PHYSICAL REVIEW A **94**, 052317 (2016)

Block-ZXZ synthesis of an arbitrary quantum circuit

A. De Vos[1,*] and S. De Baerdemacker[2,3,†]
[1]*Cmst, Imec v.z.w., vakgroep elektronica en informatiesystemen, Universiteit Gent, B-9000 Gent, Belgium*
[2]*Center for Molecular Modeling, vakgroep fysica en sterrenkunde, Universiteit Gent, B-9000 Gent, Belgium*
[3]*Ghent Quantum Chemistry Group, vakgroep anorganische en fysische chemie, Universiteit Gent, B-9000 Gent, Belgium*
(Received 31 May 2016; published 14 November 2016)

Given an arbitrary $2^w \times 2^w$ unitary matrix U, a powerful matrix decomposition can be applied, leading to four different syntheses of a w-qubit quantum circuit performing the unitary transformation. The demonstration is based on a recent theorem by H. Führ and Z. Rzeszotnik [Linear Algebra Its Appl. **484**, 86 (2015)] generalizing the scaling of single-bit unitary gates ($w = 1$) to gates with arbitrary value of w. The synthesized circuit consists of controlled one-qubit gates, such as NEGATOR gates and PHASOR gates. Interestingly, the approach reduces to a known synthesis method for classical logic circuits consisting of controlled NOT gates in the case that U is a permutation matrix.

DOI: 10.1103/PhysRevA.94.052317

I. INTRODUCTION

The group $U(2^w)$, i.e., the group of $2^w \times 2^w$ unitary matrices, describes all quantum circuits acting on w qubits [1]. In the literature, many different decompositions of a unitary matrix U have been proposed to synthesize quantum circuits performing the transformation U. These decompositions can be classified into two categories. The first category of decompositions reduces the dimension of the unitary matrix with one unit, leading to a matrix sequence $U(n)$, $U(n-1)$, $U(n-2), \ldots,$ all the way down to $U(2)$. Notable examples are based on beam-splitter transformations [2] and the Householder decompositions [3–5]. Although these decompositions can be realized physically by means of multibeam splitters or Mach-Zehnder interferometers [2], they are not in natural accordance with a multiqubit architecture. For this, the second category of decompositions is better suited, to which the cosine-sine (CSD) [6], Cartan's *KAK* [7,8], Clifford T [9,10], and related decompositions [11,12] belong. This category reduces a unitary transformation on w qubits, or the w-qubit gate, to a cascade of unitary transformations on $(w-1)$ qubits.

Recently, it was demonstrated [13], in the framework of the ZXZ matrix decomposition, that two subgroups of $U(n)$ are helpful for the first category: (i) $XU(n)$, the group of $n \times n$ unitary matrices with all line sums equal to 1, and (ii) $ZU(n)$, the group of $n \times n$ diagonal unitary matrices with the top left entry equal to 1. They allow the implementation of quantum circuits [14], with the help of 2×2 PHASOR gates and $j \times j$ Fourier-transform gates with $2 \leqslant j \leqslant 2^w = n$, which can be realized, respectively, as phase shifters and as $2n$ multiports in n-mode quantum-optical circuits [2,15,16]. However compact and elegant in mathematical form, the ZXZ decomposition belongs to the first category of decompositions and is not naturally tailored to qubit-based quantum circuits. This is due to the presence of the $j \times j$ Fourier transforms, which act on a j-dimensional subspace of the total $n = 2^w$ Hilbert space, rather than on a subset of the w qubits. The reason for this is the decomposition of an arbitrary $XU(j)$ matrix as

$$F_j \begin{pmatrix} 1 & \\ & U \end{pmatrix} F_j \ ,$$

where F_j is the $j \times j$ Fourier matrix and U is an appropriate $U(j-1)$ matrix. Hence, the size of the matrix to be synthesized decreases only one unit: from j to $j-1$.

Below we will demonstrate that a similar but more natural ZXZ-inspired method exists which respects the qubit structure of the quantum circuit to be synthesized. For this we will explicitly apply the recent block-ZXZ matrix decomposition by Führ and Rzeszotnik [17] to a multiqubit architecture. At each step, the size of the unitary matrix is reduced by a factor of $1/2$, so instead of a matrix sequence from $U(n)$, $U(n-1)$, $U(n-2), \ldots,$ we will take matrices from $U(n)$, $U(n/2)$, $U(n/4), \ldots.$ On the one hand, this means that the method is not applicable for arbitrary n and is only useful for n equal to some power of 2, i.e., for $n = 2^w$. On the other hand, the decomposition is more in line with classical reversible decompositions, respecting the bit structure of the architecture [18]. Indeed, we will also prove that the proposed block-ZXZ decomposition leads to the Birkhoff decomposition of classical reversible circuits when the unitary matrix is a permutation matrix, in contrast to previously proposed methods [6–12].

