Quantum circuits with uniformly controlled one-qubit gates

Ville Bergholm,* Juha J. Vartiainen, Mikko Möttönen, and Martti M. Salomaa
Materials Physics Laboratory, POB 2200 (Technical Physics) FIN-02015 HUT, Helsinki University of Technology, Finland
(Received 28 October 2004; revised manuscript received 18 February 2005; published 27 May 2005)

Uniformly controlled one-qubit gates are quantum gates which can be represented as direct sums of two-dimensional unitary operators acting on a single qubit. We present a quantum gate array which implements any n-qubit gate of this type using at most $2^{n-1}-1$ controlled-NOT gates, 2^{n-1} one-qubit gates, and a single diagonal n-qubit gate. To illustrate the versatility of these gates we then apply them to the decomposition of a general n-qubit gate and a state preparation procedure. Moreover, we study their implementation using only nearest-neighbor gates. We give upper bounds for the one-qubit and controlled-NOT gate counts for all the aforementioned applications. In all four cases, the proposed circuit topologies either improve on or achieve the previously reported upper bounds for the gate counts. Thus, they provide the most efficient method for general gate decompositions currently known.

DOI: 10.1103/PhysRevA.71.052330 PACS number(s): 03.67.Lx, 03.65.Fd

I. INTRODUCTION

A quantum computer is an emerging computational device based on encoding classical information into a quantum-mechanical system [1]. Since the breakthrough factorization algorithm by Shor in 1994 [2], progress in research on quantum computing has been expeditious [3]. Most quantum computers involve a collection of two-level systems, a quantum register, in which the information is stored. The two-level systems themselves, called qubits, can also be replaced by arbitrary d-level systems, known as qudits [4,5]. The computation is performed by the unitary temporal evolution of the register, followed by a measurement. In order to execute the desired algorithm, one has to be able to exert sufficient control on the Hamiltonian of the register to obtain the required propagators. These unitary propagators, acting on the register, are called quantum gates.

The current paradigm for implementing quantum algorithms is the quantum circuit model [6], in which the algorithms are compiled into a sequence of simple gates acting on one or more qubits. The detailed decomposition of an arbitrary quantum gate into such a sequence was first presented by Barenco *et al.* [7]. Recently, several effective methods for implementing arbitrary quantum gates have been reported [8–11]. In addition to these constructions, decompositions for certain special classes of gates have been considered: the preparation of quantum states [10,12–14], diagonal [15,16], and block-diagonal quantum computations [17]. The important problem of the gate-optimal implementation of an arbitrary two-qubit gate has also been recently solved [18–21]. These generic quantum circuit constructions will serve as basic building blocks for a low-level quantum compiler and facilitate the optimization of the quantum gate arrays.

The underlying motivation for the pursuit of the optimal quantum circuit decomposition is decoherence [22] which plagues the practical realizations of quantum computers [3]. The properties of the quantum compiler and the available gate primitives strongly influence the execution time of a quantum algorithm, as is the case with their classical counterparts. However, owing to the short decoherence times it is crucial to keep the usage of the computational resources as low as possible, even for the very first demonstrations of quantum computation.

In this paper, we discuss the properties of uniformly controlled one-qubit gates which extend the concept of uniformly controlled rotations introduced in Ref. [9]. We give an efficient implementation for these gates in terms of one-qubit gates and controlled-NOT gates (CNOT's). Moreover, we observe that our construction can be implemented effectively also by using only nearest-neighbor gates. To illustrate the usefulness of the uniformly controlled gates, we apply them to two concrete examples: the decomposition of an arbitrary quantum gate and a state preparation procedure. The obtained quantum circuits are quite compact; in terms of the number of CNOT's involved, the general gate decomposition is brought on par with the most efficient currently known general gate decomposition [10] while requiring roughly 30% less one-qubit gates, whereas the gate counts required to implement the state preparation circuit are halved compared to the previous implementations [10,12]. In addition to these examples, we expect that uniformly controlled one-qubit gates could serve as general intermediate-level building blocks in quantum compilers when performing local optimization of polynomial quantum circuits.

This paper is organized as follows. Section II defines uniformly controlled gates. In Sec. III, the circuit topology implementing the uniformly controlled one-qubit gates is constructed. The implementation is based on the solution of an eigenvalue equation and is thus cognate to the quantum multiplexor operation first introduced in Ref. [10]. In Sec. IV, the cosine-sine decomposition (CSD) of an arbitrary n-qubit gate [9] and a state preparation procedure [12] are improved using this construction. Finally, in Sec. V, we consider the implementation of the uniformly controlled one-qubit gates in a linear chain of qubits with only nearest-neighbor couplings. Section VI is devoted to a discussion

*Electronic address: vberghol@focus.hut.fi

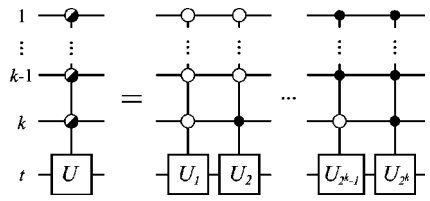

FIG. 1. Uniformly controlled one-qubit gate $F_t^k[\mathrm{U}(2)]$ stands for a sequence of k-fold controlled gates $U_i \in \mathrm{U}(2)$, where $i=1,\ldots,2^k$, acting on the qubit t.

and summary of the results obtained. In addition, a conjecture is presented.

