SANDIA REPORT
SAND2006-3440
Unlimited Release
Printed July 2006

Quantum Gate Decomposition Algorithms

Alexander Slepoy

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia is a multiprogram laboratory operated by Sandia Corporation,
a Lockheed Martin Company, for the United States Department of Energy's
National Nuclear Security Administration under Contract DE-AC04-94AL85000.

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: http://www.osti.gov/bridge

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd.
Springfield, VA 22161

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.fedworld.gov
Online order: http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online

SAND2006-3440
Unlimited Release
Printed July 2006

Quantum Gate Decomposition Algorithms

Alexander Slepoy
Multiscale Composition Materials Methods
Sandia National Laboratories
P.O. Box 5800
Albuquerque, New Mexico 87185-MS1110

Abstract

Quantum computing algorithms can be conveniently expressed in a format of a quantum logical circuits. Such circuits consist of sequential coupled operations, termed "quantum gates", on quantum analogs of bits called qubits. We review a recently proposed method [1] for constructing general "quantum gates" operating on a *n* qubits, as composed of a sequence of generic elementary "gates".

CONTENTS

FIGURES

Quantum Gate Decomposition Algorithms

A. Slepoy
Sandia National Laboratories, Albuquerque, NM
(Dated: January 27, 2006)

Quantum computing algorithms can be conveniently expressed in a format of a quantum logical circuits. Such circuits consist of sequential coupled operations, termed "quantum gates", on quantum analogs of bits called *qubits*. We review a recently proposed method [1] for constructing general "quantum gates" operating on n qubits, as composed of a sequence of generic elementary "gates".

PACS numbers: Valid PACS appear here

I. INTRODUCTION

A classical bit, an elementary unit of classical information, is allowed two mutually exclusive values only, for example, 1 or 0. Its quantum counterpart, qubit, can span the continuous space between the two values through a complex-valued superposition of the two exclusive states:

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle,$$

where α and β are complex variables. Thus, the qubit potentially stores an infinite amount of information. Processing such information could lead to extreme parallelism since a single operation could transform an infinite data set simultaneously. The resulting information, however, is not accessible directly, since an act of measurement collapses the superposition to one of the exclusive values, leaving no hint of the superposition. The superposition existence is revealed through repeated trials, which result in a statistical distribution of the outcomes, reflective of the continuous value of the superposition coefficient.

$$P(|0\rangle) = \|\alpha\|^2$$
$$P(|1\rangle) = \|\beta\|^2$$

An apparent need to query the state of the registers repeatedly to obtain the results seems to work against the advantage gained through the quantum parallelism.

The deficiency described above can be overcome through load balancing. If a significant number of sequential parallel operations can be performed on a quantum state of the system before collapsing it, then the constant cost of measurement at the end of the execution can be arbitrarily amortized by the benefits of the quantum parallelism. We do not yet understand how such load balancing can be accomplished and construction of efficient quantum algorithms is a subject of ongoing research. A set of operations can be described that transforms a collective state of a quantum bus, an enumerated collection of qubits, without collapsing the quantum state of the system. The operators that satisfy this criterion are unitary and reversible. Since a superposition state of a system can be conveniently viewed as a vector, much of the quantum operator formalism has borrowed the language of linear algebra. An operator that transforms a vector to another vector is a matrix, so a quantum operator is typically represented as such.

$$|\Psi\rangle = M|\Phi\rangle,$$

where $|\Psi\rangle$ and $|\Phi\rangle$ are vectors, and matrix elements of M are obtained through an $|e_i\rangle$ basis projection: $M_{ij} = \langle e_i|e_j\rangle$.

A unitary operator on a vector space is a linear operator that is length-preserving. A reversible operator is bijective, i.e. has a well-defined inverse. These concepts are well understood in linear algebra, have been translated to constraints on matrix properties, and time-dependent evolution of an isolated quantum system has been demonstrated to obey such rules [2].

A quantum gate can be represented by a general unitary transformation involving n-qubits. A quantum computer requires a library of quantum gates to represent or approximate a general unitary transformation. A set of such gates is termed a *universal* library of *elementary* gates. It has been demonstrated that such a library can be constructed from single qubit unitary gates and almost any fixed two-qubit gate [3]. Typically, a controlled-NOT [CNOT] gate is used as the two-qubit gate mainly chosen for its simplicity. Two-qubit gates operate through the relatively weak coupling of two qubits, making such gates more difficult to implement. Therefore, efficient decompositions attempt to minimize the number of CNOT gates. Such gates are also constrained by the physical proximity of the relevant qubits adding further requirements to the decomposition.