II. CIRCUIT DECOMPOSITION

De Vos and De Baerdemacker [13,19] noticed the following decomposition of an arbitrary member U of $U(2)$:

$$U = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \frac{1}{2} \begin{pmatrix} 1+c & 1-c \\ 1-c & 1+c \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix}, \qquad (1)$$

where a, b, c, and d are complex numbers with unit modulus. Idel and Wolf [16] proved a generalization, conjectured in [19], for an arbitrary element U of $U(n)$ with arbitrary n:

$$U = Z_1 X Z_2,$$

where Z_1 is an $n \times n$ diagonal unitary matrix, X is an $n \times n$ unitary matrix with all line sums equal to 1, and Z_2 is an $n \times n$ diagonal unitary matrix with the top left entry equal to 1. Führ and Rzeszotnik [17] proved another generalization for

*alex@elis.ugent.be
†stijn.debaerdemacker@ugent.be

an arbitrary element U of U(n), but restricted to even n values:

$$U = \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} \frac{1}{2} \begin{pmatrix} I+C & I-C \\ I-C & I+C \end{pmatrix} \begin{pmatrix} I & 0 \\ 0 & D \end{pmatrix}, \qquad (2)$$

where A, B, C, and D are matrices from U($n/2$) and I is the $n/2 \times n/2$ unit matrix. We note that, in both generalizations, the number of degrees of freedom is the same on the left- and right-hand sides of the equation. In the former case we have

$$n^2 = n + (n-1)^2 + (n-1);$$

in the latter case we have

$$n^2 = 2\left(\frac{n}{2}\right)^2 + \left(\frac{n}{2}\right)^2 + \left(\frac{n}{2}\right)^2.$$

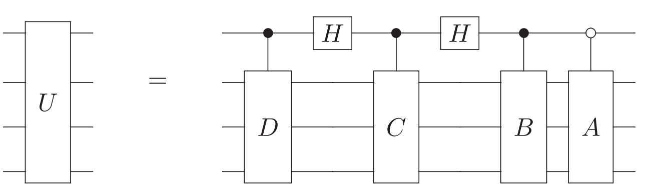
If n equals 2^w, then the decomposition (2) allows a circuit interpretation. Indeed, we can write

$$\begin{pmatrix} I+C & I-C \\ I-C & I+C \end{pmatrix} = F \begin{pmatrix} I & \\ & C \end{pmatrix} F^{-1},$$

where F is the following $n \times n$ complex Hadamard matrix [20]:

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

with I being again the $n/2 \times n/2$ unit matrix and H being the 2×2 Hadamard matrix. We conclude that an arbitrary quantum circuit acting on w qubits can be decomposed into two Hadamard gates and four quantum circuits acting on $w-1$ qubits and controlled by the remaining qubit:



We now can apply the above decomposition to each of the four circuits A, B, C, and D. By acting so again and again, we finally obtain a decomposition into (i) $h = 2(4^{w-1} - 1)/3$ Hadamard gates and (ii) $g = 4^{w-1}$ non-Hadamard quantum gates acting on a single qubit. As the former gates have no parameter and each of the latter gates has four parameters, the circuit has $4g = 4^w$ parameters, in accordance with the n^2 degrees of freedom of the matrix U. We note that all $h + g$ single-qubit gates are controlled gates, with the exception of two Hadamard gates on the first qubit.

One might continue the decomposition by decomposing each single-qubit circuit into exclusively NEGATOR gates and PHASOR gates. Indeed, we can rewrite (1) as

$$U = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & b \end{pmatrix} \frac{1}{2} \begin{pmatrix} 1+c & 1-c \\ 1-c & 1+c \end{pmatrix} \times \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix},$$

i.e., a cascade of three PHASOR gates and three NEGATOR gates. Two of the latter are simply NOT gates. In particular for the Hadamard gate, we have

$$H = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & (1-i)/\sqrt{2} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & (1+i)/\sqrt{2} \end{pmatrix} \times \frac{1}{2} \begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}.$$

Among the $3h + 3g$ NEGATOR gates, $2h + 2g$ are NOT gates, and h are square roots of the NOT.

III. GROUP STRUCTURE

We note that the U(n) matrices with all line sums equal to 1 form the subgroup XU(n) of U(n). For even n, the XU(n) matrices of the particular block type

$$\frac{1}{2} \begin{pmatrix} I+V & I-V \\ I-V & I+V \end{pmatrix}, \qquad (3)$$

with $V \in$ U($n/2$), form a subgroup bXU(n) of XU(n):[1]

$$\mathrm{U}(n) \supset \mathrm{XU}(n) \supset \mathrm{bXU}(n),$$

with the respective dimensions

$$n^2 > (n-1)^2 \geqslant n^2/4\ .$$

The group structure of bXU(n) follows directly from the group structure of the constituent unitary matrix:

$$\frac{1}{2} \begin{pmatrix} I+V_1 & I-V_1 \\ I-V_1 & I+V_1 \end{pmatrix} \frac{1}{2} \begin{pmatrix} I+V_2 & I-V_2 \\ I-V_2 & I+V_2 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} I+V_1V_2 & I-V_1V_2 \\ I-V_1V_2 & I+V_1V_2 \end{pmatrix},$$

thus demonstrating the isomorphism bXU(n) $\cong$ U($n/2$).

