Matrix Calculus for Classical and Quantum Circuits

ALEXIS DE VOS and STIJN DE BAERDEMACKER, Universiteit Gent

9

Quantum computation on w qubits is represented by the infinite unitary group $\mathrm{U}(2^w)$; classical reversible computation on w bits is represented by the finite symmetric group $\mathbf{S}_{2^w}$. In order to establish the relationship between classical reversible computing and quantum computing, we introduce two Lie subgroups $\mathrm{XU}(n)$ and $\mathrm{ZU}(n)$ of the unitary group $\mathrm{U}(n)$. The former consists of all unitary $n \times n$ matrices with all line sums equal to 1; the latter consists of all unitary diagonal $n \times n$ matrices with first entry equal to 1. Such a group structure also reveals the relationship between matrix calculus and diagrammatic zx-calculus of quantum circuits.

Categories and Subject Descriptors: F.0 [**Theory of Computation**]: General; F.1.0 [**Computation by Abstract Devices**]: General; F.1.1 [**Computation by Abstract Devices**]: Models of Computation

General Terms: Theory

Additional Key Words and Phrases: Reversible computation, quantum computation

ACM Reference Format:
Alexis De Vos and Stijn De Baerdemacker. 2014. Matrix calculus for classical and quantum circuits. ACM J. Emerg. Technol. Comput. Syst. 11, 2, Article 9 (October 2014), 11 pages.
DOI: http://dx.doi.org/10.1145/2669370

1. INTRODUCTION

Both quantum computers [Feynman 1996; Nielsen and Chuang 2000] and classical reversible computers [De Vos 2010; Feynman 1996] are prominent candidates as computers of the future. The expected high computing speed of the quantum computer and the expected low power consumption of both the quantum computer and the classical reversible computer make them attractive research subjects. The two topics are strongly related. Nevertheless, the literature tells little about this relationship. Moreover, the link between the two subjects is obscured by the fact that studies of the two subjects often make use of quite different languages. This is because quantum computing has been studied mainly by quantum physicists [Nielsen and Chuang 2000], whereas classical reversible computing has mainly been investigated by electrical engineers [De Vos 2010] and computer scientists [Perumalla 2014; Wille and Drechsler 2010].

In this article, we will represent both classical reversible functions and quantum functions by square matrices (permutation matrices and unitary matrices, respectively). Like the classical reversible circuits, which are a subset of the quantum circuits, the permutation matrices form a subgroup of the unitary matrices. In general, we will apply a bottom-up approach. For this purpose, we start with the classical reversible circuits. They are based on the `NOT` gate and the controlled `NOT` gate. By adding the square root of `NOT`, which is a nonclassical gate, we increase the number of possible circuits.

This work is supported by the Danish Council for Strategic Research, under the *MicroPower* research project. S. De Baerdemacker is an FWO-Vlaanderen post-doctoral fellow.
Contact author's address: A. De Vos, CMST, IMEC v.z.w. and vakgroep elektronika en informatiesystemen, Universiteit Gent, Sint Pietersnieuwstraat 41, B - 9000 Gent, Belgium; email: alex@elis.ugent.be.

DOI: http://dx.doi.org/10.1145/2669370

We will generalize this gate by introducing the NEGATOR gate, thus again increasing the number of possibilities. Finally, by adding the Z gate, we recover the full quantum computation world. At each step, we have a new group of matrices, ever increasing in size. Hence, step by step, group theory brings us from classical reversible computers (permutation matrices) to quantum computers (unitary matrices). The proposed 'classical + X + Z' set therefore is an alternative for the 'Clifford + T' set, studied, for example, by Amy et al. [2013] and by Selinger [2012]. We thus find a matrix-group approach, very similar to the diagrammatic approach called zx-calculus [Coecke and Duncan 2011, 2012], with matrix multiplications replacing graph compositions.

2. SINGLE-QUBIT CIRCUITS

Quantum circuits acting on a single qubit are represented by 2×2 unitary matrices [Nielsen and Chuang 2000; Yanofsky and Mannucci 2008]. These matrices form a continuous group, that is, a group of a non-countable infinity of matrices. Such groups are called Lie groups [Stillwell 2008]. The particular group discussed here is called the unitary group U(2). It is represented by a four-dimensional space, where each point represents a matrix. We say that the group is of order ∞^4, that is, that it has ∞^4 elements. Here we use the informal infinity notation ∞^p introduced by Wheeler and Penrose [Penrose 2004].