When a rotation axis corresponds to a particular Cartesian axis, the elementary single qubit rotations in matrix form are

$$R_x = e^{i\sigma_x\theta/2} = \begin{pmatrix} \cos(\theta/2) & i\sin(\theta/2) \\ i\sin(\theta/2) & \cos(\theta/2) \end{pmatrix}$$

$$R_y = e^{i\sigma_y\theta/2} = \begin{pmatrix} \cos(\theta/2) & \sin(\theta/2) \\ -\sin(\theta/2) & \cos(\theta/2) \end{pmatrix}$$

$$R_z = e^{i\sigma_z\theta/2} = \begin{pmatrix} e^{i\theta/2} & 0 \\ 0 & e^{-i\theta/2} \end{pmatrix}$$

Any $SU(2)$ operation can be accessed by at most three rotations:

$$U = R_z(\alpha)R_y(\beta)R_z(\gamma),$$

where α, β, and γ are the Euler angles.

The two-qubit gate CNOT is represented in the basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ as

$$U_{CNOT} = I \oplus \sigma_x = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

This operator performs an inversion on the state of the second cubit, if the first qubit is in $|1\rangle$ state, and does nothing if the first qubit is in $|0\rangle$ state.

The method described in the paper decomposes an arbitrary n-qubit unitary gate into a set of the elementary gates. The proposed algorithm is compared to the theoretical minimum number of gates required to represent a general unitary transformation, and arrives at the an estimated 4 times the theoretical minimum for the required number of the crucial CNOT gates. This number is allegedly the best available to date. The description of the algorithm follows.

II. DECOMPOSITION ALGORITHM

The method uses a Cosine-Sine Decomposition [CSD] [4] and uniformly controlled rotations to represent a general unitary operation in terms of elementary gates described in the introduction.

A. Cosine-Sine Decomposition

CSD is an iterative procedure for decomposing a general unitary operator into elementary operators. A single step in the recursion is based on the following idea:

$$U = \begin{pmatrix} L_0 & \\ & L_1 \end{pmatrix} \begin{pmatrix} D_{0,0} & D_{0,1} \\ D_{1,0} & D_{1,1} \end{pmatrix} \begin{pmatrix} R_0 & \\ & R_1 \end{pmatrix}.$$

A general unitary matrix can be decomposed into left and right block diagonal forms, where the dimensions of the two blocks sum to the original dimension, and a central D matrix consisting of four diagonal blocks. Here, L_0, L_1, R_0, R_1 are unitary, and $D_{0,0}, D_{0,1}, D_{1,0}, D_{1,1}$ are diagonal with $D_{0,1} = -D_{0,0}$. For equal-dimensional partition, this is a special case of the Generalized SV decomposition. Because of the unitary constraint,

$$D_{0,0} = D_{1,1} = diag(C_1, C_2, ..., C_{N/2}),$$
$$D_{0,1} = -D_{1,0} = diag(S_1, S_2, ..., S_{N/2}).$$

where $C_i = \cos(\theta_i)$ and $S_i = \sin(\theta_i)$ for some angle θ_i.

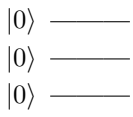
The first step in the recursion produces three matrices, L and R with two diagonal unitary blocks each, and a central D with four blocks, each diagonal. The next step in the recursion operates on L_0, L_1, R_0, R_1 in the same manner. Both L and R each become three matrices, with the decomposition applied individually to each block, resulting in a product of 7 matrices:

$$\begin{pmatrix} L_0^1 & & & \\ & L_1^1 & & \\ & & L_2^1 & \\ & & & L_3^1 \end{pmatrix} \begin{pmatrix} D_{0,0}^1 & D_{0,1}^1 & & \\ D_{1,0}^1 & D_{1,1}^1 & & \\ & & D_{3,3}^1 & D_{3,4}^1 \\ & & D_{4,3}^1 & D_{4,4}^1 \end{pmatrix} \begin{pmatrix} R_0^1 & & & \\ & R_1^1 & & \\ & & R_2^1 & \\ & & & R_3^1 \end{pmatrix} \begin{pmatrix} D_{0,0} & D_{0,1} \\ D_{1,0} & D_{1,1} \end{pmatrix} \begin{pmatrix} L_0^1 & & & \\ & L_1^1 & & \\ & & L_2^1 & \\ & & & L_3^1 \end{pmatrix}$$
$$\begin{pmatrix} D_{0,0}^1 & D_{0,1}^1 & & \\ D_{1,0}^1 & D_{1,1}^1 & & \\ & & D_{3,3}^1 & D_{3,4}^1 \\ & & D_{4,3}^1 & D_{4,4}^1 \end{pmatrix} \begin{pmatrix} R_0^1 & & & \\ & R_1^1 & & \\ & & R_2^1 & \\ & & & R_3^1 \end{pmatrix}.$$

