View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Ghent University Academic Bibliography

The group zoo of classical reversible computing and quantum computing

Alexis De Vos and Stijn De Baerdemacker

Abstract By systematically inflating the group of $n \times n$ permutation matrices to the group of $n \times n$ unitary matrices, we can see how classical computing is embedded in quantum computing. In this proces, an important role is played by two subgroups of the unitary group U(n), i.e. XU(n) and ZU(n). Here, XU(n) consists of all $n \times n$ unitary matrices with all line sums (i.e. the n row sums and the n column sums) equal to 1, whereas ZU(n) consists of all $n \times n$ diagonal unitary matrices with upper-left entry equal to 1. As a consequence, quantum computers can be built from NEGATOR gates and PHASOR gates. The NEGATOR is a 1-qubit circuit that is a natural generalization of the 1-bit NOT gate of classical computing. In contrast, the PHASOR is a 1-qubit circuit not related to classical computing.

1 Introduction

Often, in the literature, conventional computers and quantum computers are discussed like belonging to two separate worlds, far from each other. Conventional computers act on classical bits, say 'pure zeroes' and 'pure ones', by means of Boolean logic gates, such as AND gates and NOR gates. The operations performed by these gates are described by truth tables. Quantum computers act on qubits, say complex vectors, by means of quantum gates, such as ROTATOR gates and T gates [1]. The operations performed by these gates are described by unitary matrices.

Because the world of classical computation and the world of quantum computation are based on such different science models, it is difficult to see the relationship

Alexis De Vos
Vakgroep elektronika en informatiesystemen, Universiteit Gent, Sint Pietersnieuwstraat 41, B-9000 Gent, Belgium, e-mail: alex@elis.UGent.be

Stijn De Baerdemacker
Vakgroep anorganische en fysische chemie, Universiteit Gent, Krijgslaan 281 - S3, B- 9000 Gent, Belgium, e-mail: Stijn.DeBaerdemacker@UGent.be

(be it analogies or differences) between these two computation paradigms. In the present chapter, we bridge the gap between the two sciences. For this purpose, a common language is necessary. The common tool we have chosen is the representation by square matrices and the construction of matrix groups.

2 Reversible computing

The first step in bridging the gap between classical and quantum computation is replacing (or better: embedding) conventional classical computing in reversible classical computing. Whereas conventional logic gates are represented by truth tables with an arbitrary number w_i of input columns and an arbitrary number w_o of output columns, reversible logic gates are described by truth tables with an equal number w of input and output columns. Moreover, all output rows are different, such that the 2^w output words are merely a permutation of the 2^w input words [2] [3] [4] [5]. Table 1 gives an example of a conventional gate (i.e. an `AND` gate, with two input bits A and B and one output bit R), as well as an example of a reversible gate (i.e. a `TOFFOLI` gate, a.k.a. a controlled controlled `NOT` gate, with three input bits A, B, and C and three output bits P, Q, and R). The reader may verify that the irreversible `AND` function is embedded in the reversible `TOFFOLI` function, as presetting in Table 1b the input C to logic 0 leads to the output R being equal to A `AND` B, as is highlighted by boldface. In the general case, any irreversible truth table can be embedded in a reversible truth table with $w = w_i + w_o$ or less bits [6].

Table 1 Truth table of two basic Boolean functions: (a) the `AND` function, (b) the `TOFFOLI` function.

AB	*R*
0 0	0
0 1	0
1 0	0
1 1	1

(a)

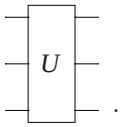
ABC	*PQR*
0 0 0	0 0 **0**
0 0 1	0 0 1
0 1 0	0 1 **0**
0 1 1	0 1 1
1 0 0	1 0 **0**
1 0 1	1 0 1
1 1 0	1 1 **1**
1 1 1	1 1 0

(b)

The next step in the journey from the conventional to the quantum world, is replacing the reversible truth table by a permutation matrix. As all eight output words 000, 001, ..., and 110 are merely a permutation of the eight input words 000, 001, ..., and 111, Table 1(b) can be replaced by an 8×8 permutation matrix, i.e.

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

An arbitrary classical reversible circuit, acting on w bits, is represented by a permutation matrix of size $2^w \times 2^w$. In contrast, a quantum circuit, acting on w qubits, is represented by a unitary matrix of size $2^w \times 2^w$. Both kind of matrices are depicted by symbols with w input lines and w output lines:



Invertible square matrices, together with the operation of ordinary matrix multiplication, form a group. The finite matrix group $\mathrm{P}(2^w)$ consisting solely of permutation matrices is a subgroup of the continuous group $\mathrm{U}(2^w)$ of unitary matrices. In the present chapter, we show a natural means how to enlarge the subgroup to its supergroup, in other words: how to upgrade a classical computer to a quantum computer.

3 NEGATORs and PHASORs

For the purpose of upgrading the permutation group $\mathrm{P}(n)$ to the unitary group $\mathrm{U}(n)$, we introduce two subgroups [7] [8] [9] of $\mathrm{U}(n)$:

the subgroup $\mathrm{XU}(n)$
consists of all $n \times n$ unitary matrices with all line sums (i.e. the n row sums and the n column sums) equal to 1

and

the subgroup $\mathrm{ZU}(n)$
consists of all $n \times n$ diagonal unitary matrices with upper-left entry equal to 1.

Whereas $\mathrm{U}(n)$ is an n^2-dimensional Lie group, $\mathrm{XU}(n)$ is only $(n-1)^2$-dimensional and $\mathrm{ZU}(n)$ is only $(n-1)$-dimensional. The two subgroups are quite distinct: their

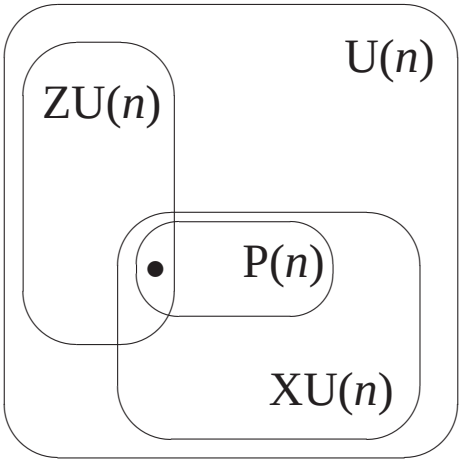


Fig. 1 Venn diagram of the Lie groups U(n), XU(n), and ZU(n) and the finite groups P(n) and **1**(n).
Note: the trivial group **1**(n) is represented by the bullet.

intersection is the trivial group **1**(n), consisting of a single matrix, i.e. the $n \times n$ unit matrix. We note that all P(n) matrices are in XU(n). See Venn diagram in Figure 1.

