On two subgroups of U(*n*), useful for quantum computing

2015 J. Phys.: Conf. Ser. 597 012030

(http://iopscience.iop.org/1742-6596/597/1/012030)

Journal of Physics: Conference Series **597** (2015) 012030 doi:10.1088/1742-6596/597/1/012030

On two subgroups of U(n), useful for quantum computing

Alexis De Vos[1] and Stijn De Baerdemacker[2]

[1]Cmst, Vakgroep elektronika en informatiesystemen, Imec v.z.w., Universiteit Gent, Sint Pietersnieuwstraat 41, B - 9000 Gent, Belgium
[2]Center for Molecular Modeling, Vakgroep fysica en sterrenkunde, Universiteit Gent, Technologiepark 903, B - 9052 Gent, Belgium
[2]Ghent Quantum Chemistry Group, Vakgroep anorganische en fysische chemie, Universiteit Gent, Krijgslaan 281 - S3, B - 9000 Gent, Belgium

E-mail: `alex@elis.UGent.be, Stijn.DeBaerdemacker@UGent.be`

Abstract. As two basic building blocks for any quantum circuit, we consider the 1-qubit `PHASOR` circuit $\Phi(\theta)$ and the 1-qubit `NEGATOR` circuit $N(\theta)$. Both are roots of the `IDENTITY` circuit. Indeed: both $\Phi(0)$ and $N(0)$ equal the 2×2 unit matrix. Additionally, the `NEGATOR` is a root of the classical `NOT` gate. Quantum circuits (acting on w qubits) consisting of controlled `PHASOR`s are represented by matrices from ZU(2^w); quantum circuits consisting of controlled `NEGATOR`s are represented by matrices from XU(2^w). Here, ZU(n) and XU(n) are subgroups of the unitary group U(n): the group XU(n) consists of all $n \times n$ unitary matrices with all $2n$ line sums (i.e. all n row sums and all n column sums) equal to 1 and the group ZU(n) consists of all $n \times n$ unitary diagonal matrices with first entry equal to 1. Any U(n) matrix can be decomposed into four parts: $U = \exp(i\alpha)\, Z_1 X Z_2$, where both Z_1 and Z_2 are ZU(n) matrices and X is an XU(n) matrix. We give an algorithm to find the decomposition. For $n = 2^w$ it leads to a four-block synthesis of an arbitrary quantum computer.

1. Introduction

The unitary group U(n) is important for quantum computing, because all quantum circuits acting on w qubits can be represented by a member of the unitary group U(2^w). For example, all quantum circuits, acting on a single qubit, are represented by a matrix from U(2). The simplest U(2) matrix is the 2×2 unit matrix. It represents the `IDENTITY` gate or `I` gate:

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

This gate is trivial, as it performs no action on the qubit: the output qubit equals the input qubit. Within U(2), the `I` matrix has a lot of square roots: four diagonal matrices

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

as well as an infinity of 'anti-diagonal' matrices:

$$\sqrt{-1} \begin{pmatrix} 0 & e^{i\chi} \\ -e^{-i\chi} & 0 \end{pmatrix},$$

where χ is an arbitrary real number. From this set, we choose two elements:

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

The latter matrix results from the choices $\sqrt{-1} = -i$ and $\chi = \pi/2$ and represents the `NOT` gate or `X` gate [1]. The former matrix represents the `Z` gate. Whereas the `X` gate is a classical computer gate, inverting the incoming bit, the `Z` gate is a true quantum gate.

