$$

$$\xrightarrow{Hadamard} \tfrac{1}{4}[|00\rangle(3S + XSX)|\psi\rangle + (|01\rangle + |10\rangle - |11\rangle)(S - XSX)|\psi\rangle] \quad (2)$$

Considering the following identities for quantum gates:

$$3S + XSX = \sqrt{10}e^{i\frac{\pi}{4}}R_z(\theta), \quad \text{where } \cos\theta = \tfrac{3}{5}$$
$$S - XSX = (1-i)Z = (1-i)S^2 \quad (3)$$

The circuit state just before the measurements are performed becomes then:

$$\longrightarrow \tfrac{\sqrt{10}}{4}e^{i\frac{\pi}{4}}|00\rangle R_z(\theta) + \tfrac{1-i}{4}(|01\rangle + |10\rangle - |11\rangle)S^2|\psi\rangle \quad (4)$$

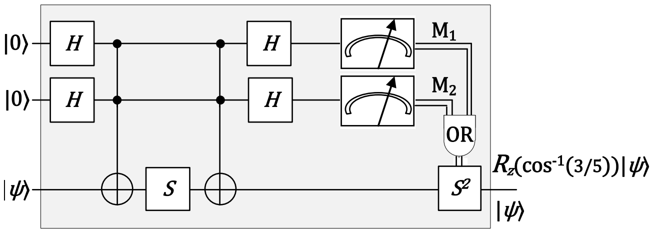

Fig. 1. Circuit "***C***" for implementing the elementary rotation operator with probability $P_{00} = 5/8$

2.2 Circuit for the elementary rotation, with unitary probability

The quantum circuit in Fig.1. applies the $R_z(\theta)$ operation to the target qubit if the measurement outcomes on the control qubits are both 0. Otherwise, if at least one measurement returns 1, the target qubit will be left unchanged, in the same state. This decision is implemented by the classic OR gate at the end, which takes as input the classic bits from the measurement and then controls the application of the final quantum gate $S^2 = Z$. The probabilities of these four different outcomes, given by the two control qubits, can be easily calculated as following:

$$P_{00} = \left|\frac{\sqrt{10}}{4}e^{i\frac{\pi}{4}}\right|^2 = \frac{5}{8}$$
$$P_{01} \equiv P_{10} \equiv P_{11} = \left|\tfrac{1-i}{4}\right|^2 = \tfrac{1}{8} \quad (5)$$

As the above equations indicate, the probability of the circuit to actually apply the desired rotation operator is much higher than the probability of performing a no-op. Still, it is possible to improve this probability, in order to make it approach 1, by successively applying the very same quantum circuit "*C*" until the rotation operation is performed. This process is schematically presented in Fig. 2.

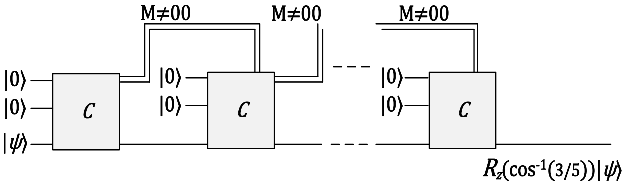

Fig. 2. Circuit for implementing the elementary rotation operator with a probability that approaches 1

The process runs as follows: if, at the current step, the measurement outcome on at least one control qubit is 1, then apply the circuit again, by using two new control qubits set to $|0\rangle$ and the same target qubit as returned by the circuit. Else, if at any step n the measurement outcomes on the control qubits are both 0, then the target qubit has been transformed with $R_z(\theta)$, and the process stops. The probability for the process to stop at step n is therefore:

$$P(n) = P_{00}[\sum_{k=0}^{n-1}(P_{01} + P_{10} + P_{11})^k] = \frac{5}{8}\sum_{k=0}^{n-1}\left(\frac{3}{8}\right)^k \quad (6)$$