We note that the diagonal U(n) matrices with the top left entry equal to 1 form the subgroup ZU(n) of U(n). For even n, the U(n) matrices of the particular block type

$$\begin{pmatrix} I & \\ & V \end{pmatrix},$$

with $V \in$ U($n/2$), form a group bZU(n), also a subgroup of U(n). The group structure of bZU(n) thus follows trivially from the group structure of U($n/2$). Whereas bXU(n) is a subgroup of XU(n), bZU(n) is neither a subgroup nor a supergroup of ZU(n). Whereas dim[bXU(n)] $\leqslant$ dim[XU(n)], the dimension of bZU(n), i.e., $n^2/4$, is greater than or equal to the dimension of ZU(n), i.e., $n-1$.

It has been demonstrated [21] that the closure of XU(n) and ZU(n) is the whole group U(n). In other words, any member of U(n) can be written as a product of XU matrices and ZU matrices. Provided n is even, a similar property holds for the block versions of XU and ZU: the closure of bXU(n) and bZU(n) is the whole group U(n). Indeed, with the help of the identity

$$\begin{pmatrix} A & \\ & B \end{pmatrix} = \begin{pmatrix} & I \\ I & \end{pmatrix} \begin{pmatrix} I & \\ & A \end{pmatrix} \begin{pmatrix} & I \\ I & \end{pmatrix} \begin{pmatrix} I & \\ & B \end{pmatrix},$$

[1] We use bXU and bZU as short notations for the block-structured XU matrices and the block-structured ZU matrices, respectively.

we can transform the decomposition (2) into a product containing exclusively bXU and bZU matrices, with (among others) the particular bXU matrix $\begin{pmatrix} & I \\ I & \end{pmatrix}$, i.e., the block NOT gate.

IV. DUAL DECOMPOSITION

Let U be an arbitrary member of U(n). We apply the Führ-Rzeszotnik theorem not to U but instead to its Fourier-Hadamard conjugate $u = FUF$:

$$u = \begin{pmatrix} a & \\ & b \end{pmatrix} F \begin{pmatrix} I & \\ & c \end{pmatrix} F \begin{pmatrix} I & \\ & d \end{pmatrix}.$$

We decompose the left factor and insert the FF product, equal to the $n \times n$ unit matrix $\begin{pmatrix} I & \\ & I \end{pmatrix}$:

$$\begin{aligned} U &= FuF \\ &= F \begin{pmatrix} I & \\ & ba^{-1} \end{pmatrix} FF \begin{pmatrix} a & \\ & a \end{pmatrix} F \begin{pmatrix} I & \\ & c \end{pmatrix} F \begin{pmatrix} I & \\ & d \end{pmatrix} F. \end{aligned}$$

Because $F \begin{pmatrix} a & \\ & a \end{pmatrix} F = \begin{pmatrix} a & \\ & a \end{pmatrix}$, we obtain

$$U = F \begin{pmatrix} I & \\ & ba^{-1} \end{pmatrix} F \begin{pmatrix} a & \\ & ac \end{pmatrix} F \begin{pmatrix} I & \\ & d \end{pmatrix} F,$$

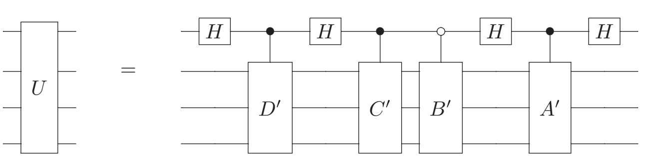
a decomposition of the form

$$\begin{aligned} U = \frac{1}{2} &\begin{pmatrix} I + A' & I - A' \\ I - A' & I + A' \end{pmatrix} \begin{pmatrix} B' & \\ & C' \end{pmatrix} \\ &\times \frac{1}{2} \begin{pmatrix} I + D' & I - D' \\ I - D' & I + D' \end{pmatrix}, \end{aligned}$$

with

$$A' = ba^{-1}, \quad B' = a, \quad C' = ac, \text{ and } D' = d. \tag{4}$$

We thus obtain a decomposition of the form bXbZbX, dual to the Führ-Rzeszotnik decomposition of the form bZbXbZ. Just like in the bZbXbZ decomposition, the number of degrees of freedom in the bXbZbX decomposition exactly matches the dimension n^2 of the matrix U. The diagram of the dual decomposition looks like



V. DETAILED PROCEDURE

Section II provides the outline for the synthesis of an arbitrary quantum circuit acting on w qubits, given its unitary transformation (i.e., its $2^w \times 2^w$ unitary matrix). However, the synthesis procedure is only complete if, given the matrix U, we are able to actually compute the four matrices A, B, C, and D.

