Symmetry **2011**, *3*, 305-324; doi:10.3390/sym3020305

OPEN ACCESS

symmetry

ISSN 2073-8994

www.mdpi.com/journal/symmetry

Article

Symmetry Groups for the Decomposition of Reversible Computers, Quantum Computers, and Computers in between

Alexis De Vos [1,⋆] **and Stijn De Baerdemacker** [2]

[1] Department of Electronics and Information Systems, Universiteit Gent, Sint Pietersnieuwstraat 41, B-9000 Gent, Belgium

[2] "FWO-Vlaanderen" post-doctoral fellow, Department of Physics and Astronomy, Universiteit Gent, Proeftuinstraat 86, B-9000 Gent, Belgium; E-Mail: stijn.debaerdemacker@UGent.be

⋆ Author to whom correspondence should be addressed; E-Mail: alex@elis.UGent.be; Tel.: +32 9 264 33 76; Fax: +32 9 264 35 94

Received: 11 January 2011; in revised form: 24 May 2011 / Accepted: 27 May 2011 / Published: 7 June 2011

Abstract: Whereas quantum computing circuits follow the symmetries of the unitary Lie group, classical reversible computation circuits follow the symmetries of a finite group, *i.e.*, the symmetric group. We confront the decomposition of an arbitrary classical reversible circuit with w bits and the decomposition of an arbitrary quantum circuit with w qubits. Both decompositions use the control gate as building block, *i.e.*, a circuit transforming only one (qu)bit, the transformation being controlled by the other $w-1$ (qu)bits. We explain why the former circuit can be decomposed into $2w-1$ control gates, whereas the latter circuit needs 2^w-1 control gates. We investigate whether computer circuits, not based on the full unitary group but instead on a subgroup of the unitary group, may be decomposable either into $2w-1$ or into 2^w-1 control gates.

Keywords: reversible computing; quantum computing; group theory

1. Introduction

Quantum computing has witnessed considerable attention in the literature in the past decennia, mainly due to the speed-up of quantum computations over their classical counterparts [1–3]. However, an aspect that is commonly tacitly referred to the background, is the *reversible* character of the quantum

mechanical processes, underlying the computations. Nevertheless, reversible computing offers the one-and-only road towards zero-power computation. This is due to the avoidance of the Landauer effect [4,5], *i.e.*, no heat is dissipated into the system as no information has been destroyed along the process. Reversibility is not monopolized by the quantum world. Also classical circuits can be designed such that no information is destroyed during the computations, which constitutes the field of (classical) reversible computing [6–10]. These circuits are very similar to common classical logical circuits, with the exception that they are reversible, *i.e.*, we can unambiguously reconstruct the input from any given output. An overview of the achievements in the field of reversible computation is given by Kerntopf [11]. Clearly, the set of classical reversible circuits can be regarded as a subset of the quantum reversible circuits, so classical reversible computing can be regarded as a step-up from the contemporary classical computers towards the development of the quantum computers of the future.

In the present paper, we compare the decomposition of both an arbitrary reversible circuit and an arbitrary quantum circuit into elementary gates. A relationship between the two architectures is established, based on group theory. Whereas reversible computing is based on finite groups, quantum computing is based on infinite groups (a.k.a. Lie groups). Whereas reversible computing reflects the symmetries of the group of permutation matrices, quantum computing displays the symmetries of unitary matrices. In spite of these differences, quite similar (but not identical) synthesis methods may be applied for both building a reversible computer and building a quantum computer from elementary gates called control circuits.

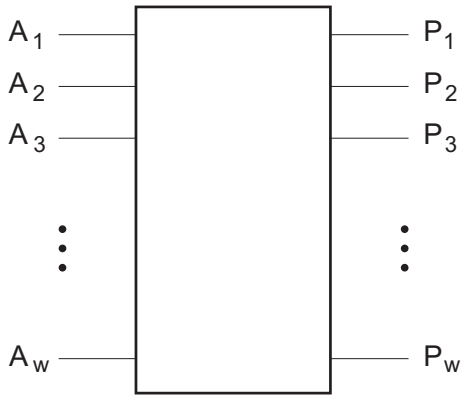
2. Control Circuits and Control Gates

Assume a circuit of width w, *i.e.*, a circuit with w input (qu)bits and w output (qu)bits. Indeed, for reversible circuits (either classical or quantum), the number of outputs necessarily equals the number of inputs. See Figure 1. With these w (qu)bits, we can build a 2^w dimensional (Hilbert) space with basis vectors $\{|e_1, e_2, \ldots, e_w\rangle; e_j = 0, 1\}$. For a typical classical reversible circuit, the input and output vector will be equal to one of these basis vectors and we can write them as $(A_1, A_2, \ldots, A_w) = |A_1, A_2, \ldots, A_w\rangle$ and $(P_1, P_2, \ldots, P_w) = |P_1, P_2, \ldots, P_w\rangle$ respectively. In the quantum world, the situation is different as superpositions or linear combinations of the basis vectors (a.k.a. basis *states*) are part of the physical reality. So, a general state can be written as

$$|\psi\rangle = \sum_{e_1,e_2,\ldots,e_w} c_{e_1,e_2,\ldots,e_w} |e_1, e_2, \ldots, e_w\rangle \tag{1}$$

Both in the classical case and in the quantum-mechanical case, we can represent a given (qu)bit state by means of a 2^w dimensional column vector with the coefficients (or amplitudes) $c_{\{e_i\}}$ as input entries. Consequently, a circuit or computation bringing one vector to another can be represented by a $2^w \times 2^w$ matrix, acting on the column vectors. These matrices are permutation matrices in the case of classical reversible computing, and become unitary matrices in the quantum case. In the classical case, the circuit is fully characterized by w Boolean functions $P_j(A_1, A_2, ..., A_w)$. Methods have been developed to synthesize both circuits performing arbitrary reversible functions [9,10] and symmetric reversible functions [12].

Figure 1. A circuit of width w.

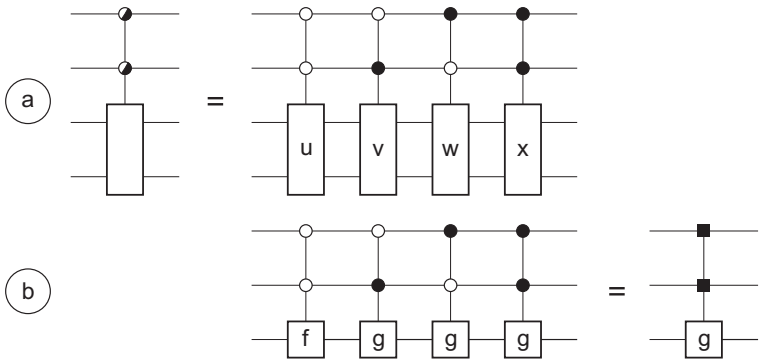


We consider a special case of circuits, where $w = u + v$. Let the circuit be such that it leaves the structure of the first u (qu)bits in the input state unaltered [13]. We will call these (qu)bits the controlling (qu)bits. The remaining v (qu)bits will be affected by the computation, however depending on the structure of the controlling (qu)bits. In the case of classical reversible computing, it means that the first u output bits will be equal to the input bits $(P_1, P_2, \ldots, P_u) = (A_1, A_2, \ldots, A_u)$ and the value of the remaining bits $(P_{u+1}, P_{u+2}, \ldots, P_{u+v})$ is a function of the input bits $(A_{u+1}, A_{u+2}, \ldots, A_{u+v})$, however depending on the values of the controlling bits $(A_1, A_2, \ldots, A_u)$. In the case of quantum computing, the circuit is based on the same general principle. However, the control does not consist of the sequence $(A_1, A_2, \ldots, A_u)$ alone, since the input state can be in a superposition of all basis states (1). As a result, the controlling will be done proportional to the amplitudes $c_{A_1,A_2,\ldots,A_u,e_{u+1},e_{u+2},\ldots,e_{u+v}}$ (with $e_{u+j} = 0, 1$) in the expansion of the input state. This will become clear when inspecting the transformation matrix. In general, these circuits can be represented by a $2^w \times 2^w$ matrix, consisting of 2^u blocks, each of size $2^v \times 2^v$, situated on the diagonal. Similarly, all matrices involved are either permutation matrices (classical reversible computing) or unitary matrices (quantum computing). We will call these circuits control circuits, e.g., for the case $u = 2$ and $v = 1$ (and thus $w = 3$), the unitary matrix looks like

$$C = \begin{pmatrix} U_{11} & U_{12} & 0 & 0 & 0 & 0 & 0 & 0 \\ U_{21} & U_{22} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & V_{11} & V_{12} & 0 & 0 & 0 & 0 \\ 0 & 0 & V_{21} & V_{22} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & W_{11} & W_{12} & 0 & 0 \\ 0 & 0 & 0 & 0 & W_{21} & W_{22} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & X_{11} & X_{12} \\ 0 & 0 & 0 & 0 & 0 & 0 & X_{21} & X_{22} \end{pmatrix}$$

