I

Publication I

M. Möttönen, J. J. Vartiainen, V. Bergholm, M. M. Salomaa, *Quantum circuits for general multiqubit gates*, Phys. Rev. Lett. **93**, 130502 (2004).

http://link.aps.org/abstract/prl/v93/p130502

Quantum Circuits for General Multiqubit Gates

Mikko Möttönen,* Juha J. Vartiainen, Ville Bergholm, and Martti M. Salomaa
Materials Physics Laboratory, POB 2200 (Technical Physics), FIN-02015 HUT, Helsinki University of Technology, Finland

(Received 7 May 2004; published 20 September 2004)

We consider a generic elementary gate sequence which is needed to implement a general quantum gate acting on n qubits—a unitary transformation with 4^n degrees of freedom. For synthesizing the gate sequence, a method based on the so-called cosine-sine matrix decomposition is presented. The result is optimal in the number of elementary one-qubit gates, 4^n, and scales more favorably than the previously reported decompositions requiring $4^n - 2^{n+1}$ controlled NOT gates.

DOI: 10.1103/PhysRevLett.93.130502 PACS numbers: 03.67.Lx

The foundation of quantum computation [1] involves the encoding of computational tasks into the temporal evolution of a quantum system. Thereby a register of n qubits, identical two-state quantum systems, is employed. Quantum algorithms can be described by unitary transformations and projective measurements acting on the 2^n-dimensional state vector of the register. In this context, unitary transformations are also called quantum gates. The recently discovered quantum algorithms [2–4] embody arbitrary unitary transformations and hence call for techniques to efficiently implement a general n-qubit gate. The complexity of an implementation is measured in terms of the number of elementary gates required [5]. Achieving gate arrays of lower complexity is crucial not only because it generally results in shorter execution times, but it may also introduce fewer errors.

Any finite-dimensional unitary transformation can be represented as a unitary matrix, and hence any n-qubit gate corresponds to a certain $2^n \times 2^n$ unitary matrix, U. Therefore, the powerful methods of matrix computation [6] can be utilized to produce quantum gate decompositions. However, only decompositions yielding matrices that correspond to gate sequences of low complexity are interesting. We choose the library of elementary gates to consist of the controlled NOT (CNOT) gate, the one-qubit rotations about the y and z axes, and a phase gate adjusting the unobservable global phase. Since the cost of physically realizing a CNOT gate may exceed that of a one-qubit gate, we count the numbers of these gates separately.

A general unitary $2^n \times 2^n$ matrix U has 4^n real degrees of freedom. Since each elementary one-qubit gate carries 1 degree of freedom, at least 4^n such gates are needed to implement U. The current theoretical lower bound for the number of CNOT gates needed in realizing an arbitrary n-qubit gate, $\lceil \frac{1}{4}(4^n - 3n - 1) \rceil$, is given in Ref. [7]. However, no circuit construction yielding these numbers of CNOT or elementary one-qubit gates has been presented in the literature. The conventional approach [5] to implementing general multiqubit gates makes use of the QR decomposition [6] for unitary matrices, yielding an array of $O(n^3 4^n)$ elementary gates. Heretofore, the most efficient implementation based on the QR decomposition, for asymptotically large n, requires approximately 8.7×4^n CNOT gates [8]. In addition, the synthesis of optimal quantum circuits for certain special classes of gates has been intensively studied. The implementation of a general two-qubit gate [7,9–11] is found to require three CNOTs and 16 elementary one-qubit gates. For a three-qubit gate, the current minimal implementation using 40 CNOTs and 98 elementary one-qubit gates [12] is based on the Khaneja-Glaser decomposition (KGD) [13]. Furthermore, an implementation of an arbitrary diagonal unitary matrix involving $2^n - 2$ CNOTs and 2^n elementary one-qubit gates is known [14].

In this Letter, we present an efficient implementation of a general unitary transformation U by recursively utilizing the cosine-sine decomposition (CSD) [15]. In the context of quantum computation, the CSD has first been considered in Ref. [16], and its relation to the KGD has recently been discussed in [17]. We decompose U into a product of matrices, each of which is identified with a new type of gate that we call a uniformly controlled rotation. To implement these gates, we present an efficient elementary gate sequence which is related to the gates recently explored in Ref. [14] as a part of the implementation of a diagonal quantum computer.