It is well-known that an arbitrary member U of U(2) can be written with the help of four real parameters:

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

De Vos and De Baerdemacker [13,19] noticed two different decompositions of this matrix according to (1): In the former decomposition, we have

$$\begin{aligned} a &= e^{i(\alpha+\phi+\psi)}, \\ b &= i\, e^{i(\alpha+\phi-\chi)}, \\ c &= e^{-2i\phi}, \\ d &= -i\, e^{i(-\psi+\chi)}, \end{aligned}$$

whereas in the latter decomposition, we have

$$\begin{aligned} a &= e^{i(\alpha-\phi+\psi)}, \\ b &= -i\, e^{i(\alpha-\phi-\chi)}, \\ c &= e^{2i\phi}, \\ d &= i\, e^{i(-\psi+\chi)}. \end{aligned}$$

Führ and Rzeszotnik proved the generalization (2) for an arbitrary element

$$U = \begin{pmatrix} U_{11} & U_{12} \\ U_{21} & U_{22} \end{pmatrix}$$

of U(n) for even n values by introducing for each of the four $n/2 \times n/2$ matrix blocks U_{11}, U_{12}, U_{21}, and U_{22} of U the polar decomposition

$$U_{jk} = P_{jk} V_{jk},$$

where P_{jk} is a positive-semidefinite Hermitian matrix and V_{jk} is a unitary matrix. Close inspection of the proof by Führ and Rzeszotnik (i.e., the proof to Theorem 8.1 in [17]) reveals the following expressions:

$$\begin{aligned} A &= (P_{11} + i\, P_{12})V_{11}, \\ B &= (P_{21} - i\, P_{22})V_{21}, \\ C &= V_{11}^{\dagger}(P_{11} - i\, P_{12})^2 V_{11} \\ &= V_{21}^{\dagger}(P_{22} - i\, P_{21})^2 V_{21}, \\ D &= -i\, V_{11}^{\dagger} V_{12} \\ &= i\, V_{21}^{\dagger} V_{22}. \end{aligned} \tag{5}$$

The equality of the two expressions for C, as well as the two expressions for D, is demonstrated in the Appendix. One can verify that $AA^\dagger = BB^\dagger = CC^\dagger = DD^\dagger = I$, such that A, B, C, and D are all unitary. For this purpose, it is necessary to observe that P_{11} and P_{12} commute, as well as P_{21} and P_{22} [17]. Finally, one may check that

$$\begin{aligned} A(I + C) &= 2\, U_{11}, \\ B(I - C) &= 2\, U_{21}, \\ A(I - C)D &= 2\, U_{12}, \\ B(I + C)D &= 2\, U_{22}, \end{aligned}$$

such that (2) is fulfilled.

It is noteworthy that there exist two formal expressions for C and D. Whenever the polar decompositions are unique, the two expressions evaluate to the same matrices. However, if one U_{jk} happens to be singular, its polar decomposition is not unique. In this case, it is important to choose C and D

consistently, i.e., to take the first or second expression for both C and D in Eq. (5).

The reader will easily verify that the above expressions for the matrices A, B, C, and D, for $n = 2$, recover the former formulas for the scalars a, b, c, and d. Just like there are two different expansions in the case $n = 2$, there also exists a second decomposition in the case of arbitrary even n. It satisfies

$$\begin{aligned} A &= (P_{11} - i\ P_{12})V_{11}, \\ B &= (P_{21} + i\ P_{22})V_{21}, \\ C &= V_{11}^{\dagger}(P_{11} + i\ P_{12})^2 V_{11} = V_{21}^{\dagger}(P_{22} + i\ P_{21})^2 V_{21}, \\ D &= i\ V_{11}^{\dagger} V_{12} = -\ i\ V_{21}^{\dagger} V_{22}. \end{aligned}$$

We now investigate in more detail the dual decomposition of Sec. IV. Because we have two matrix sets $\{a,b,c,d\}$, we obtain two sets $\{A',B',C',D'\}$:

$$\begin{aligned} A' &= (Q_{21} - i\ Q_{22})W_{21}W_{11}^{\dagger}(Q_{11} - i\ Q_{12}), \\ B' &= (Q_{11} + i\ Q_{12})W_{11}, \\ C' &= (Q_{11} - i\ Q_{12})W_{11}, \\ D' &= -i\ W_{11}^{\dagger} W_{12} \end{aligned}$$

and

$$\begin{aligned} A' &= (Q_{21} + i\ Q_{22})W_{21}W_{11}^{\dagger}(Q_{11} + i\ Q_{12}), \\ B' &= (Q_{11} - i\ Q_{12})W_{11}, \\ C' &= (Q_{11} + i\ Q_{12})W_{11}, \\ D' &= i\ W_{11}^{\dagger} W_{12}, \end{aligned}$$

respectively. Here, $Q_{jk}W_{jk}$ are the polar decompositions of the four blocks u_{jk} constituting the matrix $u = FUF$.