Why exactly these two groups? The reason becomes clear by looking at the case $n = 2$. There exist only two classical reversible circuits acting on a single bit. They are represented by the two P(2) matrices: $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ for the `IDENTITY` gate and $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ for the `NOT` gate. The latter is also known as the `X` gate. In contrast, there exists a 4-dimensional infinity of quantum circuits acting on a single qubit. They are represented by the U(2) matrices.

In order to upgrade the group P(2), we construct a unitary interpolation between its two permutation matrices. The interpolation

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

is unitary if and only if $t = (1+e^{i\theta})/2$, where θ is an arbitrary angle. We thus obtain a 1-dimensional generalization of the `NOT` matrix:

the `NEGATOR` **gate**:

$$N(\theta) = \frac{1}{2}\begin{pmatrix} 1+e^{i\theta} & 1-e^{i\theta} \\ 1-e^{i\theta} & 1+e^{i\theta} \end{pmatrix},$$

where θ is an arbitrary angle.

Because U(2) is 4-dimensional, we need some extra building block to generate the full U(2). For this purpose, it suffices to introduce a second 1-dimensional subgroup of U(2):

the PHASOR **gate**:

$$\Phi(\theta) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix} ,$$

where θ is an arbitrary angle.

Analogously as the NEGATOR is the 1-dimensional generalization of the $\left(\begin{smallmatrix} & 1 \\ 1 & \end{smallmatrix}\right)$ matrix or X gate, the PHASOR can be considered as the 1-dimensional generalization of the $\left(\begin{smallmatrix} 1 & \\ & -1 \end{smallmatrix}\right)$ matrix, a.k.a. the Z gate. The two 1-dimensional subgroups XU(2) and ZU(2) suffice to generate the whole 4-dimensional group U(2). We say: the closure of XU(2) and ZU(2) is U(2). Indeed, an arbitrary matrix U from U(2) can be written as a finite product of matrices from XU(2) and matrices from ZU(2):

$$U(\alpha,\varphi,\psi,\chi) = e^{i\alpha} \begin{pmatrix} \cos(\varphi)e^{i\psi} & \sin(\varphi)e^{i\chi} \\ -\sin(\varphi)e^{-i\chi} & \cos(\varphi)e^{-i\psi} \end{pmatrix}$$

$$= N(\pi)\,\Phi(\alpha+\varphi+\psi)\,N(\pi)\,\Phi(\alpha+\varphi-\chi+\pi/2)\,N(\varphi)\,\Phi(-\psi+\chi-\pi/2) .$$

We use the following symbols for the NEGATOR and PHASOR gates:

respectively. In the literature [5] [10] [11] [12], some of these gates have a specific notation:

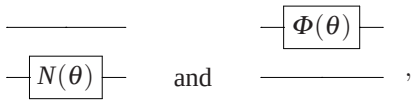
$$\begin{aligned} N(0) &= \mathtt{I} \\ N(\pi/4) &= \mathtt{W} \\ N(\pi/2) &= \mathtt{V} \\ N(\pi) &= \mathtt{X} \\ N(2\pi) &= \mathtt{I} \end{aligned}$$

$$\begin{aligned} \Phi(0) &= \mathtt{I} \\ \Phi(\pi/4) &= \mathtt{T} \\ \Phi(\pi/2) &= \mathtt{S} \\ \Phi(\pi) &= \mathtt{Z} \\ \Phi(2\pi) &= \mathtt{I} . \end{aligned}$$

In particular, the V gate is known as 'the square root of NOT' [13] [14] [15] [16].

4 Controlled NEGATORs and controlled PHASORs

Two-qubit circuits are represented by matrices from U(4). We may apply either the NEGATOR gate or the PHASOR gate from the previous section to either the first qubit or the second qubit. Here are two examples:

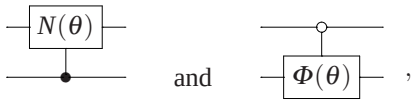


i.e. a NEGATOR acting on the second qubit and a PHASOR acting on the first qubit, respectively. These circuits are represented by the 4×4 unitary matrices

$$\frac{1}{2}\begin{pmatrix} 1+e^{i\theta} & 1-e^{i\theta} & 0 & 0 \\ 1-e^{i\theta} & 1+e^{i\theta} & 0 & 0 \\ 0 & 0 & 1+e^{i\theta} & 1-e^{i\theta} \\ 0 & 0 & 1-e^{i\theta} & 1+e^{i\theta} \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & e^{i\theta} & 0 \\ 0 & 0 & 0 & e^{i\theta} \end{pmatrix}, \tag{1}$$

respectively.

However, we also introduce more sophisticated gates: the so-called 'controlled PHASORs' and 'controlled NEGATORs'. Two examples are

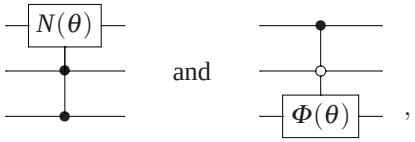


i.e. a positive-polarity controlled NEGATOR acting on the first qubit, controlled by the second qubit, and a negative-polarity controlled PHASOR acting on the second qubit, controlled by the first qubit, respectively. The former symbol is read as follows: 'if the second qubit equals 1, then the NEGATOR acts on the first qubit; if, however, the second qubit equals 0, then the NEGATOR is inactive, i.e. the first qubit undergoes no change'. The latter symbol is read as follows: 'if the first qubit equals 0, then the PHASOR acts on the second qubit; if, however, the first qubit equals 1, then the PHASOR is inactive, i.e. the second qubit undergoes no change'. The 4×4 matrices representing these two circuit examples are:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \frac{1}{2}(1+e^{i\theta}) & 0 & \frac{1}{2}(1-e^{i\theta}) \\ 0 & 0 & 1 & 0 \\ 0 & \frac{1}{2}(1-e^{i\theta}) & 0 & \frac{1}{2}(1+e^{i\theta}) \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & e^{i\theta} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \tag{2}$$

respectively.

