Transformation of quantum states using uniformly controlled rotations

Mikko Möttönen,* Juha J. Vartiainen, Ville Bergholm, and Martti M. Salomaa
Materials Physics Laboratory, P.O. Box 2200,
FIN-02015 Helsinki University of Technology, Finland

We consider a unitary transformation which maps any given state of an n-qubit quantum register into another one. This transformation has applications in the initialization of a quantum computer, and also in some quantum algorithms. Employing uniformly controlled rotations, we present a quantum circuit of $2^{n+2} - 4n - 4$ CNOT gates and $2^{n+2} - 5$ one-qubit elementary rotations that effects the state transformation. The complexity of the circuit is noticeably lower than the previously published results. Moreover, we present an analytic expression for the rotation angles needed for the transformation.

I. INTRODUCTION

Quantum algorithms are based on unitary transformations and projective measurements acting on a quantum register of n qubits [1]. Successful execution of an algorithm usually requires a certain initial state as input. However, depending on the physical realization of the quantum computer, available initialization procedures may only produce a limited range of states which may not contain the desired initial state. This brings up the problem of state preparation, i.e., how to implement the transformation of an arbitrary quantum state into another one.

The recent progress [2, 3, 4] in implementing general n-qubit gates using elementary gates has resulted in efficient gate synthesis techniques including uniformly controlled rotations [3], and more recently, quantum multiplexors [4]. These techniques are amenable also for implementing quantum gates of certain special classes of unitary transformations, such as incompletely specified transformations. These transformations have been reacently discussed in Ref. [5], in which an efficient gate decomposition was given in the case of two qubits.

The complexity of a quantum circuit is measured by the number of elementary gates included. Generally, elementary gates are unitary transformations acting on one or two qubits. We take the library of elementary gates to be the conventional set of the controlled NOT (CNOT) gate and all one-parameter rotations acting on a single qubit. We omit the phase gate since the global phase of the state vector has no physical meaning.

The configuration space of the n-qubit quantum register is 2^n-dimensional complex space. Excluding the global phase and state normalization, we find that the general unitary transformation transforming a given n-qubit state into another must have at least $2 \times 2^n - 2$ real degrees of freedom. Hence, in the worst-case scenario, the corresponding quantum circuit should involve at least $2^{n+1} - 2$ elementary rotations, each carrying one degree of freedom. Since each of the CNOT gates can bind at most four elementary rotations [6], at least $\lceil \frac{1}{4}(2^{n+1} - 3n - 2) \rceil$ of them are needed. However, no quantum circuit construction embodying the minimal complexity has been presented in the literature. Previously, the upper bound for the number of gates needed for state preparation has been considered by Knill [7], who found that no more than $O(n2^n)$ gates are needed for the circuit implementing the transformation. More recently, a sufficient circuit of $O(2^n)$ elementary gates was obtained as a special case of the method developed for QR decomposition of a general quantum gate in Ref. [2], which was also pointed out in Ref. [5].

In this paper, we describe in detail how to build a quantum circuit for making a given quantum state transformation employing the uniformly controlled rotations. We begin from the transformation which equalizes the phases of the elements of the input vector $|a\rangle$ and rotates it to the direction of the basis vector $|e_1\rangle$. In the next phase the absolute values of elements of the target vector $|b\rangle$ are generated and finally the phases are adjusted to match of those of $|b\rangle$. We simplify the circuit by merging certain consecutive gates together. The resulting quantum circuit of $2^{n+2} - 4n - 4$ CNOT gates and $2^{n+2} - 5$ one-qubit elementary rotations gives, in principle, the exact transformation from an n-qubit quantum state $|a\rangle$ into the desired one $|b\rangle$.
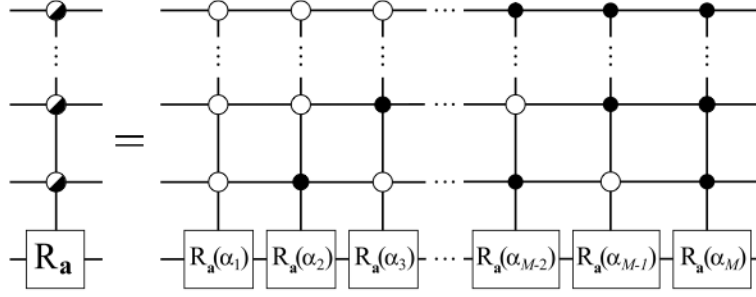
---

