The NEGATOR as a basic building block for quantum circuits

Alexis De Vos[1] and Stijn De Baerdemacker[2*]
[1]Imec v.z.w. and vakgroep elektronica en informatiesystemen,
Universiteit Gent, B - 9000 Gent, Belgium
alex@elis.ugent.be
[2] Center for Molecular Modeling,
vakgroep fysica en sterrenkunde,
Universiteit Gent, B - 9000 Gent, Belgium
Stijn.DeBaerdemacker@ugent.be

December 11, 2012

Abstract

Between (classical) reversible computation and quantum computation exists an intermediate computational world, represented by unitary matrices that have all line sums equal to 1. All of these quantum circuits can be synthesized with the help of merely two building blocks: the NEGATOR and the singly controlled square root of NOT.

1 Introduction

Quantum computing [1] [2] has become a well-established branch of computer science. A remarkable feature of quantum circuits is that they are reversible, i.e. it is possible to trace back any final state of a quantum computation to the initial state without any loss of information. This is important from an information point of view, because heat dissipation into the system due to the Landauer principle [1] [3] [4] is avoided during the process. Reversibility is a fundamental property of group theory; so it is natural to express quantum circuits as well as classical reversible circuits in a group-theoretical language. Whereas a quantum circuit acting on w qubits is represented by an $n \times n$ unitary matrix, a classical reversible circuit acting on w bits is represented by an $n \times n$ permutation matrix, where n is a short-hand notation for 2^w. The $n \times n$ unitary matrices form a continuous group, i.e. the n^2-dimensional Lie group $\mathrm{U}(n)$, called the unitary group. The $n \times n$ permutation matrices form the finite group $\mathrm{P}(n)$,

*SDB is an 'FWO-Vlaanderen' post-doctoral fellow.

isomorphic to the symmetric group $\mathbf{S}_n$ of order $n!$. It is clear that $\mathrm{P}(n)$ is a trivial subgroup of the unitary matrices in $\mathrm{U}(n)$, and moreover there is a vast world between $\mathrm{P}(n)$ and $\mathrm{U}(n)$, which has largely been left unexplored up to present. The motivation of this work is to investigate the properties of a potential quantum computer, living in a smaller and less powerful space as the full-fledged $\mathrm{U}(n)$ quantum computer, but with the salient features of quantum mechanics, lacking in classical reversible computers in $\mathrm{P}(n)$. In other words, we search for those groups that are both subgroups of $\mathrm{U}(n)$ and supergroups of $\mathrm{P}(n)$, while retaining a meaningful interpretation as computation group on a w-qubit system. In the quest for such a group, inspiration can be found in decomposition approaches for quantum circuits [5] or classical circuits [4]. These approaches start with a limited set of elementary (quantum) gates and generate a larger group by concatenation of these elementary building blocks. In the present paper, the `NEGATOR` [6] [7] and its controlled version, is selected as elementary quantum gate. On the one hand, from a subgroup point of view, the `NEGATOR` is a 1-dimensional subgroup of the unitary U(2) group acting on 1-qubit systems. On the other hand, from a supergroup point of view, the `NEGATOR` connects the `IDENTITY` gate (or follower or unity) and the classical `NOT` gate by means of a 1-parameter group. It is found that a concatenation of (controlled) `NEGATOR`s generates a group $\mathrm{V}(n)$ which is isomorphic to the unitary group with line sum equal to 1, which in its turn is isomorphic to $\mathrm{U}(n-1)$. In the next section, we introduce the `NEGATOR` and its relation to U(2) and P(2) with respect to 1-(qu)bit systems. In the subsequent section, we change gears by constructing the generated group $\mathrm{V}(n)$ of w-qubit systems. In Section 4, we prove that the `NEGATOR` gate, extendend with the singly-controlled square root of `NOT` is universal for $\mathrm{V}(n)$, and we present our conclusions in Section 5.

2 Single-qubit circuits

For $w = 1$, we have $n = 2$. There exist only two matrices in the group P(2):

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ and } \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

representing the `IDENTITY` gate and the `NOT` gate, respectively. In contrast, the group U(2) has ∞^4 members:

$$\exp(i\theta_0) \begin{pmatrix} \exp(i\theta_1 + i\theta_3)\cos(\theta_2) & \exp(i\theta_1 - i\theta_3)\sin(\theta_2) \\ -\exp(-i\theta_1 + i\theta_3)\sin(\theta_2) & \exp(-i\theta_1 - i\theta_3)\cos(\theta_2) \end{pmatrix},$$

where θ_0, θ_1, θ_2, and θ_3 are the four real parameters.

In between the 0-dimensional group P(2) and the 4-dimensional group U(2), we introduce a 1-dimensional group by interpolating between `IDENTITY` and `NOT`:

$$(1-t)\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + t\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

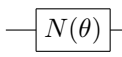
The resulting matrix is unitary iff

$$t = \frac{1}{2}\ [\ 1 - \exp(i\theta)\ ]\ ,$$

leading to the 1-dimensional group of matrices

$$N(\theta) = \frac{1}{2}\begin{pmatrix} 1+\exp(i\theta) & 1-\exp(i\theta) \\ 1-\exp(i\theta) & 1+\exp(i\theta) \end{pmatrix} = \exp(i\theta/2)\begin{pmatrix} \cos(\theta/2) & -i\sin(\theta/2) \\ -i\sin(\theta/2) & \cos(\theta/2) \end{pmatrix}\ ,$$

representing the quantum operation called the NEGATOR [6] [7], with symbol



.

This quantum gate should not be confused with any of the three well-known unitary transformations called the ROTATORs [2]:

$$R_x(\theta) = \begin{pmatrix} \cos(\theta) & -i\sin(\theta) \\ -i\sin(\theta) & \cos(\theta) \end{pmatrix}\ ,$$

$$R_y(\theta) = \begin{pmatrix} \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & \cos(\theta) \end{pmatrix} \text{ and } R_z(\theta) = \begin{pmatrix} \exp(i\theta) & 0 \\ 0 & \exp(-i\theta) \end{pmatrix}\ .$$

The 2×2 matrices $N(\theta)$ form a group V(2), simultaneously a supergroup of P(2) and a subgroup of U(2):

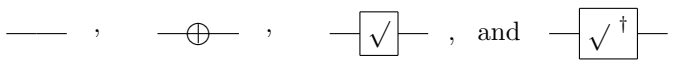
$$\mathrm{P}(2) \subset \mathrm{V}(2) \subset \mathrm{U}(2)\ .$$

Whereas the matrices of U(2) are merely unitary, each matrix of V(2) satisfies an extra restriction: all its line sums (i.e. its two row sums and its two column sums) are equal to 1. Conversely, each 2×2 unitary matrix with all line sums equal to 1 is in V(2). Whereas U(2) fills a 4-dimensional space, V(2) is only a 1-dimensional subspace. The group V(2) is isomorphic to U(1). Whereas U(1) is generated by the single 1×1 matrix (1), V(2) is generated by the 2×2 matrix $\tau = \frac{1}{2}\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$, generating all members $\exp(i\theta\tau)$ of V(2). We have $\mathrm{trace}(\tau) = 1$ and therefore $\det(N) = \exp(i\theta)$.

For the particular values $\theta = 0$, $\theta = \pi$, $\theta = \pi/2$, and $\theta = 3\pi/2$, the NEGATOR becomes the IDENTITY, the NOT, the square root of NOT, and the 'other' square root of NOT, respectively:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},\ \frac{1}{2}\begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix},\ \text{and}\ \frac{1}{2}\begin{pmatrix} 1-i & 1+i \\ 1+i & 1-i \end{pmatrix},$$

with respective symbols



.

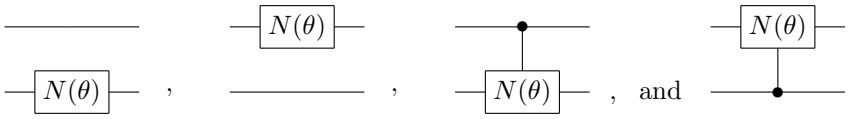
The former two transformations are classical logic gates; the latter two are quantum gates. For an arbitrary value of θ, we may write

$$\texttt{NEGATOR}(\theta) = \texttt{NOT}^{\,\theta/\pi} \ .$$

In particular, the $\sqrt{\texttt{NOT}}$ is an interesting addition to classical reversible circuits, as it allows for the decomposition of any classical computer using only a library of 2-qubit building blocks [8]. This is in contrast to purely classical libraries, where building blocks only become universal at the 3-bit level, such as e.g. the Toffoli gate [4] [9].