We now introduce a generalization of both the `X` and the `Z` matrix:

$$\begin{aligned} N(t) &= (1-t)\,\mathtt{I} + t\,\mathtt{X} \\ \Phi(t) &= (1-t)\,\mathtt{I} + t\,\mathtt{Z}\ , \end{aligned}$$

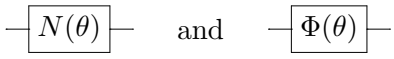
where t is an interpolation parameter [2]. We can easily prove that these matrices are unitary, iff t is of the form $(1-e^{i\theta})/2$, resulting in

$$\begin{aligned} N(\theta) &= \tfrac{1}{2}\,(1+e^{i\theta})\,\mathtt{I} + \tfrac{1}{2}\,(1-e^{i\theta})\,\mathtt{X} \\ \Phi(\theta) &= \tfrac{1}{2}\,(1+e^{i\theta})\,\mathtt{I} + \tfrac{1}{2}\,(1-e^{i\theta})\,\mathtt{Z}\ . \end{aligned}$$

We thus have constructed two 1-dimensional subgroups of the 4-dimensional group U(2):

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

The gate represented by the matrix $N(\theta)$, we call the `NEGATOR` gate. It thus constitutes a generalization of the `NOT` gate. The gate represented by the matrix $\Phi(\theta)$, we call the `PHASOR` gate. We use the following symbols for these quantum gates:



respectively. In the literature [3] [4] [5] [6], some of these gates have a particular 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`' [7] [8] [9] [10].

The subgroup of all $N(\theta)$ matrices, we denote by XU(2); the subgroup of all $\Phi(\theta)$ matrices, we denote by ZU(2). These two subgroups of U(2) have three interesting properties.

(i) Their intersection is minimal, as it equals U(2)'s trivial subgroup consisting of merely one 2×2 matrix, i.e. the identity matrix `I`.

(ii) Their closure is maximal, as it equals U(2) itself. Indeed, an arbitrary member of U(2), i.e.

$$U = e^{i\alpha} \begin{pmatrix} \cos(\varphi)\, e^{i\psi} & \sin(\varphi)\, e^{i\chi} \\ -\sin(\varphi)\, e^{-i\chi} & \cos(\varphi)\, e^{-i\psi} \end{pmatrix} \tag{1}$$

can be synthesized by cascading merely `NEGATOR`s and `PHASOR`s. The reader may verify the following two matrix decompositions:

$$\begin{aligned} U &= e^{i\alpha+i\varphi+i\psi} \begin{pmatrix} 1 & 0 \\ 0 & i\, e^{-i\psi-i\chi} \end{pmatrix} \frac{1}{2} \begin{pmatrix} 1+e^{-i2\varphi} & 1-e^{-i2\varphi} \\ 1-e^{-i2\varphi} & 1+e^{-i2\varphi} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -i\, e^{-i\psi+i\chi} \end{pmatrix} \\ U &= e^{i\alpha-i\varphi+i\psi} \begin{pmatrix} 1 & 0 \\ 0 & -i\, e^{-i\psi-i\chi} \end{pmatrix} \frac{1}{2} \begin{pmatrix} 1+e^{i2\varphi} & 1-e^{i2\varphi} \\ 1-e^{i2\varphi} & 1+e^{i2\varphi} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & i\, e^{-i\psi+i\chi} \end{pmatrix}. \end{aligned} \tag{2}$$

Because, moreover, any phase factor can be decomposed as

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

we conclude that U equals the cascade of three `NEGATOR`s and three `PHASOR`s:

$$\begin{aligned} U &= N(\pi)\, \Phi(\alpha+\varphi+\psi)\, N(\pi)\, \Phi(\alpha+\varphi-\chi+\pi/2)\, N(-2\varphi)\, \Phi(-\psi+\chi-\pi/2) \\ U &= N(\pi)\, \Phi(\alpha-\varphi+\psi)\, N(\pi)\, \Phi(\alpha-\varphi-\chi-\pi/2)\, N(2\varphi)\, \Phi(-\psi+\chi+\pi/2) \ . \end{aligned}$$

(iii) We note that the two subgroups are each other's Hadamard conjugate:

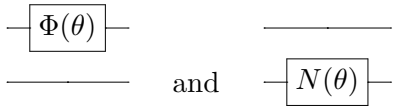
$$\mathrm{ZU}(2) = H\ \mathrm{XU}(2)\ H \quad \text{and} \quad \mathrm{XU}(2) = H\ \mathrm{ZU}(2)\ H \ ,$$

where H denotes the Hadamard matrix:

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

2. Decomposition of an arbitrary unitary matrix

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:

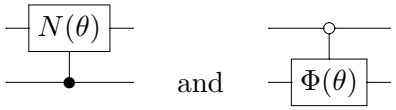


i.e. a `PHASOR` acting on the first qubit and a `NEGATOR` acting on the second qubit, respectively. These circuits are represented by the 4×4 unitary matrices

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

respectively.