*Electronic address: mpmotton@focus.hut.fi

FIG. 1: Definition of the k-fold uniformly controlled rotation $F_m^k(\mathbf{a}, \boldsymbol{\alpha})$ of qubit m about the axis $\mathbf{a}$. The left hand side defines the gate symbol used for the uniformly controlled rotation. The enumeration of the qubits is arbitrary with the exception that the target qubit is the mth one. The black control bits stand for value 1 and the white for 0. Above, $M = 2^k$.
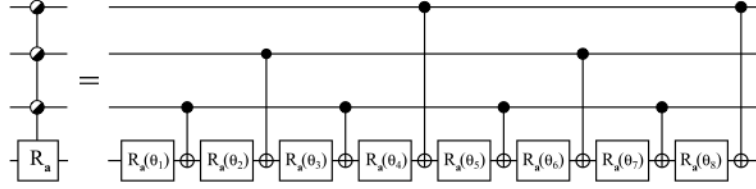

FIG. 2: Efficient gate decomposition for the uniformly controlled rotation $F_4^3(\mathbf{a}, \boldsymbol{\alpha})$. The relation of the angles $\{\theta_j\}$ to the angles $\{\alpha_j\}$ is shown in Eq. (3).

II. UNIFORMLY CONTROLLED ROTATIONS

The quantum state of an n-qubit register may be described by a complex vector of the form

$$|a\rangle = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_N \end{pmatrix} = \sum_{i=0}^{N-1} a_{i+1} \left| b_1^i b_2^i \dots b_N^i \right\rangle, \tag{1}$$

where $N = 2^n$, b_j denotes the state of the jth qubit, and the bit string $b_1^i b_2^i \dots b_N^i$ is the binary presentation of the integer i. The state is taken to be normalized to unity. Furthermore, the overall phase of the state is not observable and thus irrelevant. This means that an n-qubit state has $2^{n+1} - 2$ real degrees of freedom. Quantum gates are linear transformations on the space of these vectors and, hence, may be represented by $N \times N$ unitary matrices.

A uniformly controlled rotation $F_m^k(\mathbf{a}, \boldsymbol{\alpha})$ is a quantum gate defined by the k controlled qubits, the target qubit m, the rotation axis $\mathbf{a}$ and the angles $\{\alpha_i\}$, see Ref. [3]. As shown in Fig. 1, the uniformly controlled rotation corresponds to a sequence of controlled $R_{\mathbf{a}}(\alpha_i)$ rotations, which covers all the 2^k possible control bit sequences. Here

$$R_{\mathbf{a}}(\alpha_i) = e^{i\mathbf{a}\cdot\boldsymbol{\sigma}\alpha_i/2} = I_{2\times 2}\cos\frac{\alpha_i}{2} + i\,(\mathbf{a}\cdot\boldsymbol{\sigma})\sin\frac{\alpha_i}{2}, \tag{2}$$

where σ_x, σ_y, and σ_z are the Pauli matrices and the dot product $\mathbf{a}\cdot\boldsymbol{\sigma} = \sigma_x a_x + \sigma_y a_y + \sigma_z a_z$.

Figure 2 reviews a construction for $F_m^k(\mathbf{a}, \boldsymbol{\alpha})$ consisting of 2^k CNOT gates and 2^k one-qubit $\mathbf{a}$-rotations. The case $k = 3$ is shown. In the case of a general k, the gate sequence may be constructed from the sequence for $k - 1$ by replacing the position of the control in the rightmost CNOT gate to the new controlled qubit and repeating the obtained sequence twice for suitable rotation angles $\{\theta_j\}$. The operational principle of the gate sequence requires that $a_x = 0$. However, this limitation can be circumvented by introducing one-qubit basis changing gates on the both side of the gate.

The angles $\{\theta_i\}$ can be obtained from $\{\alpha_i\}$ using the equation

$$\begin{pmatrix} \theta_1 \\ \vdots \\ \theta_{2^k} \end{pmatrix} = M \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_{2^k} \end{pmatrix}, \qquad M_{ij} = 2^{-k}(-1)^{b_{j-1}\cdot g_{i-1}}, \tag{3}$$

where b_m and g_m stand for the binary code and binary reflected Gray code representations of the integer m, respectively. In actuality, the position of the controls of the CNOT gates in Fig. 2 may be chosen in many different ways which results in replacing g_{j-1} in Eq. (3) by another cyclic Gray code [8]. Additionally, a horizontally mirrored version of the gate sequence in Fig. 2 also qualifies to simulate the uniformly controlled rotation.