Thus, if $(A_1, A_2) = (0, 0)$ then matrix U is applied to A_3, if $(A_1, A_2) = (0, 1)$ then matrix V is applied to A_3, *etc*. As already mentioned, in quantum computing, the input state will always be in a superposition of the controlling qubits. Therefore, the computation will be controlled according to the amplitudes of the controlling qubits in the input state. Figure 2a shows an example for $u = v = 2$ (and thus $w = 4$). We follow here the notation by Möttönen *et al.* [14,15].

Figure 2. Symbols for (**a**) a control circuit and (**b**) a control gate.



In some cases, only two different submatrices F and G are present, and moreover one of them (*i.e.*, F) is the $2^v \times 2^v$ unit matrix. Figure 2b shows an example:

$$C = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & G_{11} & G_{12} & 0 & 0 & 0 & 0 \\ 0 & 0 & G_{21} & G_{22} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & G_{11} & G_{12} & 0 & 0 \\ 0 & 0 & 0 & 0 & G_{21} & G_{22} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & G_{11} & G_{12} \\ 0 & 0 & 0 & 0 & 0 & 0 & G_{21} & G_{22} \end{pmatrix}$$

In such case, the gate g of width v is applied to the controlled (qu)bits if and only if a particular boolean function $\varphi(A_1, A_2, ..., A_u)$ of the controlling (qu)bits equals 1. Such special control circuit is called a control gate [16]. The function φ is called the control function. In the example of Figure 2b, we have $\varphi(A_1, A_2) = A_1\, OR\, \mathrm{A}_2$.

Control gates are important in classical reversible computing as there exist only two different 2×2 permutation matrices, one representing the follower, the other representing the inverter. Thus a classical reversible control circuit with $v = 1$ always simplifies to a control gate. In quantum computing, even for v as small as 1, as many as ∞^4 different 2×2 unitary matrices [17] are allowed; the "probability" that two such 2×2 blocks in a control circuit matrix will be identical, is infinitesimally small. In the following, we will show from quite general principles that the control circuit plays an important role in the effective decomposition of a reversible as well as a quantum circuit.

3. Symmetric Groups

For the study of reversible computers, we consider the reversible logic circuits of width w, *i.e.*, with w binary inputs A_1, A_2, ..., A_w and w binary outputs P_1, P_2, ..., P_w. See Figure 1. The 2^w output rows of the truth table of such a logic transformation correspond to a permutation of the 2^w input rows (0, 0, ..., 0, 0), (0, 0, ..., 0, 1), (0, 0, ..., 1, 0), ..., and (1, 1, ..., 1, 1). Table 1a gives an example for $w = 3$. All reversible truth tables of the same width w form a group (with respect to the operation of cascading), which we denote by **R**. The group **R** is isomorphic to the symmetric group $\mathbf{S}_{2^w}$ of degree 2^w and order $N = (2^w)!$. It thus is also isomorphic to the group of the $2^w \times 2^w$ permutation matrices.

Table 1. Members of the group **R** with $w = 3$. (**a**) arbitrary; (**b**) linear.

$A_1A_2A_3$	$P_1P_2P_3$
0 0 0	1 1 1
0 0 1	1 1 0
0 1 0	1 0 0
0 1 1	0 0 0
1 0 0	1 0 1
1 0 1	0 1 0
1 1 0	0 0 1
1 1 1	0 1 1

(**a**)

$A_1A_2A_3$	$P_1P_2P_3$
0 0 0	0 0 0
0 0 1	0 1 0
0 1 0	1 0 1
0 1 1	1 1 1
1 0 0	1 0 0
1 0 1	1 1 0
1 1 0	0 0 1
1 1 1	0 1 1

(**b**)

A natural question is now if we can construct a given reversible function of degree x from a concatenation of circuits with lower degree. Let $N(x)$ be the number of different circuits of degree x, which we would like to build into hardware. We may assume that we can make use of a library of circuits with degree y (with $y < x$) for that particular purpose. This library again can be constructed from another library of circuits with lower degree z (with $z < y$) *etc.*, until we have reached the set of all circuits of degree 2 (*i.e.*, the 1-(qu)bit operations). We are interested in a particular kind of decomposition of a circuit with a given (non-prime) degree m:

$$m = p \times q \tag{2}$$

with p and q integers. We aim at decomposing a circuit of degree m into a cascade of three circuits:

- the first consisting of q subcircuits each of degree p,
- the second consisting of p subcircuits each of degree q, and
- the third consisting again of q subcircuits each of degree p.

With the help of $2q$ circuits of degree p and p circuits of degree q, we can make the following number of combinations:

$$F(p, q) = [\, N(p) \,]^{2q} \, [\, N(q) \,]^{p} \tag{3}$$

For the particular case of the symmetric group $\mathbf{S}_x$ of degree x, the order $N(x)$ equals $x!$. With $N(x) = x!$ and $q = m/p$, Equation (3) gives

$$F(p, m/p) = (p!)^{2m/p} \, [\, (m/p)! \,]^{p}$$

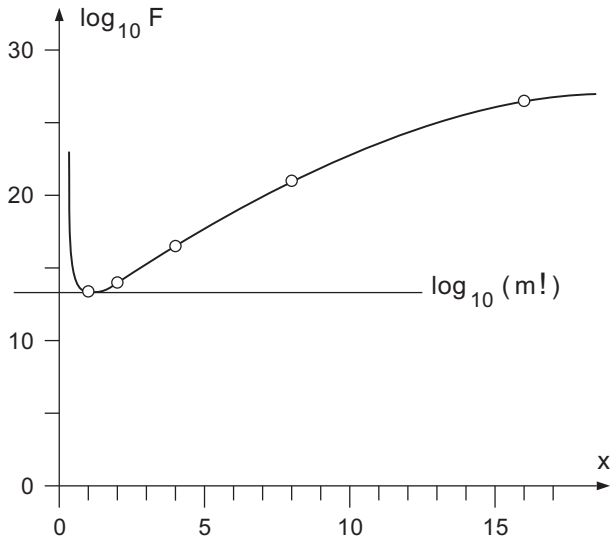
For any non-trivial divisor p of m, we have that $F(p, m/p)$ is larger than $N(m) = m!$. A proof is supplied in Appendix A. This suggests that any factorization of m is a candidate for decomposition of

an arbitrary circuit of degree m, e.g., for m equal to a power of 2 (say $m = 2^w$), we have $p = 2^k$. The value of $F(p, m/p)$ grows fast with increasing p :

$$\begin{aligned} F(1,m) &= m! \\ F(2,m/2) &= 2^m\,[\,(m/2)!\,]^2 \approx \sqrt{\frac{\pi}{2}}\,\sqrt{m}\,m! \\ &\ldots \\ F(m/2,2) &= [\,(m/2)!\,]^4\,2^{m/2} \approx \frac{\pi}{2}\,2^{-3m/2}\,m\,(m!)^2 \\ F(m,1) &= (m!)^2 \end{aligned}$$

This is illustrated by Figure 3, where m has been chosen equal to 16. The dots on the curve are located at the divisors of m, *i.e.*, at $x = 1$, $x = 2$, $x = 4$, $x = 8$, and $x = 16$. Thus all divisors $p = 2$, $p = 4$, ..., $p = \frac{m}{2}$ obey $F(p, m/p) > m!$. Therefore, the $F(p, q)$ combinations may be enough to construct the $N(m)$ different circuits. Hence, each of these choices of p may lead to a circuit synthesis method. And, in fact, they do, thanks to Birkhoff's theorem on doubly stochastic matrices. One of the versions of this theorem states that any $q \times q$ matrix with integer entries, such that all line sums are equal to p, can be written as a sum of p permutation matrices. As a result [16,18], any permutation of m objects can be decomposed as a sequence of q permutations of p objects, p permutations of q objects, and again q permutations of p objects. The most efficient synthesis method is found for that particular value of p for which $F(p, m/p)$ exceeds $m!$ as little as possible. This happens for $p = 2$ (and thus $q = \frac{m}{2}$).