We now give two examples of a 3-qubit circuit:



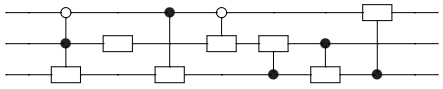
i.e. a positive-polarity controlled NEGATOR acting on the first qubit and a mixed-polarity controlled PHASOR acting on the third qubit. The 8×8 matrices representing these two circuit examples are:

$$\begin{pmatrix} 1&0&0&0&0&0&0&0 \\ 0&1&0&0&0&0&0&0 \\ 0&0&1&0&0&0&0&0 \\ 0&0&0&\frac{1}{2}(1+e^{i\theta})&0&0&0&\frac{1}{2}(1-e^{i\theta}) \\ 0&0&0&0&1&0&0&0 \\ 0&0&0&0&0&1&0&0 \\ 0&0&0&0&0&0&1&0 \\ 0&0&0&\frac{1}{2}(1-e^{i\theta})&0&0&0&\frac{1}{2}(1+e^{i\theta}) \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1&0&0&0&0&0&0&0 \\ 0&1&0&0&0&0&0&0 \\ 0&0&1&0&0&0&0&0 \\ 0&0&0&1&0&0&0&0 \\ 0&0&0&0&1&0&0&0 \\ 0&0&0&0&0&e^{i\theta}&0&0 \\ 0&0&0&0&0&0&1&0 \\ 0&0&0&0&0&0&0&1 \end{pmatrix}, \qquad (3)$$

respectively. In each of the expressions (1), (2), and (3), we note the following properties:

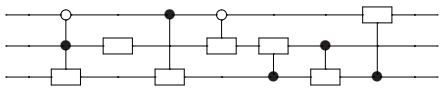
- the former matrix has all row sums and all column sums equal to 1;
- the latter matrix is diagonal and has upper-left entry equal to 1.

Because the multiplication of two square matrices with all line sums equal to 1 automatically yields a third square matrix with all line sums equal to 1, we can easily demonstrate that an arbitrary quantum circuit like



consisting merely of uncontrolled NEGATORs and controlled NEGATORs is represented by a $2^w \times 2^w$ unitary matrix with all line sums equal to 1, i.e. an XU(2^w) matrix. A laborious proof [17] demonstrates that the converse theorem is also valid: any member of XU(2^w) can be synthesized by an appropriate finite string of (un)controlled NEGATORs.

Because the multiplication of two diagonal square matrices yields a third diagonal square matrix and because the multiplication of two unitary matrices with first entry equal to 1 yields a third unitary matrix with first entry equal to 1, we can easily demonstrate that an arbitrary quantum circuit like



consisting merely of uncontrolled PHASORs and controlled PHASORs is represented by a $2^w \times 2^w$ unitary diagonal matrix with first entry equal to 1, i.e. a ZU(2^w) matrix.

It can easily be seen that the converse theorem is also true: any member of ZU(2^w) can be synthesized by an appropriate finite string of (un)controlled PHASORs.

We conclude that the study of NEGATOR and PHASOR circuits automatically leads to the introduction of the two subgroups XU(2^w) and ZU(2^w) of the unitary group U(2^w).

5 The FUF matrix decomposition

While studying the properties of the XU and ZU groups, a pivotal role is played by the $n \times n$ discrete Fourier transform, i.e. the following unitary matrix:

$$F = \frac{1}{\sqrt{n}} \begin{pmatrix} 1 & 1 & 1 & 1 & \dots & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \dots & \omega^{n-1} \\ 1 & \omega^2 & \omega^4 & \omega^6 & \dots & \omega^{2(n-1)} \\ \vdots & & & & & \\ 1 & \omega^{n-1} & \omega^{2(n-1)} & \omega^{3(n-1)} & \dots & \omega^{(n-1)(n-1)} \end{pmatrix},$$

where ω is the primitive n th root of unity, i.e. $e^{i2\pi/n}$. We have:

the FUF theorem:
Any matrix X from XU(n) can be written as the following product [17]:

$$X = F \begin{pmatrix} 1 & \\ & U \end{pmatrix} F^{-1},$$

where

- F is the $n \times n$ discrete Fourier transform and
- U is a matrix from U($n-1$).

The proof is constructive, i.e. by computation of the matrix product, taking into account the properties of the Fourier matrix. The relationship is a one-to-one mapping. In other words: with one X corresponds one U and with one U corresponds one X. As a result, the group XU(n) is isomorphic to the unitary group U($n-1$) and thus has $(n-1)^2$ dimensions. Here is an example from U(2) and XU(3):

$$\frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix} \frac{1}{2} \begin{pmatrix} 2 & 0 & 0 \\ 0 & -1+i & 1+i \\ 0 & 1-i & 1+i \end{pmatrix} \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega^2 & \omega \\ 1 & \omega & \omega^2 \end{pmatrix}$$

$$= \frac{1}{6}\begin{pmatrix} 4+2i & -(\sqrt{3}-1)+i(\sqrt{3}-1) & \sqrt{3}+1-i(\sqrt{3}+1) \\ -(\sqrt{3}-1)-i(\sqrt{3}+1) & \sqrt{3}+1+2i & 4+i(\sqrt{3}-1) \\ \sqrt{3}+1+i(\sqrt{3}-1) & 4-i(\sqrt{3}+1) & -(\sqrt{3}-1)+2i \end{pmatrix},$$

where ω is the primitive cubic root of unity, i.e. $\omega = e^{i2\pi/3} = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$.

We have two special cases of the FUF theorem. The first involves a subgroup of XU(n):

the subgroup CXU(n)
consists of all circulant XU(n) matrices.

For such matrices holds

the FZF **theorem**:
Any matrix C from CXU(n) can be written as follows:

$$C = FZF^{-1},$$

where

- F is the $n \times n$ discrete Fourier transform and
- Z is a matrix from ZU(n).