III. STATE PREPARATION

We are looking for a gate sequence corresponding to a matrix U such that $U|a\rangle = |b\rangle$ for given vectors $|a\rangle$ and $|b\rangle$. The problem may be reduced to the problem of finding a matrix V which takes an arbitrary vector to some fixed vector $|r\rangle$, since then we may take A and B such that $A|a\rangle = |r\rangle = B|b\rangle$ and, hence, $B^\dagger A|a\rangle = |b\rangle$, where the dagger denotes the Hermitian conjugate. For convenience, we take the fixed vector to be the first basis vector $|e_1\rangle = |00\ldots0\rangle = (1,0,0,\ldots,0)^T$.

Our algorithm for transforming $|a\rangle = (|a_1|e^{i\omega_1}, |a_2|e^{i\omega_2}, \ldots, |a_N|e^{i\omega_N})^T$ into $|e_1\rangle$ works as follows:

- First we equalize the phases ω_i using a cascade of uniformly controlled z-rotations Ξ_z, rendering the vector real up to the global phase ϕ: $\Xi_z|a\rangle = e^{i\phi}|\hat{a}\rangle$.

- Then we rotate the real state vector $|\hat{a}\rangle$ into the direction of $|e_1\rangle$ using a similar sequence of uniformly controlled y-rotations Ξ_y, thus achieving our goal.

The first step can be readily accomplished using a general diagonal n-qubit quantum gate first considered in Ref. [9]. It is efficiently produced by a sequence of uniformly controlled z-rotations as

$$\Xi_z = \prod_{j=1}^{n} F_j^{j-1}(\mathbf{z}, \boldsymbol{\alpha}_{n-j+1}^z) \otimes I_{2^{n-j}}, \tag{4}$$

where the gate $F_j^{j-1}(\mathbf{z}, \boldsymbol{\alpha}_{n-j+1}^z)$ equalizes the phases of the elements connected through the qubit j. The rotation angles $\{\alpha_{j,k}^z\}_j$, the elements of $\boldsymbol{\alpha}_k^z$, are found to be

$$\alpha_{j,k}^z = \sum_{l=1}^{2^{k-1}} (\omega_{(2j-1)2^{k-1}+l} - \omega_{(2j-2)2^{k-1}+l})/2^{k-1}, \tag{5}$$

where $j = 1, 2, \ldots, 2^{n-k}$ and $k = 1, 2, \ldots, n$.

Next we apply a uniformly controlled y-rotation $F_n^{n-1}(\mathbf{y}, \boldsymbol{\alpha}^y)$ with angles $\{\alpha_j^y\} = \{2\operatorname{asin}\left(|a_{2j}|/\sqrt{|a_{2j-1}|^2 + |a_{2j}|^2}\right)\}$. This has the effect of zeroing the elements of the vector that correspond to the states standing for bit value one in the qubit n:

$$F_n^{n-1}(\mathbf{y}, \boldsymbol{\alpha}^y)|\hat{a}\rangle = (a_{1,2}, 0, a_{2,2}, 0, \ldots, a_{N/2,2}, 0)^T = (a_{1,2}, a_{2,2}, \ldots, a_{N/2,2})^T \otimes (1, 0)^T \tag{6}$$

where $\{a_{j,2}\} = \{\sqrt{|a_{2j-1}|^2 + |a_{2j}|^2}\}$. In effect we have zeroed the last qubit of the register. This procedure can be repeated on the remaining nonzero elements, until we reach $|e_1\rangle = (1, 0)^T \otimes \ldots \otimes (1, 0)^T$.

Employing the above steps one obtains the desired decomposition

$$\Xi_y \Xi_z |a\rangle = \left(\prod_{j=1}^{n} F_j^{j-1}(\mathbf{y}, \boldsymbol{\alpha}_{n-j+1}^y) \otimes I_{2^{n-j}}\right)\left(\prod_{j=1}^{n} F_j^{j-1}(\mathbf{z}, \boldsymbol{\alpha}_{n-j+1}^z) \otimes I_{2^{n-j}}\right)|a\rangle = e^{i\sum_{j=1}^{N}\omega_j/N}|e_1\rangle. \tag{7}$$