Figure 3. The function $F(x, \frac{m}{x}) = [\,\Gamma(x+1)\,]^{2m/x}\,[\,\Gamma(\frac{m}{x}+1)\,]^x$ for $m = 16$.



In the case of reversible computing, we have $m = 2^w$. Thus factorizing this number as $p \times q = 2 \times 2^{w-1}$ is the best choice for efficient synthesis of a reversible circuit. Figure 4a shows the resulting 3-part circuit. Figure 5 shows how we may apply such decomposition $w-1$ times. De Vos and Van Rentergem [16,18] have demonstrated that this eventually leads to a circuit synthesis consisting of a cascade or chain of as little as $2w-1$ control gates. The synthesis approach is very efficient, as no synthesis is possible with less than $2w-3$ control gates. Indeed, any synthesis method [18,19] leads to a cascade of length L satisfying

$$L \geq \left\lceil \frac{\log(N)}{\log(B)} \right\rceil$$

with $N = (2^w)!$ and $B = 2^{2^{w-1}}$ (the number of different building blocks). Together with Stirling's formula, this yields [18]

$$L \geq \left\lceil \frac{(w - \frac{3}{2})2^w \log(2)}{2^{w-1} \log(2)} \right\rceil = 2w - 3$$

Figure 4. Decomposition of a circuit into three parts. (**a**) a member of $\mathbf{S}_{16}$ into two members of $\mathbf{S}_2^8$ and one member of $\mathbf{S}_8^2$ and (**b**) a member of U(16) into two members of $\mathrm{U}(8)^2$ and one member of $\mathrm{U}(2)^8$.

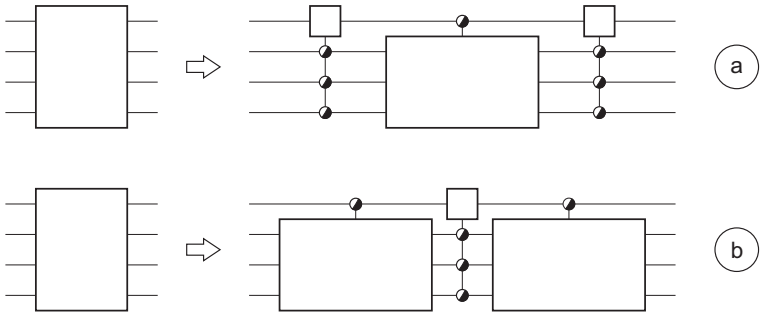
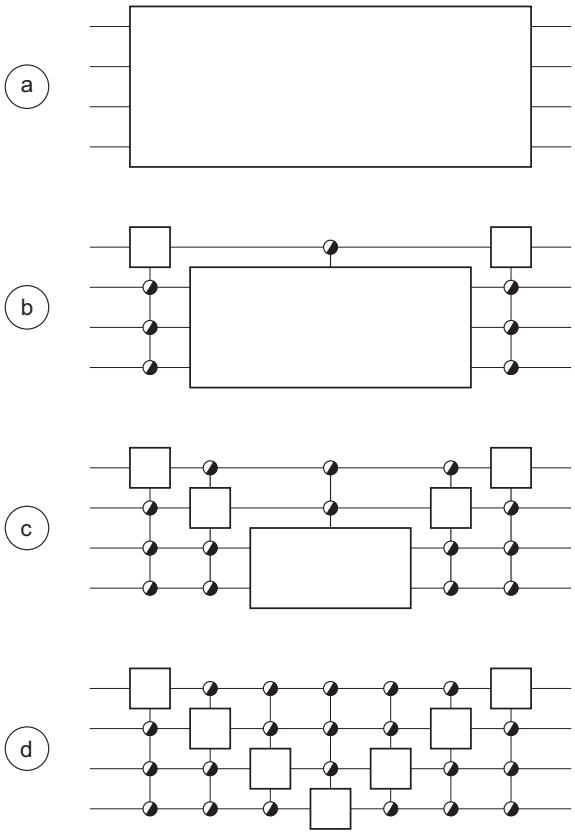


Figure 5. Decomposition of a reversible logic circuit of width $w = 4$. (**a**) original logic circuit; (**b**) and (**c**) intermediate steps; (**d**) final decomposition.



4. Unitary Groups

4.1. Dimensional Analysis

Let $n(x)$ be the dimension of the space of circuits of degree x. With the help of $2q$ circuits of degree p and p circuits of degree q, we can span a space of dimension

$$f(p,q) = 2qn(p) + pn(q) \tag{4}$$

For the particular case of the unitary group U(x), the dimension $n(x)$ equals x^2. With $n(x) = x^2$ and $q = m/p$, Equation (4) gives

$$f(p, m/p) = 2mp + \frac{m^2}{p}$$

For most non-trivial divisors of m, we have that $f(p, m/p)$ is smaller than $n(m) = m^2$. Indeed, in the range $0 < x < +\infty$, the function $f(x, m/x) = 2mx + m^2/x$ first is decreasing (in the range $0 < x < \sqrt{m/2}$), then is increasing (in the range $\sqrt{m/2} < x < \infty$). This is illustrated by Figure 6, where again m has been chosen equal to 16 and dots on the curve are located at the divisors of 16. The curve, in fact, is just a hyperbola. It can be noted from Figure 6 that three and only three dots are located above the horizontal line $f = m^2$: the points at $p = 1$, $p = m/2$, and $p = m$. Only the point $p = m/2$ hints at a plausible decomposition, as both $p = 1$ and $p = m$ do not lead towards a simplification of the original circuit. For all x-values in the range of interest (*i.e.*, for $2 \leq x \leq m/2$), $f(x, m/x)$ is smaller than $n(m) = m^2$, except in the range $(m + \sqrt{m^2 - 8m})/4 \leq x \leq m/2$, e.g., for m equal to a power of 2 (say $m = 2^w$), we have $p = 2^k$ and only one choice of p is viable in the latter range, *i.e.*, $p = m/2$:

$$f(m/2, 2) = m^2 + 2m$$

Thus only the divisor $p = \frac{m}{2}$ may lead to a synthesis method. If such synthesis really exists, recursive application would eventually lead to a cascade of as little as $L(w) = 2^w - 1$ control gates.

We summarize the present section applying the notion of Young subgroup. A Young subgroup of a symmetric group $\mathbf{S}_m$ is any direct-product group of the form $\mathbf{S}_{m_1} \times \mathbf{S}_{m_2} \times ... \mathbf{S}_{m_z}$, where $(m_1, m_2, ..., m_z)$ is a partition of the given number m:

$$m = m_1 + m_2 + ... + m_z$$

Let this m be an even integer. Then:

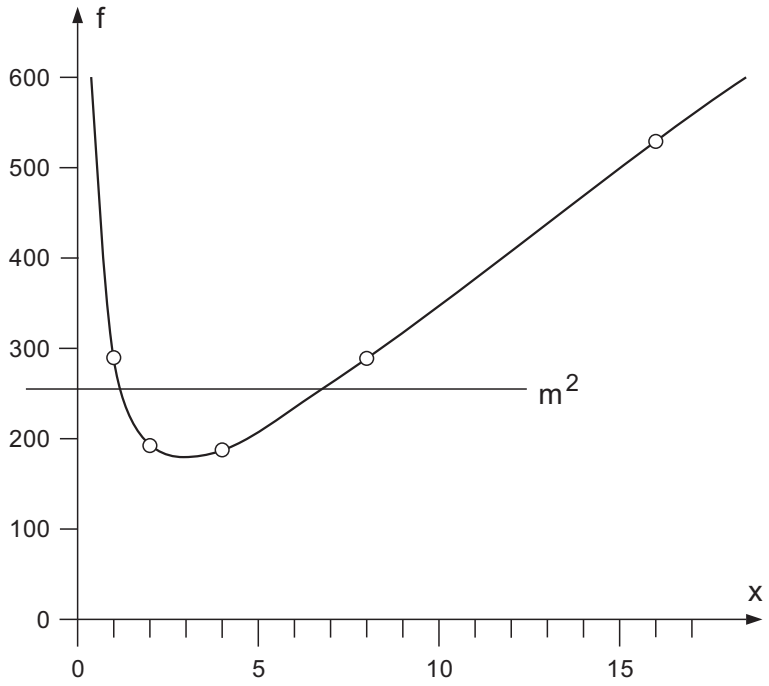
- For <u>any</u> factorization $m = p \times q$, an arbitrary member a of the symmetric group $\mathbf{S}_m$ can be decomposed as the product $b_1 c b_2$, where both b_1 and b_2 are member of a same Young subgroup $\mathbf{S}_p^q$ and c is a member of a dual Young subgroup $\mathbf{S}_q^p$.
- <u>Only</u> for the factorization $m = p \times q = \frac{m}{2} \times 2$, an arbitrary member a of the unitary group U(m) can be decomposed as the product $b_1 c b_2$, where both b_1 and b_2 are members of a same subgroup U$(p)^q$ and c is a member of a dual subgroup U$(q)^p$.

We close this section by noting that we may rewrite Equation (3) as follows:

$$\log[F(p,q)] = 2q \log[N(p)] + p \log[N(q)]$$

Comparison with Equation (4), leads to the conclusion that $\log(F)$ and $\log(N)$ for finite groups play a role similar to the dimensions f and n of infinite groups. A similar conclusion was made earlier [18,19].

Figure 6. The function $f(x, m/x) = 2mx + m^2/x$ for $m = 16$.



4.2. Decomposition

In order to find the synthesis method of a quantum circuit, we successively decompose the U(2^w)-matrix according to Figure 7b, e.g., for $w = 3$, we have $m = 2^w = 8$, $p = 2^{w-1} = 4$, and $q = 2$. The first step in the series of $w - 1$ decompositions looks as follows:

$$\begin{pmatrix} U_{11} & U_{12} & U_{13} & U_{14} & U_{15} & U_{16} & U_{17} & U_{18} \\ U_{21} & U_{22} & U_{23} & U_{24} & U_{25} & U_{26} & U_{27} & U_{28} \\ U_{31} & U_{32} & U_{33} & U_{34} & U_{35} & U_{36} & U_{37} & U_{38} \\ U_{41} & U_{42} & U_{43} & U_{44} & U_{45} & U_{46} & U_{47} & U_{48} \\ U_{51} & U_{52} & U_{53} & U_{54} & U_{55} & U_{56} & U_{57} & U_{58} \\ U_{61} & U_{62} & U_{63} & U_{64} & U_{65} & U_{66} & U_{67} & U_{68} \\ U_{71} & U_{72} & U_{73} & U_{74} & U_{75} & U_{76} & U_{77} & U_{78} \\ U_{81} & U_{82} & U_{83} & U_{84} & U_{85} & U_{86} & U_{87} & U_{88} \end{pmatrix} = \begin{pmatrix} L_{11} & L_{12} & L_{13} & L_{14} & 0 & 0 & 0 & 0 \\ L_{21} & L_{22} & L_{23} & L_{24} & 0 & 0 & 0 & 0 \\ L_{31} & L_{32} & L_{33} & L_{34} & 0 & 0 & 0 & 0 \\ L_{41} & L_{42} & L_{43} & L_{44} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & L_{55} & L_{56} & L_{57} & L_{58} \\ 0 & 0 & 0 & 0 & L_{65} & L_{66} & L_{67} & L_{68} \\ 0 & 0 & 0 & 0 & L_{75} & L_{76} & L_{77} & L_{78} \\ 0 & 0 & 0 & 0 & L_{85} & L_{86} & L_{87} & L_{88} \end{pmatrix}$$

$$\begin{pmatrix} M_{11} & 0 & 0 & 0 & M_{15} & 0 & 0 & 0 \\ 0 & M_{22} & 0 & 0 & 0 & M_{26} & 0 & 0 \\ 0 & 0 & M_{33} & 0 & 0 & 0 & M_{37} & 0 \\ 0 & 0 & 0 & M_{44} & 0 & 0 & 0 & M_{48} \\ M_{51} & 0 & 0 & 0 & M_{55} & 0 & 0 & 0 \\ 0 & M_{62} & 0 & 0 & 0 & M_{66} & 0 & 0 \\ 0 & 0 & M_{73} & 0 & 0 & 0 & M_{77} & 0 \\ 0 & 0 & 0 & M_{84} & 0 & 0 & 0 & M_{88} \end{pmatrix} \begin{pmatrix} R_{11} & R_{12} & R_{13} & R_{14} & 0 & 0 & 0 & 0 \\ R_{21} & R_{22} & R_{23} & R_{24} & 0 & 0 & 0 & 0 \\ R_{31} & R_{32} & R_{33} & R_{34} & 0 & 0 & 0 & 0 \\ R_{41} & R_{42} & R_{43} & R_{44} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & R_{55} & R_{56} & R_{57} & R_{58} \\ 0 & 0 & 0 & 0 & R_{65} & R_{66} & R_{67} & R_{68} \\ 0 & 0 & 0 & 0 & R_{75} & R_{76} & R_{77} & R_{78} \\ 0 & 0 & 0 & 0 & R_{85} & R_{86} & R_{87} & R_{88} \end{pmatrix} \quad (5)$$

This decomposition indeed corresponds to the proposed (p, q, p) cascading, as the L and R matrix can be regarded as the product of $q = 2$ transformations in two different (orthogonal) $p^2 = 16$-dimensional spaces. This can be made clear by introducing the identity

$$\begin{pmatrix} L_{11} & L_{12} & L_{13} & L_{14} & 0 & 0 & 0 & 0 \\ L_{21} & L_{22} & L_{23} & L_{24} & 0 & 0 & 0 & 0 \\ L_{31} & L_{32} & L_{33} & L_{34} & 0 & 0 & 0 & 0 \\ L_{41} & L_{42} & L_{43} & L_{44} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & L_{55} & L_{56} & L_{57} & L_{58} \\ 0 & 0 & 0 & 0 & L_{65} & L_{66} & L_{67} & L_{68} \\ 0 & 0 & 0 & 0 & L_{75} & L_{76} & L_{77} & L_{78} \\ 0 & 0 & 0 & 0 & L_{85} & L_{86} & L_{87} & L_{88} \end{pmatrix} =$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & L_{55} & L_{56} & L_{57} & L_{58} \\ 0 & 0 & 0 & 0 & L_{65} & L_{66} & L_{67} & L_{68} \\ 0 & 0 & 0 & 0 & L_{75} & L_{76} & L_{77} & L_{78} \\ 0 & 0 & 0 & 0 & L_{85} & L_{86} & L_{87} & L_{88} \end{pmatrix} \begin{pmatrix} L_{11} & L_{12} & L_{13} & L_{14} & 0 & 0 & 0 & 0 \\ L_{21} & L_{22} & L_{23} & L_{24} & 0 & 0 & 0 & 0 \\ L_{31} & L_{32} & L_{33} & L_{34} & 0 & 0 & 0 & 0 \\ L_{41} & L_{42} & L_{43} & L_{44} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Similarly, M can be written as $p = 4$ successive transformations in different orthogonal $2^2 = 4$-dimensional spaces.