VI. EXAMPLES

As an example, we synthesize here the two-qubit circuit realizing the unitary transformation

$$\frac{1}{12}\begin{pmatrix} 8 & 0 & 4+8i & 0 \\ 2+i & 3-9i & -2i & -3-6i \\ 1-7i & 6 & -6+2i & -3+3i \\ 3+4i & 3-3i & 2-4i & 9i \end{pmatrix}.$$

We perform the algorithm of Sec. V, applying Heron's iterative method for constructing the four polar decompositions [22], although other algorithms can be used equally. Using ten iterations for each Heron decomposition, we thus obtain the following two numerical results:

$$A = \begin{pmatrix} 0.67+0.72i & -0.19+0.03i \\ 0.18+0.06i & 0.80-0.57i \end{pmatrix},$$

$$B = \begin{pmatrix} -0.33-0.64i & 0.50-0.47i \\ 0.69+0.00i & -0.20-0.70i \end{pmatrix},$$

$$C = \begin{pmatrix} -0.04-0.95i & -0.01-0.30i \\ -0.07+0.29i & 0.25-0.92i \end{pmatrix},$$

$$D = \begin{pmatrix} 0.87-0.43i & -0.15+0.20i \\ -0.08-0.24i & -0.68-0.68i \end{pmatrix}$$

and

$$A = \begin{pmatrix} 0.67-0.72i & 0.19-0.03i \\ 0.16+0.10i & -0.30-0.93i \end{pmatrix},$$

$$B = \begin{pmatrix} 0.50-0.52i & 0.50+0.47i \\ -0.19+0.66i & 0.70+0.20i \end{pmatrix},$$

$$C = \begin{pmatrix} -0.04+0.95i & -0.07-0.29i \\ -0.01+0.30i & 0.25+0.92i \end{pmatrix},$$

$$D = \begin{pmatrix} -0.87+0.43i & 0.15-0.20i \\ 0.08+0.24i & 0.68+0.68i \end{pmatrix}.$$

In contrast to the numerical approach in the first example, we will now perform an analytic decomposition of a second example:

$$U = \begin{pmatrix} 1 & & & \\ & \cos(t) & \sin(t) & \\ & -\sin(t) & \cos(t) & \\ & & & 1 \end{pmatrix},$$

i.e., a typical evolution matrix for spin-spin interaction, often discussed in physics. We have the following four matrix blocks and their polar decompositions:[2]

$$U_{11} = \begin{pmatrix} 1 & 0 \\ 0 & c \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & c \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

$$U_{12} = \begin{pmatrix} 0 & 0 \\ s & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & s \end{pmatrix}\begin{pmatrix} 0 & y \\ 1 & 0 \end{pmatrix},$$

$$U_{21} = \begin{pmatrix} 0 & -s \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} s & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ z & 0 \end{pmatrix},$$

$$U_{22} = \begin{pmatrix} c & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} c & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

where c and s are short-hand notations for $\cos(t)$ and $\sin(t)$, respectively. Two blocks, i.e., U_{12} and U_{21}, are singular and therefore have a polar decomposition which is not unique: both y and z are arbitrary numbers on the unit circle in the complex plane. By choosing consistently the "second expressions" of C and D, we find the following decompositions of U:

$$\begin{pmatrix} 1 & & & \\ & e & & \\ & & & ie \\ & & -iz & \end{pmatrix} \frac{1}{2}\begin{pmatrix} 2 & & & \\ & 1+1/e^2 & & 1-1/e^2 \\ & & 2 & \\ & 1-1/e^2 & & 1+1/e^2 \end{pmatrix}$$

$$\times \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & & -i/z \\ & & -i & \end{pmatrix}$$

[2]In fact, the presented polar decompositions are only valid if $0 \leqslant t \leqslant \pi/2$ (i.e., if both $c \geqslant 0$ and $s \geqslant 0$). However, the reader can easily treat the three other cases.

and

$$\begin{pmatrix} 1 & & & \\ & 1/e & & \\ & & & -i/e \\ & & iz & \end{pmatrix} \frac{1}{2} \begin{pmatrix} 2 & & & \\ & 1+e^2 & & 1-e^2 \\ & & 2 & \\ & 1-e^2 & & 1+e^2 \end{pmatrix} \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & & i/z \\ & & i & \end{pmatrix},$$

where e is short-hand notation for $c + is$. In spite of the singular nature of both P_{12} and P_{21}, this leaves only a one-dimensional infinitum of decompositions. The fact that some matrices U have infinite decompositions is further discussed in the next section.