II. UNIFORMLY CONTROLLED GATES

We define a uniformly controlled one-qubit gate $F_t^k[\mathrm{U}(2)]$ to be a sequence of k-fold controlled one-qubit gates in which all the 2^k control node configurations are utilized. All the one-qubit gates in the sequence act on the qubit t; see Fig. 1. We use the symbol $F_t^k[\mathrm{U}(2)]$ to denote a generic gate of this type, whereas the full definition of a particular $F_t^k[\mathrm{U}(2)]$ gate entails the definition of all the U(2) gates $\{U_i\}_{i=1}^{2^k}$.

Let us now consider the set $G_t(2^n) \subset \mathrm{U}(2^n)$ of all gates of the form $F_t^{n-1}[\mathrm{U}(2)]$. Each $U \in G_t(2^n)$ is a 2^n-dimensional unitary operator that can be expressed as a direct sum of two-dimensional unitary operators U_i, all operating in subspaces whose basis vectors differ only in the qubit t: $U=\oplus_{i=1}^{2^{n-1}} U_i$. Since all the operators in $G_t(2^n)$ have identical invariant subspaces, the set is closed under multiplication and inversion; assuming that $A,B \in G_t(2^n)$, we have

$$AB = \bigoplus_{i=1}^{2^{n-1}} A_i B_i \in G_t(2^n), \tag{1}$$

$$A^{-1} = \bigoplus_{i=1}^{2^{n-1}} A_i^{-1} \in G_t(2^n). \tag{2}$$

These properties make $G_t(2^n)$ a subgroup of $\mathrm{U}(2^n)$. We point out that the matrix representations of all the gates in $G_t(2^n)$ can be made simultaneously 2×2 block diagonal in the standard basis using a similarity transformation—namely, a permutation of the qubits, in which the qubit t is mapped to the qubit n.

As a special case of uniformly controlled one-qubit gates, we define uniformly controlled rotations [9], in which all the two-dimensional operators U_i belong to the same one-parameter subgroup of U(2)—e.g., the group of rotations about the z axis. The elements of this particular subgroup are denoted as $F_t^k[R_z]$.

We extend the notation to accommodate also uniformly controlled multiqubit gates; by $F_{\mathcal{T}}^k[\mathrm{U}(2^s)]$ we denote a sequence of k-fold controlled s-qubit gates which act on the set $\mathcal{T}$ of target qubits.

For convenience, we use a shorthand notation for the CNOT and the below-defined two-qubit gate D. The symbol

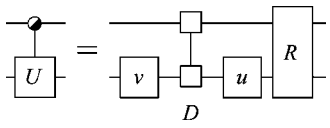

FIG. 2. Two-qubit constant quantum multiplexor where v and u are SU(2) gates, D is a fixed diagonal gate, and R is an adjustable diagonal gate.

C_t^k is used to denote a CNOT whose control and target qubits are the kth and tth, respectively. Similarly, D_j^i refers to a D gate acting on the qubits i and j.

III. CONSTANT QUANTUM MULTIPLEXOR

Let us start by studying the two-qubit gate $F_2^1[\mathrm{U}(2)]$, the matrix representation of which consists of two unitary 2×2 blocks. We show that it can be implemented using the circuit presented in Fig. 2. We call this circuit a constant quantum multiplexor after a related circuit in Ref. [10]. It can be used to construct any 2×2 block-diagonal two-qubit gate by multiplexing the contents of the one-qubit gates u and v together with the help of a fixed diagonal entangling two-qubit gate, whence the name.

The main difference between the proposed and the original constructions is that we can effect the operation using a fixed entangling gate D, which is locally equivalent to a single CNOT. The trade-off is an additional diagonal gate R trailing the circuit, but in many applications it can be eliminated by merging it with an adjacent gate.

In matrix form, the implementation of the gate $F_2^1[\mathrm{U}(2)]$ is

$$\begin{pmatrix} a & \\ & b \end{pmatrix} = \underbrace{\begin{pmatrix} r^\dagger & \\ & r \end{pmatrix}}_{R} \underbrace{\begin{pmatrix} u & \\ & u \end{pmatrix}}_{I\otimes u} \underbrace{\begin{pmatrix} d & \\ & d^\dagger \end{pmatrix}}_{D} \underbrace{\begin{pmatrix} v & \\ & v \end{pmatrix}}_{I\otimes v}, \tag{3}$$

where a, b, u, and v are unitary and r and d are diagonal unitary 2×2 matrices. This yields the matrix equations

$$a = r^\dagger u d v, \tag{4}$$

$$b = r u d^\dagger v \tag{5}$$

or, equivalently,

$$X := ab^\dagger = r^\dagger u d^2 u^\dagger r^\dagger, \tag{6}$$

$$v = d u^\dagger r^\dagger b = d^\dagger u^\dagger r a. \tag{7}$$

Equation (6) may be recast into a form reminiscent of an eigenvalue decomposition:

$$rXr = u d^2 u^\dagger. \tag{8}$$

Note that X is fixed by the matrices a and b, but r can be chosen freely. By diagonalizing the matrix rXr, we find the similarity transformation u and the eigenvalue matrix d^2. The matrix v is obtained by inserting the results into Eq. (7).