Similarly, we can write any ZU(n) as an FCF^{-1} product. These two relationships constitute a one-to-one mapping between ZU(n) and CXU(n). The two $(n-1)$-dimensional groups thus are isomorphic. An example for CXU(4) and ZU(4) is

$$\frac{1}{8}\begin{pmatrix} 1+i & 7+i & -1-i & 1-i \\ 1-i & 1+i & 7+i & -1-i \\ -1-i & 1-i & 1+i & 7+i \\ 7+i & -1-i & 1-i & 1+i \end{pmatrix} =$$

$$\frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & i & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & (1-i)/2 \end{pmatrix} \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -i & -1 & i \\ 1 & -1 & 1 & -1 \\ 1 & i & -1 & -i \end{pmatrix}.$$

The second special case of the FUF theorem is

the FXF theorem:
For any matrix X from XU(n), the following property holds:

$$F\begin{pmatrix}1 & \\ & X\end{pmatrix}F^{-1}=\begin{pmatrix}1 & \\ & X'\end{pmatrix},$$

where

- F is the $(n+1)\times(n+1)$ discrete Fourier transform and
- X' is a matrix from XU(n).

Proof of this theorem is quite simple. Suffice it to note two facts:

- $F\begin{pmatrix}1 & \\ & \chi\end{pmatrix}$ is a matrix with an upper row consisting of $n+1$ entries all equal to $1/\sqrt{n+1}$, such that $F\begin{pmatrix}1 & \\ & \chi\end{pmatrix}F^{-1}$ is a matrix with an upper-left entry equal to 1;
- $F\begin{pmatrix}1 & \\ & \chi\end{pmatrix}F^{-1}$ is of the form $F\begin{pmatrix}1 & \\ & U\end{pmatrix}F^{-1}$, and therefore an XU($n+1$) matrix, by virtue of the FUF theorem.

A matrix with these two properties is necessarily of the form $\begin{pmatrix}1 & \\ & X'\end{pmatrix}$ with X' a member of XU(n).

For $n=2$, the matrix X' is equal to the matrix X. For $n>2$, usually, the matrix X' is different from X. The relationship thus is a one-to-one mapping from XU(n) to itself. We give an example from XU(3):

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

$$\frac{1}{4}\begin{pmatrix}4&0&0&0\\0&3&-1-i&2+i\\0&-1+i&2&3-i\\0&2-i&3+i&-1\end{pmatrix}.$$

Note that here the Fourier matrices are of larger size than the XU matrices. A relationship like $FXF^{-1}=X'$ with F, X, and X' of the same size does not hold.

6 The ZXZ matrix decomposition

A quite different theorem is

the ZXZ theorem:
Any matrix U from U(n) can be written as follows [18] [19]:

$$U = aZ_1XZ_2 \ , \tag{4}$$

where

- a is a member of U(1), i.e. a complex number with unit modulus,
- X is a member of XU(n), and
- both Z_1 and Z_2 are member of ZU(n).

The proof of the theorem is non-constructive and based on symplectic topology [19]. We note that the sum of 1 (number of parameters in a), $n-1$ (parameters in Z_1), $(n-1)^2$ (in X) and $n-1$ (in Z_2) equals the dimensionality n^2 of U(n):

$$1+(n-1)+(n-1)^2+(n-1) = n^2 \ .$$

Thus the number of degrees of freedom in aZ_1XZ_2 exactly matches the number of degrees of freedom in U. This might suggest that the decomposition is unique. However, this is not true: unlike the FUF theorem, the ZXZ theorem is not a one-to-one relationship. As an example, we give here the same matrix from U(2) as in the illustration of the FUF theorem. It has two (and only two) ZXZ decompositions:

$$\begin{aligned}\frac{1}{2}\begin{pmatrix} -1+i & 1+i \\ 1-i & 1+i \end{pmatrix} &= (-1)\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}\frac{1}{2}\begin{pmatrix} 1-i & 1+i \\ 1+i & 1-i \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \\ &= i\begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix}\frac{1}{2}\begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \ .\end{aligned}$$

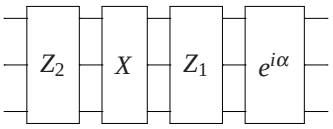
Usually a U(n) matrix has a discrete number of decompositions. But sometimes there are as many as a noncountable infinity of decompositions, as is illustrated by another U(2) matrix:

$$\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = e^{i\beta}\begin{pmatrix} 1 & 0 \\ 0 & ie^{-i\beta} \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -ie^{-i\beta} \end{pmatrix} \ ,$$

where the angle β is allowed to have any value.

Except in some special cases, no analytical method is known to find the ZXZ decompositons of U. Only a numerical procedure is known. It yields one of the solutions with an arbitrarily small error. Which solution is found, depends on the starting conditions of the numerical algorithm [18].

We thus can conclude that any quantum computer looks like



,

i.e. the cascade of an overall phase factor, an input section consisting merely of (un)controlled PHASORs, a core section consisting merely of (un)controlled NEGATORs, and an output section consisting merely of (un)controlled PHASORs.

By combining the FUF, the ZXZ, the FZF, and the FXF theorems, we can prove the following decomposition of an XU(n) matrix:

the CXC **theorem**:
For any matrix X from XU(n), the following property holds:

$$X = C' \begin{pmatrix} 1 & \\ & X' \end{pmatrix} C'' , \tag{5}$$

where

- X' is a member of XU($n-1$) and
- both C' and C'' are member of CXU(n).

Indeed:

$$X = F \begin{pmatrix} 1 & \\ & U \end{pmatrix} F^{-1} = F \begin{pmatrix} 1 & \\ & aZ'X''Z'' \end{pmatrix} F^{-1} = F \begin{pmatrix} 1 & \\ & aZ' \end{pmatrix} \begin{pmatrix} 1 & \\ & X'' \end{pmatrix} \begin{pmatrix} 1 & \\ & Z'' \end{pmatrix} F^{-1}$$
$$= F \begin{pmatrix} 1 & \\ & aZ' \end{pmatrix} F^{-1} F \begin{pmatrix} 1 & \\ & X'' \end{pmatrix} F^{-1} F \begin{pmatrix} 1 & \\ & Z'' \end{pmatrix} F^{-1} = C' \begin{pmatrix} 1 & \\ & X' \end{pmatrix} C'' .$$

Because the ZXZ decomposition is not unique, also the CXC decomposition is not unique.