The superscript refers to the iteration number. The subscripts indicate position of block in its matrix structure. L, D and R matrices on the right are not the same as the ones on the left, except in structure. Their entries are given by their respective decompositions. At the end of the recursion, we are left with a product of matrices that have a special form. All the resulting L and R matrices now have a 2×2 block-diagonal structure. The D matrices have two entries in each row connected with a complimentary pair in another row by the cosine-sine relation. Each of these resulting matrices is termed a *uniformly controlled rotation*.

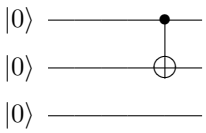
B. Quantum Circuits.

A quantum circuit is a convenient representation of the operators as they transform the state of a multi-qubit array. In such circuits, the wires represent the state of a qubit as they progress through the operations. The following quantum circuits were rendered using public domain software [5]. The circuit directly below is a representation of three qubits, initialized to state $|000\rangle$.



The operators are represented as quantum gates in the order from left to right. This order is inverted with respect to the "bra-ket" notation, where the next operator is right-most with respect to the "ket". For example, contrast operation $CBA|0\rangle$ with the circuit below.

Single qubit gates cannot represent coupling between qubits. Mulit-qubit gates often take form of control gates, where the operation on a given qubit is conditional on the state of another qubit. The circuit below expresses a controlled operation in which the second qubit state is flipped with a CNOT operation if the first qubit is set:



C. Uniformly Controlled Gate.

The decomposed form of the arbitrary unitary operator now consists of a product of operators, each of which is a *uniformly controlled rotation*. These are single-qubit rotations controlled by a joint classical state of the rest of the qubits. The paper defines this rotation as $F_m^k(R_a)$, where the m-th qubit is controlled by the 2^k classical states of k other qubits, example in Fig.1.

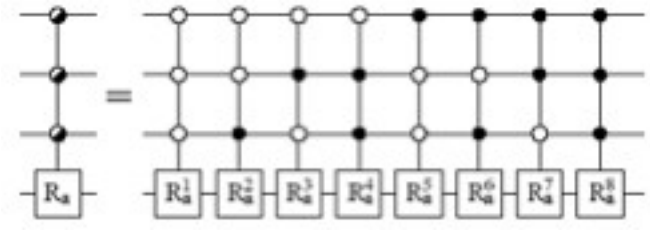


FIG. 1: Definition of the uniformly controlled rotation $F_4^3(R_a)$. Here **a** is a three-dimensional vector fixing the rotation axis of the matrices $R_a^j = R_(\alpha_j)$.

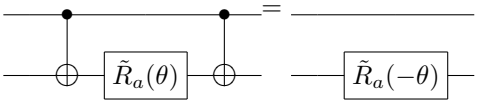
Let $F_m^k(R_\mathbf{a})$ represent an uniformly controlled rotation. A special case of such rotation is $F_{k+1}^k(R_\mathbf{a})$, which has a matrix representation

$$\begin{pmatrix} R_\mathbf{a}(\alpha_1)^1 & & & \\ & \cdot & & \\ & & \cdot & \\ & & & R_\mathbf{a}(\alpha_{2^k}) \end{pmatrix}.$$

where the rotation matrices are of the form

$$R_\mathbf{a}(\phi) = e^{i\mathbf{a}\cdot\overrightarrow{\sigma}\phi/2} = I \quad (1)$$
$$cos(\phi/2) + i(\mathbf{a}\cdot\overrightarrow{\sigma}) \quad (2)$$
$$sin(\phi/2). \quad (3)$$

Here, $\mathbf{a}\cdot\overrightarrow{\sigma} = a_x\sigma_x + a_y\sigma_y + a_z\sigma_z$. Setting $a_x = 0$ produces the following result: $\sigma_x R_a(\theta)\sigma_x = R_a(-\theta)$. Clearly, single qubit control can now undo a rotation of another qubit. The fact that the CNOT gate is exactly the "controlled σ_x" leads to a decomposition of the uniformly controlled gate into 2^k CNOTs and 2^k single qubit rotations.



This is an important piece of information in understanding the decomposition procedure.