Since $X \in \mathrm{U}(2)$, we may express it using the parametrization

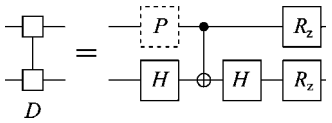

FIG. 3. Elementary gate sequence for the D gate, where H is the Hadamard gate and $R_z = R_z(\pi/2)$. Gate $P = e^{-i\pi/4}$ is an adjustment of the global phase and may be omitted.

$$X = \begin{pmatrix} x_1 & x_2 \\ -\overline{x_2} & \overline{x_1} \end{pmatrix} e^{i\phi/2}, \tag{9}$$

where $|x_1|^2 + |x_2|^2 = 1$ and $\det(X) = e^{i\phi}$. The characteristic polynomial of the matrix rXr is

$$\det(rXr - \lambda I) = \lambda^2 - \lambda(r_1^2 x_1 + r_2^2 \overline{x_1}) e^{i\phi/2} + r_1^2 r_2^2 e^{i\phi}. \tag{10}$$

The main result of this section is that for any X, we can find r such that the roots of the polynomial, and hence the eigenvalues of rXr, are two fixed antipodal points on the unit circle in the complex plane. This is accomplished by choosing

$$r_1 = e^{(i/2)[\delta - \phi/2 - \arg(x_1) + k\pi]}, \tag{11}$$

$$r_2 = e^{(i/2)[\delta - \phi/2 + \arg(x_1) + m\pi]}. \tag{12}$$

Above, k and m are arbitrary integers with $k+m$ odd and δ is the desired argument for one of the eigenvalues λ_i:

$$d^2 = \begin{pmatrix} e^{i\delta} & \\ & -e^{i\delta} \end{pmatrix}. \tag{13}$$

For convenience, let us choose $\delta = \pi/2$. Hence the diagonal gate D obtains the fixed form $D = e^{i(\pi/4)\sigma_z \otimes \sigma_z}$. It can be realized straightforwardly using an Ising-type Hamiltonian or, alternatively, it can be decomposed into a CNOT and one-qubit gates as shown in Fig. 3. The resulting diagonal gate R assumes the form of a uniformly controlled z rotation in the most significant bit, $F_1^1[R_z]$. The entire circuit is shown in Fig. 4.

Now we turn our attention to the decomposition of an arbitrary $F_t^k[\mathrm{U}(2)]$ gate, where $k > 1$. First we pick one of the control qubits, m. This qubit pairs the two-dimensional invariant subspaces of the gate in a unique fashion. Hence the method of Eq. (3) may be used 2^{k-1} times in parallel, which effectively eliminates the uniform control node on the chosen qubit m. The operation may be performed using a single D_t^m gate and a compensating diagonal gate which again assumes the form of a uniformly controlled z rotation $F_m^k[R_z]$:

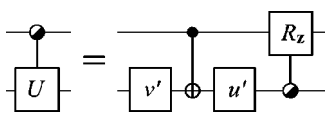

FIG. 4. Constant quantum multiplexor for two qubits. Here the SU(2) gates u' and v' include some of the local gates which transform the CNOT into a D gate. For the implementation of the gate $F_1^1[R_z]$, see Fig. 10(a).

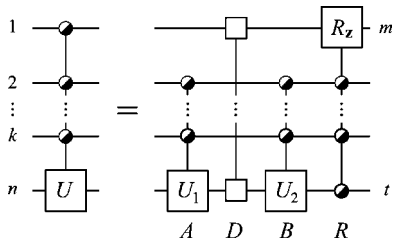

FIG. 5. Constant multiplexor step for a k-fold uniformly controlled U(2) gate, eliminating the uniform control node on the qubit m.

$$F_t^k[\mathrm{U}(2)] = F_m^k[R_z] F_t^{k-1}[\mathrm{U}(2)] D_t^m F_t^{k-1}[\mathrm{U}(2)]. \tag{14}$$

This elimination step is presented in Fig. 5.

The elimination of uniform control nodes can be continued recursively until only one-qubit gates, CNOT's and uniformly controlled R_z gates remain. The recursive decomposition f proceeds as follows:

Function $f(F_t^k[\mathrm{U}(2)])$:

(i) If $k=0$, return.

(ii) Choose one of the control qubits m. Perform the elimination step of Fig. 5 which results in the gates A, D, B, and R.

(iii) Replace the $F_t^{k-1}[\mathrm{U}(2)]$ gate A with $f(A)$.