Let $F_m^k(R_{\mathbf{a}})$ denote a uniformly controlled rotation. It consists of k-fold controlled rotations of qubit m about the three-dimensional vector $\mathbf{a}$, one rotation for each of the 2^k different classical values of the control qubits. The index m may acquire the values $1, 2, \ldots, n$ and k the values $1, 2, \ldots, n-1$. An example of $F_m^k(R_{\mathbf{a}})$, where $m = 4$ and $k = 3$, is shown in Fig. 1. The relative order of the controlled rotations is irrelevant; the gates commute. For instance, the uniformly controlled rotation $F_{k+1}^k(R_{\mathbf{a}})$ has the matrix representation

$$F_{k+1}^k(R_{\mathbf{a}}) = \begin{pmatrix} R_{\mathbf{a}}(\alpha_1) & & \\ & \ddots & \\ & & R_{\mathbf{a}}(\alpha_{2^k}) \end{pmatrix}, \quad (1)$$

where the angles $\alpha_1, \alpha_2, \ldots, \alpha_{2^k}$ may be freely chosen and

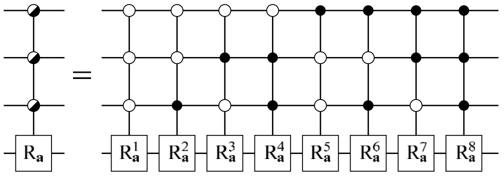

FIG. 1. Definition of the uniformly controlled rotation $F^3_4(R_{\mathbf{a}})$. Here $\mathbf{a}$ is a three-dimensional vector fixing the rotation axis of the matrices $R^j_{\mathbf{a}} = R_{\mathbf{a}}(\alpha_j)$.

the rotation matrix $R_{\mathbf{a}}(\phi)$ is given by

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

Above I is the unit matrix, and the product $\mathbf{a}\cdot\boldsymbol{\sigma} = a_x\sigma_x + a_y\sigma_y + a_z\sigma_z$ involves the Pauli matrices σ_x, σ_y, and σ_z [1]. In general, $F^k_m(R_{\mathbf{a}})$ is a product of 2^k two-level matrices.

We propose an implementation of $F^k_m(R_{\mathbf{a}})$ with $a_x = 0$ using an alternating sequence of 2^k CNOTs and 2^k one-qubit rotations $R_{\mathbf{a}}(\theta_i)$ acting on the qubit m. The position of the control node in the lth CNOT gate is set to match the position where the lth and $(l+1)$th bit strings g_{l-1} and g_l of the binary reflected Gray code [18] differ. In binary Gray codes, the adjacent bit strings differ by definition only in a single bit, and hence the position is well defined. As an example, the quantum circuit for the gate $F^3_4(R_{\mathbf{a}})$ is shown in Fig. 2(a) while Fig. 2(b) illustrates the correspondence of the Gray code to the positions of the control nodes in the CNOT gates.

In the proposed construction, each of the control qubits regulates an even number of NOT gates, since in a cyclic Gray code each bit is flipped an even number of times. On the other hand, Eq. (2) yields

$$a_x = 0 \Rightarrow \sigma_x R_{\mathbf{a}}(\theta)\sigma_x = R_{\mathbf{a}}(-\theta). \quad (3)$$

Hence, for any of the standard basis vectors acting as an input all the induced NOT gates annihilate each other and negate some of the angles $\{\theta_i\}$. Furthermore, subsequent rotations about any single axis $\mathbf{a}$ are additive, i.e., $R_{\mathbf{a}}(\phi)R_{\mathbf{a}}(\omega) = R_{\mathbf{a}}(\phi + \omega)$ for arbitrary angles ϕ and ω. Thus, the construction yields a rotation of the qubit m about the axis $\mathbf{a}$ through an angle which is a linear combination of the angles $\{\theta_i\}$. Consequently, the proposed quantum circuit is equivalent to the gate $F^k_m(R_{\mathbf{a}})$ provided that the angles $\{\theta_i\}$ are a solution of the linear system of equations

$$M^k\begin{pmatrix}\theta_1\\ \vdots\\ \theta_{2^k}\end{pmatrix} = \begin{pmatrix}\alpha_1\\ \vdots\\ \alpha_{2^k}\end{pmatrix}, \quad (4)$$

where the matrix elements M^k_{ij} can be determined using Eq. (3). The rotation angle θ_j is negated, provided that the control nodes attached to the lth qubit are active and the lth bit of g_{j-1} has the value one. The negations must be applied for each control qubit independently, which results in

$$M^k_{ij} = (-1)^{b_{i-1}\cdot g_{j-1}}, \quad (5)$$

where b_i is the standard binary code representation of the integer i and the dot in the exponent denotes the bitwise inner product of the binary vectors.