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

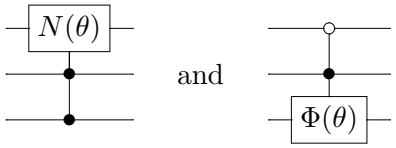


i.e. a positive-polarity controlled NEGATOR acting on the first qubit, controlled by the second qubit, and a negative-polarity controlled PHASOR acting on the second qubit, controlled by the first qubit, respectively. The former symbol is read as follows: 'if the second qubit equals 1, then the NEGATOR 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 matrices representing these circuit examples are:

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

respectively.

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



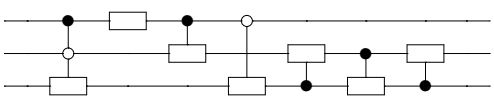
i.e. a positive-polarity controlled NEGATOR acting on the first qubit and a mixed-polarity controlled PHASOR acting on the third qubit. The 8×8 matrices representing these circuit examples are:

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

respectively. We note the following properties:

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

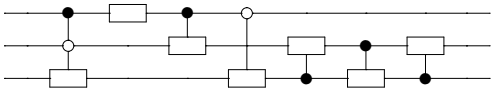
Because the multiplication of two square matrices with all line sums equal to 1 automatically yields a third square matrix with all line sums equal to 1, we can easily demonstrate that an arbitrary quantum circuit like



,

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. The $n \times n$ unitary matrices with all line sums equal to 1 form a group XU(n), subgroup of U(n). We thus can say that an arbitrary NEGATOR circuit is represented by an XU(2^w) matrix. A laborious proof [11] demonstrates that the converse theorem is also valid: any member of XU(2^w) can be synthesized by an appropriate 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. The $n \times n$ unitary diagonal matrices with upper-left entry equal to 1 form a group ZU(n), subgroup of U(n). We thus can say that an arbitrary PHASOR circuit is represented by a ZU(2^w) matrix. The converse theorem is also valid: any member of ZU(2^w) can be synthesized by an appropriate string of (un)controlled PHASORs.

We summarize: the study of NEGATOR and PHASOR circuits leads to the introduction of two subgroups of the unitary group U(n):

- the subgroup XU(n), consisting of all $n \times n$ unitary matrices with all of their $2n$ line sums are equal to 1;
- the subgroup ZU(n), consisting of all $n \times n$ diagonal unitary matrices with upper-left entry equal to 1.

These subgroups have properties similar to the three properties of XU(2) and ZU(2), discussed in the previous section.

(i) The intersection of XU(n) and ZU(n) is minimal, as it is the trivial subgroup consisting of a single matrix, i.e. the $n \times n$ unit matrix.

(ii) The closure of XU(n) and ZU(n) is U(n). Indeed, any U(n) matrix U can be decomposed as

$$U = e^{i\alpha}\, Z_1 X_1 Z_2 X_2 Z_3 ... Z_{p-1} X_{p-1} Z_p \ , \tag{3}$$

with $p \leq n$ and where all Z_j are ZU(n) matrices and all X_j are XU(n) matrices [12]. Because we have the identity

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

where a is a short-hand notation for $e^{i\alpha}$ and P_0 is the circulant permutation matrix

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

we can conclude that U equals the product of $n+1$ or less XU(n) members and $n+2$ or less ZU(n) members.