(iv) (optional) Transform the D gate into a CNOT as shown in Fig. 3; merge the resulting one-qubit gates to surrounding gates.

(v) Replace the $F_t^{k-1}[\mathrm{U}(2)]$ gate B with $f(B)$.

(vi) If there is a D gate from another level of the recursion following the $F_m^k[R_z]$ gate R, commute R through it towards the right and merge R with the next $F_t^k[\mathrm{U}(2)]$ gate. Note that diagonal gates always commute.

(vii) Return.

The simplification rules of Fig. 6 are used throughout the decomposition. Because of step (vi), only the rightmost of the $F_j^{k-i}[R_z]$ gates actually needs to be implemented on each level of the recursion. The resulting quantum circuit consists of two parts: an alternating sequence of 2^k one-qubit gates and $2^k - 1$ CNOT gates, which we denote by $\tilde{F}_t^k[\mathrm{U}(2)]$, and a cascade of k distinct uniformly controlled z rotations, which corresponds to a single diagonal $(k+1)$-qubit gate Δ_{k+1}. Figure 7(a) presents this decomposition for the gate $F_4^3[\mathrm{U}(2)]$.

IV. EXAMPLES

This section illustrates how the uniformly controlled one-qubit gates can be applied to efficiently solve two problems:

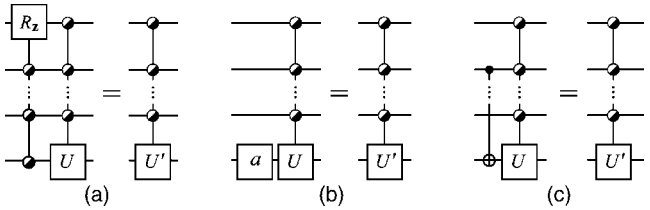

FIG. 6. Some simplification rules for uniformly controlled U(2) gates.

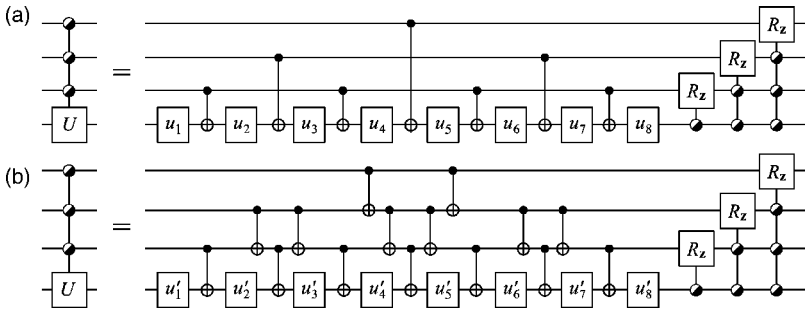

FIG. 7. Implementation of the gate $F_4^3[\mathrm{U}(2)]$ using (a) general CNOT's, (b) only nearest-neighbor CNOT's. The gates $\{u_i\}$ and $\{u_i'\}$ belong to SU(2). The alternating sequence of CNOT's and SU(2) gates is denoted by $\tilde{F}_4^3[\mathrm{U}(2)]$. The rightmost sequence of uniformly controlled z rotations corresponds to a single diagonal gate, denoted by Δ_4. For the nearest-neighbor implementation of uniformly controlled rotations, see Fig. 11.

the decomposition of a general n-qubit gate and the preparation of an arbitrary quantum state.

A. Cosine-sine decomposition

Recently, we introduced a method [9] for decomposing a given general n-qubit gate U into a sequence of elementary gates using the cosine-sine decomposition. In this approach, the CSD is applied recursively. Each recursion step decomposes a k-fold uniformly controlled s-qubit gate, where $k+s=n$, into two $(k+1)$-fold uniformly controlled $(s-1)$-qubit gates and a single $(n-1)$-fold uniformly controlled y rotation:

$$F_{\mathcal{T}}^{k}[\mathrm{U}(2^s)] = F_{\mathcal{T}\setminus\{m\}}^{k+1}[\mathrm{U}(2^{s-1})]F_m^{n-1}[R_y]F_{\mathcal{T}\setminus\{m\}}^{k+1}[\mathrm{U}(2^{s-1})]. \tag{15}$$

Above, $\mathcal{T}$ is the set of s target qubits for the $\mathrm{U}(2^s)$ gates and m is the operational qubit for the step. Note that, in this notation, a $\mathrm{U}(2^n)$ gate may be denoted as $F_{\mathcal{N}}^0[\mathrm{U}(2^n)]$, where $\mathcal{N}$ is the set of all the n qubits. When applied to an arbitrary n-qubit gate, the recursion of Eq. (15) finally yields the decomposition

$$\mathrm{U}(2^n) = F_n^{n-1}[\mathrm{U}(2)]\prod_{i=1}^{2^{n-1}-1} F_{n-\gamma(i)}^{n-1}[R_y]F_n^{n-1}[\mathrm{U}(2)], \tag{16}$$

where γ is the so-called ruler function, given by Sloane's sequence A001511 [23]. The order of the noncommuting operators in the product is always taken to be from left to right. Note that the $F_{n-\gamma(i)}^{n-1}[R_y]$ gates may as well be considered as general $F_{n-\gamma(i)}^{n-1}[\mathrm{U}(2)]$ gates.