By applying the CXC theorem again and again, we find the following decomposition of an arbitrary element X of XU(n):

$$X = C'_n \begin{pmatrix} 1 & \\ & C'_{n-1} \end{pmatrix} \cdots \begin{pmatrix} \mathbf{1}_{n-3} & \\ & C'_3 \end{pmatrix} \begin{pmatrix} \mathbf{1}_{n-2} & \\ & C_2 \end{pmatrix} \begin{pmatrix} \mathbf{1}_{n-3} & \\ & C''_3 \end{pmatrix} \cdots \begin{pmatrix} 1 & \\ & C''_{n-1} \end{pmatrix} C''_n , \tag{6}$$

where $\mathbf{1}_k$ is a short-hand notation for the $k \times k$ unit matrix, and where all C'_k and all C''_k are CXU(k) matrices and C_2 is a CXU(2) matrix. We conclude: any matrix from XU(n) can be decomposed as a product of $2n-2$ matrices of the form $\left(\begin{smallmatrix} \mathbf{1}_{n-k} & \\ & C_k \end{smallmatrix}\right)$. We note that a similar reasoning is applicable to permutation matrices, i.e. to classical computation. See Appendix 1.

7 The U circuit synthesis

The phase factor $a = e^{i\alpha}$ in the ZXZ product may be decomposed into two NEGATOR circuits and two uncontrolled PHASORs. Indeed, if $n = 2^w$, then n is even. If n is even, then we note the following diagonal-matrix property:

$$\mathrm{diag}(a,a,a,a,a,...,a,a) = P_0\,\mathrm{diag}(1,a,1,a,1,...,1,a)\,P_0^{-1}\,\mathrm{diag}(1,a,1,a,1,...,1,a)\ ,$$

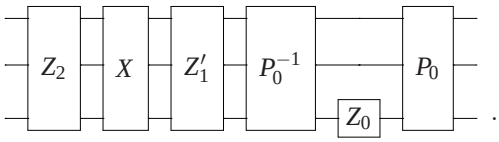
where P_0 is the $n \times n$ (circulant) permutation matrix

$$\begin{pmatrix} 0&1&0&0&...&0&0\\ 0&0&1&0&...&0&0\\ 0&0&0&1&...&0&0\\ \vdots & & & & & & \\ 0&0&0&0&...&0&1\\ 1&0&0&0&...&0&0 \end{pmatrix}\ ,$$

a.k.a. the cyclic-shift matrix, which can be implemented with classical reversible gates (i.e. one NOT and $w-1$ controlled NOTs [4] [20]). We thus can rewrite (4) as a decomposition containing exclusively XU and ZU matrices:

$$U = P_0 Z_0 P_0^{-1} Z_1' X Z_2\ ,$$

where $Z_0 = \mathrm{diag}(1,a,1,a,1,...,1,a)$ is a ZU matrix which can be implemented by a single (uncontrolled) PHASOR gate and where Z_1' is the product $Z_0 Z_1$:



Because both P_0 and P_0^{-1} belong to XU(n), we conclude that any matrix from U(n) can be synthesized by a cascade of XU(n) blocks and ZU(n) blocks. In group-theoretical terms: the closure of XU(n) and ZU(n) is U(n). We note that this circuit decomposition is not unique, because the ZXZ matrix decomposition is not unique.

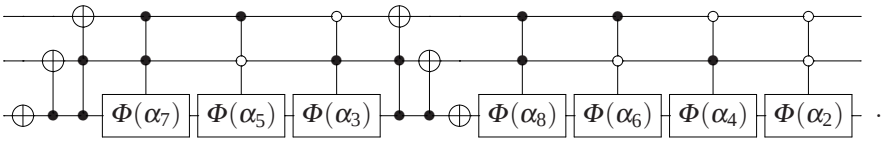
In the next two sections, we will look in detail to the synthesis of the ZU block and the XU blocks.

8 The ZU circuit synthesis

The decomposition of an arbitrary member of ZU(n) is straigthforward. Indeed, for even n, the matrix can be written as the following product of four matrices:

$$\mathrm{diag}(1,a_2,a_3,a_4,a_5,a_6,...,a_n) =$$
$$\mathrm{diag}(1,a_2,1,a_4,1,a_6,...,1,a_n)\,P_0\,\mathrm{diag}(1,1,1,a_3,1,a_5,...,1,a_{n-1})\,P_0^{-1}\ ,$$

where a_j is a short-hand notation for $e^{i\alpha_j}$. If n equals 2^w, then the diagonal matrix $\mathrm{diag}(1,a_2,1,a_4,\,1,a_6,...)$ represents 2^{w-1} PHASORs, each controlled $(w-1)$ times, and the diagonal matrix $\mathrm{diag}(1,1,1,a_3,\;1,a_5,...)$ represents $2^{w-1}-1$ PHASORs, each controlled $(w-1)$ times. E.g. for $w=3$, we obtain



We thus have a total of 2^w-1 controlled PHASORs. According to Lemma 7.5 of Barenco et al. [21], each multiply-controlled gate $\Phi(\alpha)$ can be replaced by classical gates and three singly-controlled PHASORs $\Phi(\pm\alpha/2)$. According to De Vos and De Baerdemacker [7], each singly-controlled PHASOR $\Phi(\beta)$ can be decomposed into two controlled NOTs and three uncontrolled PHASORs $\Phi(\pm\beta/2)$. We thus obtain a circuit with a total of $9(2^w-1)$ uncontrolled PHASORs.

We conclude that any matrix from ZU(n) can be synthesized by a cascade of P(n) blocks and ZZU(n) blocks. Here, ZZU(n) denotes the 1-dimensional subgroup of ZU(n) consisting of all $n\times n$ diagonal unitary matrices with all diagonal elements equal to 1, except the lower-right entry. It is isomorphic to ZU(2) and thus to U(1).

9 The XU circuit synthesis

Because of (6), the synthesis of an XU circuit is reduced to the synthesis of matrices consisting of two blocks on the diagonal: a unit submatrix and a CXU submatrix. We will call such matrices block-circulant, as they are composed of two circulant blocks.