(iii) We have that

$$\mathrm{ZU}(n) \subset H_n\ \mathrm{XU}(n)\ H_n \ \text{ and } \ \mathrm{XU}(n) \supset H_n\ \mathrm{ZU}(n)\ H_n\ ,$$

where H_n is an $n \times n$ complex Hadamard matrix [13]. In particular, the group $H_n\ \mathrm{ZU}(n)\ H_n$ is the subgroup of $\mathrm{XU}(n)$ consisting of all circulant $\mathrm{XU}(n)$ matrices. For arbitrary n, one may choose for H_n the $n \times n$ discrete Fourier transform F_n:

$$F_n = \begin{pmatrix} 1 & 1 & 1 & 1 & ... & 1 \\ 1 & \omega & \omega^2 & \omega^3 & ... & \omega^{n-1} \\ 1 & \omega^2 & \omega^4 & \omega^6 & ... & \omega^{2(n-1)} \\ \vdots & & & & & \\ 1 & \omega^{n-1} & \omega^{2(n-1)} & \omega^{3(n-1)} & ... & \omega^{(n-1)(n-1)} \end{pmatrix}\ ,$$

where ω is the primitive n th root of unity. For $n = 2^w$, also the real Hadamard matrix $H^{\otimes w}$ (Kronecker product of 2×2 Hadamard matrices H) is a possible choice:

$$\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes ... \otimes \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\ ,$$

with w factors in the tensor product.

Because of the identity

$$\begin{aligned} \mathrm{diag}(1, a_2, a_3, ..., a_{n-1}, a_n) \ &= \ \mathrm{diag}(1, a_2, 1, ..., 1, 1)\ \mathrm{diag}(1, 1, a_3, ..., 1, 1)\ ... \\ &\quad\ \mathrm{diag}(1, 1, 1, ..., a_{n-1}, 1)\ \mathrm{diag}(1, 1, 1, ..., 1, a_n)\ , \end{aligned}$$

it is clear that the group $\mathrm{ZU}(n)$ is isomorphic to the direct product $\mathrm{U}(1)^{n-1}$ and thus is an $(n-1)$-dimensional Lie group. The group $\mathrm{XU}(n)$ is isomorphic to its conjugate

$$F_n\ \mathrm{XU}(n)\ F_n^{-1}\ .$$

One can verify that, if X is an $\mathrm{XU}(n)$ matrix, then the matrix $F_n X F_n^{-1}$ is an $n \times n$ unitary matrix with first row $1, 0, 0, ..., 0$ and thus also first column $1, 0, 0, ..., 0$. Conversely, it is possible to prove that a matrix of the form

$$X = F_n \begin{pmatrix} 1 & \mathbf{0}_{1\times(n-1)} \\ \mathbf{0}_{(n-1)\times 1} & Y \end{pmatrix} F_n^{-1}\ , \tag{4}$$

where $\mathbf{0}_{a\times b}$ denotes the $a \times b$ zero matrix and Y is an arbitrary member of $\mathrm{U}(n-1)$, is an $\mathrm{XU}(n)$ matrix [11]. Thus $\mathrm{XU}(n)$ is isomorphic to $\mathrm{U}(n-1)$ and therefore is an $(n-1)^2$-dimensional subgroup of the n^2-dimensional group $\mathrm{U}(n)$. We summarize by noting the beautiful symmetry

$$\mathrm{ZU}(n) \cong \mathrm{U}(1)^{n-1} \ \text{ and } \ \mathrm{XU}(n) \cong \mathrm{U}(n-1)^1\ .$$

In the past, properties of the subgroup $\mathrm{XU}(n)$ of $\mathrm{U}(n)$ have not been studied. Here, we note in particular the group chain

$$\mathrm{P}(n) \subset \mathrm{XU}(n) \subset \mathrm{U}(n)\ ,$$

where $\mathrm{P}(n)$ denotes the finite group of $n \times n$ permutation matrices. As all classical reversible circuits (acting on w bits) are represented by a matrix from $\mathrm{P}(2^w)$, we may say that the group $\mathrm{XU}(2^w)$ represents computers, situated 'between' classical computers and full-fledged quantum computers.