D. Gray Code Ordering.

The authors propose an algorithm where a CNOT gate is sandwiched between two single-qubit rotation operators on the slave qubit. These rotations are perpendicular to the x axis to assure the decoupled action of the CNOTs. They minimize the number of single control CNOTs needed to accomplish this by ordering the rotations and their control states according to a cyclic binary Grey code. The reordering is permitted because the operations commute. Gray code arranges the control states so that they only differ by a value of a single bit. A realization of the uniform rotation $F_4^3(R_\mathbf{a})$ with the associated Gray code ordering is depicted in Fig. 2. The position of the control node in the l^{th} CNOT gate matches the position where the l^{th} and $(l+1)^s t$ bit strings g_{l-1} and g_l of the Gray code are different.

The first CNOT gate is set by the state of the 3^{rd} bit, the second CNOT gate is set by the 2^{nd} bit, and so on. It is clear that, for any of the basis vector input states, CNOT gates destroy each other. The rotations are additive since they share a common axis $R_\mathbf{a}(\phi)R_\mathbf{a}(\omega) = R_\mathbf{a}(\phi+\omega)$ for any ϕ and ω. The resulting operation is a rotation of the slave qubit through an angle which is

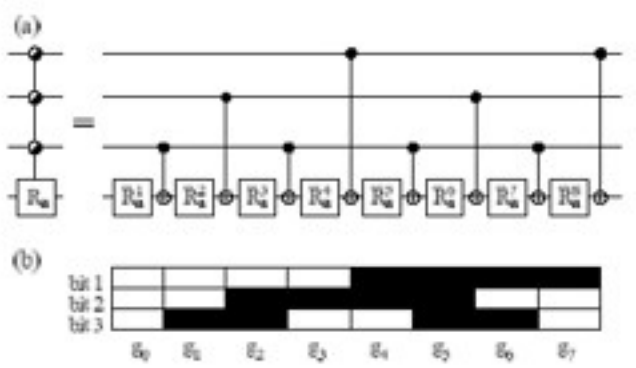


FIG. 2: (a) Quantum circuit realizing the gate $F_4^3(R_{\mathbf{a}})$, where $\mathbf{a}$ is perpendicular to the x axis. Here the authors have used a notation $\tilde{R}^j(\mathbf{a}) = R_{\mathbf{a}}(\theta_j)$. (b) Binary reflected 3-bit Gray code used to define the positions of the control nodes. The black and white rectangles denote bit values one and zero, respectively.

linearly constructed of the angles θ_j. The circuits in the figures 1 and 2 are equivalent if the angles θ_i can be found that solve a linear system of equations

$$M_k \begin{pmatrix} \theta_1 \\ . \\ . \\ \theta_{2^k} \end{pmatrix} = \begin{pmatrix} \alpha_1 \\ . \\ . \\ \alpha_{2^k} \end{pmatrix} \tag{4}$$

.

The matrix elements of M_k can be obtained from equation 1. A rotation angle θ_j is reversed if the l^{th} bit of the g_{j-1} bit string is 1. Then

$$M_{ij}^k = (-1)^{b_{i-1} \cdot g_{j-1}}, \tag{5}$$

where b_i is a standard binary representation of the integer i and the exponent is a bitwise product of binary vectors. The inverse of M_k is $(M_k)^{-1} = 2^{-k}(M^k)^T$, so θ_i can be calculated by applying the inverse to the right hand side of Eqn. 4. This means that any uniform rotation operation $F_m^k(R_{\mathbf{a}})$ around the x-axis with $k \geq 1$ needs at most 2^k CNOT gates and 2^k single qubit rotations $R_{\mathbf{a}}(\theta_i)$.

III. REFERENCES

1. M. Mottonen, J. J. Vartiainen, V. Bergholm, and M. M. Salomaa, Physical Review Letters 93, 130502 (2004, ISSN 0031-9007.

2. A. Peres, *Physical Review A 32*, 32663276 (1985).

3. A. Barenco, *Proceedings of the Royal Society of London Series A-Mathematical and Physical Sciences 449*, 679 (1995), ISSN 0962-8444.

4. G. H. Golub and C. F. V. Loan, *Matrix Computations* (The Johns Hopkins University Press, Baltimore, MD, USA, 1989), 2nd ed.

5. S. Flammia and B. Eastin, *Q-circuit.*

DISTRIBUTION:

1	MS0321	William J. Camp	1400
1	MS0672	L. Pierson	5616
1	MS1318	David Womble	1410
1	MS1318	John B. Aidun	1435
1	MS1318	Erik DeBenedictis	1423
5	MS1318	Alex Slepoy	1435
2	MS9018	Central Technical Files	8944
2	MS0899	Technical Library	4536