This is because in all the previous steps (1..n-1) the measurement outcome was either $|01\rangle$ or $|10\rangle$ or $|11\rangle$, and at the current step (n) the measurement outcome was $|00\rangle$. And it can be easily observed that the sum above is the sum of a geometrical series, therefore as n raises, the probability P(n) approaches 1:

$$\lim_{n\to\infty}(P(n)) = \frac{5}{8}\frac{1}{1-\frac{3}{8}} = 1 \quad (7)$$

3. UNIVERSAL SET OF QUANTUM GATES

3.1 Approximating unitary operators

Since the set of unitary operations is continuous, it is clear that a discrete set of gates is not sufficient to implement an arbitrary unitary operation. Rather, a discrete set can be used to only approximate any unitary operation. Considering *U* and *V* are two unitary operators on the same state space, *U* being the required target operator and *V* being the operator that is actually implemented, the error in approximation is defined by:

$$E(U, V) \equiv \max_{|\psi\rangle}||(U - V)|\psi\rangle|| \quad (8)$$

This definition guarantees that if the respective error is small, then a measurement performed on the actually implemented operator, using any initial state and any measurement operator, gives similar statistics as if the same measurement were to be performed on the required target operator. Furthermore, if a sequence of gates is used to approximate another sequence of gates, the errors add up at most linearly:

$$E(U_m U_{m-1} \dots U_1, V_m V_{m-1} \dots V_1) \le \sum_{j=1}^{m} E(U_j, V_j) \quad (9)$$

3.2 Approximating the rotation operator

With respect to this error definition, a demonstration similar to the one provided by (Nielsen & Chuang, 2004), which would also rely on the fact that $\cos^{-1}(3/5)$ is an irrational multiple of 2π (Boykin et al. 1999), proves that the rotation operator $R_z(\theta)$ implemented by the circuit above (Fig. 2.) can be used to approximate a rotation by the *z* axis with any angle, where the number *n* depends on the desired accuracy:

$$E(R_z(\alpha), R_z(\theta)^n) < \frac{\epsilon}{3} \quad (10)$$

Now, it can be shown that the discrete set of quantum gates formed by the normalizer group, plus the Toffoli gate is universal for quantum computation; that is an arbitrary unitary operation on *d* qubits can be approximated to an arbitrary accuracy using a circuit composed only from these gates. The circuit obtained will most likely have to be applied several times, the number of applications being direct proportional with the desired accuracy in the approximation. Firstly, any single qubit unitary operation can be factored into a product of rotations and Hadamard operators:

$$U \cong R_z(\alpha) H R_z(\beta) H R_z(\gamma) \quad (11)$$

Then, from the last two equations, it follows that the circuit "*C*", together with two more Hadamard gates, can be used to successfully approximate any single qubit unitary operation:

$$E(U, R_z(\theta)^{n_\alpha} H R_z(\theta)^{n_\beta} R_z(\theta)^{n_\gamma}) < 3\frac{\epsilon}{3} + 2E(H, H) = \epsilon \quad (12)$$

Furthermore, because any unitary operator on *d* qubits can be factored into a product of two-level unitary operators on *d* qubits (Deutsch et al., 1995); and because these two-level unitary operators on *d* qubits can in turn be exactly (i.e. no approximation needed) implemented using only single qubit gates and CNOT gates, this implies that any unitary operator on *d* qubits can be approximately implemented, with arbitrary accuracy ϵ, using only Hadamard, phase, CNOT and Toffoli gates, i.e. the gates from Shor's basis.

4. CONCLUSION

The direct proof provided for the universality of the Shor basis raises a few questions regarding the efficiency of the quantum circuit models and the amount of computing resources required to approximate unitary operations. Unfortunately it is not possible to approximate generic unitary operators on *d* qubits using a circuit of size polynomial in *d*. Yet, the search for universal fault-tolerant bases must always consider the efficiency aspect.

Although most of the unitary transformations can only be implemented by approximation very inefficiently, that is the number of fault-tolerant gates is exponential in the number of qubits of the operator, it may be possible that some universal bases are more efficient than others to approximate some specific set of unitary operators.

5. REFERENCES

Barenco, A. (1995). A Universal Two-Bit Gate for Quantum Computation, *Available from:* http://arxiv.org/abs/quant-ph/9505016 *Accessed:* 2010-07-07

Boykin, O. P.; Mor, T.; Pulver, M.; Roychowdhury, V. & Vatan, F. (1999). On Universal and Fault-Tolerant Quantum Computing, *Available from:* http://arxiv.org/abs/quant-ph/9906054 *Accessed:* 2010-07-07

Deutsch, D.; Barenco, A. & Ekert, A. (1995). Universality in Quantum Computation, *Available from:* http:// arxiv.org/abs/quant-ph/9505018 *Accessed:* 2010-07-07

Nielsen, M. & Chuang, I. (2004). *Quantum Computation and Quantum Information*, Cambridge University Press, 0-521-63503-9, Cambridge

Shor, P. W. (1997). Fault-tolerant Quantum Computation, *Available from:* http://arxiv.org/abs/quant-ph/9605011 *Accessed:* 2010-07-07