The most trivial element of the group is the IDENTITY gate, represented by the 2×2 unit matrix $u = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Among the many square roots of this matrix [De Vos and Boes 2011], we choose two of them:

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

describing the NOT gate and the Z gate, respectively. Each of these two matrices generates a group, isomorphic to the cyclic group $\mathbf{Z}_2$ of order 2. The set $\{x, z\}$ generates a group of order 8, isomorphic to the dihedral group $\mathbf{D}_8$ [Asche 1989; Carmichael 1956]. We note that x and z are each other's Hadamard conjugate: $z = HxH$ and $x = HzH$, where

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

We now construct a linear interpolation between the IDENTITY gate and its square root:

$$X = (1-t)\,u + t\,x \quad \text{and} \quad Z = (1-t)\,u + t\,z.$$

The resulting matrices are unitary if and only if the interpolation parameter t satisfies

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

The fact that we find the same restriction in both cases is not a coincidence, as is explained in Appendix A. The condition leads to

$$X(\theta) = \frac{1}{2} \begin{pmatrix} 1+e & 1-e \\ 1-e & 1+e \end{pmatrix} \text{ and } Z(\theta) = \begin{pmatrix} 1 & 0 \\ 0 & e \end{pmatrix},$$

where e is a shorthand notation for $\exp(i\theta)$. The generators of these one-dimensional Lie groups are found by derivation with respect to θ, followed by division by i:

$$\xi = \frac{1}{i} \lim_{\theta \to 0} \frac{dX}{d\theta} = \frac{1}{2} \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$$

$$\text{and} \quad \zeta = \frac{1}{i} \lim_{\theta \to 0} \frac{dZ}{d\theta} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix},$$

respectively. Also the matrices X and Z and matrices ξ and ζ are each other's Hadamard conjugate: $Z = HXH$, $X = HZH$, $\zeta = H\xi H$, and $\xi = H\zeta H$.

The matrices $X(\theta)$ and $Z(\theta)$ correspond with matrices $X_1^1(-\theta)$ and $Z_1^1(\theta)$, introduced by Coecke and Duncan [2011, 2012] in the framework of zx-calculus. The matrix $X(\theta)$ also corresponds with matrix $N(\theta)$, called NEGATOR and introduced by De Vos and De Baerdemacker [2010, 2012a, 2012b], as a 'natural extension' of the NOT gate. If the angle θ equals an integer part of π, then we recover the 'discrete roots' $X(\pi/k)$ and $Z(\pi/k)$ of the matrices x and z, respectively. These kth roots $\sqrt[k]{x}$ and $\sqrt[k]{z}$ have been discussed by Soeken et al. [2013]. In the special case that parameter θ has the value 0, we recover the IDENTITY gate: $X(0) = Z(0) = u$. If $\theta = \pi$, then we recover the NOT gate and the Z gate, respectively: $X(\pi) = x$ and $Z(\pi) = z$. Finally, if $\theta = \pi/2$, then we find the square root of x and the square root of z, respectively:

$$X(\pi/2) = \frac{1}{2} \begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix} \quad \text{and} \quad Z(\pi/2) = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}.$$

The latter is also referred to as the phase gate [Nielsen and Chuang 2000].

THEOREM 1. *Any U(2) matrix U can be decomposed as*

$$\exp(i\theta_0)\, Z(\theta_1) X(\theta_2) Z(\theta_3), \tag{1}$$

for some real θ_0, θ_1, θ_2, *and* θ_3.

This product indeed is equivalent with

$$\exp(i\theta_0 + i\theta_1/2 + i\theta_2/2 + i\theta_3/2) \begin{pmatrix} \exp(-i\theta_1/2 - i\theta_3/2)\cos(\theta_2/2) & -i\exp(-i\theta_1/2 + i\theta_3/2)\sin(\theta_2/2) \\ -i\exp(i\theta_1/2 - i\theta_3/2)\sin(\theta_2/2) & \exp(i\theta_1/2 + i\theta_3/2)\cos(\theta_2/2) \end{pmatrix},$$

and this new expression can be identified with the standard expression for an arbitrary 2×2 unitary matrix, that is, with

$$\exp(i\alpha) \begin{pmatrix} \exp(i\psi)\cos(\phi) & \exp(i\chi)\sin(\phi) \\ -\exp(-i\chi)\sin(\phi) & \exp(-i\psi)\cos(\phi) \end{pmatrix},$$

by choosing

$$\begin{aligned} \theta_0 &= \alpha + \psi - \phi \\ \theta_1 &= -\psi - \chi - \pi/2 \\ \theta_2 &= 2\phi \\ \theta_3 &= -\psi + \chi + \pi/2. \end{aligned}$$

As an example, we have two decompositions of the 2×2 Hadamard matrix:

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

such that $H = \exp(-i\pi/4)\, Z(\pi/2) X(\pi/2) Z(\pi/2) = \exp(i\pi/4)\, Z(-\pi/2) X(-\pi/2) Z(-\pi/2)$.

Because of the identity

$$\begin{pmatrix} e & 0 \\ 0 & e \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & e \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & e \end{pmatrix} = X(\pi) Z(\theta) X(\pi) Z(\theta),$$

Expression (1) becomes

$$U = X(\pi)Z(\theta_0)X(\pi)Z(\theta_0+\theta_1)X(\theta_2)Z(\theta_3).$$

Hence, we have the following.