Decomposition (3) should be compared with other factorizations of U(n), described in the literature. Diţă [14] has proposed a product $D_nO_nD_{n-1}O_{n-1}...D_2O_2D_1$, where all D_j are diagonal unitary matrices and all O_j are orthogonal matrices. Reck et al. [15] have derived a decomposition of the form $T_1T_2...T_pD$, where all T_j are 2-parameter unitary matrices (describing a beam splitter plus phase shifter), D is a diagonal matrix, and $p \leq n(n-1)/2$. Rowe et al. [16] have applied two mutually commuting subgroups of U(n). Finally, Patera and Zassenhaus [17] have introduced the generalized Pauli group $\mathcal{P}_n$. We note that, for odd n, this finite group is generated by the permutation matrix P_0 together with a particular member of ZU(n), i.e. diag$(1, \omega, \omega^2, ..., \omega^{n-1})$, where ω is the primitive n th root of unity.

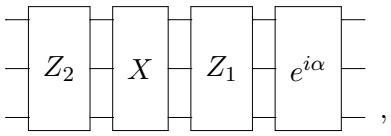
3. Short decomposition of an arbitrary unitary matrix

In Reference [18], it is conjectured that a shorter decomposition (3) exists: with $p \leq 2$. Thus an arbitrary member U of U(n) may be decomposed as

$$U = \exp(i\alpha)\, Z_1 X Z_2 \ , \tag{5}$$

with X a member of XU(n) and both Z_1 and Z_2 member of ZU(n). For $n = 2$, the conjecture is proved by eqns (2). For an arbitrary unitary matrix U with $n > 2$, a recent (non-constructive) proof is provided by Idel and Wolf [19], based on symplective topology. For a given unitary matrix U, De Vos and De Baerdemacker [18] provide a numerical procedure (reminiscent of Sinkhorn's construction [20] of a doubly stochastic matrix) in order to find the scalar $\exp(i\alpha)$, as well as the three matrices Z_1, X, and Z_2. For thousands of examples (from $3 \leq n \leq 32$), the algorithm converges to a solution. We conjecture that the algorithm always converges.

Thus any quantum circuit looks like

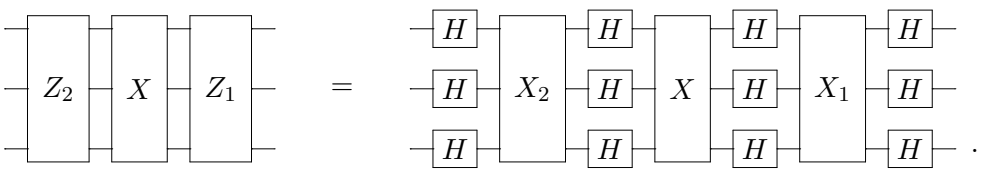


i.e. the cascade of an overall phase factor, an input section consisting merely of (un)controlled PHASORs, a core section consisting merely of (un)controlled NEGATORs, and an output section consisting merely of (un)controlled PHASORs. In turn, the phase factor $e^{i\alpha}$ may be decomposed into two NEGATOR circuits (i.e. two classical cyclic-shift circuits [21] [22]) and two uncontrolled PHASORs. We note that this circuit decomposition is not unique, because the matrix decomposition (5) is not unique. See Appendix.

Instead of synthesizing a quantum circuit with X and Z building-blocks, one can also opt for X and Hadamard blocks. Indeed, introducing the circulant XU(2^w) matrices

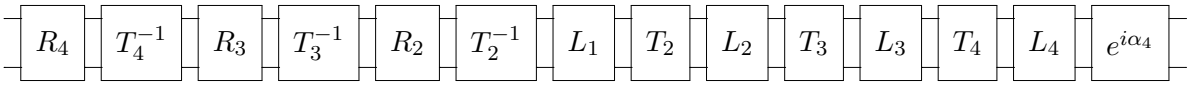
$$\begin{aligned} X_1 &= H^{\otimes w}\, Z_1\, H^{\otimes w} \\ X_2 &= H^{\otimes w}\, Z_2\, H^{\otimes w} \ , \end{aligned}$$

we have



Thus any quantum computer (up to an overall phase) consists of three (or less) NEGATOR circuits and $4w$ (or less) HADAMARD gates.

