# II

Publication II

M. Möttönen, J. J. Vartiainen, V. Bergholm, M. M. Salomaa, *Transformation of quantum states using uniformly controlled rotations*, Quantum Information and Computation **5**, 467 (2005).

Quantum Information and Computation, Vol. 5, No. 6 (2005) 467–473


# TRANSFORMATION OF QUANTUM STATES USING UNIFORMLY CONTROLLED ROTATIONS

MIKKO MÖTTÖNEN, JUHA J. VARTIAINEN, VILLE BERGHOLM, and MARTTI M. SALOMAA
*Materials Physics Laboratory, Helsinki University of Technology, P.O. Box 2200 Helsinki FIN-02015 HUT, Finland*

Received July 10, 2004
Revised June 20, 2005

We consider a unitary transformation which maps any given pure 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.

*Keywords*: quantum computation, quantum state preparation

*Communicated by*: R Jozsa & G Milburn

## 1 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.

Experimentalists face this same problem when trying to synthesize non-trivial multi-qubit states having desired entanglement properties, for example, the $n$-qubit generalization of the GHZ state. Moreover, state preparation may be useful in speeding up some known quantum algorithms. As a concrete example, it can be used to construct initial states with non-flat probability distributions for the quantum database search algorithm, which may be advantageous if there is some prior knowledge on the distribution of the data constituting the database.

The recent progress [5, 6, 7] in implementing general $n$-qubit gates using elementary gates has resulted in efficient gate synthesis techniques including uniformly controlled rotations [6], and more recently, quantum multiplexors [7]. 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 recently discussed in Ref. [8], 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-qubit rotations about the $y$ and $z$ axes.

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.

One CNOT gate can bind at most four elementary rotations [9]. This is seen by considering a circuit consisting of a CNOT gate followed by an arbitrary local transformation on each qubit. Writing the one-qubit gates as Euler rotations about the $x$ and $z$ axes and noting that $z$ rotations commute with the control node and $x$ rotations commute with the target node of the CNOT, we find that all but four of the elementary rotations may be commuted through the CNOT gate. Thus at least $\lceil \frac{1}{4}(2^{n+1} - 3n - 2) \rceil$ CNOT gates 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 [10], who found that no more than $O(n2^n)$ gates are needed for the circuit implementing the transformation. A sufficient circuit of $O(2^n)$ elementary gates is obtained as a special case of the method developed for QR decomposition of a general quantum gate in Ref. [5], as was first pointed out in Ref. [8].

In this paper, we describe in detail how to build a generic quantum circuit for making any desired pure state transformation employing uniformly controlled rotations. A uniformly controlled rotation, defined explicitly in Sec. 2, is a sequence of multiply controlled one-qubit rotations about a common axis. In the sequence, all the different control node combinations are present. 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 circuit topology of $2^{n+2} - 4n - 4$ CNOT gates and $2^{n+2} - 5$ one-qubit elementary rotations gives, in principle, the exact transformation from the $n$-qubit quantum state $|a\rangle$ into the desired one, $|b\rangle$.

It should be noted, however, that this is a worst-case complexity. In the case of initial and target states with suitable internal symmetries, the construction will be significantly simplified. Hence the proposed method, perhaps with additional simplification algorithms, can also be used as a practical tool for finding efficient implementations of some specific states, for example the aforementioned $n$-qubit GHZ state. On the other hand, certain models of measurement-based quantum computing require specific, highly entangled initial states involving all the qubits of the register. An example of such states are the cluster states used by "one-way quantum computers" [2], attractive due to their fault tolerance and potential scalability [3]. These states, however, tend to be rather symmetric and efficient methods to create them are already known, see for example Ref. [4]. Hence we do not expect our algorithm to be very useful in this specific area.

## 2 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 $j^{\text{th}}$ 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 $k$ control nodes, the target qubit $m$, the rotation axis $\mathbf{a}$ and the angles $\{\alpha_i\}$, see Ref. [6]. 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 node combinations. The rotation $R_{\mathbf{a}}(\alpha_i)$ is defined as

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

where $\sigma_x$, $\sigma_y$, and $\sigma_z$ are the Pauli matrices and the dot product $\mathbf{a}\cdot\boldsymbol{\sigma} = a_x\sigma_x + a_y\sigma_y + a_z\sigma_z$. A black control node restricts the action of the target rotation to the subspace in which the corresponding qubit is in the state $|1\rangle$, and a white control node to the subspace where the qubit is in the state $|0\rangle$. The positions of the control nodes in the definition of the gate $F_m^k(\mathbf{a}, \boldsymbol{\alpha})$ are implicit and may be, in general, arbitrary with the exception that the target qubit is the $m^{\text{th}}$ one.