THEOREM 2. *Any U(2) matrix can be decomposed as a product of $X(\theta)$ and $Z(\theta)$ matrices.*

We again take the 2×2 Hadamard matrix as an example:

$$\begin{aligned} H &= X(\pi)Z(-\pi/4)X(\pi)Z(\pi/4)X(\pi/2)Z(\pi/2) \\ &= X(\pi)Z(\pi/4)X(\pi)Z(-\pi/4)X(-\pi/2)Z(-\pi/2). \end{aligned}$$

Thus, the two generators ξ and ζ together generate not merely a two-dimensional Lie group, but the full four-dimensional Lie group U(2). The Lie algebra (i.e., the linear vector space of the generators of the Lie group [Gilmore 1974]) thus consists of ξ and ζ plus two additional vectors, for example, the commutators

$$2i\,[\,\xi,\zeta\,] = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \text{and} \quad -2\,[\,\xi,[\,\xi,\zeta\,]\,] = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

where $[\,a,b\,]$ denotes the commutator $ab-ba$ of the two matrices a and b.

3. THE GROUPS XU(*N*) AND ZU(*N*)

The invertible $n \times n$ matrices with all $2n$ line sums (i.e., all n row sums and all n column sums) equal to 1 form a group, which we denote by X(n). All $n \times n$ unitary matrices with unit line sums, we call XU(n). The latter group represents all quantum circuits generated by cascading controlled NEGATORs [De Vos and De Baerdemacker 2012a]. The same circuits can also be synthesized by combining exclusively uncontrolled NEGATOR gates and singly controlled NOT gates [De Vos and De Baerdemacker 2013]. The Lie group XU(n) is a subgroup of the unitary group U(n). As proved in Reference [De Vos and De Baerdemacker 2013], the group is isomorphic to the unitary group U($n-1$). Each $n \times n$ matrix X, member of XU(n), can be deduced from a corresponding $(n-1) \times (n-1)$ matrix Y, member of U($n-1$), by means of the conjugation

$$X = F_n \begin{pmatrix} 1 & \mathbf{0}^T \\ \mathbf{0} & Y \end{pmatrix} F_n^{-1},$$

where F_n denotes the $n \times n$ Fourier matrix and $\mathbf{0}$ is the $(n-1) \times 1$ zero matrix. In particular, the reader may check that the matrices X of the previous section form the group XU(2) and are indeed recovered by the preceding equation, as F_2 equals H and Y is a 1×1 matrix (e):

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

The invertible $n \times n$ diagonal matrices with upper-left entry equal to 1 form a group, which we denote by Z(n). All $n \times n$ unitary diagonal matrices with unit upper entry, we call ZU(n). The latter group is isomorphic to $\mathrm{U}(1)^{n-1}$. In particular, the reader may check that the matrices Z of Section 2 form the group ZU(2).

The two subgroups XU(n) and ZU(n) of U(n) display an intriguing duality, as one is isomorphic to $\mathrm{U}(n-1)^1$ and the other to $\mathrm{U}(1)^{n-1}$. Besides, they have only one member in common and that is the $n \times n$ unit matrix. Section 4 will demonstrate how together they are building blocks of U(n). However, although XU(2) and ZU(2) are each other's Hadamard conjugate, such is not the case for XU(n) and ZU(n), as $F_n\mathrm{XU}(n)F_n^{-1}$ is a supergroup of ZU(n) and $F_n\mathrm{ZU}(n)F_n^{-1}$ is only a subgroup of XU(n).

4. THE GROUP U(*N*)

According to Hurwitz [1897], Poźniak et al. [1998], and Zyczkowski and Kuś [1994], an arbitrary member U of U(n) can be decomposed into a product $\exp(i\alpha)\,U_1U_2...U_m$ of matrices, where $m = n(n-1)/2$. Each matrix U_j is of the following form:

—the entries located at the four places $(k(j),k(j))$, $(k(j),l(j))$, $(l(j),k(j))$, and $(l(j),l(j))$ form a 2×2 matrix[1]

$$M_j = \begin{pmatrix} \exp(i\psi_j)\cos(\phi_j) & \exp(i\chi_j)\sin(\phi_j) \\ -\exp(-i\chi_j)\sin(\phi_j) & \exp(-i\psi_j)\cos(\phi_j) \end{pmatrix};$$

—the entries located at the $n-2$ remaining diagonal places equal 1;
—the entries located at the n^2-n-2 remaining off-diagonal places equal 0.