3 Multiple-qubit circuits

For $w = 2$, we have $n = 4$. The one-qubit gate $N(\theta)$ naturally leads to four different 2-qubit building blocks:



(1)

The former two are NEGATORs; the latter two are 'controlled NEGATORs'. They are represented by the four 4×4 unitary matrices

$$\frac{1}{2}\begin{pmatrix} 1+e & 1-e & 0 & 0 \\ 1-e & 1+e & 0 & 0 \\ 0 & 0 & 1+e & 1-e \\ 0 & 0 & 1-e & 1+e \end{pmatrix}, \frac{1}{2}\begin{pmatrix} 1+e & 0 & 1-e & 0 \\ 0 & 1+e & 0 & 1-e \\ 1-e & 0 & 1+e & 0 \\ 0 & 1-e & 0 & 1+e \end{pmatrix},$$

$$\frac{1}{2}\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 1+e & 1-e \\ 0 & 0 & 1-e & 1+e \end{pmatrix}, \text{ and } \frac{1}{2}\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 1+e & 0 & 1-e \\ 0 & 0 & 2 & 0 \\ 0 & 1-e & 0 & 1+e \end{pmatrix},$$

where e is a short-hand notation for $\exp(i\theta)$. Each of these four 4×4 matrices represents a 1-dimensional subspace of the 16-dimensional Lie group U(4).

We note that each of these four matrices has all eight line sums equal to 1. The reader will easily realize that a similar property holds for $w > 2$. Any NEGATOR and any controlled NEGATOR, either controlled by a single line or by multiple lines (up to $w - 1$ lines), either with positive-polarity controls or with negative-polarity controls, give rise to unitary $2^w \times 2^w$ matrices with all 2^{w+1} line sums equal to 1. It therefore is very useful to investigate in detail the $n \times n$ unitary matrices with all $2n$ line sums equal to 1. They form a group, as the product of two such matrices again yields such matrix. They thus form a subgroup of the n^2-dimensional Lie group U(n). We denote the group by V(n). Below, we prove that V(n) is an $(n-1)^2$-dimensional subgroup of U(n), isomorphic to U($n-1$). For this purpose, we note that any generator of V(n)

has to be an $n \times n$ Hermitian matrix with all $2n$ line sums equal to zero[1]. E.g. the four above subgroups of V(4) are generated by the 4×4 Hermitian matrices

$$\begin{pmatrix} 1 & -1 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & -1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \\ -1 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & -1 & 1 \end{pmatrix}, \text{ and } \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 1 \end{pmatrix},$$

respectively.

Let $a_1, a_2, ..., a_q$ be Hermitian matrices forming an algebra with structure constants C_{jkl}:

$$[a_j, a_k] = \sum_l C_{jkl} a_l \ .$$

Then,

$$b_1 = \begin{pmatrix} 0 & \mathbf{0}^T \\ \mathbf{0} & a_1 \end{pmatrix}, \ b_2 = \begin{pmatrix} 0 & \mathbf{0}^T \\ \mathbf{0} & a_2 \end{pmatrix}, ..., \ b_q = \begin{pmatrix} 0 & \mathbf{0}^T \\ \mathbf{0} & a_q \end{pmatrix} \ ,$$

where $\mathbf{0}$ is the zero column vector, also form an algebra, with the same structure constants, because

$$\begin{pmatrix} 0 & \mathbf{0}^T \\ \mathbf{0} & a_j \end{pmatrix} \begin{pmatrix} 0 & \mathbf{0}^T \\ \mathbf{0} & a_k \end{pmatrix} = \begin{pmatrix} 0 & \mathbf{0}^T \\ \mathbf{0} & a_j a_k \end{pmatrix} \ .$$

One can easily check the following property: if Y is a Hermitian matrix, then also TYT^{-1} is Hermitian, iff T is a unitary matrix (of the same size). Therefore, if T is a unitary matrix of the same size as the matrices b_j, then the conjugate matrices Tb_jT^{-1} also form an algebra with the same structure constants, because

$$[Tb_jT^{-1}, Tb_kT^{-1}] = T\,[b_j, b_k]\,T^{-1} \ .$$

As a result, the $(n-1) \times (n-1)$-dimensional generators $a_1, a_2, ..., a_{(n-1)^2}$ of U$(n-1)$ lead to $n \times n$ generators

$$c_j = T \begin{pmatrix} 0 & \mathbf{0}^T \\ \mathbf{0} & a_j \end{pmatrix} T^{-1} \ ,$$

where $\mathbf{0}$ stands for the $(n-1) \times 1$ zero matrix. It now suffices to find an $n \times n$ unitary matrix T, such that all $(n-1)^2$ new generators c_j have constant line sum equal to 0, i.e. such that

$$\sum_m (c_j)_{km} = 0 \ \text{ and } \ \sum_k (c_j)_{km} = 0 \ . \tag{2}$$

[1] If a unitary matrix M is the exponential map of a Hermitian matrix μ, i.e. if $M = \exp(i\theta\mu)$, then a constant line sum $\mathrm{Sum}(\mu)$ for μ automatically implies a constant line sum $\mathrm{Sum}(M)$ for M and vice versa, with the relation $\mathrm{Sum}(M) = \exp(i\theta\ \mathrm{Sum}(\mu))$, an expression reminiscent of the well-known relation $\mathrm{Det}(M) = \exp(i\theta\,\mathrm{Trace}(\mu))$. In particular, $\mathrm{Sum}(M) = 1$ leads to $\mathrm{Sum}(\mu) = 0$ and vice versa.

E.g. the latter condition leads to

$$\sum_k \sum_p \sum_q T_{kp} \; (b_j)_{pq} \; (T^{-1})_{qm} = 0$$

and thus to

$$\sum_{p \neq 1} \sum_{q \neq 1} (b_j)_{pq} \; (T^{-1})_{qm} \sum_k T_{kp} = 0 \; .$$

As this condition must be fulfilled for each matrix a_j, we need (for all $p \neq 1$ and $q \neq 1$) that

$$(T^{-1})_{qm} \sum_k T_{kp} = 0 \; .$$

For this purpose, it is sufficient that

$$\sum_k T_{kp} = 0 \text{ for all } p \neq 1 \; . \tag{3}$$

The former condition in (2) leads to a similar sufficient condition:

$$\sum_p (T^{-1})_{kp} = 0 \text{ for all } k \neq 1 \; . \tag{4}$$

Because T is unitary, it fulfils (4) as soon as it fulfils (3). The question remains whether, for an arbitrary integer n, an $n \times n$ unitary matrix with property (3) exists[2]. The fact that

- the second and all following columns of T are perpendicular to each other,
- the vector $(1, 1, 1, ..., 1)^T$ is perpendicular to all these $(n-1)$ vectors (because their column sums equal 0), and
- the first column has to be perpendicular to all these $(n-1)$ vectors,

leads to the conclusion that the first column of T is necessarily equal to $(1, 1, 1, ..., 1)^T$, up to a constant $(1/\sqrt{n}\,)\, \exp(i\alpha)$. The question remains whether there exists such an $n \times n$ unitary matrix, with constant-entry first column and subsequent zero-sum columns. The answer is yes, as all dephased complex $n \times n$ Hadamard matrices [11] have all column sums equal to 0 except the first column sum equal to $\sqrt{n}\,$.

For arbitrary n, we can choose (among the complex Hadamards) the $n \times n$ Fourier transform. E.g. for $n = 3$, the Fourier transform

$$F = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix} \; ,$$

[2]Such existence is not obvious, as e.g. unitary matrices with all column sums (i.e. $p = 1$ included) equal 0 do not exist. Indeed, if a unitary matrix has constant column sum, then this sum is on the unit circle of the complex plane [10].

where ω is the cubic root of unity, i.e. $\omega = -1/2 + i\sqrt{3}/2$, transforms the four Pauli matrices

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

generators of U(2), into the four matrices τ_j generating V(3):

$$\tau_j = F \begin{pmatrix} 0 & \mathbf{0}^T \\ \mathbf{0} & \sigma_j \end{pmatrix} F^{-1} \qquad \text{for } j \in \{0,1,2,3\} \ .$$

Appendix A gives more details about the resulting group V(3).