Whereas the original matrix U has $n(m) = n(8) = 8^2 = 64$ parameters, the decomposition (5) has $f(4, 2) = m^2 + 2m = 8^2 + 16 = 80$ parameters, *i.e.*, $qp^2 = m^2/2 = 32$ parameters for matrix L, $pq^2 = 2m = 16$ parameters for matrix M, and $qp^2 = m^2/2 = 32$ parameters for matrix R. Whereas the matrix at the left-hand side of (5) is an arbitrary member of U(8), each of the three matrices at the right-hand side is member of a subgroup of U(8): two are member of a same subgroup isomorphic to $\mathrm{U}(4)^2$ and one is member of a subgroup isomorphic to $\mathrm{U}(2)^4$. Figure 4b shows the resulting 3-part circuit. Note that the matrix M represents a control circuit, however not with the wth qubit controlled, but with the first qubit controlled and the other $w - 1$ controlling. Applying such decomposition $w - 1$ times (Figure 7), one should be able to demonstrate that this eventually leads to a synthesis consisting of a cascade of as little as $L(w) = 2^w - 1$ control circuits (Figure 7d).

The above synthesis approach is rather efficient, as one can prove that no synthesis is possible with less than 2^{w-1} control gates. Indeed, any synthesis method [18,19] leads to a cascades of length L satisfying

$$L \geq \left\lceil \frac{n}{b} \right\rceil$$

With $n = (2^w)^2 = 2^{2w}$ the dimension of the total space and $b = 4 \times 2^{w-1}$ the dimension of each control circuits, this yields

$$L \geq \left\lceil \frac{2^{2w}}{2^{w+1}} \right\rceil = 2^{w-1}$$

We conclude that the synthesis contains an overkill of approximately a factor 2. The reason is as follows. The decomposition (5) has $m^2 + 2m$ parameters; therefore for only m^2 constraints, there are as many

as $2m$ degrees of freedom extra. In other words: after the whole decomposition is executed (Figure 7d), a total of $t(w) = Lb = (2^w - 1)2^{w+1}$ free parameters are introduced to describe the 2^{2w} variables of the original unitary transformation U. See Figure 8. Because of these extra degrees of freedom, we are allowed to choose a controlled ROTATOR as control circuit. Each of the 2×2 blocks within the M-matrix then has the form

$$\begin{pmatrix} M_{j,j} & M_{j,j+\frac{m}{2}} \\ M_{j+\frac{m}{2},j} & M_{j+\frac{m}{2},j+\frac{m}{2}} \end{pmatrix} = C(\theta_j) = \begin{pmatrix} \cos(\theta_j) & \sin(\theta_j) \\ -\sin(\theta_j) & \cos(\theta_j) \end{pmatrix}$$

Such matrices form a well-known 1-dimensional subgroup of the 4-dimensional group U(2). See Appendix B. As a result, decomposition (5) is the well-known cosine-sine decomposition [20]. Of the $2m$ degrees of freedom, only $m/2$ remain: the rotation angles θ_1, θ_2, ..., $\theta_{m/2}$. The cosine-sine decomposition has indeed been applied for quantum circuit synthesis [14,21–24].

With the cosine-sine approach, each of the blocks in Figure 7d comes from a space with dimension $1 \times 2^{w-1}$, except the blocks in the lowermost line, which come from a space still with dimension $4 \times 2^{w-1}$. Thus the total dimension is

$$(2^{w-1} - 1) \times 1 \times 2^{w-1} + 2^{w-1} \times 4 \times 2^{w-1} = \frac{5}{4}\, 2^{2w}$$

such that there is only an overkill anymore of 5/4 with respect to the dimension 2^{2w} of Figure 7a, instead of a factor 2.

Figure 7. Decomposition of a quantum circuit of width $w = 4$. (**a**) original logic circuit; (**b**) and (**c**) intermediate steps; (**d**) final decomposition.

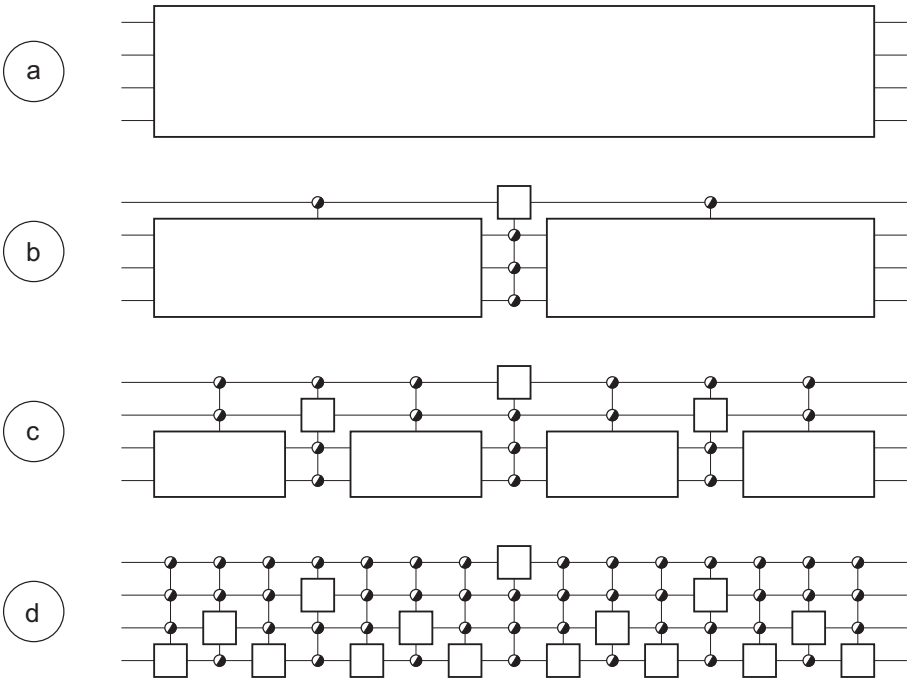
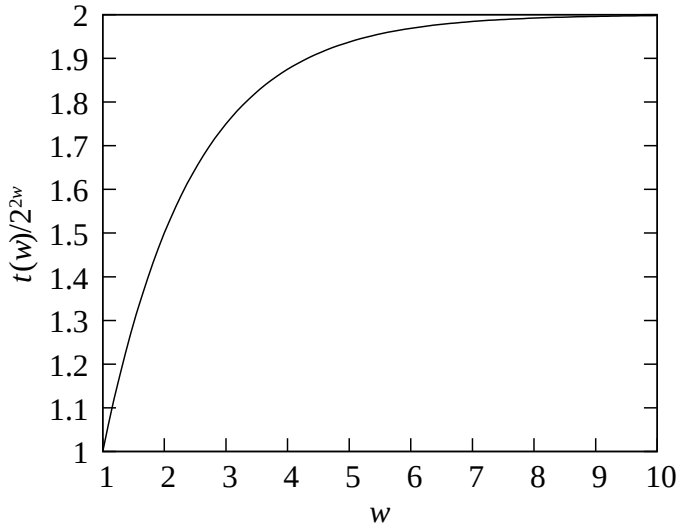


Figure 8. The total number $t(w)$ of free parameters in the decomposition, as a function of the number w of qubits, relative to the total number of parameters in the original unitary transformation.



4.3. Alternative Approaches

Möttönen *et al.* [14] first apply the cosine-sine decomposition (as in Section 4.2), then apply 2^{w-1} times the identity

$$\begin{pmatrix} \cos(\theta_j) & \sin(\theta_j) \\ -\sin(\theta_j) & \cos(\theta_j) \end{pmatrix} = \begin{pmatrix} \cos(\theta_j)\exp(i\alpha_j) & \sin(\theta_j)\exp(-i\alpha_j) \\ -\sin(\theta_j)\exp(i\alpha_j) & \cos(\theta_j)\exp(-i\alpha_j) \end{pmatrix} \begin{pmatrix} \exp(-i\alpha_j) & 0 \\ 0 & \exp(i\alpha_j) \end{pmatrix}$$

The former factor of the right-hand side becomes a block of the M-matrix in (5); the latter factor is absorbed by the R-matrix. By clever choice of the parameters α_j and subsequent application of a "mirroring trick", all the blocks in Figure 7d are member of a 2-dimensional subspace of U(2). The total dimension of their final synthesis exactly matches 2^{2w}.