According to Section 2, matrix M_j can be decomposed into 2×2 matrices: $\exp(i\psi_j - i\phi_j)\,Z(-\psi_j-\chi_j-\pi/2)X(2\phi_j)Z(-\psi_j+\chi_j+\pi/2)$. Therefore, the matrix U_j can be decomposed into $n\times n$ matrices:

—either a product $Z'XZ''$, if $k(j)\neq 1$
—or a product $\exp(i\alpha_j)Z'XZ''$, if $k(j)=1$,

where X is a matrix from XU(n) and both Z' and Z'' are matrices from ZU(n). This finally leads (after collecting all $\exp(i\alpha_j)$ factors) to the decomposition of U:

$$\exp(i\alpha)\,(Z'XZ'')_1(Z'XZ'')_2...(Z'XZ'')_m.$$

Introducing $Z_j = (Z'')_{j-1}(Z')_j$ for $2\le j\le m$, $Z_1=(Z')_1$, and $Z_{m+1}=(Z'')_m$, we finally obtain

$$U = \exp(i\alpha)\,Z_1X_1Z_2X_2Z_3...Z_mX_mZ_{m+1}.$$

We thus can conclude as follows.

THEOREM 3. *Any $U(n)$ matrix can be decomposed as* $\exp(i\alpha)$ *times a product of $n(n-1)+1$ or less matrices from either $XU(n)$ or $ZU(n)$.*

Because of the identity

$$\begin{pmatrix} e & & & \\ & e & & \\ & & e & \\ & & & \ddots \\ & & & & e \end{pmatrix} = \begin{pmatrix} & 1 & & \\ 1 & & & \\ & & 1 & \\ & & & \ddots \\ & & & & 1 \end{pmatrix} \begin{pmatrix} 1 & & & \\ & e & & \\ & & 1 & \\ & & & \ddots \\ & & & & 1 \end{pmatrix} \begin{pmatrix} & 1 & & \\ 1 & & & \\ & & 1 & \\ & & & \ddots \\ & & & & 1 \end{pmatrix} \begin{pmatrix} 1 & & & \\ & e & & \\ & & e & \\ & & & \ddots \\ & & & & e \end{pmatrix},$$

we have the following.

THEOREM 4. *Any $U(n)$ matrix can be decomposed as a product of $n(n-1)+4$ or less matrices from either $XU(n)$ or $ZU(n)$.*

This means that the $(n-1)^2$ generators[2] of $XU(n)$ together with the $n-1$ generators[3] of $ZU(n)$ do not generate a Lie group of mere dimension $(n-1)^2+(n-1)=n^2-n$, but instead generate the full n^2-dimensional Lie group $U(n)$.

[1]Without any loss of generality, we assume here that $k(j)<l(j)$.
[2]These generators are $n\times n$ Hermitian matrices with all line sums equal to 0.
[3]These generators are $n\times n$ Hermitian matrices with all entries equal to 0, except one diagonal entry equal to 1.

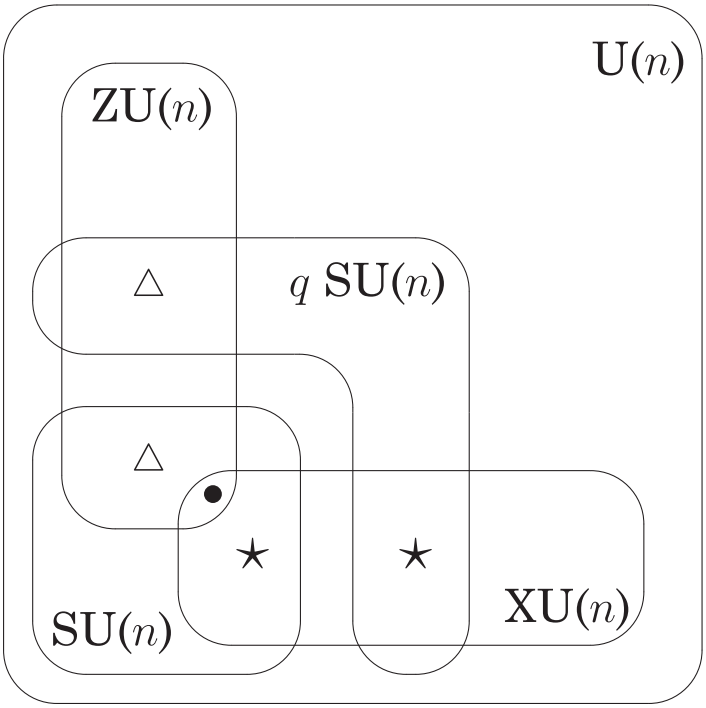

Fig. 1. Venn diagram of the groups XU(n) and ZU(n) and their closure U(n), i.e. the unitary group. *Note:* the group SU(n) is the special unitary group and q is an $n \times n$ matrix with determinant -1; the bullet denotes the unit matrix, the stars denote the permutation matrices, whereas the triangles denote the flip matrices.

5. DISCUSSION

We have identified within the unitary group U(n) two subgroups XU(n) and ZU(n). For the particular case $n = 2^w$, the group U(n) represents all possible quantum computers acting on w qubits, whereas XU(n) is a 'natural extension' of the classical computers acting on w bits. The $(n-1)$-dimensional group ZU(n) suffices to close the gap between the $(n-1)^2$-dimensional group XU(n) and its n^2-dimensional supergroup U(n).