For $n = 4$, we can choose for T a real Hadamard matrix, e.g.

$$T = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \end{pmatrix} .$$

An example is the transformation of the nine Gell-Mann matrices [12]

$$\mu_0 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \ \mu_1 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \ \mu_2 = \begin{pmatrix} 0 & -i & 0 \\ i & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \ \mu_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \ \mu_4 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix},$$

$$\mu_5 = \begin{pmatrix} 0 & 0 & -i \\ 0 & 0 & 0 \\ i & 0 & 0 \end{pmatrix}, \ \mu_6 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \ \mu_7 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & -i \\ 0 & i & 0 \end{pmatrix}, \text{ and } \mu_8 = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -2 \end{pmatrix},$$

generators of U(3), into the nine generators of V(4), presented in Reference [7]. We obtain e.g.

$$\begin{aligned} T \begin{pmatrix} 0 & \mathbf{0}^T \\ \mathbf{0} & \mu_2 \end{pmatrix} T^{-1} &= \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & -i & 0 \\ 0 & i & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \end{pmatrix} \\ &= \frac{1}{2} \begin{pmatrix} 0 & 0 & -i & i \\ 0 & 0 & i & -i \\ i & -i & 0 & 0 \\ -i & i & 0 & 0 \end{pmatrix} = \tau_2 \ . \end{aligned}$$

Appendix B gives more details about the resulting group V(4).

For arbitrary n, we choose an appropriate set of generators of U$(n-1)$, e.g. the generalized Pauli matrices, the generalized Gell-Mann matrices, or the generalized Dirac matrices, and construct with them the $(n-1)^2$ generators τ_j (with $j \in \{0,1,2,...,(n-1)^2-1\}$) of V$(n)$. Among these matrices, $(n-1)^2-1$ have trace 0. They generate the $((n-1)^2-1)$-dimensional subgroup SV(n) of

$\mathrm{V}(n)$, consisting of the $\mathrm{V}(n)$-elements with unit determinant. The full group $\mathrm{V}(n)$ has one additional generator, i.e. the idempotent circulant matrix

$$\tau_0 = \frac{1}{n} \begin{pmatrix} n-1 & -1 & -1 & ... & -1 \\ -1 & n-1 & -1 & ... & -1 \\ ... & & & & \\ -1 & -1 & -1 & ... & n-1 \end{pmatrix} ,$$

with trace $n-1$, generating the 1-dimensional matrix group

$$V_0(\theta) = \frac{1}{n} \begin{pmatrix} 1+(n-1)e & 1-e & 1-e & ... & 1-e \\ 1-e & 1+(n-1)e & 1-e & ... & 1-e \\ & ... & & & \\ 1-e & 1-e & 1-e & ... & 1+(n-1)e \end{pmatrix} .$$

This corresponds to the well-known group decomposition

$$\mathrm{U}(n-1) = \mathrm{SU}(n-1) \otimes \mathrm{U}(1) ,$$

which translates here into

$$\mathrm{V}(n) = \mathrm{SV}(n) \otimes \mathrm{U}(1) .$$

The matrix $V_0(\theta)$ has determinant $e^{n-1} = \exp((n-1)i\theta)$. The particular matrix with determinant equal to -1 thus is $V_0(\frac{\pi}{n-1})$. If n is even, then also

$$V_0(\pi) = \frac{1}{n} \begin{pmatrix} 2-n & 2 & 2 & ... & 2 \\ 2 & 2-n & 2 & ... & 2 \\ ... & & & & \\ 2 & 2 & 2 & ... & 2-n \end{pmatrix} ,$$

has determinant equal to -1. This matrix is called 'almost Hadamard' [13]. One easily verifies that it can be written as the Hadamard-conjugate of a diagonal matrix:

$$T \begin{pmatrix} 1 & 0 & 0 & ... & 0 \\ 0 & -1 & 0 & ... & 0 \\ 0 & 0 & -1 & ... & 0 \\ ... & & & & \\ 0 & 0 & 0 & ... & -1 \end{pmatrix} T^{-1} ,$$

where T is allowed to be any dephased complex Hadamard matrix. We note that, for $n = 2^w$, the matrix $V_0(\pi)$ is nothing else but the Grover diffusion operator, which plays a pivotal role in Grover's quantum search algorithm [2] [14].

We now focus on the cases $n = 2^w$, where the positive integer w is the width of the quantum circuit. Also for $n = 2^w$ with arbitrary w, we can choose T from the real Hadamard matrices. This has the great advantage that one of them can be written as the tensor product of w small (i.e. 2×2) Hadamard matrices:

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes ... \otimes \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}^{\otimes w}$$

and thus can be implemented by w single-qubit gates. E.g., for $w = 2$, we have

$$H = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} .$$

The w-qubit Fourier circuit lacks this useful property.

Above, we have demonstrated that with each generator of $\mathrm{U}(n-1)$ corresponds one generator of $\mathrm{V}(n)$, by adding a zero row and a zero column and conjugating under an appropriate Hadamard matrix T. Conversely, by conjugating a generator of $\mathrm{V}(n)$ under T^{-1} (resulting automatically in a matrix with a zero row in top and a zero column to the left) and subsequently deleting the zero row and the zero column, we demonstrate that with each generator of $\mathrm{V}(n)$ corresponds one generator of $\mathrm{U}(n-1)$. By thus establishing a 1-to-1 mapping between $\mathfrak{u}(n-1)$ and $\mathfrak{v}(n)$, the isomorphism is proved.

Because of the well-known theorem

$$\exp(i\,\theta\,XYX^{-1}) = X\ \exp(i\,\theta\,Y)\ X^{-1}$$

and because

$$\exp(i\,\theta \begin{pmatrix} 0 & \mathbf{0}^T \\ \mathbf{0} & a \end{pmatrix}) = \begin{pmatrix} 1 & \mathbf{0}^T \\ \mathbf{0} & \exp(i\,\theta\,a) \end{pmatrix} ,$$

not only the generators of $\mathrm{V}(n)$ and $\mathrm{U}(n-1)$ can be converted into one another, but also the group members. Hadamard conjugation thus allows to relate a group member V of $\mathrm{V}(2^w)$ to a group member U of $\mathrm{U}(2^w-1)$:

$$V = H \begin{pmatrix} 1 & \mathbf{0}^T \\ \mathbf{0} & U \end{pmatrix} H$$

and vice versa:

$$\begin{pmatrix} 1 & \mathbf{0}^T \\ \mathbf{0} & U \end{pmatrix} = HVH , \tag{5}$$

where we have taken into account that $H^{-1} = H$.

4 A universality theorem

In the present Section, we prove the following theorem:

> The entire group $\mathrm{V}(2^w)$, isomorphic to $\mathrm{U}(2^w-1)$, can be generated by merely `NEGATOR`s and controlled $\sqrt{\texttt{NOT}}$s.

For $w = 1$, the theorem is trivial. For $w = 2$, the theorem is illustrated and proved in Appendix B. For $w > 2$, we consider an arbitrary member V of the Lie group $\mathrm{V}(2^w)$. We construct the corresponding $(2^w-1) \times (2^w-1)$ matrix U of $\mathrm{U}(2^w-1)$, by applying the 1-to-1 mapping of (5). According to Poźniak et al. [15], the matrix U can be decomposed into a product $U_0U_1U_2...U_m$ of

matrices, all belonging to one of the following four categories: the matrix U_0 equals $\exp(i\,\theta)$ times the $(2^w-1)\times(2^w-1)$ unit matrix (Category # 0), whereas all the other matrices (Categories # 1, # 2, and # 3) equal

- either a $(2^w-1)\times(2^w-1)$ permutation matrix,
- or a $(2^w-1)\times(2^w-1)$ matrix, consisting of
  - a 2×2 matrix
    $$\begin{pmatrix} \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & \cos(\theta) \end{pmatrix}$$
    in the lower-right corner,
  - ones on the 2^w-3 remaining diagonal places, and
  - zeroes in all $(2^w-1)^2-2^w-1$ remaining places,
- or a $(2^w-1)\times(2^w-1)$ matrix, consisting of
  - a 2×2 matrix
    $$\begin{pmatrix} \exp(i\,\theta) & 0 \\ 0 & \exp(-i\,\theta) \end{pmatrix}$$
    in the lower-right corner,
  - ones on the remaining diagonal places, and
  - zeroes in all remaining places.