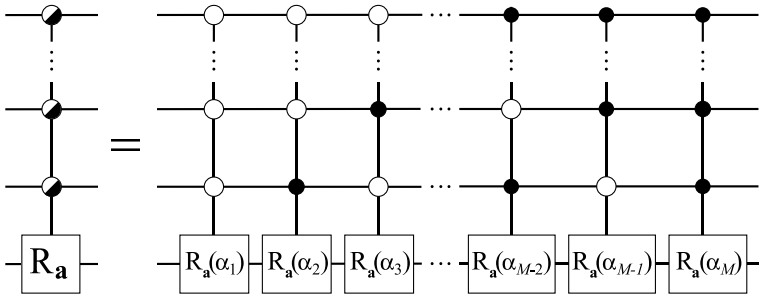


Fig. 1. Definition of the $k$-fold uniformly controlled rotation $F_m^k(\mathbf{a}, \boldsymbol{\alpha})$ of qubit $m$ about the axis $\mathbf{a}$. A black control node restricts the action of the target rotation to the subspace in which the corresponding qubit is in the state $|1\rangle$, and a white control node to the subspace where the qubit is in the state $|0\rangle$. The left hand side of the figure 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 $m^{\text{th}}$ one. Above, $M = 2^k$.

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 changing the position of the control in the

rightmost CNOT gate to the new control qubit and repeating the obtained sequence twice with 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 both sides of the gate.

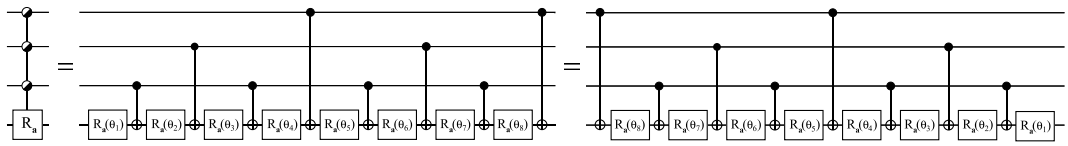

Fig. 2. Efficient gate decomposition for the uniformly controlled rotation $F_4^3(\mathbf{a}, \boldsymbol{\alpha})$ with $a_x = 0$. The relation of the angles $\{\theta_j\}$ to the angles $\{\alpha_j\}$ is shown in Eq. (3). The last equality shows that the circuit may be horizontally mirrored.

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 $g$ in Eq. (3) by another cyclic Gray code [11]. Additionally, a horizontally mirrored version of the gate sequence in Fig. 2, where the relative order of the gates has been reversed, also qualifies to simulate the uniformly controlled rotation.

## 3 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 $|e_1\rangle = |00\ldots0\rangle = (1,0,0,\ldots,0)^T = (1,0)^T \otimes \ldots \otimes (1,0)^T$.

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 $\omega_i$ using a cascade of uniformly controlled $z$-rotations $\Xi_z$, rendering the vector real up to the global phase $\phi$: $\Xi_z|a\rangle = e^{i\phi}|\hat{a}\rangle$.
- 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 $\Xi_y$, thus achieving our goal.

The first step can be readily accomplished using a general diagonal $n$-qubit quantum gate first considered in Ref. [12]. 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

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

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

$$\{\alpha_j^y\} = \left\{ 2 \arcsin\left( |a_{2j}| \Big/ \sqrt{|a_{2j-1}|^2 + |a_{2j}|^2} \right) \right\}.$$

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 $|e_1\rangle$.

Employing the above steps one obtains the desired decomposition

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

The product of non-commuting matrices in Eq. (7) is to be taken from left to right. To eliminate the remaining global phase one could apply a phase gate. The rotation angles $\{\boldsymbol{\alpha}_j^y\}$ in Eq. (7) are found to acquire the values

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

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 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 two CNOT gates from each pair by mirroring the circuit for the uniformly controlled $y$ rotation.

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 $k$-fold uniformly 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.