Many other variations to the cosine-sine decomposition are possible, e.g., in order to obtain a decomposition of an arbitrary quantum circuit more closely resembling the decomposition of a reversible circuit (as given in Section 3), we may apply the identities

$$\begin{pmatrix} \cos(\theta_j) & \sin(\theta_j) \\ -\sin(\theta_j) & \cos(\theta_j) \end{pmatrix} = \begin{pmatrix} \exp(-i\theta_j) & 0 \\ 0 & \exp(-i\theta_j) \end{pmatrix} \begin{pmatrix} \frac{1+i}{\sqrt{2}} & 0 \\ 0 & \frac{1-i}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} \cos(\theta_j)\exp(i\theta_j) & -i\sin(\theta_j)\exp(i\theta_j) \\ -i\sin(\theta_j)\exp(i\theta_j) & \cos(\theta_j)\exp(i\theta_j) \end{pmatrix} \begin{pmatrix} \frac{1-i}{\sqrt{2}} & 0 \\ 0 & \frac{1+i}{\sqrt{2}} \end{pmatrix}$$

We let the first two factors of the right-hand side be absorbed by the L-matrix and the last factor by the R-matrix. This leaves the third factor of the right-hand side as a block of the M-matrix. Thus, the blocks (in the $w-1$ upper rows) of Figure 7d become controlled NEGATORs (See Appendix C) instead of controlled ROTATORs.

5. Intermediate Groups

The symmetric group $\mathbf{S}_{2^w}$ is a subgroup of U(2^w). As a result, any member of $\mathbf{S}_{2^w}$ can obviously be decomposed by means of the cosine-sine decomposition (Figure 7). However, this is not a very cost-efficient way of proceeding because we know, by virtue of the Birkhoff theorem, that a decomposition according Figure 5 is also possible. Moreover, every elementary control gate in the latter decomposition is a member of $\mathbf{S}_2$, which also belongs to the family of symmetric groups ($\mathbf{S}_m$). From this perspective, it would be interesting to investigate whether any member of a notable subgroup X(2^w) of U(2^w) (or supergroup of $\mathbf{S}_{2^w}$) can be decomposed into elementary control gates within the same family of those subgroups (e.g., decomposing the elements of the orthogonal group O(2^w) into multiple controlled O(2) gates). Furthermore, it is of interest to know whether such a decomposition is necessarily "cosine-sine"-like (Figure 4b & Figure 7) or may be achieved by means of a cheaper Birkhoff-like architecture (Figure 4a & Figure 5).

Consider Lie groups of $m \times m$ matrices with dimension $n(m)$, not necessarily equal to m^2 (unitary matrices) or to 0 (permutation matrices). In particular, we focus on functions satisfying

$$n(2) \geq 0, \qquad n(m+1) \geq n(m), \qquad (\forall m \geq 2) \tag{6}$$

which are natural assumptions when dealing with matrix groups. For convenience, we put forward the quadratic form

$$n(m) = Am^2 + Bm + C \tag{7}$$

in accordance to the classical groups [25]. This assumption will enable us to analyze the decomposition for groups ranging in between reversible and quantum computing. In general, the basis assumptions (6) lead to

$$A \geq 0, \qquad 5A + B \geq 0, \qquad \text{and} \qquad 4A + 2B + C \geq 0 \tag{8}$$

By means of the dimensional analysis performed in the previous sections, we can extract necessary (but not sufficient) conditions for a decomposition to be feasible. For both the "cosine-sine"-like and Birkhoff-like architecture, the analysis breaks down to the level of Figure 4. We obtain:

1. For a decomposition like Figure 4a to be possible, it is necessary that

$$f(2, \tfrac{m}{2}) \geq n(m) \qquad (\forall m \geq 4)$$

i.e., that

$$mn(2) + 2n(\tfrac{m}{2}) \geq n(m) \qquad (\forall m \geq 4) \tag{9}$$

Substitution of (7) into (9) gives

$$-\tfrac{1}{2}Am^2 + (4A + 2B + C)m + C \geq 0 \qquad (\forall m \geq 4)$$

leading to the additional condition $A \leq 0$. This result, together with $A \geq 0$ from (8) sets $A = 0$, such that $n(m) = Bm + C$. As a result, the necessary conditions for a decomposition according to Figure 4a (and subsequently a Birkhoff like decomposition) are

$$A = 0, \quad B \geq 0, \quad \text{and} \quad 8B + 5C \geq 0 \tag{10}$$

This is illustrated by the dark gray domain in the upper left panel of Figure 9. It may be noted that the conditions for a Birkhoff-like decomposition almost coincide with the general conditions (8) for $A = 0$. Therefore, a linear-dimensional matrix group ($A = 0$) is likely to be decomposable by means of a Birkhoff architecture. An example would be the Heisenberg group $\mathrm{H}_m(\mathbb{R})$, which is a linear-dimensional Lie group [26] of dimension $n(m) = 2m - 3$ and is depicted in the upper left panel of Figure 9 by (h). At this point, it is worth stressing that (10) is a necessary and not a sufficient condition. Therefore, once a particular group has passed the test (10), it is not guaranteed that it is Birkhoff-style decomposable. The Heisenberg group is a notable example, because deeper analysis points out that a general 8×8 Heisenberg matrix of $\mathrm{H}_8(\mathbb{R})$ cannot be decomposed into a member of $\mathrm{H}_4^2\ \mathrm{H}_2^4\ \mathrm{H}_4^2$. So, although the Heisenberg group fulfills relation (10), in general it can not be decomposed into a Birkhoff-style architecture. For quadratic groups, the conclusion we can draw from (10) is much more straightforward: since $A \neq 0$, a general Birkhoff-like decomposition is impossible on dimensional grounds.

2. For a decomposition like Figure 4b to be possible, it is necessary that

$$f(\tfrac{m}{2}, 2) \geq n(m) \qquad (\forall m \geq 4)$$

i.e., that

$$4n(\tfrac{m}{2}) + \tfrac{m}{2}n(2) \geq n(m) \qquad (\forall m \geq 4). \tag{11}$$

Substitution of (7) into (11) gives

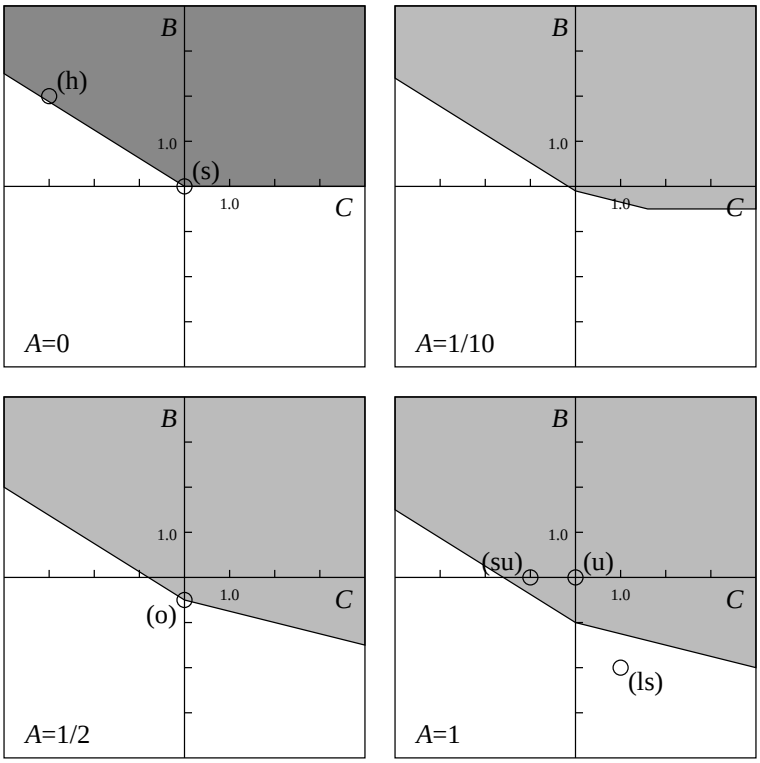
$$(2A + 2B + \tfrac{1}{2}C)m + 3C \geq 0 \qquad (\forall m \geq 4)$$

leading to the additional condition $A + B + \frac{1}{4}C \geq 0$. As a result, the necessary conditions for a decomposition according to Figure 4b (and subsequently a "cosine-sine"-like decomposition) are

$$A \geq 0, \quad 5A + B \geq 0, \quad 8A + 8B + 5C \geq 0, \quad \text{and} \quad 4A + 4B + C \geq 0 \tag{12}$$