We subsequently apply the reverse 1-to-1 mapping, in order to obtain a decomposition of the original $2^w\times 2^w$ matrix V:

$$\begin{aligned} V &= H\begin{pmatrix} 1 & \mathbf{0}^T \\ \mathbf{0} & U \end{pmatrix} H \\ &= H\begin{pmatrix} 1 & \mathbf{0}^T \\ \mathbf{0} & U_0 \end{pmatrix}\begin{pmatrix} 1 & \mathbf{0}^T \\ \mathbf{0} & U_1 \end{pmatrix}\ldots\begin{pmatrix} 1 & \mathbf{0}^T \\ \mathbf{0} & U_m \end{pmatrix} H \\ &= H\begin{pmatrix} 1 & \mathbf{0}^T \\ \mathbf{0} & U_0 \end{pmatrix} H\; H\begin{pmatrix} 1 & \mathbf{0}^T \\ \mathbf{0} & U_1 \end{pmatrix} H\;\ldots\; H\begin{pmatrix} 1 & \mathbf{0}^T \\ \mathbf{0} & U_m \end{pmatrix} H\ . \end{aligned}$$

If we have a synthesis for each factor $H\begin{pmatrix} 1 & \mathbf{0}^T \\ \mathbf{0} & U_j \end{pmatrix} H$ separately, then we are done. Therefore, we investigate each of the above four categories successively:

4.1 Category # 1

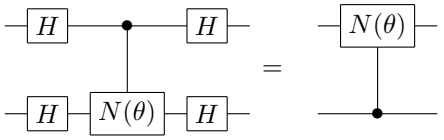
If U_j is a $(2^w-1)\times(2^w-1)$ permutation matrix, then $\begin{pmatrix} 1 & \mathbf{0}^T \\ \mathbf{0} & U_j \end{pmatrix}$ is a $2^w\times 2^w$ permutation matrix and thus represents a classical reversible circuit. Such circuit can, in turn, be decomposed into `NOT` gates and singly controlled k th roots of `NOT` [8]. We first investigate the latter gates, then the former ones:

4.1.1 Subcategory # 1a

A controlled root of NOT, under Hadamard conjugation, yields just another controlled root of NOT:

$$\frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \frac{1}{2}\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 1+e & 1-e \\ 0 & 0 & 1-e & 1+e \end{pmatrix} \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 1+e & 0 & 1-e \\ 0 & 0 & 2 & 0 \\ 0 & 1-e & 0 & 1+e \end{pmatrix},$$

where e stands for $\exp(i\pi/2^k)$ with integer k. This result is, by the way, merely a special case of the remarkable identity



where θ is allowed to have any real value. We thus end up with singly controlled roots of NOT, which are singly controlled NEGATORs. As singly controlled NEGATORs can be reduced to uncontrolled NEGATORs and singly controlled square roots of NOT (see Appendix B), we thus end up with a circuit containing merely NEGATORs and singly controlled square roots of NOT.

4.1.2 Subcategory # 1b

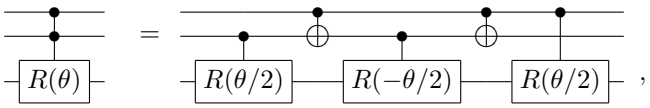
The uncontrolled NOT gives rise to problems when conjugated under a Hadamard:

$$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

i.e. a gate that cannot be synthesized with (controlled) NEGATORs, because not all its line sums are equal to 1. Fortunately, however, the circuit $\begin{pmatrix} 1 & \mathbf{0}^T \\ \mathbf{0} & U_j \end{pmatrix}$ is a $2^w \times 2^w$ permutation matrix of a special type. The 1 at the upper-left corner guarantees that decomposition of the reversible circuit according to the Miller–Maslov–Dueck algorithm [16] gives rise to a cascade without uncontrolled NOTs.

4.2 Categories # 2 and # 3

The two remaining matrix categories give rise to the circuits HRH, where H is the $2^w \times 2^w$ real Hadamard and R is either the $w-1$ times controlled R_y ROTATOR or the $w-1$ times controlled R_z ROTATOR. Now, it is well-known that multiply controlled ROTATORs can be replaced by singly-controlled ROTATORs. E.g. the doubly controlled ROTATOR is reduced to three singly controlled ROTATORs, by straightforward application of the notorious Lemma 6.1 of Reference [5]:

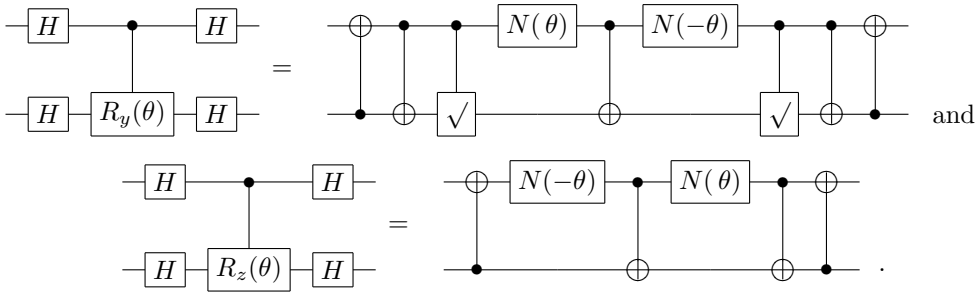


where R stands either for R_y or for R_z. Hence, we only have to demonstrate that the singly controlled ROTATORs (between two Hadamards) can be built from NEGATORs. Straigthforward calculations lead to

$$H \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & c & s \\ 0 & 0 & -s & c \end{pmatrix} H = \frac{1}{2} \begin{pmatrix} 1+c & -s & 1-c & s \\ s & 1+c & -s & 1-c \\ 1-c & s & 1+c & -s \\ -s & 1-c & s & 1+c \end{pmatrix} \text{ and}$$

$$H \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & e & 0 \\ 0 & 0 & 0 & 1/e \end{pmatrix} H = \frac{1}{2} \begin{pmatrix} 1+c & is & 1-c & -is \\ is & 1+c & -is & 1-c \\ 1-c & -is & 1+c & is \\ -is & 1-c & is & 1+c \end{pmatrix},$$

where c and s are short-hand notations for $\cos(\theta)$ and $\sin(\theta)$, respectively. The former result equals, up to a row and column permutation, the matrices $V_2(\theta)$ and $V_5(\theta)$ of Appendix B; the latter result equals, up to a row and column permutation, the matrix $V_3(\theta)$ of Appendix B. We thus may write these two results schematically:

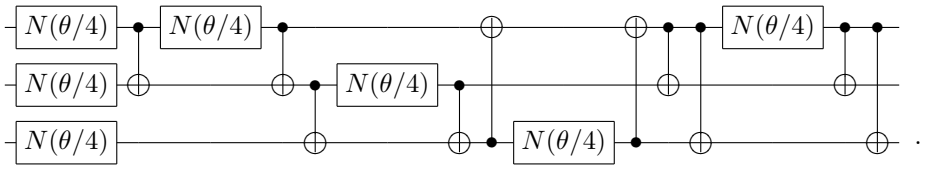


4.3 Category # 0

The matrix U_0, equal to e times the $(2^w-1)\times(2^w-1)$ unit matrix, yields the $2^w \times 2^w$ matrix $\begin{pmatrix} 1 & \mathbf{0}^T \\ \mathbf{0} & U_0 \end{pmatrix}$ consisting of a diagonal with one 1 and 2^w-1 numbers e. Its Hadamard conjugate is

$$V_0(\theta) = \frac{1}{2^w} \begin{pmatrix} 1+(2^w-1)e & 1-e & \ldots & 1-e \\ 1-e & 1+(2^w-1)e & \ldots & 1-e \\ \ldots & & & \\ 1-e & 1-e & \ldots & 1+(2^w-1)e \end{pmatrix}.$$

To implement such matrix with the help of NEGATORs is demonstrated in Appendix B for the case $w=2$. For $w=3$, we have the following decomposition:



For arbitrary w, a similar synthesis with $2^w - 1$ NEGATORs can be constructed. In order to convince ourselves that indeed a construction is possible, whatever the value of w, we may decompose U_0 into permutation matrices and diagonal matrices with only one non-unit entry, i.e. the number e in the most lower-right position. The former matrices are treated like in Section 4.1. The latter matrices are treated like in Section 4.2:

$$H \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e \end{pmatrix} H = \frac{1}{4} \begin{pmatrix} 3+e & 1-e & 1-e & -1+e \\ 1-e & 3+e & -1+e & 1-e \\ 1-e & -1+e & 3+e & 1-e \\ -1+e & 1-e & 1-e & 3+e \end{pmatrix}$$

$$= \frac{1}{4} V_3(\theta) \begin{pmatrix} 1+e & 1-e & 0 & 0 \\ 1-e & 1+e & 0 & 0 \\ 0 & 0 & 1+e & 1-e \\ 0 & 0 & 1-e & 1+e \end{pmatrix},$$

i.e. a NEGATOR followed by a V_3 circuit. As demonstrated in Appendix B, the latter can be constructed from two NEGATORs and two controlled NOTs. Finally, a controlled NOT can be decomposed into two controlled $\sqrt{\text{NOT}}$s.