As a third and final example, we consider for U a permutation matrix. Such a choice is particularly interesting as a $2^w \times 2^w$ permutation matrix represents a classical reversible computation on w bits [18,23]. For $w = 2$, we investigate the example

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

We have

$$U_{11} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ x & 0 \end{pmatrix},$$

$$U_{12} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} y & 0 \\ 0 & 1 \end{pmatrix},$$

$$U_{21} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & z \end{pmatrix},$$

$$U_{22} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & w \\ 1 & 0 \end{pmatrix},$$

where x, y, z, and w are arbitrary unit-modulus numbers. If, in particular, we choose $x = w = -i$ and $y = z = i$, then we find a bZUbXUbZU decomposition of U consisting exclusively of permutation matrices:

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

In the next section, we will demonstrate that this is possible for any $n \times n$ permutation matrix (provided n is even).

VII. LIGHT MATRICES AND CLASSICAL COMPUTING

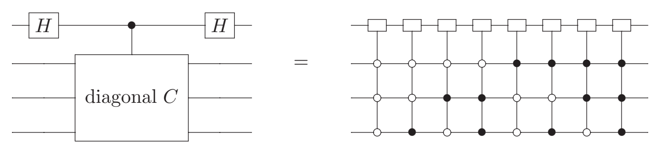
The second and third examples in the previous section lead us to a deeper analysis of sparse unitary matrices.

Definition 1. Let M be an $m \times m$ matrix with, in each line and each column, a maximum of one nonzero entry. We call such a sparse matrix "light." Let μ be the number of nonzero entries of M. We call μ the weight of M. We have $0 \leqslant \mu \leqslant m$. If $\mu = m$, then M is regular; if $\mu < m$, then M is singular. The reader will easily prove the following two lemmas.

Lemma 1. Let PU (with P being a positive-semidefinite matrix and U being a unitary matrix) be the polar decomposition of a light matrix M. Then P is a diagonal matrix, and U is a complex permutation matrix. If μ, the weight of M, equals m, then U is unique; otherwise, we have an $(m - \mu)$-dimensional infinity of choices for U.

Lemma 2. If P is a diagonal matrix and U is a complex permutation matrix, then $U^\dagger P U$ is a diagonal matrix, with the same entries as P in a permuted order.

We now combine these two lemmas. Assume that the $n \times n$ matrix U consists of four $n/2 \times n/2$ blocks, such that the two blocks U_{11} and U_{12} are light. Then, by virtue of Lemma 1, the positive-semidefinite matrices P_{11} and P_{12} are diagonal. Therefore, $P_{11} - iP_{12}$ is diagonal and so is $(P_{11} - iP_{12})^2$. By virtue of Lemma 1 again, the matrix V_{11} is a complex permutation matrix. Finally, because of Lemma 2, the matrix $C = V_{11}^\dagger (P_{11} - iP_{12})^2 V_{11}$ is diagonal, and so are $I + C$ and $I - C$. As a result, for $n = 2^w$, the matrix $F\begin{pmatrix} I & \\ & C \end{pmatrix}F = \frac{1}{2}\begin{pmatrix} I+C & I-C \\ I-C & I+C \end{pmatrix}$ represents a cascade of 2^{w-1} NEGATOR gates acting on the first qubit and controlled by the $w - 1$ other qubits:



We now are in a position to discuss the case of U being an $n \times n$ permutation matrix. Its special interest results from the fact that, for n equal to a power of 2, such a matrix represents a classical reversible computation.

First, we will prove that $\frac{1}{2}\begin{pmatrix} I+C & I-C \\ I-C & I+C \end{pmatrix}$ is a structured permutation matrix. If U is an $n \times n$ permutation matrix, then both $n/2 \times n/2$ blocks U_{11} and U_{12} are light, the sum of their weights μ_{11} and μ_{12} being equal to $n/2$. The matrices P_{11} and P_{12} are diagonal, with entries equal to 0 or 1, with the special feature that, wherever there is a zero entry in P_{11}, the matrix P_{12} has a 1 in the same row and vice versa. The matrix $P_{11} - iP_{12}$ thus is diagonal, with all diagonal entries either equal to 1 or to $-i$. Hence, the matrix $(P_{11} - iP_{12})^2$ is diagonal, with all diagonal entries equal to either 1 or -1, and so is matrix C. Hence, the matrices $I + C$ and $I - C$ are diagonal with entries either 0 or 2. As a result, for $n = 2^w$, the matrix $F\begin{pmatrix} I & \\ & C \end{pmatrix}F = \frac{1}{2}\begin{pmatrix} I+C & I-C \\ I-C & I+C \end{pmatrix}$ represents a cascade of one-qubit IDENTITY and NOT gates acting on the first qubit and controlled by the $w - 1$ other qubits. Thus, the above 2^{w-1} NEGATOR gates all equal a classical gate: either an IDENTITY gate or a NOT gate.