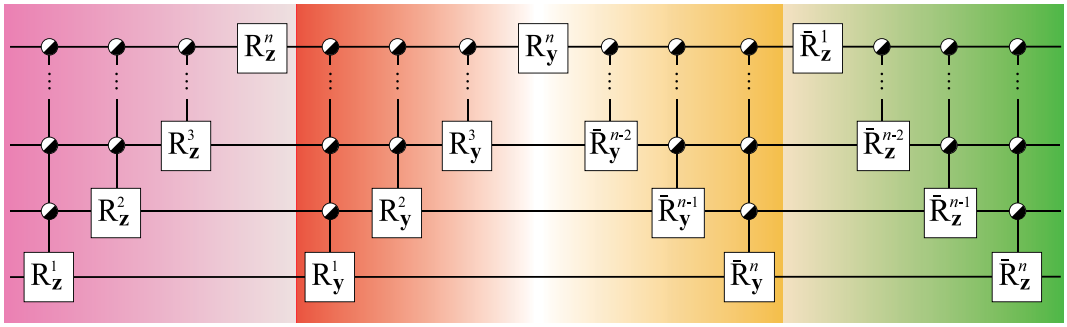


Fig. 3. Gate sequence for state preparation using uniformly controlled rotations. The rotation angles $\{\alpha_{j,k}^q\}$ for the uniformly controlled rotations are given in Eqs. (8) and (5).

## 4 Conclusion

In conclusion, 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 a given arbitrary state of the quantum register transforms into a desired state.

The gate count is small compared to the incomplete QR decomposition which takes approximately $6.3 \times 2^n$ CNOT gates to transform $|a\rangle \to |e_1\rangle$ and thus $12.6 \times 2^n$ 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 required.

### Acknowledgements

This research is supported by the Academy of Finland through the project "Quantum Computation" (No. 206457). MM thanks the Foundation of Technology (Finland), the Academy of Finland, and Jenny and Antti Wihuri's foundation, JJV the Nokia Foundation, MM and VB the Finnish Cultural Foundation, and MMS the Japan Society for the Promotion of Science for financial support. Sami Virtanen is acknowledged for stimulating discussions.

### *Note added*

After the submission of this manuscript, we have managed to further improve the state preparation algorithm and essentially halve the number of CNOT gates required, see Refs. [13] and [14]. This has been accomplished by implementing the method presented in this paper using general uniformly controlled one-qubit gates rather than just uniformly controlled

rotations.

## References


1. M. A. Nielsen and I. L. Chuang (2000), *Quantum Computation and Quantum Information*, Cambridge University Press.
2. R. Raussendorf and H. J. Briegel (2001), *A One-Way Quantum Computer*, Phys. Rev. Lett. **86**, 5188.
3. M. A. Nielsen and C. M. Dawson (2005), *Fault-tolerant quantum computation with cluster states*, Phys. Rev. A **71**, 042323.
4. M. Borhani and D. Loss (2005), *Cluster states from Heisenberg interactions*, Phys. Rev. A **71**, 034308.
5. J. J. Vartiainen, M. Möttönen, and M. M. Salomaa (2004), *Efficient decomposition of quantum gates*, Phys. Rev. Lett. **92**, 177902.
6. M. Möttönen, J. J. Vartiainen, V. Bergholm, and M. M. Salomaa (2004), *Quantum Circuits for General Multiqubit Gates*, Phys. Rev. Lett. **93**, 130502.
7. V. V. Shende, S. S. Bullock, and I. L. Markov (2004), *A Practical Top-down Approach to Quantum Circuit Synthesis*, `quant-ph/0406176 v3`.
8. V. V. Shende and I. L. Markov (2004), *Quantum Circuits for Incompletely Specified Operators*, Quant. Inf. and Comp. **5**, 48.
9. V. V. Shende, I. L. Markov and S. S. Bullock (2003), *Minimal Universal Two-qubit Quantum Circuits*, Phys. Rev. A **69**, 062321.
10. E. Knill (1995), *Approximation by Quantum Circuits*, `quant-ph/9508006`.
11. C. Savage (1997), *A survey of combinatorial Gray codes*, SIAM Rev. **39**, 605.
12. S. S. Bullock and I. L. Markov (2004), *Asymptotically optimal circuits for arbitrary n-qubit diagonal computations*, Quant. Inf. and Comp. **4**, 27.
13. V. Bergholm, J. J. Vartiainen, M. M. Möttönen, and M. M. Salomaa (2005), *Quantum circuits with uniformly controlled one-qubit gates*, Phys. Rev. A **71**, 052330.
14. M. Möttönen and J. J. Vartiainen (2005), *Decompositions of general quantum gates*, `quant-ph/0504100`.