This completes the proof: the NEGATOR (together with the controlled square root of NOT) indeed is a building block, sufficient to synthesize any member of the group V(n).

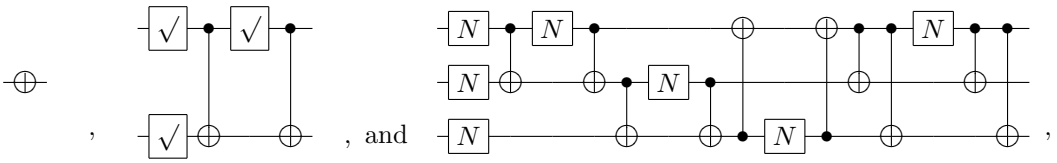
5 Conclusion

In a 'natural' way, we have constructed a group intermediate to the 0-dimensional permutation group P(n) and the n^2-dimensional unitary group U(n), i.e. the $(n-1)^2$-dimensional group V(n) of all $n \times n$ unitary matrices that have all line sums (i.e. its n row sums and its n column sums) equal to 1. We have demonstrated that V(n) is isomorphic to U($n-1$). For $n = 2^w$, the group P(n) represents all (classical) reversible computers acting on w bits and the group U(n) represents all quantum computers acting on w qubits. Any w-qubit circuit built from controlled square roots of NOT and NEGATORs, is a member of the new group V(n), for the simple reason that the product of two matrices with unit line sums is a new matrix with unit line sums. We have demonstrated that, conversely, all members of V(n) can be built with the help of controlled square roots of NOT and NEGATORs. In this way, the NEGATOR gate, a 'natural' generalization of the NOT gate, bridges the gap between the finite group P(2^w) and the infinite group V(2^w).

We end by illustrating the obtained results by giving the application to the

Grover diffusion operators for $w = 1$, $w = 2$, and $w = 3$, i.e. to the matrices

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \frac{1}{2}\begin{pmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{pmatrix}, \text{ and } \frac{1}{4}\begin{pmatrix} -3 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -3 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & -3 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & -3 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & -3 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & -3 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & -3 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & -3 \end{pmatrix}:$$



where N stands for the `NEGATOR` $N(\pi/4)$, i.e. the quartic root of `NOT`, a.k.a. the `W` gate [8]:

$$\frac{1}{2\sqrt{2}}\begin{pmatrix} \sqrt{2}+1+i & \sqrt{2}-1-i \\ \sqrt{2}-1-i & \sqrt{2}+1+i \end{pmatrix}.$$

References

[1] Feynman, R.: " Feynman lectures on computation ", Addison–Wesley, Reading (1996).

[2] Nielsen, M., and Chuang, I.: " Quantum computation and quantum information ", Cambridge University Press, Cambridge (2000).

[3] Landauer, R.: " Irreversibility and heat generation in the computational process ", *I.B.M. Journal of Research and Development*, volume 5 (1961), pp. 183 - 191.

[4] De Vos, A.: " Reversible computing ", Wiley–VCH, Weinheim (2010).

[5] Barenco, A., Bennett, C., Cleve, R., DiVincenzo, D., Margolus, N., Shor, P., Sleator, T., Smolin, J., and Weinfurter, H.: " Elementary gates for quantum computing ", *Physical Review A*, volume 52 (1995), pp. 3457 - 3467.

[6] De Vos, A., and De Baerdemacker, S.: " Symmetry groups for the decomposition of reversible computers, quantum computers, and computers in between ", *Symmetry*, volume 3 (2011), pp. 305 - 324.

[7] De Vos, A., and De Baerdemacker, S.: " The roots of the `NOT` gate ", *42 nd International Symposium on Multiple-Valued Logic*, Victoria, 14 - 16 May 2012, pp. 167 - 172.

[8] Sasanian, Z., and Miller, D.: " Transforming MCT circuits to NCVW circuits ", *3 rd Workshop on Reversible Computation*, Gent, 4 - 5 July 2011, pp. 163 - 174.

[9] Fredkin, E., and Toffoli, T.: " Conservative logic ", *International Journal of Theoretical Physics*, volume 21 (1982), pp. 219 - 253.

[10] De Vos, A., Van Laer, R., and Vandenbrande, S.: " The group of dyadic unitary matrices ", *Open Systems & Information Dynamics*, volume 19 (2012), 1250003.

[11] Tadej, W., and Życzkowski, K.: " A concise guide to complex Hadamard matrices ", *Open Systems & Information Dynamics*, volume 13 (2006), pp. 133 - 177.

[12] Greiner, W., and Müller, B.: " Quantum mechanics: symmetries ", Springer, Berlin (2001).

[13] Banica, T., Nechita, I., and Życzkowski, K.: " Almost Hadamard matrices: general theory and examples ", `arXiv:1202:2025` (2012).

[14] Yanofsky, N., and Mannucci, M.: " Quantum computing for computer scientists ", Cambridge University Press, Cambridge (2008).

[15] Poźniak, M., Życzkowski, K., and Kuś, M.: " Composed ensembles of random unitary matrices ", *Journal of Physics A: Mathematical and General*, volume 31 (1998), pp. 1059 - 1071.

[16] Miller, D., Maslov, D., and Dueck, G.: " A transformation based algorithm for reversible logic synthesis ", *40 th Design Automation Conference*, Anaheim, 2 - 6 June 2003, pp. 318 - 323.

[17] Hermann, R.: " Lie groups for physicists ", Benjamin Inc., New York (1966), pp. 30 - 39.

[18] Biedenharn, L., and Dothan, Y.: " Monopolar harmonics in SU(3) as eigenvalues of the Skyrme–Witten model for baryons ", In: " From SU(3) to gravity ", edited by Gotsman, E., and Tauber, G., Cambridge University Press, Cambridge (1985), pp. 15 - 34.

[19] Byrd, M.: " The geometry of SU(3) ", `arXiv:physics/9708015v1` (1997).

[20] Byrd, M.: " Differential geometry on SU(3) with applications to three state systems ", *Journal of Mathematical Physics*, volume 39 (1998), pp. 6125 - 6136.

[21] Tilma, T., Byrd, M., and Sudarshan, E.: " A parametrization of bipartite systems based on SU(4) Euler angles ", *Journal of Physics A: Mathematical and General*, volume 35 (2002), pp. 10445 - 10465.

[22] Loss, D., and DiVincenzo, D.: " Quantum computation with quantum dots ", *Physical Review A*, volume 57 (1998), pp. 120 - 126.

[23] Burkard, G., Loss, D., and DiVincenzo, D.: " Coupled quantum dots as quantum gates ", *Physical Review B*, volume 59 (1999), pp. 2070 - 2078.

[24] Kane, B.: " Can we build a large-scale quantum computer using semiconductor materials? ", *MRS Bulletin*, volume 30 (February 2005), pp. 1 - 6.

[25] Soeken, M., Sasanian, Z., Wille, R., Miller, D., and Drechsler, R.: " Optimizing the mapping of reversible circuits to four-valued quantum gate circuits ", *42 nd International Symposium on Multiple-Valued Logic*, Victoria, 14 - 16 May 2012, pp. 173 - 178.

[26] Sasanian, Z., Wille, R., and Miller, D.: " Realizing reversible circuits using a new class of quantum gates ", *49 th Design Automation Conference*, San Francisco, 3 - 7 June 2012, pp. 36 - 41.