Figure 1 and Table I summarize the results. We see the following Lie groups:

—U(n) with ∞^{n^2} members,
—SU(n) with ∞^{n^2-1} members,
—XU(n) with $\infty^{(n-1)^2}$ members, and
—ZU(n) with ∞^{n-1} members.

The special unitary group SU(n) contains, by definition, all members of U(n) that have determinant equal to 1; the set q SU(n) contains all members of U(n) that have determinant equal to -1. The latter is not a group[4], as it does not contain the unit element. For the matrix q, one can choose any particular member of U(n) with determinant -1,

[4]Together, SU(n) and q SU(n) form a group, compact but not connected, consisting of all $n \times n$ unitary matrices with determinant ± 1.

Table I. Number of Elements in the Unitary Group U(n) and Some of Its Subgroups

n	U(n)	XU(n)	ZU(n)	P(n)	Q(n)
2	∞^4	∞^1	∞^1	2	2
4	∞^{16}	∞^9	∞^3	24	8
8	∞^{64}	∞^{49}	∞^7	40,320	128
16	∞^{256}	∞^{225}	∞^{15}	20,922,789,888,000	32,768

for example, the following member of ZU(n) or the following member of XU(n):

$$\begin{pmatrix} 1 & 0 & \dots & 0 & 0 & 0 \\ 0 & 1 & & 0 & 0 & 0 \\ \dots & & & & & \\ 0 & 0 & & 1 & 0 & 0 \\ 0 & 0 & & 0 & 1 & 0 \\ 0 & 0 & & 0 & 0 & -1 \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} 1 & 0 & \dots & 0 & 0 & 0 \\ 0 & 1 & & 0 & 0 & 0 \\ \dots & & & & & \\ 0 & 0 & & 1 & 0 & 0 \\ 0 & 0 & & 0 & 0 & 1 \\ 0 & 0 & & 0 & 1 & 0 \end{pmatrix}.$$

We note that the intersection of ZU(n) and XU(n) contains only one element, that is, the $n \times n$ unit matrix (displayed by the bullet). Finally, we locate the $n!$ matrices of the permutation group P(n), representing classical reversible computing: half of them are located in the intersection of SU(n) and XU(n), and half of them are located in the intersection of q SU(n) and XU(n). In the figure, they are highlighted by the stars (and by the bullet, of course). Their counterpart within ZU(n) consists of all diagonal matrices with first entry equal to 1 and all others equal to ± 1. This finite group Q(n) is briefly discussed in Reference [Boes et al. 2010]. It is isomorphic to $\mathbf{Z}_2^{n-1}$ of order 2^{n-1}. It consists of 2^{n-2} matrices within SU(n) and 2^{n-2} matrices within q SU(n). In the figure, they are highlighted by the triangles (and by the bullet). Appendix B gives some more group properties.

In contrast to previous sections, in the last paragraph, we have applied a top-down approach, shrinking the group U(n) and its subgroups XU(n) and ZU(n) by restricting all real parameters θ_j to the set $\{0, \pi\}$. As a result, the infinite groups XU(n) and ZU(n) shrink to finite groups P(n) and Q(n). We may study an intermediate case by restricting the angles θ_j to the set $\{0, \pi/2, \pi, 3\pi/2\}$. The result consists neither of continuous infinite groups (or Lie groups) nor of finite groups, but of infinite discrete groups, that is, groups with a countably infinite order. See Appendix C. Another top-down approach leads to a study of the subgroups XO(n) and ZO(n) of the orthogonal group O(n). See Appendix D.

Just as XU(n) and ZU(n) are fundamental parts of U(n), the groups X(n) and Z(n) are basic parts of their supergroup, the general linear group GL($n, \mathbb{C}$) of dimension $2n^2$, with Z(n) isomorphic to GL$(1, \mathbb{C})^{n-1}$ and X(n) related to GL$(n-1, \mathbb{C})$.

The two groups XU(n) and ZU(n) spanning their supergroup U(n) and the two groups X(n) and Z(n) spanning their supergroup GL($n, \mathbb{C}$) are reminiscent of the two groups of building blocks of the analog reversible computers: the lifting circuits and the scale gates [Burignat et al. 2012; De Vos 2010; De Vos and De Baerdemacker 2010]. The $n \times n$ lifting matrices have 1s on the diagonal; elsewhere, they have entries equal to 0 except on one particular row. The $n \times n$ scaling matrices have 0s on the off-diagonal places; elsewhere, they have entries equal to 1 except on one diagonal place. For $n = 3$,

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ r & t & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & s \end{pmatrix}$$

form an example of a lifting matrix (with lifting coefficients r and t) and a scaling matrix (with scaling factor s), respectively. However, here n is not equal to 2^w, but to w, that is, the number of analog inputs (and also analog outputs) of the (linear) analog computer. The group of analog computers is isomorphic to the general linear group $\mathrm{GL}(n, \mathbb{R})$. Whereas in the unitary case, the subgroup $\mathrm{XU}(n)$ is isomorphic to $\mathrm{U}(n-1)$ and the subgroup $\mathrm{ZU}(n)$ is isomorphic to $\mathrm{U}(1)^{n-1}$, in the analog case, the subgroup of lifting circuits is isomorphic to the special linear group $\mathrm{SL}(n, \mathbb{R})$ and the subgroup of scaling circuits is isomorphic to $\mathrm{GL}(1, \mathbb{R})^n$.