We continue by decomposing the uniformly controlled gates into one-qubit gates and CNOT's. Starting from the last gate in Eq. (16), we write the diagonal part Δ_n separately:

$$F_n^{n-1}[\mathrm{U}(2)] = \Delta_n\tilde{F}_n^{n-1}[\mathrm{U}(2)]. \tag{17}$$

The diagonal part Δ_n can then be merged with the neighboring $F_{n-1}^{n-1}[R_y]$ gate, which is transformed into a general gate of type $F_{n-1}^{n-1}[\mathrm{U}(2)]$. Again, the diagonal part can be separated and merged into the next gate $F_n^{n-1}[\mathrm{U}(2)]$. Continuing this process sequentially, we finally obtain

$$\mathrm{U}(2^n) = \Delta_n\tilde{F}_n^{n-1}[\mathrm{U}(2)]\prod_{i=1}^{2^{n-1}-1}\tilde{F}_{n-\gamma(i)}^{n-1}[\mathrm{U}(2)]\tilde{F}_n^{n-1}[\mathrm{U}(2)]. \tag{18}$$

This decomposition involves 2^n-1 gates of type $\tilde{F}_t^{n-1}[\mathrm{U}(2)]$, each of which takes $2^{n-1}-1$ CNOT's and 2^{n-1} one-qubit rotations to implement. The final diagonal gate Δ_n is implemented using the same construction as in Ref. [9]. After eliminating one CNOT and n one-qubit gates, we obtain a circuit of $\frac{1}{2}4^n-\frac{1}{2}2^n-2$ CNOT's and $\frac{1}{2}4^n+\frac{1}{2}2^n-n-1$ one-qubit gates.

Table I presents a comparison between the improved CSD and the most efficient previously known decomposition, the NQ decomposition [10]. The number of CNOT's in the NQ decomposition is from Ref. [10]. None of the other results have been published previously.

B. State preparation

We have recently addressed [12] the problem of preparing an arbitrary n-qubit quantum state $|b\rangle_n$ starting from an arbitrary state $|a\rangle_n$. This transformation could be used, e.g., to produce complex entangled multiqubit states for studying or to prepare the required initial state for a quantum algorithm starting from the natural initial state of the quantum computer.

The state preparation circuit first transforms the state $|a\rangle_n$ into $|e_1\rangle_n$ and, then, using the same strategy, backwards from $|e_1\rangle_n$ to $|b\rangle_n$. The $|a\rangle_n$ to $|e_1\rangle_n$ transformation consists of a sequence of gate pairs

$$S_a = \prod_{i=1}^{n}\{(F_i^{i-1}[R_y]F_i^{i-1}[R_z])\otimes I_{2^{n-i}}\}. \tag{19}$$

The effect of the gate pair $F_i^{i-1}[R_y]F_i^{i-1}[R_z]$ on the state $|a\rangle_i$ is to nullify half of its elements:

TABLE I. Comparison of the upper bounds for the gate counts required to implement a general n-qubit gate using the n-qubit (NQ) decomposition [10] and the improved CSD. The fixed U(4) gates may be taken to be CNOT's.

Gate type	NQ	iCSD
Fixed U(4)	$\frac{1}{2}4^n-\frac{3}{2}2^n+1$	$\frac{1}{2}4^n-\frac{1}{2}2^n-2$
R_y, R_z	$\frac{9}{8}4^n-\frac{3}{2}2^n+3$	4^n-1
or SU(2)	$\frac{17}{24}4^n-\frac{3}{2}2^n-\frac{1}{3}$	$\frac{1}{2}4^n+\frac{1}{2}2^n-n-1$

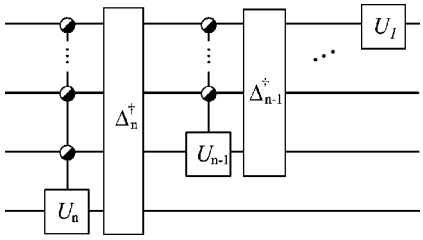

FIG. 8. Quantum circuit for transforming an arbitrary n-qubit state $|a\rangle_n$ into the standard basis state $|e_1\rangle_n$. The diagonal gates $\Delta_i^\dagger$ exactly cancel the Δ_i part of the adjacent $F_i^{i-1}[\mathrm{U}(2)]$ gate. The resulting gates are of the form $\tilde{F}_i^{i-1}[\mathrm{U}(2)]$ which is efficient to implement.

$$F_i^{i-1}[R_y]F_i^{i-1}[R_z]|a\rangle_i = |a'\rangle_{i-1} \otimes |0\rangle_1. \tag{20}$$

Hence, each successive gate pair nullifies half of the elements of the state vector that have not yet been nullified, and we have $S_a|a\rangle_n = |e_1\rangle_n$ up to a global phase.