This is illustrated by the light gray domains in the panels of Figure 9. It should be noted that, for $A = 0$, the conditions (10) and (12) coincide exactly. The result suggests that a large set of Lie groups may profit from a decomposition according Figure 4b. As an example, we consider the unitary $m \times m$ matrices with all line sums equal to 1. They form a Lie group with dimension $n(m) = m^2 - 2m + 1$ and are depicted by (ls) in Figure 9. The group is both a subgroup of $\mathrm{U}(m)$ and a supergroup of $\mathbf{S}_m$. Here, neither (10) nor (12) is fulfilled. Thus these matrices cannot be decomposed, neither as in Figure 4a nor as in Figure 4b, and consequently neither as in Figure 5d nor as in Figure 7d. Another example consists of the unitary $m \times m$ matrices with only real entries. These matrices form the orthogonal group $\mathrm{O}(m)$ with dimension $n(m) = \frac{1}{2}m^2 - \frac{1}{2}m$ and are depicted by (o) in Figure 9. This time, (10) is not fulfilled, but (12) is, such that the Birkhoff-like decomposition is not applicable, but the "cosine-sine"-like decomposition may be applicable. As a matter of fact, it is. This is no surprise, as the cosine-sine decomposition is proved for orthogonal matrices [27]. In contrast to the general case treated in Section 4.2, the lowermost row of blocks in Figure 7d, in the orthogonal case, are member of the same O(2) group as the other blocks. The same is valid for the special unitary groups $\mathrm{SU}(m)$ with $n(m) = m^2 - 1$, depicted by (su) in Figure 9.

Figure 9. Illustration of the necessary conditions for a Birkhoff-like (10) and for a "cosine-sine"-like (12) architecture. The parameter regions (B, C) for (10) & (12) are given by respectively dark gray and light gray domains, for four different values of the parameter A. Several examples of matrix groups are placed in the plots: symmetric groups (s), Heisenberg groups (h), orthogonal groups (o), unitary groups (u), and special unitary groups (su). It should be noted that, for case $A = 0$, conditions (10) (*i.e.*, dark gray) imply (12) (*i.e.*, light gray).



6. Conclusions

An arbitrary classical reversible computer can be decomposed into $2w - 1$ controlled NOT gates. In a similar way, an arbitrary quantum computer can be decomposed into $2^w - 1$ control circuits (either controlled ROTATOR circuits, or controlled NEGATOR circuits, or ...). Whereas the reversible circuit decomposition is based on the Birkhoff decomposition of doubly stochastic matrices, the quantum circuit decomposition is based on the cosine-sine decomposition of unitary matrices. Lie groups, other than the unitary groups, may either profit of similar decompositions or not, depending on their dimension.

References and Notes

1. Shor, P. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.* **1997**, *26*, 1484–1509.
2. Grover L. Quantum mechanics helps in searching for a needle in a haystack. *Phys. Rev. Lett.* **1997**, *79*, 325–328.

3. Deutsch, D.; Jozsa, R. Rapid solution of problems by quantum computation. *Proc. R. Soc. London Ser. A* **1992**, *439*, 553–558.
4. Landauer, R. Irreversibility and heat generation in the computational process. *IBM J. Res. Dev.* **1961**, *5*, 183–191.
5. Keyes, R.; Landauer, R. Minimal energy dissipation in logic. *IBM J. Res. Dev.* **1970**, *14*, 153–157.
6. Markov, I. An introduction to reversible circuits. In *Proceedings of the 12th International Workshop on Logic and Synthesis*, Laguna Beach, CA, USA, May 2003; pp. 318–319.
7. De Vos, A.; Van Rentergem, Y. From group theory to reversible computers. *Int. J. Unconv. Comput.* **2007**, *4*, 79–88.
8. Hayes, B. Reverse engineering. *Am. Sci.* **2006**, *94*, 107–111.
9. Wille, R.; Drechsler, R. *Towards a Design Flow for Reversible Logic*; Springer: Dordrecht, The Netherlands, 2010.
10. De Vos, A. *Reversible Computing*; Wiley-VCH: Weinheim, Germany, 2010.
11. Kerntopf P. Research on reversible computation in the year 2010. In *Proceedings of the 3rd Reversible Computation Workshop*, Gent, Belgium, July 2011.
12. Wille, R.; Drechsler, R. BDD-based synthesis of reversible logic for large functions. In *Proceedings of the 46th Design Automation Conference*, San Francisco, CA, USA, July 2009; pp. 270–275.
13. Thus a *measurement* of these (qu)bits before or after the computation would lead to the same results.
14. Möttönen, M.; Vartiainen, J.; Bergholm, V.; Salomaa, M. Quantum circuits for general multi-qubit gates. *Phys. Rev. Lett.* **2004**, *93*, 130502.
15. Bergholm, V.; Vartiainen, J.; Möttönen, M.; Salomaa, M. Quantum circuits with uniformly controlled one-qubit gates. *Phys. Rev. A* **2005**, *71*, 052330.
16. De Vos, A.; Van Rentergem, Y. Young subgroups for reversible computers. *Adv. Math. Commun.* **2008**, *2*, 183–200.
17. Here the infinity sign ∞ refers to the cardinality of the real numbers, *i.e.*, to an uncountable infinity. As an $m \times m$ complex matrix has m^2 comples entries, there are ∞^{2m^2} such matrices. The unitarity condition, however, introduces m^2 restrictions, leaving m^2 degrees of freedom and hence ∞^{m^2} such matrices.
18. De Vos, A.; Van Rentergem, Y. Networks for reversible logic. In *Proceedings of the 8th International Workshop on Boolean Problems*, Freiberg, Germany, September 2008; pp. 41–47.
19. De Vos, A.; De Baerdemacker, S. Linear reversible computing: Digital versus analog. *Int. J. Unconv. Comput.* **2010**, *6*, 239–263.
20. Bhatia, R. *Matrix Analysis*; Springer: New York, NY, USA, 1997; pp. 195–203.
21. Khan, F.; Perkowski, M. Synthesis of ternary quantum logic circuits by decomposition. In *Proceedings of the 7th International Symposium on Representations and Methodology of Future Computing Technologies*, Tokyo, Japan, September 2005; pp. 114–118.
22. Slepoy, A. *Quantum Gate Decomposition Algorithms*; Sandia Report, SAND2006-3440; Sandia National Laboratories: Albuquerque, NM, USA, 2006.
23. Shende, V.; Bullock, S.; Markov, I. Synthesis of quantum-logic circuits. *IEEE Trans. Comput. Aided Des. Integr. Circuits Syst.* **2006**, *25*, 1000–1010.

24. Nakajima, Y.; Kawano, Y.; Sekigawa, H. A new algorithm for producing quantum circuits using *KAK* decompositions. *Quantum Inf. Comput.* **2006**, *6*, 67–80.
25. Gilmore, R. *Lie Groups, Lie Algebras and Some of Their Applications*; John Wiley & Sons: New York, NY, USA, 1974.
26. Hall, B. *Lie Groups, Lie Algebras, and Representations*; Springer: New York, NY, USA, 2003; pp. 18–25.
27. Golub, G.; Van Loan, C. *Matrix Computations*; John Hopkins University Press: Baltimore, MD, USA, 1996; pp. 75–79.
28. Barenco, A.; Bennett, C.; Cleve, R.; DiVincenzo, D.; Margolus, N.; Shor, P.; Sleator, T.; Smolin, J.; Weinfurter, H. Elementary gates for quantum computation. *Phys. Rev. A* **1995**, *52*, 3457–3467.
29. Gasiorowicz, S. *Quantum Physics*; John Wiley: New York, NY, USA, 1974; p. 232.
30. Deutsch, D. Quantum computation. *Phys. World* **1992**, *5*, 57–61.
31. Deutsch, D.; Ekert, A.; Lupacchini, R. Machines, logic and quantum physics. *Bull. Symbolic Log.* **2000**, *3*, 265–283.
32. Galindo, A.; Martín-Delgado, M. Information and computation: Classical and quantum aspects. *Rev. Mod. Phys.* **2002**, *74*, 347–423.
33. Miller, D. Decision diagram techniques for reversible and quantum circuits. In *Proceedings of the 8th International Workshop on Boolean Problems*, Freiberg, Germany, September 2008; pp. 1–15.