Next, we proceed with proving that D is also a permutation matrix. The matrices V_{11} and V_{12} are complex permutation matrices and thus are light. The matrix V_{11} contains $n/2$ nonzero entries. Among them, $n/2 - \mu_{11}$ can be chosen arbitrarily, with μ_{11} being the weight of U_{11}. We denote these arbitrary numbers by x_j, in analogy to x in the third example of Sec. VI. Analogously, we denote by y_k the $n/2 - \mu_{12}$ arbitrary entries of V_{12}. Because U is a permutation matrix, the weight sum $\mu_{11}+\mu_{12}$ necessarily equals $n/2$. The matrix $-iV_{11}^\dagger V_{12}$ also is a complex permutation matrix and thus has $n/2$ nonzero entries. This number matches the total number of degrees of freedom $(n/2-\mu_{11})+(n/2-\mu_{12})=n/2$. Because U is a permutation matrix, V_{11} and V_{12} can be chosen such that the nonzero entries of the product $-iV_{11}^\dagger V_{12}$ depend only on an x_j or on a y_k but not on both. More specifically, these entries are either of the form $-i/x_j$ or of the form $-iy_k$. By choosing all x_j equal to $-i$ and all y_k equal to i, the matrix $-iV_{11}^\dagger V_{12}$, and thus D, is a permutation matrix.

Because U, $\frac{1}{2}\begin{pmatrix} I+C & I-C \\ I-C & I+C\end{pmatrix}$, and $\begin{pmatrix} I & \\ & D\end{pmatrix}$ are permutation matrices, $\begin{pmatrix} A & \\ & B\end{pmatrix}$ is also an $n\times n$ permutation matrix. Ergo, given an $n\times n$ permutation matrix U, we can construct four $n/2\times n/2$ permutation matrices A, B, C, and D. Therefore, we recover here the Birkhoff decomposition method for permutation matrices and thus, for $n=2^w$, a well-known synthesis method for classical reversible logic circuits [18,24,25] based on the Young subgroups of the symmetric group $\mathbf{S}_{2^w}$

VIII. CONCLUSION

Thanks to the Führ and Rzeszotnik decomposition of U(n) matrices with even n and three more decompositions presented above, we can synthesize the quantum circuit performing an arbitrary unitary transformation from U(2^w) in four systematic and straightforward ways. The present bZbXbZ and bXbZbX decompositions are more practical than the ZXZ decomposition because no Fourier transforms F_j (with $2\leqslant j\leqslant 2^w$) are necessary. Only controlled XU(2) or NEGATOR gates and controlled ZU(2) or PHASOR gates are necessary. Alternatively, one can apply controlled PHASOR gates combined with controlled Hadamard gates, i.e., F_2 transforms.

In contrast to previously developed synthesis methods for quantum circuits (based, e.g., on the sine-cosine or the KAK decomposition), the present four matrix decompositions naturally include the synthesis of classical reversible circuits. This would allow for a better understanding of how classical reversible computing is embedded within quantum computation.

ACKNOWLEDGMENT

The authors thank the European COST Action IC 1405 “Reversible computation” for its valuable support.

APPENDIX

Lemma 3. Let P and P' be positive-semidefinite matrices, let U and U' be unitary matrices, and let $PU=P'U'$. Then, U is equal to U', provided P and P' are regular.

Lemma 4. Let P_j and U_j be positive-semidefinite and unitary matrices, respectively. Then any equality of the form $P_1U_1P_2U_2P_3U_3\cdots=P_1'U_1'P_2'U_2'P_3'U_3'\dots$ implies $U_1U_2U_3\cdots=U_1'U_2'U_3'\dots$, provided all P_j and all P_j' are regular. The proof is based on repeated application of $PU=UQ$, with $Q=U^\dagger PU$ also being a positive-semidefinite matrix, followed by use of Lemma 3. ∎

From the unitarity condition $U^\dagger U=UU^\dagger=\begin{pmatrix} I & 0\\ & I\end{pmatrix}$ follows

$$P_{11}^2+P_{12}^2=I,$$
$$P_{21}^2+P_{22}^2=I,$$
$$V_{11}^\dagger P_{11}^2V_{11}+V_{21}^\dagger P_{21}^2V_{21}=I, \quad \text{(A1)}$$
$$V_{12}^\dagger P_{12}^2V_{12}+V_{22}^\dagger P_{22}^2V_{22}=I, \quad \text{(A2)}$$

as well as

$$P_{11}V_{11}V_{21}^\dagger P_{21}+P_{12}V_{12}V_{22}^\dagger P_{22}=0,$$
$$V_{11}^\dagger P_{11}P_{12}V_{12}+V_{21}^\dagger P_{21}P_{22}V_{22}=0. \quad \text{(A3)}$$

If P_{11}, P_{12}, P_{21}, and P_{22} are regular, then, by virtue of Lemma 4, this leads to

$$V_{11}V_{21}^\dagger=-V_{12}V_{22}^\dagger, \quad \text{(A4)}$$
$$V_{11}^\dagger V_{12}=-V_{21}^\dagger V_{22}. \quad \text{(A5)}$$