10 The CXU circuit synthesis

In spite of the fact that CXU(n) is isomorphic to ZU(n), its synthesis is not as straightforward. The group ZU(n) is isomorphic to U(1)$^{n-1}$. Therefore, the group CXU(n) is equally isomorphic to the direct product U(1)$^{n-1}$. The $n-1$ generators of ZU(n) are the matrices

$$g_k = \begin{pmatrix} \mathbf{0}_{k-1} & & \\ & 1 & \\ & & \mathbf{0}_{n-k} \end{pmatrix},$$

where $2\leq k\leq n$ and $\mathbf{0}_j$ is a short-hand notation for the $j\times j$ zero matrix. As an example, we give here the two generators of ZU(3):

$$g_2 = \begin{pmatrix} 0&0&0\\ 0&1&0\\ 0&0&0 \end{pmatrix} \text{ and } g_3 = \begin{pmatrix} 0&0&0\\ 0&0&0\\ 0&0&1 \end{pmatrix} .$$

For each set $\{j,k\}$, we have that the two generators g_j and g_k commute:

$$[g_j, g_k] = g_j g_k - g_k g_j = 0 .$$

That is exactly the reason why ZU(n) is a direct product of its $n-1$ subgroups isomorphic to ZZU(n) and thus to U(1). Each 1-dimensional subgroup is of the form

$$m_k(\theta) = \begin{pmatrix} \mathbf{0}_{k-1} & & \\ & e^{i\theta} & \\ & & \mathbf{0}_{n-k} \end{pmatrix} .$$

By Fourier conjugating the ZU(n) generators, we find the CXU(n) generators. They look like:

$$g_k = \frac{1}{n} \begin{pmatrix} 1 & \Omega & \Omega^2 & \dots & \Omega^{n-1} \\ \Omega^{-1} & 1 & \Omega & \dots & \Omega^{n-2} \\ \vdots & & & & \\ \Omega^{-n+1} & \Omega^{-n+2} & \Omega^{-n+3} & \dots & 1 \end{pmatrix} ,$$

where Ω is a short-hand notation for ω^{1-k}. All $n-1$ generators of CXU(n) equally commute. Whereas in general a single generator g generates a 1-dimensional matrix group given by the matrix eponentiation $m(\theta) = e^{ig\theta}$, in this particular case (because of the property $g_k^2 = g_k$), the generated matrices have the simple expression

$$m_k(\theta) = \mathbf{1}_n + (e^{i\theta} - 1) g_k .$$

As an example, we give here the two generators of CXU(3):

$$g_2 = \frac{1}{3} \begin{pmatrix} 1 & \omega^2 & \omega \\ \omega & 1 & \omega^2 \\ \omega^2 & \omega & 1 \end{pmatrix} \text{ and } g_3 = \frac{1}{3} \begin{pmatrix} 1 & \omega & \omega^2 \\ \omega^2 & 1 & \omega \\ \omega & \omega^2 & 1 \end{pmatrix} .$$

Each generates a 1-dimensional subgroup of CXU(3):

$$m_2(\theta) = \frac{1}{3} \begin{pmatrix} 2+x & \omega^2(x-1) & \omega(x-1) \\ \omega(x-1) & 2+x & \omega^2(x-1) \\ \omega^2(x-1) & \omega(x-1) & 2+x \end{pmatrix} \text{ and}$$

$$m_3(\theta) = \frac{1}{3} \begin{pmatrix} 2+x & \omega(x-1) & \omega^2(x-1) \\ \omega^2(x-1) & 2+x & \omega(x-1) \\ \omega(x-1) & \omega^2(x-1) & 2+x \end{pmatrix} ,$$

where x is a short-hand notation for $e^{i\theta}$.

The $n \times n$ matrices $m_k(\theta)$ are a generalization of the 2×2 NEGATOR $N(\theta)$: they are a unitary interpolation between the $n \times n$ unit matrix $m_k(0)$ and the $n \times n$

generalized NOT matrix $m_k(\pi) = \mathbf{1}_n - 2g_k$. We have only one 2×2 generalized NOT, i.e. the classical NOT:

$$m_2(\pi) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} ;$$

we have two 3×3 generalized NOTs:

$$m_2(\pi) = \frac{1}{3}\begin{pmatrix} 1 & -2\omega^2 & -2\omega \\ -2\omega & 1 & -2\omega^2 \\ -2\omega^2 & -2\omega & 1 \end{pmatrix} \text{ and } m_3(\pi) = \frac{1}{3}\begin{pmatrix} 1 & -2\omega & -2\omega^2 \\ -2\omega^2 & 1 & -2\omega \\ -2\omega & -2\omega^2 & 1 \end{pmatrix} ;$$

we have three 4×4 generalized NOTs:

$$m_2(\pi) = \frac{1}{2}\begin{pmatrix} 1 & -i & 1 & i \\ i & 1 & -i & 1 \\ 1 & i & 1 & -i \\ -i & 1 & i & 1 \end{pmatrix} , m_3(\pi) = \frac{1}{2}\begin{pmatrix} 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \\ -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \end{pmatrix} , \text{ and}$$

$$m_4(\pi) = \frac{1}{2}\begin{pmatrix} 1 & i & 1 & -i \\ -i & 1 & i & 1 \\ 1 & -i & 1 & i \\ i & 1 & -i & 1 \end{pmatrix} ;$$

etcetera.

By applying the KAK decomposition [22] [23] of U(3), it is proved in [17] that any XU circuit can be decomposed into a cascade of

- uncontrolled NEGATORs,
- singly controlled V gates, and
- doubly controlled NOTs.