The product of non-commuting matrices in Eq. (7) is to be taken from left to right. Here, to eliminate the remaining global phase one could apply a phase gate. After solving the recursion, the rotation angles in Eq. (7) are found to acquire the values

$$\alpha_{j,k}^y = 2\operatorname{asin}\left(\sqrt{\sum_{l=1}^{2^{k-1}}|a_{(2j-1)2^{k-1}+l}|^2} \Big/ \sqrt{\sum_{l=1}^{2^k}|a_{(j-1)2^k+l}|^2}\right), \tag{8}$$

where $j = 1, 2, \ldots, 2^{n-k}$ and $k = 1, 2, \ldots, n$. Fig. 3 shows the quantum circuit corresponding to Eq. (7). The resulting gate sequence is slightly simplified by noting that uniformly controlled z-rotations, being diagonal, can
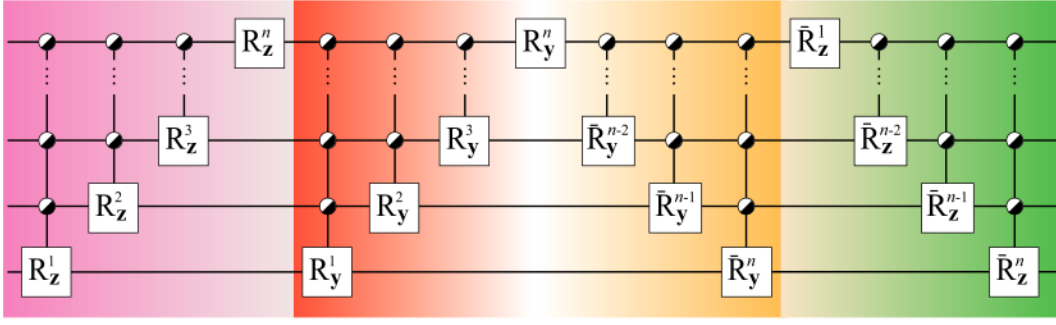
FIG. 3: Gate sequence for state preparation using uniformly controlled rotations. The rotation angles $\{\alpha_{j,k}^q\}$ for the uniformly controlled rotations are given in Eqs. (8) and (5).

always be commuted through the control bits of another uniformly controlled gate. Hence, uniformly controlled z and y rotations acting on the same set of qubits can be commuted next to each other, whereby we can cancel one CNOT from each gate by mirroring the y gate.

To transform the state $|a\rangle$ to $|b\rangle$ we need to construct two circuits; the first one takes $|a\rangle$ to $|e_1\rangle$ and the second one $|e_1\rangle$ to $|b\rangle$. Since the uniformly k-fold controlled rotation may be constructed from 2^k CNOT gates and 2^k one-qubit rotations, the entire state preparation circuit requires $2^{n+2} - 4n - 4$ CNOT gates and $2^{n+2} - 5$ one-qubit rotations.

IV. CONCLUSION

In conclusions, we have shown how to construct a general state preparation circuit using a sequence of uniformly controlled rotations. The resulting gate sequence of $2^{n+2} - 4n - 4$ CNOT gates and $2^{n+2} - 5$ one-qubit elementary rotations establishes a new upper bound for the complexity of the transformation. By counting the degrees of freedom of the problem, we find a lower bound of $2^{n+1} - 2$ for the number of one-qubit elementary rotations. This implies the lower bound $\lceil \frac{1}{4}(2^{n+1} - 3n - 2) \rceil$ for the number of CNOT gates.

Provided that the initial or final state coincides with some basis vector $|e_i\rangle$ only half of the CNOT and one-qubit rotation gates are needed. In other special cases some simplifications to the gate sequence also occur. We have also introduced a closed-form scheme for determining the rotation angles in such way that an arbitrary state of the quantum register transforms into desired state.

The gate count is small compared to the incomplete QR decomposition which takes approximately 6.3×2^n CNOT gates to transform $|a\rangle \rightarrow |e_1\rangle$ and thus 12.6×2^n for the whole transformation. It is still an open question if the transformation could be done more directly, i.e., merging some of the consecutive gates together and finding efficient gate array for implementing them. This would reduce the number of elementary gates needed.

[1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, 2000).
[2] J. J. Vartiainen, M. Möttönen, and M. M. Salomaa (2004), quant-ph/0312218.
[3] M. Mikko Möttönen, J. J. Vartiainen, V. Bergholm, and M. M. Salomaa (2004), quant-ph/0404089.
[4] V. V. Shende, S. S. Bullock, and I. L. Markov (2004), quant-ph/0406176.
[5] V. V. Shende and I. L. Markov (2004), quant-ph/0401162.
[6] V. V. Shende, I. L. Markov, and S. S. Bullock (2003), quant-ph/0308033.
[7] E. Knill (1995), quant-ph/9508006.