In the expression

$$V_{11}^\dagger(P_{11}-i\ P_{12})^2V_{11}$$

or

$$V_{11}^\dagger P_{11}^2V_{11}-iV_{11}^\dagger P_{11}P_{12}V_{11}-iV_{11}^\dagger P_{12}P_{11}V_{11}-V_{11}^\dagger P_{12}^2V_{11},$$

we eliminate P_{11}^2 with the help of (A1), $P_{11}P_{12}$ with the help of (A3), $P_{12}P_{11}$ with the help of (A3), and P_{12}^2 with the help of (A2). Subsequently, we eliminate V_{11} and $V_{11}^\dagger$ with the help of (A4) and (A5). We thus obtain

$$V_{21}^\dagger P_{22}^2V_{21}-iV_{21}^\dagger P_{21}P_{22}V_{21}-iV_{21}^\dagger P_{22}P_{21}V_{21}-V_{21}^\dagger P_{21}^2V_{21}$$
$$=V_{21}^\dagger(P_{22}-iP_{21})^2V_{21}.$$

[1] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).

[2] M. Reck, A. Zeilinger, H. Bernstein, and P. Bertani, Experimental Realization of Any Discrete Unitary Operator, Phys. Rev. Lett. **73**, 58 (1994).

[3] P. Ivanov, E. Kyoseva, and N. Vitanov, Engineering of arbitrary U(N) transformations by quantum Householder reflections, Phys. Rev. A **74**, 022323 (2006).

[4] J. Urías, Householder factorization of unitary matrices, J. Math. Phys. **51**, 072204 (2010).

[5] R. Cabrera, T. Strohecker, and H. Rabitz, The canonical coset decomposition of unitary matrices through Householder transformations, J. Math. Phys. **51**, 082101 (2010).

[6] M. Möttönen, J. Vartiainen, V. Bergholm, and M. Salomaa, Quantum Circuits for General Multi-Qubit Gates, Phys. Rev. Lett. **93**, 130502 (2004).

[7] N. Khaneja, R. Brockett, and S. J. Glaser, Time optimal control in spin systems, Phys. Rev. A **63**, 032308 (2001).

[8] S. Bullock and I. Markov, An arbitrary two-qubit computation in 23 elementary gates, Phys. Rev. A **68**, 012318 (2003).

[9] A. Bocharov and K. Svore, Resource-Optimal Single-Qubit Quantum Circuits, Phys. Rev. Lett. **109**, 190501 (2012).

[10] M. Soeken, D. Miller, and R. Drechsler, Quantum circuits employing roots of the Pauli matrices, Phys. Rev. A **88**, 042322 (2013).

[11] A. Barenco, C. Bennett, R. Cleve, D. DiVincenzo, N. Margolus, P. Shor, T. Sleator, S. Smolin, and H. Weinfurter, Elementary gates for quantum computation, Phys. Rev. A **52**, 3457 (1995).

[12] V. Shende, S. Bullock, and I. Markov, Synthesis of quantum-logic circuits, IEEE Trans. Comput. Aided Des. Integr. Circuits Syst. **25**, 1000 (2006).

[13] A. De Vos and S. De Baerdemacker, On two subgroups of U(n), useful for quantum computing, J. Phys. Conf. Ser. **597**, 012030 (2015).

[14] A. De Vos and S. De Baerdemacker, The synthesis of a quantum circuit, in *Problems and New Solutions in the Boolean Domain*, edited by B. Steinbach (Cambridge Scholars Publishing, Cambridge, 2016), pp. 357–368.

[15] K. Mattle, M. Michler, H. Weinfurter, A. Zeilinger, and M. Zukowski, Non-classical statistics at multiport beam splitters, Appl. Phys. B **60**, S111 (1995).

[16] M. Idel and M. Wolf, Sinkhorn normal form for unitary matrices, Linear Algebra and Its Appl. **471**, 76 (2015).

[17] H. Führ and Z. Rzeszotnik, On biunimodular vectors for unitary matrices, Linear Algebra and Its Appl. **484**, 86 (2015).

[18] A. De Vos, *Reversible Computing* (VCH-Wiley, Weinheim, 2010).

[19] A. De Vos and S. De Baerdemacker, Scaling a unitary matrix, Open Syst. Inf. Dyn. **21**, 1450013 (2014).

[20] W. Tadej and K. Życzkowski, A concise guide to complex Hadamard matrices, Open Syst. Inf. Dyn. **13**, 133 (2006).

[21] A. De Vos and S. De Baerdemacker, Matrix calculus for classical and quantum circuits, ACM J. Emerging Technol. Comput. Syst. **11**, 9 (2014).

[22] N. Higham, Computing the polar decomposition with applications, SIAM J. Sci. Stat. Comput. **7**, 1160 (1986).

[23] R. Wille, M. Soeken, and R. Drechsler, *Introduction to Reversible and Quantum Circuits* (Springer, Berlin, 2016).

[24] Y. Van Rentergem, A. De Vos, and L. Storme, Implementing an arbitrary reversible logic gate, J. Phys. A **38**, 3555 (2005).

[25] A. De Vos and Y. Van Rentergem, Young subgroups for reversible computers, Adv. Math. Commun. **2**, 183 (2008).