Now we note that the pair of gates $F_n^{n-1}[R_y]F_n^{n-1}[R_z] = F_n^{n-1}[\mathrm{U}(2)]$ may be replaced by the gate

$$\tilde{F}_n^{n-1}[\mathrm{U}(2)] = \Delta_n^\dagger F_n^{n-1}[\mathrm{U}(2)], \tag{21}$$

since the diagonal gate

$$\Delta_n^\dagger = \Delta_{n-1}^{0\dagger} \otimes |0\rangle\langle 0| + \Delta_{n-1}^{1\dagger} \otimes |1\rangle\langle 1| \tag{22}$$

does not mix the states:

$$\begin{aligned}\Delta_n^\dagger F_n^{n-1}[\mathrm{U}(2)]|a\rangle_n &= \Delta_n^\dagger(|a'\rangle_{n-1} \otimes |0\rangle_1) = (\Delta_{n-1}^{0\dagger}|a'\rangle_{n-1}) \otimes |0\rangle_1 \\ &= |a''\rangle_{n-1} \otimes |0\rangle_1.\end{aligned} \tag{23}$$

After combining $n-1$ pairs of adjacent $F_{k+1}^k[R_y]F_{k+1}^k[R_z]$ gates where $k=1,\ldots,n-1$ we find that the entire circuit for transforming $|a\rangle$ to $|b\rangle$ requires $2\times 2^n - 2n - 2$ CNOT's and $2\times 2^n - n - 2$ one-qubit gates. If $|a\rangle$ or $|b\rangle$ coincides with one of the basis vectors $|e_i\rangle$, the gate counts are halved in the leading order. The method presented here yields a factor-of-2 improvement in the gate counts compared to the previous results [12,10]. The circuit for this transformation is illustrated in Fig. 8.

V. LINEAR CHAIN OF QUBITS WITH NEAREST-NEIGHBOR COUPLINGS

In many of the proposed physical implementations of quantum computers, such as charge-coupled quantum dots [24] and NMR-based systems [25], the qubits are spatially situated in such a way that only nearest-neighbor interactions are feasible. This does not imply that long-range gates are impossible to construct, but it renders such operations rather hard to implement. In this section we consider a quantum register consisting of a chain of qubits with only nearest-neighbor interactions and show that the construction presented for $\tilde{F}_t^k[\mathrm{U}(2)]$ can be translated into an efficient nearest-neighbor CNOT implementation. The technique is based on the circuit identity shown in Fig. 9.

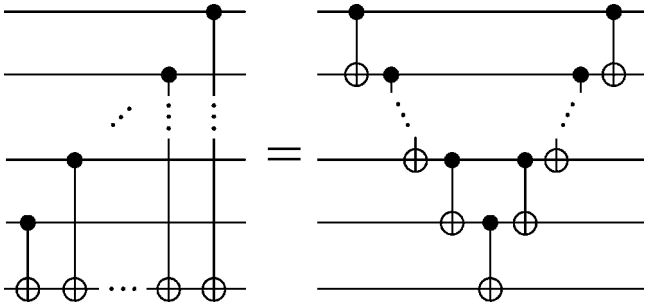

FIG. 9. CNOT cascade which can be efficiently implemented using nearest-neighbor CNOT's [26].

A. Uniformly controlled one-qubit gates

To get the recursion rule for the nearest-neighbor implementation of a uniformly controlled one-qubit gate, we simply modify the function f of Sec. III by making step (iv) obligatory and adding a new step after it:

(iv a) Insert an identity in the form of a CNOT cascade and its inverse, a similar cascade, into the circuit next to the CNOT gate C_t^m. The cascades consist of the gates C_t^i, where i runs over the qubits connecting the qubits m and t. Absorb one of the cascades into the $F_t^j[\mathrm{U}(2)]$ gate B and replace the other, together with the original CNOT, using nearest-neighbor CNOT's as illustrated in Fig. 9.

The complexity of the nearest-neighbor implementation depends on the relative order of the target and control qubits, and the order in which the uniform control nodes are eliminated. Since the number of nearest-neighbor CNOT's required increases linearly with the distance between the control and target qubits of the entangling CNOT, we first eliminate the nodes that are farthest apart from the target qubit. Let us assume that a $\tilde{F}_t^{n-1}[\mathrm{U}(2)]$ gate acts on a chain of n consequent qubits. If $n \geqslant 5$, it is advantageous to use a sequence of swap gates to move the target qubit next to the center of the chain before the operation and back after it. A swap gate can be realized using three consecutive CNOT's. Taking this into account, a $\tilde{F}_t^{n-1}[\mathrm{U}(2)]$ gate can be implemented using at most

$$C_{U(2)}(n,s) = \frac{5}{6}2^n + 2n - 6s - \begin{cases} \frac{1}{3}, & n \text{ even}, \\ \frac{5}{3}, & n \text{ odd}, \end{cases} \tag{24}$$

nearest-neighbor CNOT's, where $s=1,\ldots,\lceil n/2\rceil$ is the distance of the target qubit t from the end of the chain. Figure 7(b) depicts the resulting circuit for the case $n=4$ and $s=1$.