By applying alternatingly (4) and (5), again and again, i.e. for $n = 2^w$, $n = 2^w - 1$, $n = 2^w - 2$, ..., and finally for $n = 2$, we find yet another decomposition of an arbitrary quantum computer [19] [23]:



Here the circuits T_2, T_3, ..., and T_{2^w} implement the constant block-diagonal matrices

$$T_j = \begin{pmatrix} \mathbf{1}_{2^w-j} & \\ & F_j \end{pmatrix} ,$$

where $\mathbf{1}_a$ is the $a \times a$ unit matrix and F_j is the $j \times j$ discrete Fourier transform. The $2^w - 1$ circuits R_j and the 2^w circuits L_j are

- either ZU(2^w) circuits
- or circulant XU(2^w) circuits.

4. Conclusion

Like the qubit being a quantum counterpart of the classical bit, the `NEGATOR` gate is the quantum counterpart of the classical `NOT` gate and the controlled `NEGATOR` is the quantum counterpart of the classical controlled `NOT` (a.k.a. the `TOFFOLI` gate). Any quantum circuit can be built from (un)controlled `NEGATOR`s, supplemented with either (un)controlled `PHASOR` gates or `HADAMARD` gates.

Appendix

The matrix decomposition (5) is not unique. For $n = 2$, eqns (2) show two different solutions. E.g. the 2×2 discrete Fourier transform (a.k.a. the Hadamard transform)

$$F_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

has two and only two decompositions:

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

and

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

However, if, in (1), either $\cos(\varphi)$ or $\sin(\varphi)$ is zero, decompositions (2) constitute an infinity of decompositions. This is confirmed by the identities

$$\begin{pmatrix} e^{ix} & 0 \\ 0 & e^{iy} \end{pmatrix} = e^{ix} \begin{pmatrix} 1 & 0 \\ 0 & e^{-ix+iz} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & e^{iy-iz} \end{pmatrix} \quad \text{and}$$

$$\begin{pmatrix} 0 & e^{ix} \\ e^{iy} & 0 \end{pmatrix} = e^{iz} \begin{pmatrix} 1 & 0 \\ 0 & e^{iy-iz} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & e^{ix-iz} \end{pmatrix} ,$$

where, in both cases, z may take any value.

If $n > 2$, then an infinity of decompositions of the matrix U arises whenever the matrix contains a row with $n - 1$ zeroes and thus automatically also a column with $n - 1$ zeroes

(provided that row is not the first row and that column is not the first column). If no such row (and column) is present, there may be either a finite or an infinite number of decompositions. The former is illustrated by the example of the 3×3 discrete Fourier transform:

$$F_3 = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix} ,$$

where ω is the primitive cubic root of unity, i.e. $-\frac{1}{2} + i\frac{\sqrt{3}}{2}$. Indeed, for this matrix six and only six decompositions are possible:

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

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

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

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

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

and

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

The latter is illustrated by the decomposition of the 4×4 Fourier matrix:

$$\begin{aligned} F_4 &= \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix} \\ &= 1 \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & a & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -a \end{pmatrix} \frac{1}{2} \begin{pmatrix} 1 & -ia & 1 & ia \\ 1/a & 1 & -1/a & 1 \\ 1 & ia & 1 & -ia \\ -1/a & 1 & 1/a & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & i/a & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -i/a \end{pmatrix} \\ &= \frac{1}{b} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & b & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & b \end{pmatrix} \frac{1}{2} \begin{pmatrix} b & 1 & -b & 1 \\ 1 & i/b & 1 & -i/b \\ -b & 1 & b & 1 \\ 1 & -i/b & 1 & i/b \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & b & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & b \end{pmatrix} , \end{aligned}$$

where both a and b are allowed to have any value on the unit circle of the complex plane.