6. CONCLUSION

Within a family of matrix groups $\mathrm{G}(n)$, we have defined two different subgroups:

—the subgroup $\mathrm{ZG}(n)$, consisting of all $n \times n$ diagonal matrices with upper-left entry equal to 1 and other diagonal entries from $\mathrm{G}(1)$;
—the subgroup $\mathrm{XG}(n)$ with all $n \times n$ matrices from $\mathrm{G}(n)$, such that all their $2n$ line sums are equal to 1.

For different families $\mathrm{G}(n)$, we have studied the properties of $\mathrm{XG}(n)$ and $\mathrm{ZG}(n)$. Whereas for any $\mathrm{G}(n)$, the group $\mathrm{ZG}(n)$ is isomorphic to $\mathrm{G}(1)^{n-1}$, the properties of $\mathrm{XG}(n)$ depend on the choice of G. As quantum computers are represented by the unitary group $\mathrm{U}(2^w)$, we have studied in detail the case $\mathrm{G}(n) = \mathrm{U}(n)$. By proving that any member of $\mathrm{U}(n)$ can be written as a product of members of $\mathrm{XU}(n)$ and members of $\mathrm{ZU}(n)$, we have demonstrated that $\mathrm{U}(n)$ is the closure of $\mathrm{XU}(n)$ and $\mathrm{ZU}(n)$. We have shown that $\mathrm{XU}(n)$ is isomorphic to $\mathrm{U}(n-1)$ and represents all quantum computers based on the (controlled) `NEGATOR` building block. The `NEGATOR` gate is just a complex generalization of the real `NOT` gate. Therefore, the group $\mathrm{XU}(n)$ contains all classical reversible computers, as those are based on the (controlled) `NOT`. The classical reversible computers are represented by the permutation group $\mathrm{P}(2^w)$. We therefore summarize:

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

One can only hope that the computers represented by the group $\mathrm{XU}(2^w)$ will bring together the best of two worlds as follows.

—They will be (almost) as easily built as the classical computers.
—They will be (almost) as powerful as the quantum computers.

APPENDIX

A. THE ROOTS OF THE UNIT MATRIX

Let the unitary matrix q be a square root of the unit matrix u. We thus have both $qq^\dagger = u$ and $q^2 = u$. As a consequence, q is a Hermitian operator:

$$q^\dagger = q. \tag{2}$$

If the linear interpolation $(1-t)u + tq$ is unitary, then

$$(u - tu + tq)(u - \bar{t}u + \bar{t}q^\dagger) = u,$$

leading to

$$(2t\bar{t} - t - \bar{t}\,)\,u + t(1-\bar{t}\,)\,q + (1-t)\,\bar{t}\,q^\dagger = 0.$$

With Eq. (2), this yields $(2t\bar{t} - t - \bar{t}\,)(u - q) = 0$, and thus either $q = u$ (trivial case) or $2t\bar{t} - (\,t + \bar{t}\,) = 0$, and thus $t = 1/2 - (1/2)\exp(i\theta)$.

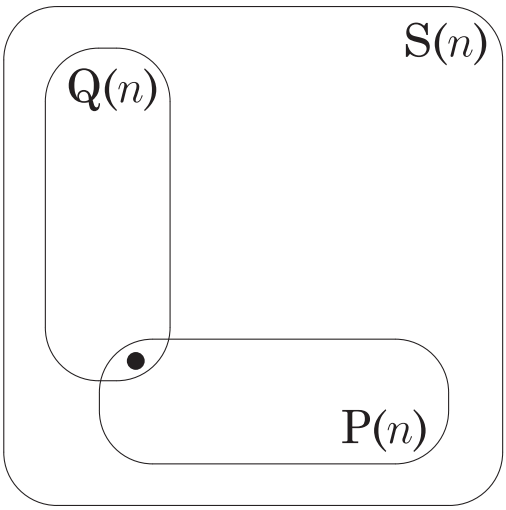

Fig. 2. Venn diagram of the permutation group P(n) and the flip group Q(n) and their closure S(n), that is, the group of signed permutations.

B. THE SIGNED PERMUTATION MATRICES

In order to better understand the dual properties of the infinite groups XU(n) and ZU(n), it is advantageous to study their finite subgroups P(n) and Q(n).