E.g. the above CXU(3) matrix $m_3(\theta)$ has the following XU(3) KAK decomposition:

$$V_0(\theta_0)V_3(\theta_1)V_2(\theta_2)V_3(\theta_3) = V_0(\theta/2)V_3(\pi-\theta/2)V_2(\pi)V_3(0)$$

$$= \frac{1}{3}\begin{pmatrix} 1+2y & 1-y & 1-y \\ 1-y & 1+2y & 1-y \\ 1-y & 1-y & 1+2y \end{pmatrix} \frac{1}{3}\begin{pmatrix} 1-2c & 1+c+\sqrt{3}s & 1+c-\sqrt{3}s \\ 1+c-\sqrt{3}s & 1-2c & 1+c+\sqrt{3}s \\ 1+c+\sqrt{3}s & 1+c-\sqrt{3}s & 1-2c \end{pmatrix} \frac{1}{3}\begin{pmatrix} -1 & 2 & 2 \\ 2 & -1 & 2 \\ 2 & 2 & -1 \end{pmatrix} ,$$

where we follow the notations V_0, V_1, V_2, and V_3 of Appendix A of Reference [17] and where c and s are short-hand notations for $\cos(\theta/2)$ and $\sin(\theta/2)$, respectively, and y is $c+is = \sqrt{x}$. Subsequently, we can apply to each of these three matrices the XU(4) KAK decomposition. E.g. the rightmost matrix appears in the 2-qubit block-circulant matrix

$$\frac{1}{3}\begin{pmatrix} 3 & 0 & 0 & 0 \\ 0 & -1 & 2 & 2 \\ 0 & 2 & -1 & 2 \\ 0 & 2 & 2 & -1 \end{pmatrix}$$

with decomposition

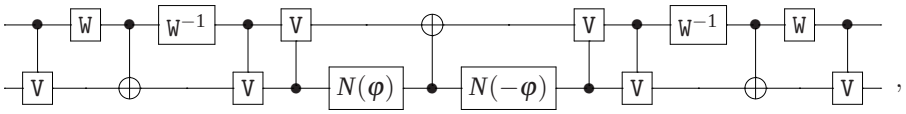
$$\begin{aligned} & V_0(\theta_0)V_3(\theta_1)V_2(\theta_2)V_3(\theta_3)V_5(\theta_4)V_3(\theta_5)V_2(\theta_6)V_3(\theta_7)V_8(\theta_8) \\ &= V_0(0)V_3(0)V_2(7\pi/4)V_3(0)V_5(\varphi)V_3(0)V_2(\pi/4)V_3(0)V_8(0) \end{aligned}$$

$$= \frac{1}{4}\begin{pmatrix} 2-\sqrt{2} & 2+\sqrt{2} & \sqrt{2} & -\sqrt{2} \\ 2+\sqrt{2} & 2-\sqrt{2} & -\sqrt{2} & \sqrt{2} \\ -\sqrt{2} & \sqrt{2} & 2-\sqrt{2} & 2+\sqrt{2} \\ \sqrt{2} & -\sqrt{2} & 2+\sqrt{2} & 2-\sqrt{2} \end{pmatrix}$$

$$\frac{1}{3}\begin{pmatrix} 1 & -\sqrt{2} & 2 & \sqrt{2} \\ \sqrt{2} & 1 & -\sqrt{2} & 2 \\ 2 & \sqrt{2} & 1 & -\sqrt{2} \\ -\sqrt{2} & 2 & \sqrt{2} & 1 \end{pmatrix} \frac{1}{4}\begin{pmatrix} 2+\sqrt{2} & 2-\sqrt{2} & \sqrt{2} & -\sqrt{2} \\ 2-\sqrt{2} & 2+\sqrt{2} & -\sqrt{2} & \sqrt{2} \\ -\sqrt{2} & \sqrt{2} & 2+\sqrt{2} & 2-\sqrt{2} \\ \sqrt{2} & -\sqrt{2} & 2-\sqrt{2} & 2+\sqrt{2} \end{pmatrix},$$

where, this time, we follow the notations V_0, V_1, ..., and V_8 of Appendix B of Reference [17] and where φ is the angle $\pi + \text{Arccos}(1/3)$. This matrix decomposition leads to the circuit synthesis with

- six uncontrolled NEGATORs,
- six controlled V gates, and
- three controlled NOTs:



,

where $\mathsf{W}^{-1} = \mathsf{XVW} = N(7\pi/4)$.

11 Conclusion

With the help of truth tables, we have demonstrated that conventional Boolean computation can be embedded in classical reversible computation. With the help of square matrices, we have demonstrated that classical reversible computation is a subspace of quantum computation. Classical reversible computing relates to quantum computing like permutation matrices relate to unitary matrices. The permutation matrix group P(n) forms a subgroup of the unitary matrix group U(n). The main leap from P(n) matrices to U(n) matrices happens by interpolation between two or more permutation matrices, thus enlarging the finite group P(n) to the infinite group XU(n). Figure 2 shows in detail the hierarchy of groups and subgroups, revealing the relationship between the finite group P(n) and the infinite group U(n). The decomposition of a given U(2^w) matrix into ZU(2^w) and CXU(2^w) matrices leads to a w-qubit synthesis of the U(2^w) circuit with PHASOR and NEGATOR building blocks.

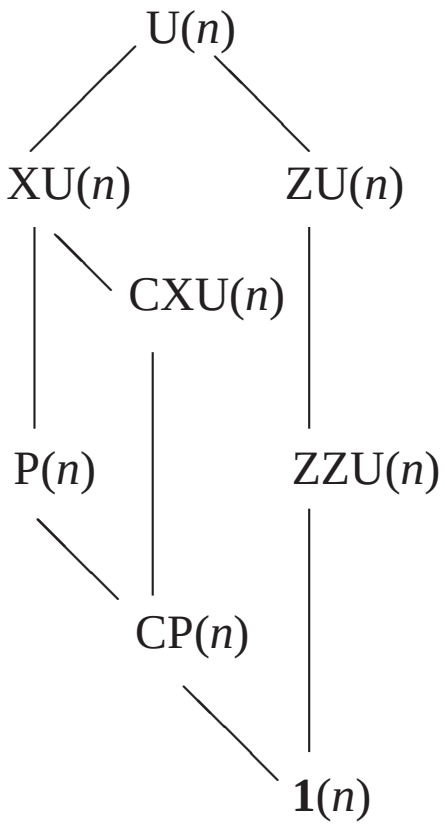


Fig. 2 Hierarchy of the Lie groups U(n), XU(n), ZU(n), CXU(n), and ZZU(n) and the finite groups P(n), CP(n), and **1**(n).

Acknowledgements The authors thank prof. Andrew Adamatzky, editor of the present book, for inviting them to write the present chapter. They acknowledge the support by the European COST Action IC 1405 'Reversible Computation'.