The matrix M^k bears a strong resemblance to the k-bit Walsh-Hadamard matrix $H^k_{ij} = 2^{-k/2}(-1)^{b_{i-1}\cdot b_{j-1}}$, which is by construction orthogonal. Since a Gray code is a permutation of the standard binary code, $2^{-k/2}M^k$ is a column-permuted version of H^k and thus also orthogonal. Consequently, we obtain the inverse matrix $(M^k)^{-1} = 2^{-k}(M^k)^T$, and the determination of $\{\theta_i\}$ for any desired angles $\{\alpha_i\}$ is immediate. Thus any uniformly controlled rotation $F^k_m(R_{\mathbf{a}})$ with $a_x = 0$ and $k \geq 1$ can be realized using 2^k CNOT gates and 2^k one-qubit rotations $R_{\mathbf{a}}(\theta_i)$. We note that although we chose to use the binary reflected Gray code to determine the positions of the control nodes in the CNOT gates, any cyclic k-bit binary Gray code will also qualify. Furthermore, $F^k_m(R_{\mathbf{a}})$ can also be achieved by a horizontally mirrored version of the quantum circuit presented.

The CSD of a unitary $2^n \times 2^n$ matrix may be expressed as [15]

$$U = \underbrace{\begin{pmatrix}u^1_{11} & 0\\ 0 & u^1_{12}\end{pmatrix}}_{U^1_1}\underbrace{\begin{pmatrix}c^1_{11} & s^1_{11}\\ -s^1_{11} & c^1_{11}\end{pmatrix}}_{A^1_1}\underbrace{\begin{pmatrix}u^1_{21} & 0\\ 0 & u^1_{22}\end{pmatrix}}_{\tilde{U}^1_2}, \quad (6)$$

where the exact form of the submatrices is given below. The decomposition may be applied recursively to the submatrices of U^i_j, until a 2×2 block-diagonal form is encountered. In our indexing scheme, the upper index denotes the level of recursion, whereas the lower index denotes the position of the matrix within the resulting

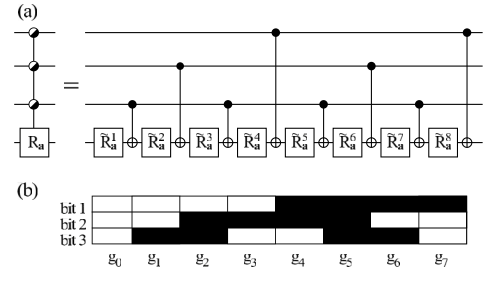
(a)
$R_{\mathbf{a}}$
=
$\tilde{R}^1_{\mathbf{a}}$
$\tilde{R}^2_{\mathbf{a}}$
$\tilde{R}^3_{\mathbf{a}}$
$\tilde{R}^4_{\mathbf{a}}$
$\tilde{R}^5_{\mathbf{a}}$
$\tilde{R}^6_{\mathbf{a}}$
$\tilde{R}^7_{\mathbf{a}}$
$\tilde{R}^8_{\mathbf{a}}$
(b)
bit 1
bit 2
bit 3
g_0
g_1
g_2
g_3
g_4
g_5
g_6
g_7

FIG. 2. (a) Quantum circuit realizing the gate $F^3_4(R_{\mathbf{a}})$, where $\mathbf{a}$ is perpendicular to the x axis. Here we 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.

matrix product. We note that CSD is not unique, and one should take the possible internal symmetries of the matrix U into account to obtain the simplest achievable form for the matrices U_j^i.

In the decomposition, u_{jk}^i $(k = 1, \ldots, 2^i)$ are unitary $2^{n-i} \times 2^{n-i}$ matrices and the real diagonal matrices c_{jk}^i and s_{jk}^i $(k = 1, \ldots, 2^{i-1})$ are of the form $c_{jk}^i = \mathrm{diag}_l(\cos\theta_l)$ and $s_{jk}^i = \mathrm{diag}_l(\sin\theta_l)$ $(l = 1, \ldots, 2^{n-i})$. For a general $i = 1, \ldots, n-1$, the matrices U_j^i and A_j^i assume the forms

$$U_j^i = \mathrm{diag}_k(u_{jk}^i); \qquad (k = 1, \ldots, 2^i), \tag{7}$$

and

$$A_j^i = \mathrm{diag}_k\left[\begin{pmatrix} c_{jk}^i & s_{jk}^i \\ -s_{jk}^i & c_{jk}^i \end{pmatrix}\right]; \qquad (k = 1, \ldots, 2^{i-1}), \tag{8}$$

where Eq. (7) applies also for $\tilde{U}_j^i$. For the ith level of the recursion we obtain