The group P(n) consists of the $n \times n$ permutation matrices, that is, the $n \times n$ unitary matrices where all lines (i.e., all rows and all columns) contain exactly one 1. It is isomorphic to the symmetric group $\mathbf{S}_n$. Half of these matrices (the even permutations) have determinant equal to 1; half of these matrices (the odd permutations) have determinant -1. The group Q(n) consists of the $n \times n$ flip matrices, that is, the $n \times n$ unitary diagonal matrices where all diagonal entries equal ± 1, except the first entry which equals 1. It is isomorphic to the group $\mathbf{S}_2^{n-1}$. Half of these matrices (the even flips) have determinant equal to 1; half of these matrices (the odd flips) have determinant -1. The group P(n) has $n!$ members; the group Q(n) has 2^{n-1} members. The two groups have only one element in common, that is, the $n \times n$ unit matrix. Their closure, that is, the group consisting of all possible products of permutation matrices and flip matrices, is the group S(n) of signed permutation matrices, isomorphic to the hyperoctahedral group (in fact the wreath product $\mathbf{S}_2$ wr $\mathbf{S}_n$), of order $n!\,2^n$. It consists of all $n \times n$ unitary matrices where all lines contain exactly one ± 1. Figure 2 summarizes the group structure. For the sake of completeness, it is worth mentioning that in spite of the close analogy between Figures 1 and 2, we also have some differences. For example, in spite of the property that XU(n) is isomorphic to U($n-1$), the group P(n) is not isomorphic to S($n-1$), as is immediately clear from their different orders, $n!$ and $(n-1)!\,2^{n-1}$, respectively.

Each S(n) matrix can be decomposed into a product of four (or less) building blocks: two or less P(n) matrices and two or less Q(n) matrices. This is illustrated by an example for $n = 3$:

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

C. THE SQUARE ROOTS OF THE NOT AND Z MATRICES

The square root of NOT, that is, the 2×2 matrix $X(\pi/2)$, generates a group of order 4, isomorphic to the cyclic group $\mathbf{Z}_4$; also the square root of Z, that is, the 2×2 matrix $Z(\pi/2)$, generates a group of order 4, equally isomorphic to $\mathbf{Z}_4$. Together, these two generators generate a group of order 96, isomorphic to the semidirect product $\mathrm{SL}(2,3){:}\mathbf{Z}_4$ and subgroup of the Clifford group of order 192.

The group of $n \times n$ diagonal matrices with upper entry equal to 1 and all others from the set $\{1, i, -1, -i\}$ form a finite group of order 4^{n-1}, isomorphic to $\mathbf{Z}_4^{n-1}$. In contrast, the group of $n \times n$ matrices with all line sums equal to 1 and all entries from the set $\{1, (1+i)/2, 0, (1-i)/2\}$ do not form a group on their own, as soon as $n > 2$. They generate a group with a countable infinity of elements [De Vos and Boes 2011; De Vos et al. 2009]. The group consists of all $\mathrm{XU}(n)$ matrices with all entries equal to a Gaussian integer divided by a power of 2 [De Vos et al. 2012]. The closure of the former (finite) matrix group and the latter (infinite discrete) matrix group is an infinite discrete group. The resulting matrix group is related to the zx-calculus with phases restricted to $\{0, \pi/2, \pi, 3\pi/2\}$ [Backens 2012].

D. THE ORTHOGONAL MATRICES

Restricting the matrix entries of the unitary matrices of $\mathrm{U}(n)$ to real values gives rise to a group, isomorphic to the orthogonal group $\mathrm{O}(n)$. The latter has dimension $n(n-1)/2$. In particular, the one-dimensional orthogonal group $\mathrm{O}(2)$ consists of the ∞^1 matrices

$$\begin{pmatrix} c & s \\ -s & c \end{pmatrix} \text{ and } \begin{pmatrix} s & c \\ c & -s \end{pmatrix},$$

where c and s are shorthand notations for $\cos(\theta)$ and $\sin(\theta)$, respectively. Only two of these matrices have all four line sums equal to 1, that is, the unit matrix and the NOT matrix. Thus, $\mathrm{XO}(2)$ is a finite group of order 2. The group $\mathrm{XO}(3)$ is of infinite order (order ∞^1):

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

For arbitrary n, we have $\dim(\mathrm{XO}(n)) = (n-1)(n-2)/2$. Just like the isomorphism $\mathrm{XU}(n) \simeq \mathrm{U}(n-1)$, we have that $\mathrm{XO}(n)$ is isomorphic to $\mathrm{O}(n-1)$, as proved by Banica and Speicher [2009]. In particular, the isomorphism $\mathrm{XO}(3) \simeq \mathrm{O}(2)$ can be demonstrated by the 1-to-1 mapping

$$F \begin{pmatrix} 1 & 0 & 0 \\ 0 & c & s \\ 0 & -s & c \end{pmatrix} F^{-1},$$

where F is the 'Fourier-like' matrix

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

The group $\mathrm{ZO}(n)$ is identical to the group $\mathrm{Q}(n)$ of Appendix B and thus is finite with order 2^{n-1}. Unlike $\mathrm{closure}(\mathrm{XU}(n), \mathrm{ZU}(n)) = \mathrm{U}(n)$, the closure of $\mathrm{XO}(n)$ and $\mathrm{ZO}(n)$ is only a subgroup of $\mathrm{O}(n)$.