Appendix

For any matrix P from the group P(n), the following property holds:

$$P = C \begin{pmatrix} 1 & \\ & P' \end{pmatrix} ,$$

where

- P' is a member of P($n-1$) and
- C is a member of CP(n).

Here, CP(n) denotes the group of $n \times n$ circulant permutation matrices. It is a group isomorphic with the cyclic group $\mathbf{Z}_n$, a finite group of order n. Remarkable is the fact that here $\begin{pmatrix} 1 & \\ & P' \end{pmatrix}$ is only multiplied to the left with a circulant matrix, whereas in decomposition (5), the matrix $\begin{pmatrix} 1 & \\ & X' \end{pmatrix}$ is multiplied both to the left and to the right with a circulant matrix.

The decomposition algorithm is very straightforward: suffice it to choose C such that it has the same leftmost column as the given matrix P. Subsequently, the matrix $\begin{pmatrix} 1 & \\ & P' \end{pmatrix}$ follows automatically by computing $C^{-1}P$. Here follows an example from P(4):

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

By applying the theorem again and again, we find the following decomposition:

$$P = C_n \begin{pmatrix} 1 & \\ & C_{n-1} \end{pmatrix} \ldots \begin{pmatrix} \mathbf{1}_{n-3} & \\ & C_3 \end{pmatrix} \begin{pmatrix} \mathbf{1}_{n-2} & \\ & C_2 \end{pmatrix} , \tag{7}$$

where all C_k are CP(k) matrices. We conclude: any $n \times n$ permutation matrix can be decomposed as a product of $n-1$ matrices of the form $\begin{pmatrix} \mathbf{1}_{n-k} & \\ & C_k \end{pmatrix}$. We give an example:

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

Decomposition (6) is not a straightforward generalization of (7). This constitutes an illustration of the fact that, in spite of an overall similarity between the group P(n) and the group XU(n), literal translations from P(n) properties to XU(n) properties sometimes fail [24].

References

1. Nielsen, M., Chuang, I.: Quantum computation and quantum information. Cambridge University Press, Cambridge (2000)
2. Fredkin, E., Toffoli, T.: Conservative logic. *International Journal of Physics* **21**, 219 (1982)
3. De Vos A., Van Rentergem, Y.: From group theory to reversible computers. In: Adamatzky, A., Teuscher, C.: From utopian to genuine unconventional computers, Luniver Press, Frome (2006) pp 183-208
4. De Vos, A.: Reversible computing. Wiley–VCH, Weinheim (2010)
5. Wille, R., Drechsler, R.: Towards a design flow for reversible logic. Springer, Dordrecht (2010)
6. Soeken, M., Wille, R., Keszöcze, O., Miller, M., Drechsler, R.: Embedding of large Boolean functions for reversible logic. *ACM Journal on Emerging Technologies in Computing Systems*, in press
7. De Vos, A., De Baerdemacker, S.: The decomposition of U(n) into XU(n) and ZU(n). In: *Proc. 44 th Int. Symposium on Multiple-Valued Logic*, Bremen, 19-21 May 2014, pp 173-177

8. De Vos, A., De Baerdemacker, S.: Matrix calculus for classical and quantum circuits. *ACM Journal on Emerging Technologies in Computing Systems* **11**, 9 (2014)
9. De Vos, A., De Baerdemacker, S.: On two subgroups of U(n), useful for quantum computing. *Proc. 30 th Int. Colloquium on Group-theoretical Methods in Physics*, Gent, 14-18 July 2014, *Journal of Physics: Conference Series* **597**, 012030 (2015)
10. Sasanian, Z., Miller, D.: Transforming MCT circuits to NCVW circuits. In: *Proc. 3 rd Int. Workshop on Reversible Computation*, Gent, 4-5 July 2011, pp 163–174
11. Amy, M., Maslov, D., Mosca, M.: Polynomial-time T-depth optimization of Clifford+T circuits via matroid partitioning. *IEEE Trans. on Computer-Aided Design of Integrated Circuits and Systems* **33**, 1486 (2013)
12. Selinger, P.: Efficient Clifford+T approximations of single-qubit operators. *Quantum Information & Computation* **15**, 159 (2015)
13. Deutsch, D.: Quantum computation. *Physics World* **5**, 57 (1992)
14. Galindo, A., Martín-Delgado, M.: Information and computation: classical and quantum aspects. *Review of Modern Physics* **74**, 347 (2002)
15. De Vos, A., De Beule, J., Storme, L.: Computing with the square root of NOT. *Serdica Journal of Computing* **3**, 359 (2009)
16. Vandenbrande, S., Van Laer, R., De Vos, A.: The computational power of the square root of NOT. In: *Proc. 10 th Int. Workshop on Boolean Problems*, Freiberg, 19-21 September 2012, pp 257–262
17. De Vos, A., De Baerdemacker, S.: The NEGATOR as a basic building block for quantum circuits. *Open Systems & Information Dynamics* **20**, 1350004 (2013)
18. De Vos, A., De Baerdemacker, S.: Scaling a unitary matrix. *Open Systems & Information Dynamics* **21**, 1450013 (2014)
19. Idel, M., Wolf, M.: Sinkhorn normal form for unitary matrices. *Linear Algebra and its Applications* **471**, 76 (2015)
20. Beth, T., Rötteler, M.: Quantum algorithms: applicable algebra and quantum physics, In: Alber, G., Beth, T., Horodecki, M., Horodecki, P., Horodecki, R., Rötteler, M., Weinfurter, H., Werner, R., Zeilinger, A.: Quantum information. Springer Verlag, Berlin (2001), pp 96–150
21. Barenco, A., Bennett, C., Cleve, R., DiVincenzo, D., Margolus, N., Shor, P., Sleator, T., Smolin, J., Weinfurter, H.: Elementary gates for quantum computation. *Physical Review A* **52**, 3457 (1995)
22. Hermann, R.: Lie groups for physicists. Benjamin Inc., New York (1966), pp 30-39
23. Bullock, S., Markov, I.: An arbitrary two-qubit computation in 23 elementary gates. *Physical Review A* **68**, 012318 (2003)
24. De Vos, A., De Baerdemacker, S.: Symmetry groups for the decomposition of reversible computers, quantum computers, and computers in between. *Symmetry* **3**, 305 (2011)