A The group V(3)

V(3) is the group of unitary 3×3 matrices with all six line sums equal to 1. The 3×3 Hermitian generators thus have all six line sums equal to 0:

$$\tau_0 = \frac{1}{3} \begin{pmatrix} 2 & -1 & -1 \\ -1 & 2 & -1 \\ -1 & -1 & 2 \end{pmatrix} \ , \ \tau_1 = \frac{1}{3} \begin{pmatrix} 2 & -1 & -1 \\ -1 & -1 & 2 \\ -1 & 2 & -1 \end{pmatrix} \ ,$$

$$\tau_2 = \frac{1}{\sqrt{3}} \begin{pmatrix} 0 & 1 & -1 \\ 1 & -1 & 0 \\ -1 & 0 & 1 \end{pmatrix} \ , \text{ and } \ \tau_3 = \frac{1}{\sqrt{3}} \begin{pmatrix} 0 & -i & i \\ i & 0 & -i \\ -i & i & 0 \end{pmatrix} \ .$$

We have the commutation relations

$$[\tau_0, \tau_1] = [\tau_0, \tau_2] = [\tau_0, \tau_3] = 0$$

and

$$[\tau_1, \tau_2] = 2i\tau_3 \ , \qquad [\tau_2, \tau_3] = 2i\tau_1 \ , \qquad [\tau_3, \tau_1] = 2i\tau_2 \ .$$

Thus within V(3), the set $\{\tau_0, \tau_1, \tau_2, \tau_3\}$ plays the role the Pauli matrices $\{\sigma_0, \sigma_1, \sigma_2, \sigma_3\}$ play in U(2).

If we compute the exponentials $V_j = \exp(i\,\theta\tau_j)$, then we find (taking advantage of the properties $\tau_j^2 = \tau_0$ and $\tau_j^3 = \tau_j$):

$$V_0(\theta) = \frac{1}{3} \begin{pmatrix} 1+2e & 1-e & 1-e \\ 1-e & 1+2e & 1-e \\ 1-e & 1-e & 1+2e \end{pmatrix} \ ,$$

$$V_1(\theta) = \frac{1}{3} \begin{pmatrix} 1+2e & 1-e & 1-e \\ 1-e & 1-e+3c & 1+2e-3c \\ 1-e & 1+2e-3c & 1-e+3c \end{pmatrix} \ ,$$

$$V_2(\theta) = \frac{1}{3} \begin{pmatrix} 1+2c & 1-c+i\sqrt{3}\,s & 1-c-i\sqrt{3}\,s \\ 1-c+i\sqrt{3}\,s & 1+2c-i\sqrt{3}\,s & 1-c \\ 1-c-i\sqrt{3}\,s & 1-c & 1+2c+i\sqrt{3}\,s \end{pmatrix} \ , \text{ and}$$

$$V_3(\theta) = \frac{1}{3} \begin{pmatrix} 1+2c & 1-c+\sqrt{3}\,s & 1-c-\sqrt{3}\,s \\ 1-c-\sqrt{3}\,s & 1+2c & 1-c+\sqrt{3}\,s \\ 1-c+\sqrt{3}\,s & 1-c-\sqrt{3}\,s & 1+2c \end{pmatrix} \ ,$$

with determinant equal to e^2, 1, 1, and 1, respectively. Here, e, c, and s are the short-hand notations for $\exp(i\theta)$, $\cos(\theta)$, and $\sin(\theta)$, respectively.

The well-known decomposition of an arbitrary element U of U(2), i.e.

$$U(\theta_0, \theta_1, \theta_2, \theta_3) = U_0(\theta_0)\, U_3(\theta_1)\, U_2(\theta_2)\, U_3(\theta_3) \ , \tag{6}$$

leads us to the decomposition of an arbitrary element V of V(3):

$$V(\theta_0, \theta_1, \theta_2, \theta_3) = V_0(\theta_0)\, V_3(\theta_1)\, V_2(\theta_2)\, V_3(\theta_3) \ .$$

For an arbitrary member V of V(3), for finding the appropriate values of θ_0, θ_1, θ_2, and θ_3, we may construct the appropriate member U of U(2) by means of (5) and subsequently consider the equality (6) as a matrix equation. Solving it is equivalent to solving a set of 4 scalar equations with 4 unknowns. As an example, we apply the procedure to some permutation matrices. Even permutation matrices have determinant equal to 1. It is therefore no surprise we find $\theta_0 = 0$. The three even permutations (which form a 3-cycle) of $\mathbf{S}_3$ turn out to be located in the 1-dimensional subgroup $V_3(\theta)$:

$$\left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix} \right) = V_3(0), \ \left(\begin{smallmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{smallmatrix} \right) = V_3(2\pi/3), \text{ and } \left(\begin{smallmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{smallmatrix} \right) = V_3(4\pi/3) \ .$$

The odd permutations have determinant equal to -1. It is therefore no surprise we find $\theta_0 = \pi/2$, leading to the decomposition factor $V_0(\pi/2) = \frac{1}{3}\left(\begin{smallmatrix} 1+2i & 1-i & 1-i \\ 1-i & 1+2i & 1-i \\ 1-i & 1-i & 1+2i \end{smallmatrix} \right)$. We find

$$\left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{smallmatrix} \right) = V_0(\pi/2)V_1(-\pi/2), \quad \left(\begin{smallmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{smallmatrix} \right) = V_0(\pi/2)V_1(-\pi/2)V_3(2\pi/3),$$

$$\text{and } \left(\begin{smallmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{smallmatrix} \right) = V_0(\pi/2)V_1(-\pi/2)V_3(4\pi/3) \ .$$

The three odd permutation matrices thus lay on a same 1-dimensional subspace (not subgroup !) $V_0(\pi/2)V_1(-\pi/2)V_3(\theta)$. The three 2-cycles of $\mathbf{S}_3$ are located on three different 1-dimensional subgroups, respectively

$$V_0(\theta)V_1(-\theta) = \frac{1}{2}\left(\begin{smallmatrix} 2 & 0 & 0 \\ 0 & 1+E & 1-E \\ 0 & 1-E & 1+E \end{smallmatrix} \right), \ V_0(\theta)V_1(-\theta)V_3(2\pi/3) = \frac{1}{2}\left(\begin{smallmatrix} 0 & 2 & 0 \\ 1-E & 0 & 1+E \\ 1+E & 0 & 1-E \end{smallmatrix} \right),$$

$$\text{and } V_0(\theta)V_1(-\theta)V_3(4\pi/3) = \frac{1}{2}\left(\begin{smallmatrix} 0 & 0 & 2 \\ 1+E & 1-E & 0 \\ 1-E & 1+E & 0 \end{smallmatrix} \right),$$

where E stands for $e^2 = \exp(2i\theta)$.

B The group V(4)

The four building blocks in (1) generate the group V(4), a subgroup of U(4), which is larger than merely 4-dimensional [7]. Indeed, V(4) is a 9-dimensional subgroup of U(4). In order to put this fact in perspective, we first recall some properties of U(2), U(3), and U(4).

We remind the reader that the Lie group U(2) is generated by the four 2×2 Pauli matrices. These give rise to the four 1-dimensional subgroups

$$U_0(\theta) = \exp(i\theta\,\sigma_0) = \begin{pmatrix} e & 0 \\ 0 & e \end{pmatrix} \ , \ U_1(\theta) = \exp(i\theta\,\sigma_1) = \begin{pmatrix} c & is \\ is & c \end{pmatrix} \ ,$$

$$U_2(\theta) = \exp(i\theta\,\sigma_2) = \begin{pmatrix} c & s \\ -s & c \end{pmatrix} \ , \text{ and } U_3(\theta) = \exp(i\theta\,\sigma_3) = \begin{pmatrix} e & 0 \\ 0 & 1/e \end{pmatrix} \ .$$

An arbitrary element U of U(2) has the well-known decomposition

$$U = U_0(\theta_0)\,U_3(\theta_1)\,U_2(\theta_2)\,U_3(\theta_3) \ ,$$

called a KAK decomposition by Hermann [17].

For U(3) and U(4), a similar approach exists [18] [19] [20] [21]. In particular, U(3) is generated by the nine 3×3 Gell-Mann matrices μ_j. An arbitrary element of U(3) can be decomposed as

$$U = U_0(\theta_0)U_3(\theta_1)U_2(\theta_2)U_3(\theta_3)U_5(\theta_4)U_3(\theta_5)U_2(\theta_6)U_3(\theta_7)U_8(\theta_8) \ , \qquad (7)$$

where the matrix $U_j(\theta)$ is the matrix exponential $\exp(i\theta\mu_j)$ of μ_j. This constitutes a nested KAK decomposition [17].