Now consider a k-fold uniformly controlled rotation gate $F_t^k[R_\mathbf{a}]$, where the rotation axis $\mathbf{a}$ is perpendicular to the x axis. It can be decomposed using the recursion step presented in Fig. 10(b). To minimize the CNOT count, we mirror at each recursion step the circuit of the latter uniformly controlled gate, which results in the cancellation of two nearest-neighbor CNOT cascades. For the same reason as in the previous paragraph, the recursion step is first applied to the control qubits furthest apart from the target. The implementation for the gate $F_t^{n-1}[R_\mathbf{a}]$ requires at most

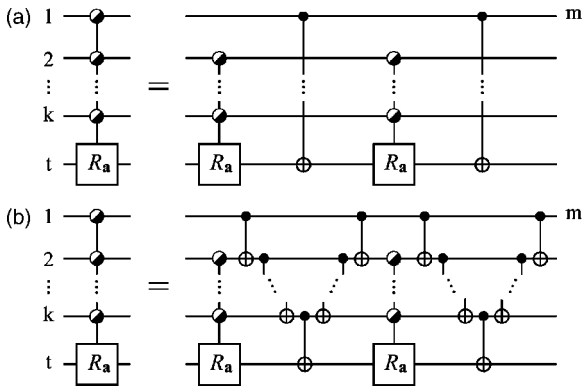

FIG. 10. Recursion step for decomposing a uniformly controlled rotation using (a) CNOT's and (b) nearest-neighbor CNOT's, applied to the qubit m. Note that the circuit diagrams may also be mirrored horizontally.

$$C_R(n,s) = \frac{5}{6}2^n + 3n - 6s - \begin{cases} \frac{4}{3}, & n \text{ even}, \\ \frac{5}{3}, & n \text{ odd}, \end{cases} \tag{25}$$

nearest-neighbor CNOT's. Figure 11 displays an example circuit for the case $n=5$ and $s=2$.

B. Cosine-sine decomposition

The decomposition of an arbitrary n-qubit gate is achieved exactly as in Sec. IV A, but now the order in which the CSD steps of Eq. (15) are applied to the qubits affects the final gate count. As seen in Eq. (24), it is favorable to have the target qubit of a uniformly controlled one-qubit gate as close to the center of the chain as possible. Consequently, we start the decomposition from the ends of the qubit chain, moving alternatingly towards the center. In this fashion, a general n-qubit gate can be implemented using at most

$$C_U(n) = \frac{5}{6}4^n - n2^n - 2n + \begin{cases} \frac{5}{6}2^n - \frac{5}{3}, & n \text{ even}, \\ \frac{1}{2}2^n - \frac{1}{3}, & n \text{ odd}, \end{cases} \tag{26}$$

nearest-neighbor CNOT's.

C. State preparation

With the help of the results derived above, the implementation of the general state preparation circuit using nearest-neighbor gates is straightforward. We follow the reasoning of Sec. IV B and simply replace the $\tilde{F}_i^{i-1}[\mathrm{U}(2)]$ gates with their nearest-neighbor counterparts, using the decomposition derived in the beginning of this section. We find that the implementation of the state preparation circuit requires at most

$$C_{\mathrm{SP}}(n) = \frac{10}{3}2^n + 2n^2 - 12n + \begin{cases} \frac{14}{3}, & n \text{ even}, \\ \frac{10}{3}, & n \text{ odd}, \end{cases} \tag{27}$$

nearest-neighbor CNOT's.

VI. DISCUSSION

In this paper we have studied the properties and the utilization of uniformly controlled one-qubit gates. We have derived a recursive circuit topology which implements an arbitrary k-fold uniformly controlled one-qubit gate using at most 2^k one-qubit gates, 2^k-1 CNOT's and a single diagonal $(k+1)$-qubit gate. This construction is especially efficient if the gate is to implemented only up to a diagonal—e.g., when the phase factors of each basis vector can be freely chosen. We have also shown that this kind of freedom appears in the implementation of an arbitrary n-qubit quantum gate and in the rotation of an arbitrary state vector into another. The leading-order complexity of the circuit for an arbitrary n-qubit gate is $\frac{1}{2}4^n$ CNOT's and an equal number of one-qubit gates, which are the lowest gate counts reported.

The techniques presented above are also amenable to experimental realizations of a quantum computer in which the quantum register consists of a one-dimensional chain of qubits with only nearest-neighbor interactions. For example, the number of the nearest-neighbor CNOT's in the presented decomposition of an n-qubit gate is in the leading order $\frac{5}{6}4^n$, which is appreciably below the lowest previously reported value of $\frac{9}{2}4^n$ [10]. Furthermore, the structure of the nearest-neighbor circuit allows several gate operations to be executed in parallel, which may further reduce the execution time of the algorithm.