Appendix

A. Proof of a Theorem in Combinatorics

We assume p and q are integers, satisfying $p \geq 2$ and $q \geq 1$. We prove that

$$(p!)^{2q}\,(q!)^{p} > (pq)! \tag{13}$$

by induction in q:

A1. The hypothesis holds for $q = 1$, because $(p!)^2$ is larger than $p!$.

A2. We assume that (13) holds for $q = Q$. Then:

$$\begin{aligned}
& (p!)^{2(Q+1)}\,[(Q+1)!]^{p} \\
= \;& (p!)^{2Q}\,(Q!)^{p}\,(Q+1)^{p}\,(p!)^{2} \\
> \;& (pQ)!\,(Q+1)^{p}(p!)^{2} \\
= \;& \frac{[p(Q+1)]!}{(pQ+1)(pQ+2)...(pQ+p)}\,(Q+1)^{p}\,(p!)^{2} \\
\geq \;& [p(Q+1)]!\,\frac{(Q+1)^{p}\,p^{p}}{(pQ+1)(pQ+2)...(pQ+p)} \\
= \;& [p(Q+1)]!\,\frac{pQ+p}{pQ+1}\,\frac{pQ+p}{pQ+2}\cdots\frac{pQ+p}{pQ+p} \\
> \;& [p(Q+1)]!
\end{aligned}$$

such that (13) also holds for $q = Q + 1$. Note that in the $\geq$ step above, we have taken advantage of the property that $(p!)^2 \geq p^p$. This, in turn, is a consequence of

$$(p!)^2 = [1.p][2.(p-1)][3.(p-2)]...[(p-1).2][p.1]$$

where all p factors of the right-hand side (except the first one and the last one) are larger than p.

A3. Because of A1 and A2, the hypothesis is true for all $q \geq 1$.

B. Lie Algebra of U(2)

An arbitrary 2×2 matrix with complex entries has eight real parameters:

$$\begin{pmatrix} a\exp(i\alpha) & b\exp(i\beta) \\ c\exp(i\gamma) & d\exp(i\delta) \end{pmatrix}$$

By imposing unitarity, we obtain 4 constraints for the 8 parameters a, b, c, d, α, β, γ, and δ, leaving only four degrees of freedom for a member of the unitary group U(2):

$$\begin{pmatrix} a\exp(i\alpha) & b\exp(i\beta) \\ b\exp(i\gamma) & a\exp(-i\alpha + i\beta + i\gamma + i\pi) \end{pmatrix}_{a^2+b^2=1}$$

By performing the substitution

$$\begin{aligned} \alpha &= u + w \\ \beta &= v + w \\ \gamma &= -v + w - \pi \end{aligned}$$

we obtain [26]

$$\begin{aligned} U &= \begin{pmatrix} a\exp(iu+iw) & b\exp(iv+iw) \\ -b\exp(-iv+iw) & a\exp(-iu+iw) \end{pmatrix}_{a^2+b^2=1} \\ &= \begin{pmatrix} \exp(iw) & 0 \\ 0 & \exp(iw) \end{pmatrix} \begin{pmatrix} a\exp(iu) & b\exp(iv) \\ -b\exp(-iv) & a\exp(-iu) \end{pmatrix}_{a^2+b^2=1} \end{aligned} \quad (14)$$

i.e., a product of two commutating matrices, the former representing a group isomorphic to U(1), the latter representing the special unitary group SU(2). Often [28], a further decomposition (into three non-commuting matrices) is performed:

$$\begin{pmatrix} a\exp(iu) & b\exp(iv) \\ -b\exp(-iv) & a\exp(-iu) \end{pmatrix}_{a^2+b^2=1} =$$

$$\begin{pmatrix} \exp(i\,\frac{u+v}{2}) & 0 \\ 0 & \exp(-i\,\frac{u+v}{2}) \end{pmatrix} \begin{pmatrix} \cos(z) & \sin(z) \\ -\sin(z) & \cos(z) \end{pmatrix} \begin{pmatrix} \exp(i\,\frac{u-v}{2}) & 0 \\ 0 & \exp(-i\,\frac{u-v}{2}) \end{pmatrix} \quad (15)$$

where the substitution $a = \cos(z)$ has been performed.

The above two decompositions are strongly related to the algebra of the Lie group U(2). The algebra u(2) is a space spanned by the four generators

$$\begin{aligned}\sigma_0 &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\ \sigma_1 &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ \sigma_2 &= \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \\ \sigma_3 &= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\end{aligned}$$

i.e., the four Pauli matrices [25,26,29]. The generator σ_0 commutes with each of the three others, emphasizing that U(2) is a direct product of SU(2) and a group isomorphic to U(1). Straightforward computation leads to the remaining commutators:

$$[\sigma_1, \sigma_2] = 2i\sigma_3 \qquad [\sigma_2, \sigma_3] = 2i\sigma_1 \qquad [\sigma_3, \sigma_1] = 2i\sigma_2$$

The exponential maps $U_k = \exp(ix\sigma_k)$ are:

$$\begin{aligned}U_0(x) &= \begin{pmatrix} \exp(ix) & 0 \\ 0 & \exp(ix) \end{pmatrix} \\ U_1(x) &= \begin{pmatrix} \cos(x) & i\sin(x) \\ i\sin(x) & \cos(x) \end{pmatrix} \\ U_2(x) &= \begin{pmatrix} \cos(x) & \sin(x) \\ -\sin(x) & \cos(x) \end{pmatrix} \\ U_3(x) &= \begin{pmatrix} \exp(ix) & 0 \\ 0 & \exp(-ix) \end{pmatrix}\end{aligned}$$

The above decomposition (14-15) can be rewritten as

$$U(u,v,w,z) = U_0(w)\, U_3(\frac{u+v}{2})\, U_2(z)\, U_3(\frac{u-v}{2})$$

Equally valid is the decomposition

$$U(u,v,w,z) = U_0(w)\, U_3(\frac{u+v}{2} - \frac{\pi}{4})\, U_1(z)\, U_3(\frac{u-v}{2} + \frac{\pi}{4})$$

C. NEGATORs

We introduce a linear combination of two of the four generators of u(2):

$$\sigma = \sigma_0 - \sigma_1 = \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$$

Its exponential mapping is

$$D = \exp(i\phi\sigma) = \begin{pmatrix} \cos(\phi)\exp(i\phi) & -i\sin(\phi)\exp(i\phi) \\ -i\sin(\phi)\exp(i\phi) & \cos(\phi)\exp(i\phi) \end{pmatrix}$$

As σ_0 and σ_1 commute, it is no surprise that D can be written as a product of a U_0-matrix and a U_1-matrix. And indeed we have

$$D(\phi) = U_0(\phi)\, U_1(-\phi)$$

The matrices D form a 1-dimensional space, containing four particular points:

- The identity matrix (representing the 1-qubit follower) is recovered by setting $\phi = 0$:

$$D(0) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

- The 1-qubit NOT gate is recovered by setting $\phi = \pi/2$:

$$D(\pi/2) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

- The notorious square-root of NOT [30–33] is found by choosing $\phi = \pi/4$:

$$D(\pi/4) = \frac{1}{2}\begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix}$$

- Finally, the 'other' square-root of NOT is found by $\phi = -\pi/4$:

$$D(-\pi/4) = \frac{1}{2}\begin{pmatrix} 1-i & 1+i \\ 1+i & 1-i \end{pmatrix}$$

For an arbitrary value of ϕ, the matrix D may be interpreted either as a quantum superposition of the identity and the NOT :

$$D(\phi) = \cos(\phi)\exp(i\phi)\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + [\,1 - \cos(\phi)\exp(i\phi)\,]\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

or as a root of NOT :

$$D(\pi/2n) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{1/n}$$

In analogy to the name ROTATOR for $C(\theta)$, we call $D(\phi)$ the NEGATOR.

It may be noted that other choices σ of the generators will lead towards other realizations of the U(2) transformations and it will depend on the physical implementation which one will be the preferred one in future developments.