The group V(4) is isomorphic to U(3). Each generator τ_j of V(4) plays the same role as the corresponding generator μ_j of U(3), i.e. each commutator $[\tau_j, \tau_k]$ has the same structure constants as the corresponding commutator $[\mu_j, \mu_k]$. Therefore, an arbitrary element of V(4) can be decomposed as

$$V = V_0(\theta_0)V_3(\theta_1)V_2(\theta_2)V_3(\theta_3)V_5(\theta_4)V_3(\theta_5)V_2(\theta_6)V_3(\theta_7)V_8(\theta_8) \ , \qquad (8)$$

where $V_j(\theta)$ equals $\exp(i\theta\tau_j)$. Thus, if we can synthesize each of the five elements $V_0(\theta)$, $V_2(\theta)$, $V_3(\theta)$, $V_5(\theta)$, and $V_8(\theta)$, then we can synthesize an arbitrary element $V(\theta_0, \theta_1, \theta_2, \theta_3, \theta_4, \theta_5, \theta_6, \theta_7, \theta_8)$ of V(4).

The generators of V(4) are given explicitly by [7]:

$$\tau_0 = \frac{1}{4}\begin{pmatrix} 3 & -1 & -1 & -1 \\ -1 & 3 & -1 & -1 \\ -1 & -1 & 3 & -1 \\ -1 & -1 & -1 & 3 \end{pmatrix}, \ \tau_1 = \frac{1}{2}\begin{pmatrix} 1 & -1 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ 0 & 0 & -1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix}, \ \tau_2 = \frac{1}{2}\begin{pmatrix} 0 & 0 & -i & i \\ 0 & 0 & i & -i \\ i & -i & 0 & 0 \\ -i & i & 0 & 0 \end{pmatrix},$$

$$\tau_3 = \frac{1}{2}\begin{pmatrix} 0 & 0 & -1 & 1 \\ 0 & 0 & 1 & -1 \\ -1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \end{pmatrix}, \ \tau_4 = \frac{1}{2}\begin{pmatrix} 1 & 0 & -1 & 0 \\ 0 & -1 & 0 & 1 \\ -1 & 0 & 1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix}, \ \tau_5 = \frac{1}{2}\begin{pmatrix} 0 & -i & 0 & i \\ i & 0 & -i & 0 \\ 0 & i & 0 & -i \\ -i & 0 & i & 0 \end{pmatrix},$$

$$\tau_6 = \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 & -1 \\ 0 & -1 & 1 & 0 \\ 0 & 1 & -1 & 0 \\ -1 & 0 & 0 & 1 \end{pmatrix}, \ \tau_7 = \frac{1}{2}\begin{pmatrix} 0 & -i & i & 0 \\ i & 0 & 0 & -i \\ -i & 0 & 0 & i \\ 0 & i & -i & 0 \end{pmatrix}, \text{ and } \tau_8 = \frac{1}{2\sqrt{3}}\begin{pmatrix} 0 & -2 & 1 & 1 \\ -2 & 0 & 1 & 1 \\ 1 & 1 & 0 & -2 \\ 1 & 1 & -2 & 0 \end{pmatrix}.$$

We have $\tau_0^2 = \tau_0$, such that $V_0 = \epsilon + [\,\exp(i\theta) - 1\,]\,\tau_0$, where ϵ is the 4×4 unit matrix. This yields

$$V_0(\theta) = \frac{1}{4}\begin{pmatrix} 1+3e & 1-e & 1-e & 1-e \\ 1-e & 1+3e & 1-e & 1-e \\ 1-e & 1-e & 1+3e & 1-e \\ 1-e & 1-e & 1-e & 1+3e \end{pmatrix}.$$

We have $\mathrm{trace}(\tau_0) = 3$, such that $\det(V_0) = \exp(3i\theta)$. In contrast, for j in $\{1, 2, ..., 8\}$, we have $\mathrm{trace}(\tau_j) = 0$ and therefore $\det(V_j) = 1$. For j restricted to $\{1, 2, ..., 7\}$, we have $\tau_j^3 = \tau_j$, such that $V_j = \epsilon + i\sin(\theta)\,\tau_j + [\,\cos(\theta) - 1\,]\,\tau_j^2$, yielding

$$V_2(\theta) = \frac{1}{2}\begin{pmatrix} 1+c & 1-c & s & -s \\ 1-c & 1+c & -s & s \\ -s & s & 1+c & 1-c \\ s & -s & 1-c & 1+c \end{pmatrix}, \ V_3(\theta) = \frac{1}{2}\begin{pmatrix} 1+c & 1-c & -is & is \\ 1-c & 1+c & is & -is \\ -is & is & 1+c & 1-c \\ is & -is & 1-c & 1+c \end{pmatrix},$$

$$\text{and } V_5(\theta) = \frac{1}{2} \begin{pmatrix} 1+c & s & 1-c & -s \\ -s & 1+c & s & 1-c \\ 1-c & -s & 1+c & s \\ s & 1-c & -s & 1+c \end{pmatrix} .$$

Finally, the computation of V_8 is somewhat more laborious. First, one checks that (for $k > 0$) we have

$$\tau_8^k = \frac{1}{2} \left(\frac{1}{\sqrt{3}}\right)^k \tau_8' - \frac{1}{4} \left(\frac{-2}{\sqrt{3}}\right)^k \tau_8'' ,$$

where

$$\tau_8' = \begin{pmatrix} 1 & -1 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & -1 & 1 \end{pmatrix} \text{ and } \tau_8'' = \begin{pmatrix} -1 & -1 & 1 & 1 \\ -1 & -1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 \end{pmatrix} .$$

Next, one applies $V_8 = \epsilon + \frac{1}{2} [\, \exp(\frac{1}{\sqrt{3}}\, i\theta) - 1 \,]\, \tau_8' - \frac{1}{4} [\, \exp(-\frac{2}{\sqrt{3}}\, i\theta) - 1 \,]\, \tau_8''$, yielding

$$V_8(\theta) = \frac{1}{4} \begin{pmatrix} 1+2e'+e'' & 1-2e'+e'' & 1-e'' & 1-e'' \\ 1-2e'+e'' & 1+2e'+e'' & 1-e'' & 1-e'' \\ 1-e'' & 1-e'' & 1+2e'+e'' & 1-2e'+e'' \\ 1-e'' & 1-e'' & 1-2e'+e'' & 1+2e'+e'' \end{pmatrix} ,$$

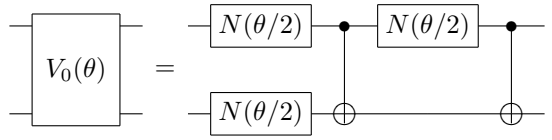
where e' and e'' stand for $\exp(\frac{1}{\sqrt{3}}\, i\,\theta)$ and $\exp(-\frac{2}{\sqrt{3}}\, i\,\theta)$, respectively.

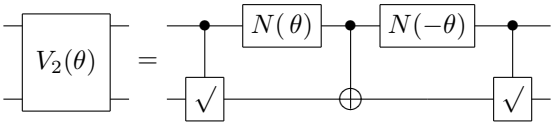
By application of (5), the 4×4 matrices V_0, V_2, V_3, V_5, and V_8 yield the following (surprisingly simple) 3×3 matrices:

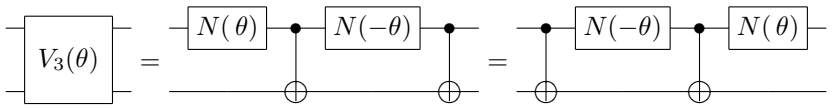
$$U_0 = \begin{pmatrix} e & 0 & 0 \\ 0 & e & 0 \\ 0 & 0 & e \end{pmatrix} , \; U_2 = \begin{pmatrix} c & 0 & -s \\ 0 & 1 & 0 \\ s & 0 & c \end{pmatrix} , \; U_3 = \begin{pmatrix} 1/e & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & e \end{pmatrix} ,$$

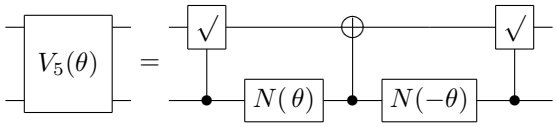
$$U_5 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & c & -s \\ 0 & s & c \end{pmatrix} , \text{ and } U_8 = \begin{pmatrix} e' & 0 & 0 \\ 0 & e'' & 0 \\ 0 & 0 & e' \end{pmatrix} .$$