$$U_j^{i-1} = U_{2j-1}^i A_{\zeta(i,j)}^i \tilde{U}_{2j}^i, \tag{9}$$

where the indexing function $\zeta(i, j) = 2^{n-i-1}(2j - 1)$ has been introduced to make the result of the recursion more feasible. The matrix A_1^1 is also referred to as $A_{\zeta(1,1)}^1$. As compared with the original matrix U_j^{i-1}, the above decomposition contains 2^{n-1} additional degrees of freedom. To specify them explicitly, we define unitary diagonal matrices

$$P_j^i = \mathrm{diag}_k(p_{j,\lceil k/2 \rceil}^i), \tag{10}$$

where $j, k = 1, \ldots, 2^i$ and the diagonal matrix $p_{jk}^i = \mathrm{diag}_l(e^{i\alpha_l})$, where $l = 1, \ldots, 2^{n-i}$. The angles $\{\alpha_l\}$ may be chosen arbitrarily for each p_{jk}^i and, as shown below, we can use them to reduce the total number of gates needed in the final decomposition. We insert $I = P_{\zeta(i,j)}^i (P_{\zeta(i,j)}^i)^\dagger$ into Eq. (9), next to $A_{\zeta(i,j)}^i$ with which $P_{\zeta(i,j)}^i$ commutes, and obtain

$$U_j^{i-1} = U_{2j-1}^i P_{\zeta(i,j)}^i A_{\zeta(i,j)}^i U_{2j}^i, \tag{11}$$

where the matrix $(P_{\zeta(i,j)}^i)^\dagger$ is absorbed into the definition of $U_{2j}^i = (P_{\zeta(i,j)}^i)^\dagger \tilde{U}_{2j}^i$, and $P_{\zeta(i,j)}^i$ is kept intact.

Finally, the decomposition leads to the result

$$U = \left(\prod_{j=1}^{2^{n-1}-1} \underbrace{U_j^{n-1} P_j^{\gamma(j)}}_{B_j} A_j^{\gamma(j)} \right) \underbrace{U_{2^{n-1}}^{n-1}}_{B_{2^{n-1}}}, \tag{12}$$

where the function $\gamma(j) + 1$ indicates the position of the least significant nonzero bit in the n-bit binary presentation of the number j. The matrices $P_j^{\gamma(j)}$ are determined by the preceding matrix U_j^{n-1}. This fixes the order in which the recursion must be applied, since the absorbed matrices $(P_j^{\gamma(j)})^\dagger$ affect consequent decompositions. Thus, the recursion in Eq. (11) is first applied to the matrix U_j^i with the largest upper index and, upper indices being equal, the smallest lower index subject to the stopping criterion $i = n - 1$.

We find that each of the matrices A_j^i in Eq. (12) corresponds to a gate $F_i^{n-1}(R_y)$. Furthermore, the 2×2 block-diagonal matrices B_j may, with a suitable choice of $P_j^{\gamma(j)}$, be expressed as

$$B_j = F_n^{n-1}(R_z) F_n^{n-1}(R_y) F_{\gamma(j)}^{n-1}(R_z), \tag{13}$$

and combined with the subsequent $A_j^{\gamma(j)}$ into a BA section:

$$(BA)_j = F_n^{n-1}(R_z) F_n^{n-1}(R_y) F_{\gamma(j)}^{n-1}(R_z) F_{\gamma(j)}^{n-1}(R_y). \tag{14}$$

The final matrix $B_{2^{n-1}}$, for which we have no extra degrees of freedom left, must be implemented as

$$\begin{aligned} B_{2^{n-1}} = {} & F_n^{n-1}(R_z) F_n^{n-1}(R_y) \\ & \times F_n^{n-1}(R_z) F_{n-1}^{n-2}(R_z) \cdots F_1^0(R_z)\Phi, \end{aligned} \tag{15}$$

where Φ is an elementary phase gate which serves to fix the unobservable global phase. To illustrate the method, the complete decomposition of a general three-qubit gate is shown in Fig. 3.

Each of the BA sections consists of two uniformly controlled z rotations and two uniformly controlled y rotations. By mirroring the circuits of the y rotations, we may cancel four CNOT gates in each section. Hence the cost of each of the $2^{n-1} - 1$ sections is 2^{n+1} elementary one-qubit rotations and $2^{n+1} - 4$ CNOTs. The final B matrix decomposes into uniformly controlled z and y rotations followed by a cascade of uniformly controlled z rotations which fixes the phases. This cascade corresponds to the diagonal quantum computer of Ref. [14]. Applying the mirroring trick, two more CNOT gates are cancelled between the z and y rotations. The cost of the last B section is 2^{n+1} elementary one-qubit gates and $2^{n+1} - 4$ CNOTs. Finally, we arrive at the total complexity of the decomposition: $4^n - 2^{n+1}$ CNOT gates and 4^n elementary one-qubit gates.