REFERENCES

M. Amy, D. Maslov, and M. Mosca. 2013. Polynomial-time T-depth optimization of Clifford+T circuits via matroid partitioning. arXiv:quant-ph 1303.2042.

D. Asche. 1989. *An Introduction to Groups*. IOP Publishing, Bristol, UK.

M. Backens. 2012. The zx-calculus is complete for stabilizer quantum mechanics. In *Proceedings of the 9th International Workshop on Quantum Physics and Logic*. 15–28.

T. Banica and R. Speicher. 2009. Liberation of orthogonal Lie groups. *Adv. Math.* 222, 1461–1501.

M. Boes, A. De Vos, and J. De Beule. 2010. Almost-classical quantum computers. In *Proceedings of the 9th International Workshop on Boolean Problems.* 51–56.

S. Burignat, K. Vermeirsch, A. De Vos, and M. Thomsen. 2012. Garbageless reversible implementation of integer linear transformations. In *Proceedings of the 4th International Workshop on Reversible Computation.* 187–197.

R. Carmichael. 1956. *Introduction to the Theory of Groups of Finite Order*. Dover Publications, New York, NY.

B. Coecke and R. Duncan. 2011. Interacting quantum observables: Categorical algebra and diagrammatics. *New J. Phys.* 13.

B. Coecke and R. Duncan. 2012. Tutorial: Graphical calculus for quantum circuits. In *Proceedings of the 4th International Workshop on Reversible Computation*. 145–157.

A. De Vos. 2010. *Reversible Computing*. Wiley–VCH, Weinheim, Germany.

A. De Vos and M. Boes. 2011. Creating subgroups of $U(2^w)$ for quantum-minus computers. In *Proceedings of the 28th International Colloquium on Group-Theoretical Methods in Physics.* In *Physical and Mathematical Aspects of Symmetry*, Journal of Physics: Conference Series, Vol. 284.

A. De Vos and S. De Baerdemacker. 2010. Decomposition of a linear reversible computer: Digital versus analog. *Int. J. Unconventional Comput.* 6, 239–263.

A. De Vos and S. De Baerdemacker. 2012a. The roots of the NOT gate. In *Proceedings of the 42nd International Symposium on Multiple-Valued Logic.* 167–172.

A. De Vos and S. De Baerdemacker. 2012b. Logics between classical reversible logic and quantum logic. In *Proceedings of the 9th International Workshop on Quantum Physics and Logic.* 123–128.

A. De Vos and S. De Baerdemacker. 2013. The NEGATOR as a basic building block for quantum circuits. *Open Syst. Inf. Dynamics* 20.

A. De Vos, J. De Beule, and L. Storme. 2009. Computing with the square root of NOT. *Serdica J. Comput.* 3, 359–370.

A. De Vos, R. Van Laer, and S. Vandenbrande. 2012. The group of dyadic unitary matrices. *Open Syst. Inf. Dynamics* 19.

R. Feynman. 1996. *Feynman Lectures on Computation*. Addison–Wesley, Reading, MA.

R. Gilmore. 1974. *Lie Groups, Lie Algebras, and Some of Their Applications.*Wiley, New York, NY.

A. Hurwitz. 1897. Ueber die Erzeugung der Invarianten durch Integration. *Nachrichten von der Königliche Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-physikalische Klasse*, Vol. 1897, 71–90.

M. Nielsen and I. Chuang. 2000. *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge, UK.

R. Penrose. 2004. *The Road to Reality – A Complete Guide to the Laws of the Universe*. Vintage Books, London, UK, 378–382.

K. Perumalla. 2014. *Introduction to Reversible Computing*. CRC Press, Boca Raton, FL.

M. Poźniak, K. Życzkowski, and M. Kuś. 1998. Composed ensembles of random unitary matrices. *J. Phys. A: Math. Gen.* 31, 1059–1071.

P. Selinger. 2012. Efficient Clifford+T approximations of single-qubit operations. arXiv:quant-ph 1212.6253.

M. Soeken, D. Miller, and R. Drechsler. 2013. Quantum circuits employing roots of the Pauli matrices. *Phys. Rev. A* 88.

J. Stillwell. 2008. *Naive Lie Theory*. Springer, New York, NY.

R. Wille and R. Drechsler. 2010. *Towards a Design Flow for Reversible Logic*. Springer, Dordrecht, The Netherlands.

N. Yanofsky and M. Mannucci. 2008. *Quantum Computing for Computer Scientists*. Cambridge University Press, Cambridge, UK.

K. Życzkowski and M. Kuś. 1994. Random unitary matrices. *J. Phy. A: Math. Gen.* 27, 4235–4245.

Received August 2013; accepted December 2013