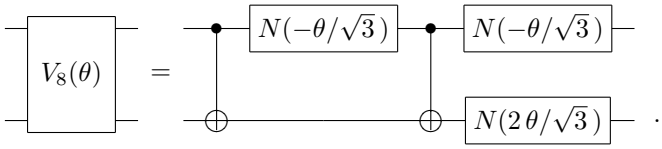
The five circuits V_0, V_2, V_3, V_5, and V_8 can be synthesized with the help of NEGATORs, controlled NOTs, and controlled $\sqrt{\texttt{NOT}}$s. Indeed, one can check the following identities:











We note that circuit V_5 equals circuit V_2 upside-down. This is no surprise, as V_2 and V_5 are conjugate matrices:

$$V_5(\theta) = S\, V_2(\theta)\, S$$

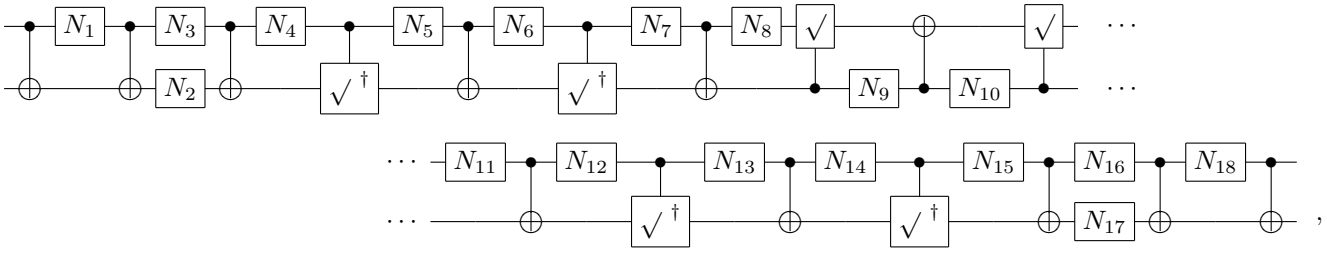
where S is the swap matrix:

$$S = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} .$$

This, in turn, is an immediate consequence of the fact that τ_2 and τ_5 are conjugate:

$$\tau_5 = S\, \tau_2\, S \ .$$

Concatenating the nine circuits of (8) and applying some simplifications leads to the wanted synthesis of $V(\theta_0, \theta_1, ..., \theta_8)$:



where

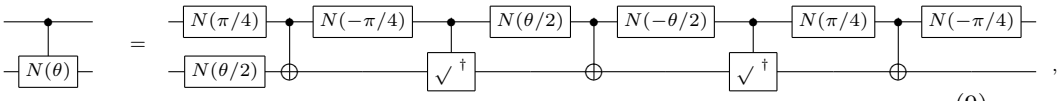
$$
\begin{aligned}
N_1 &= N(-\theta_8/\sqrt{3}\,) & N_{10} &= N(-\theta_4)\\
N_2 &= N(2\,\theta_8/\sqrt{3}\,) & N_{11} &= N(\,\theta_3)\\
N_3 &= N(-\theta_8/\sqrt{3}+\theta_7) & N_{12} &= N(-\theta_3)\\
N_4 &= N(-\theta_7) & N_{13} &= N(\,\theta_2)\\
N_5 &= N(\,\theta_6) & N_{14} &= N(-\theta_2)\\
N_6 &= N(-\theta_6) & N_{15} &= N(-\theta_1)\\
N_7 &= N(-\theta_5) & N_{16} &= N(\,\theta_1+\theta_0/2)\\
N_8 &= N(\,\theta_5) & N_{17} &= N(\,\theta_0/2)\\
N_9 &= N(\,\theta_4) & N_{18} &= N(\,\theta_0/2)\;.
\end{aligned}
$$

We thus have

- eightteen NEGATORs,
- six controlled square roots of NOT, and
- eleven controlled NOTs.

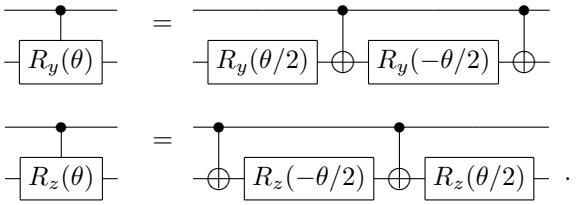
For an arbitrary member V of V(4), finding the appropriate values of θ_0, θ_1, ..., θ_8 needs the construction of the corresponding member U of U(3) and subsequent solution of the matrix equation (7), i.e. a set of 9 scalar equations with 9 unknowns. This (computationally hard) task can be somewhat simplified by first computing θ_0. Indeed, eqn (8) leads to $\det(V_0(\theta_0)) = \det(V)$ and thus to $\exp(3i\theta_0) = \det(V)$, yielding immediately the value of θ_0. We subsequently have to solve a set of 8 equations in the 8 unknowns $\{\theta_1, \theta_2, ..., \theta_8\}$.

It is remarkable that (except for the controlled NOTs and controlled $\sqrt{\texttt{NOT}}$s) no controlled NEGATORs appear in the decomposition. This property leads to the conclusion that a controlled NEGATOR can be synthesized by uncontrolled NEGATORs. And indeed, the above procedure, followed by some simplifications, leads to



(9)

a synthesis consisting of a NEGATOR followed by a $V_3(-\pi/4)V_2(\theta/2)V_3(\pi/4)$ string. This identity constitutes the counterpart of the well-known identities for controlled ROTATORs [5]:

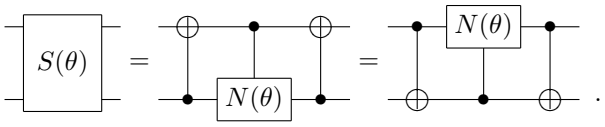


.

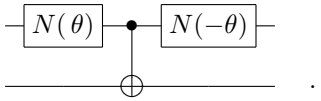
The controlled NEGATOR, in turn, allows to implement the roots of the SWAP gate:

$$S(\theta) = \frac{1}{2} \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 1+e & 1-e & 0 \\ 0 & 1-e & 1+e & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix} .$$

This gate is the SWAP gate if θ equals π and is the square root of SWAP gate [22] [23] [24] if θ equals $\pi/2$. We indeed have the following identities:



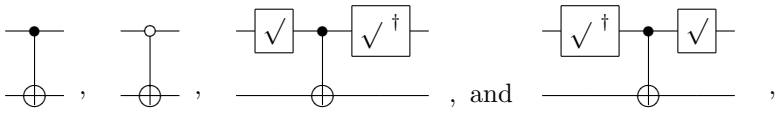
We close the present appendix by discussing a particular subset of the 9-dimensional group V(4), because it appears again and again, e.g. in the above decompositions of V_2, V_3, and V_5. It is depicted by



One easily constructs its transformation and finds

$$\frac{1}{2} \begin{pmatrix} 1+c & 1-c & -is & is \\ 1-c & 1+c & is & -is \\ is & -is & 1-c & 1+c \\ -is & is & 1+c & 1-c \end{pmatrix} .$$

We stress that we have here a 1-dimensional set of matrices, not a 1-dimensional group of matrices. The set e.g. lacks the 4×4 unit matrix. The particular parameter values 0, π, $\pi/2$, and $-\pi/2$ lead to the respective circuits



with respective matrices

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} , \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} , \frac{1}{2} \begin{pmatrix} 1 & 1 & -i & i \\ 1 & 1 & i & -i \\ i & -i & 1 & 1 \\ -i & i & 1 & 1 \end{pmatrix} , \text{ and } \frac{1}{2} \begin{pmatrix} 1 & 1 & i & -i \\ 1 & 1 & -i & i \\ -i & i & 1 & 1 \\ i & -i & 1 & 1 \end{pmatrix} .$$

The first circuit is simply the controlled NOT gate (a.k.a. Feynman gate); the second circuit is the negatively controlled NOT; the last two gates have recently been introduced by Sasanian et al., as useful quantum building-blocks [25] [26].

Finally, we note that the particular case $\theta = \pi/4$, i.e.

$$\frac{1}{2\sqrt{2}} \begin{pmatrix} \sqrt{2}+1 & \sqrt{2}-1 & -i & i \\ \sqrt{2}-1 & \sqrt{2}+1 & i & -i \\ i & -i & \sqrt{2}-1 & \sqrt{2}+1 \\ -i & i & \sqrt{2}+1 & \sqrt{2}-1 \end{pmatrix},$$

appears twice in eqn (9).