The Fourier matrices F_n not only are important in quantum computing [1], but also in quantum optics. In the latter application, they constitute the canonical form of the $n \times n$ unitary matrices with all entries having the same modulus (i.e. having modulus $1/\sqrt{n}$). Constant-modulus unitary matrices are important for multiports (particle beam splitters) [24].

References

[1] Nielsen M and Chuang I 2000 *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press)
[2] De Vos A and De Baerdemacker S 2014 Matrix calculus for classical and quantum circuits *A.C.M. Journal on Emerging Technologies in Computing Systems* **11** 9
[3] Wille R and Drechsler R 2010 *Towards a Design Flow for Reversible Logic* (Dordrecht: Springer)
[4] Sasanian Z and Miller D 2011 Transforming MCT circuits to NCVW circuits *Proc. 3 rd Int. Workshop on Reversible Computation (Gent)* pp 163–174
[5] Selinger P 2015 Efficient Clifford+T approximations of single-qubit operators *Quantum Information & Computation* **15** 159
[6] Amy M, Maslov D and Mosca M 2013 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
[7] Deutsch D 1992 Quantum computation *Physics World* **5** 57
[8] Galindo A and Martín-Delgado M 2002 Information and computation: classical and quantum aspects *Review of Modern Physics* **74** 347
[9] De Vos A, De Beule J and Storme L 2009 Computing with the square root of `NOT` *Serdica Journal of Computing* **3** 359
[10] Vandenbrande S, Van Laer R and De Vos A 2012 The computational power of the square root of `NOT` *Proc. 10 th Int. Workshop on Boolean Problems (Freiberg)* pp 257–262
[11] De Vos A and De Baerdemacker S 2013 The `NEGATOR` as a basic building block for quantum circuits *Open Systems & Information Dynamics* **20** 1350004
[12] De Vos A and De Baerdemacker S 2014 The decomposition of U(n) into XU(n) and ZU(n) *Proc. 44 th Int. Symposium on Multiple-Valued Logic (Bremen)* pp 173–177
[13] Tadej W and Życzkowski K 2006 A concise guide to complex Hadamard matrices *Open Systems & Information Dynamics* **13** 133
[14] Diţă P 2003 Factorization of unitary matrices *Journal of Physics A: Mathematical and General* **36** 2781
[15] Reck M, Zeilinger A, Bernstein H and Bertani P 1994 Experimental realization of any discrete unitary operator *Physical Review Letters* **73** 58
[16] Rowe D, Sanders B and de Guise H 1999 Representations of the Weyl group and Wigner functions for SU(3) *Journal of Mathematical Physics* **40** 3604
[17] Patera J and Zassenhaus H 1988 The Pauli matrices in n dimensions and finest gradings of simple Lie algebras of type A_{n-1} *Journal of Mathematical Physics* **29** 667
[18] De Vos A and De Baerdemacker S 2014 Scaling a unitary matrix *Open Systems & Information Dynamics* **21** 1450013
[19] Idel M and Wolf M 2014 Sinkhorn normal form for unitary matrices (`arXiv:math-ph` 1408.5728)
[20] Sinkhorn R 1964 A relationship between arbitrary positive matrices and doubly stochastic matrices *The Annals of Mathematical Statistics* **35** 876
[21] Beth T and Rötteler M 2001 Quantum algorithms: applicable algebra and quantum physics In: Alber G, Beth T, Horodecki M, Horodecki P, Horodecki R, Rötteler M, Weinfurter H, Werner R and Zeilinger A 2001 *Quantum Information* (Berlin: Springer Verlag) pp 96–150
[22] De Vos A 2010 *Reversible Computing* (Weinheim: Wiley–VCH Verlag) p 49
[23] De Vos A and De Baerdemacker S 2014 The synthesis of a quantum circuit *Proc. 11 th Int. Workshop on Boolean Problems (Freiberg)* pp 129–136
[24] Mattle K, Michler M, Weinfurter H, Zeilinger A and Zukowski M 1995 Non-classical statistics at multiport beam splitters *Applied Physics B* **60** S111