In Ref. [9], it was speculated that the gate count of the quantum CSD could be reduced by combining adjacent uniformly controlled rotations into single uniformly controlled one-qubit gates, which was realized in this paper. To further reduce the number of CNOT's in the circuit, also the control nodes of the CNOT's should be used to separate the one-qubit gates carrying the degrees of freedom. However, uniformly controlled one-qubit gates cannot be used as the sole basic building blocks of the circuit in this kind of a construction.

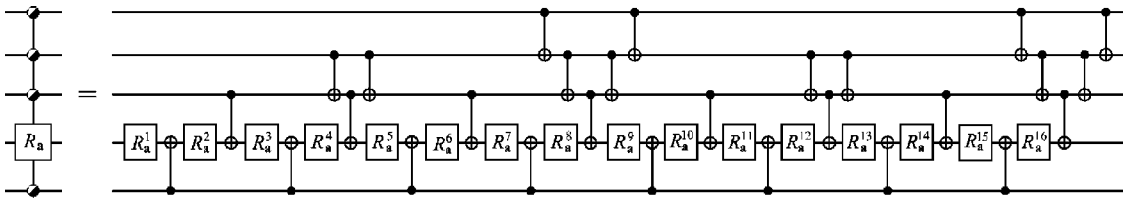

FIG. 11. Implementation of a uniformly controlled **a** rotation using nearest-neighbor CNOT's.

Finally, the authors conjecture that the constant quantum multiplexor circuit, presented for 2×2 gates in Eqs. (3)–(14), could be extended to handle general $2^n\times 2^n$ gates as well. If this proves to be the case, a straightforward generalization of the techniques presented in this paper would lead to a further reduction of the CNOT's needed for the synthesis of a general multiqubit gate.

ACKNOWLEDGMENTS

This research is supported by the Academy of Finland (Project No. 206457, "Quantum Computing"). V.B. and M.M. thank the Finnish Cultural Foundation, J.J.V. and M.M. the Jenny and Antti Wihuri Foundation, and J.J.V. the Nokia Foundation for financial support.

[1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England, 2000).
[2] P. W. Shor, in *IEEE Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, edited by S. Goldwasser (IEEE, New York, 1994), pp. 124–134.
[3] A. Galindo and M. A. Martin-Delgado, Rev. Mod. Phys. **74**, 347 (2002).
[4] S. Lloyd, Phys. Rev. Lett. **75**, 346 (1995).
[5] J.-L. Brylinski and R. Brylinski, in *Mathematics of Quantum Computation*, edited by R. Brylinski and G. Chen (Chapman and Hall/CRC, London, 2002).
[6] D. Deutsch, Proc. R. Soc. London, Ser. A **425**, 73 (1989).
[7] 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).
[8] J. J. Vartiainen, M. Möttönen, and M. M. Salomaa, Phys. Rev. Lett. **92**, 177902 (2004).
[9] M. Möttönen, J. J. Vartiainen, V. Bergholm, and M. M. Salomaa, Phys. Rev. Lett. **93**, 130502 (2004).
[10] V. V. Shende, S. S. Bullock, and I. L. Markov, e-print quant-ph/0406176.
[11] R. R. Tucci, e-print quant-ph/9902062, V. 2.
[12] M. Möttönen, J. J. Vartiainen, V. Bergholm, and M. M. Salomaa, Quantum Inf. Comput.(to be published).
[13] V. V. Shende and I. L. Markov, e-print quant-ph/0401162.
[14] G. Vidal, Phys. Rev. A **62**, 062315 (2000).
[15] S. S. Bullock and I. L. Markov, Quantum Inf. Comput. **4**, 27 (2004).
[16] N. Schuch and J. Siewert, Phys. Rev. Lett. **91**, 027902 (2003).
[17] T. Hogg, C. Mochon, W. Polak, and E. Rieffel, Int. J. Mod. Phys. C **10**, 1347 (1999).
[18] V. V. Shende, I. L. Markov, and S. S. Bullock, Phys. Rev. A **69**, 062321 (2004).
[19] J. Zhang, J. Vala, S. Sastry, and K. B. Whaley, Phys. Rev. Lett. **91**, 027903 (2003).
[20] F. Vatan and C. P. Williams, Phys. Rev. A **69**, 032315 (2004).
[21] G. Vidal and C. M. Dawson, Phys. Rev. A **69**, 010301(R) (2004).
[22] W. H. Zurek, Rev. Mod. Phys. **75**, 715 (2003).
[23] R. K. Guy, in *Unsolved Problems in Number Theory*, 2nd ed. (Springer-Verlag, New York, 1994), p. 224.
[24] J. H. Jefferson, M. Fearn, D. L. J. Tipton, and T. P. Spiller, Phys. Rev. A **66**, 042328 (2002).
[25] L. M. K. Vandersypen and I. L. Chuang, Rev. Mod. Phys. **76**, 1037 (2004).
[26] R. R. Tucci, e-print quant-ph/0407215.