In conclusion, the proposed decomposition of a general multiqubit gate, based on the CSD and uniformly con-

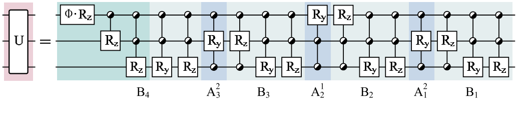

FIG. 3 (color online). Quantum circuit for a three-qubit gate obtained using the cosine-sine decomposition. The sequences of gates B_j correspond to the 2×2-block-diagonal matrices and the gates A_j^i to the cosine-sine matrices. The leftmost gate sequence corresponds to the diagonal quantum computer of Ref. [14].

trolled rotations, provides a quantum circuit that contains the minimal number of elementary one-qubit gates and on the order of 4 times the minimal number of CNOT gates. Compared with the minimal decomposition of a two-qubit gate [7,9–11] the CSD method requires five extra CNOT gates. For a three-qubit gate the CSD requires 48 CNOT gates and 64 elementary one-qubit gates, as opposed to the circuit of 40 CNOTs and 98 elementary one-qubit gates obtained using the KGD in Ref. [12]. For four-qubit gates the CSD provides a quantum circuit of 256 elementary one-qubit gates and 224 CNOTs, which is the shortest elementary gate array known to implement such a gate. Thus, for a general n-qubit gate, where $n \geq 4$, the method presented provides the most efficient quantum circuit known to implement the gate.

To further improve the implementation of a particular quantum gate one may optimize the synthesized quantum circuit. The possible methods for optimization include finding the most efficient CSD factorizations, varying the Gray codes, mirroring the gate arrays of the uniformly controlled rotations and possibly combining the uniformly controlled y and z rotations into general uniformly controlled gates. Certain quantum gates that are likely to be useful in quantum computation comprise internal symmetries and can thus be implemented using only a polynomial number of elementary gates. For example, $O(n^2)$ gates are needed to implement a quantum Fourier transformation of n qubits [1]. Although the method presented apparently requires $O(4^n)$ elementary gates, it is still possible that, using proper optimizations, the gate array will appreciably simplify and the result will resemble that of the polynomial decompositions.

This research is supported by the Academy of Finland through the project “Quantum Computation” (No. 206457). M. M. and J. J. V. thank the Foundation of Technology (Finland), J. J. V. the Nokia Foundation, M. M. and V. B. the Finnish Cultural Foundation, and M. M. S. the Japan Society for the Promotion of Science for financial support. S. M. M. Virtanen is acknowledged for stimulating discussions.

*Electronic address: mpmotton@focus.hut.fi

[1] M. L. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).

[2] P. Jaksch and A. Papageorgiou, Phys. Rev. Lett. **91**, 257902 (2003).

[3] J. P. Paz and A. Roncaglia, Phys. Rev. A **68**, 052316 (2003).

[4] D. S. Abrams and S. Lloyd, Phys. Rev. Lett. **83**, 5162 (1999).

[5] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. H. Margolus, P.W. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter, Phys. Rev. A **52**, 3457 (1995).

[6] G. H. Golub and C. F. Van Loan, *Matrix Computations* (Johns Hopkins Press, Baltimore, 1996), 3rd ed.

[7] V. V. Shende, I. L. Markov, and S. S. Bullock, Phys. Rev. A **69**, 062321 (2004).

[8] J. J. Vartiainen, M. Möttönen, and M. M. Salomaa, Phys. Rev. Lett. **92**, 177902 (2004).

[9] F. Vatan and C. P. Williams, Phys. Rev. A **69**, 032315 (2004).

[10] J. Zhang, J. Vala, S. Sastry, and K. B. Whaley, Phys. Rev. Lett. **93**, 020502 (2004).

[11] G. Vidal and C. M. Dawson, Phys. Rev. A **69**, 010301 (2004).

[12] F. Vatan and C. P. Williams, quant-ph/0401178.

[13] N. Khaneja and S. Glaser, Chem. Phys. **267**, 11 (2001).

[14] S. S. Bullock and I. L. Markov, Quantum Inf. Comput. **4**, 27 (2004).

[15] C. C. Paige and M. Wei, Linear Algebra Appl. **208**, 303 (1994).

[16] R. R. Tucci, quant-ph/9902062 (2001, 2nd version).

[17] S. S. Bullock, quant-ph/0403141.

[18] C. Savage, SIAM Rev. **39**, 605 (1997).