Open Systems & Information Dynamics
Vol. 19, No. 1 (2012) 1–28
DOI: xxx

The Group of Dyadic Unitary Matrices

Alexis De Vos, Raphaël Van Laer, and Steven Vandenbrande

Vakgroep elektronica en informatiesystemen
Universiteit Gent
Sint Pietersnieuwstraat 41, B–9000 Gent, Belgium

(Received: September 2, 2011)

Abstract. We introduce the group DU(m) of $m \times m$ dyadic unitary matrices, i.e. unitary matrices with all entries having a real and an imaginary part that are both rational numbers with denominator of the form 2^p (with p a non-negative integer). We investigate in detail the finite groups DU(1) and DU(2) and the discrete, but infinite groups DU(3) and DU(4). We further introduce the subgroup XDU(m) of DU(m), consisting of those members of DU(m) that have constant line sum 1. The study of XDU(2) and XDU(4) leads to conclusions concerning the synthesis of quantum computers acting on one and two qubits, respectively.

1. Introduction

Basically, there exist three kinds of groups:

- finite groups, i.e. groups with a finite order,
- infinite but nevertheless discrete groups, i.e. groups with a countably infinite order, and
- Lie groups, i.e. groups with an uncountably infinite order.

Whereas the size of a finite group is quantified by its order, the size of a Lie group is quantified by its dimensionality. Quantifying sizes of infinite discrete groups is a more difficult task. It necessitates a detailed study of the group.

The most basic example of a countably infinite nonabelian group is the discrete group $\mathrm{SL}_2(\mathbb{Z})$, i.e. the special linear group of 2×2 matrices with integer entries. Conrad [1] demonstrates that the group can be generated with merely two generators and shows how to decompose an arbitrary group member into a finite product of factors, each equal to one of these two building blocks. In the present paper, we follow a basically similar approach for describing the group of rational unitary matrices where all matrix elements have a denominator of the form 2^p. The motivation to study this group is inspired by its importance in computer theory. Whereas classical reversible computation is described by finite groups and quantum computation is represented by

Lie groups, computing with the so-called square-root-of-`NOT` logic gate leads to infinite discrete groups [2] of such rational matrices. Whereas classical reversible circuits are generated by controlled `NOT` gates (a.k.a. Toffoli gates), below we will investigate all circuits generated by controlled square roots of `NOT`. They constitute a generalization of the classical reversible circuits, but only a small fraction of the set of all quantum circuits.

2. The Group DU(m)

First, we consider all unitary $m \times m$ matrices. It is well known that they form an infinite group, i.e. the unitary group U(m), an m^2-dimensional Lie group.

Next, we consider, within the group U(m), the matrices which have exclusively Gaussian entries. This means that the matrix entries are Gaussian rationals

$$\frac{a}{A} + i\,\frac{b}{B}\,, \quad \frac{c}{C} + i\,\frac{d}{D}\,, \quad \dots\,,$$

where a, A, b, B, ... are integers. These matrices form a group. Indeed, being unitary, such matrix has an inverse. The entries of the inverse automatically are also Gaussian rationals. And the product of two such matrices automatically is also such a matrix. We call this group the Gaussian unitary group GU(m). The group is discrete, as the matrix contains only a finite number (i.e. $2m^2$) of rational numbers $\frac{a}{A}, \frac{b}{B}, \dots$ and there exist only a countably infinite number of rationals.

Finally, within the group GU(m), we consider the subset of matrices where all denominators $A, B, \dots$ are a power of 2. Thus all entries may be written

$$\frac{a}{2^p} + i\,\frac{b}{2^p}\,,$$

where the non-negative integer p is chosen such that at least one entry is not reducible, i.e. such that at least one of the $2m^2$ numerators a, b, ... is odd. As the real part and the imaginary part of each matrix entry is a dyadic rational, we call such a matrix a dyadic matrix. Whereas m is called the dimension (or degree) of the matrix, the number 2^p is called the level [3] of the matrix. As illustrated by the example

$$\begin{pmatrix} \frac{5}{2} & 1 \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}^{-1} = \begin{pmatrix} \frac{2}{3} & -\frac{4}{3} \\ -\frac{2}{3} & \frac{10}{3} \end{pmatrix},$$

the inverse of a dyadic matrix is not necessarily a dyadic matrix. The inverse of dyadic unitary matrix, however, is a dyadic unitary matrix (with the same level), for the simple reason that the inverse of a unitary matrix is its Hermitian transpose. The product of a dyadic matrix with level equal to 2^{p_1} and a dyadic matrix with level equal to 2^{p_2} is a dyadic matrix with level lower than or equal to $2^{p_1+p_2}$. We thus may conclude that the dyadic unitary matrices form a group. We call this group the dyadic unitary group DU(m).

3. Two Subgroups of DU(m)

In the present section, we discuss two (out of the many) subgroups of DU(m).

An $m \times m$ matrix has $2m$ lines, i.e. m rows and m columns. We consider the matrices whose line sums are all equal. If the matrix is unitary, then the constant line sum is on the unit circle (See Appendix A). If the matrix is dyadic, then the constant line sum is a dyadic rational. Now, on the unit circle there exist only four such Gaussian rationals $\frac{x}{2^p} + i\,\frac{y}{2^p}$. Indeed, the condition $(\frac{x}{2^p})^2 + (\frac{y}{2^p})^2 = 1$ leads to $x^2 + y^2 = (2^p)^2$, which implies that $\{x, y, 2^p\}$ forms a Pythagorean triple. However, there exist no primitive Pythagorean triples where the greatest number is even. We conclude that either x or y has to be zero. Therefore, if the matrix is both unitary and dyadic, the constant line sum equals one of the four complex numbers 1, i, -1, and $-i$, known as the four Gaussian units. The product of a matrix with constant line sum equal to s and a matrix with constant line sum equal to t is a matrix with constant line sum st. Proof is provided in [4, p. 239]. Therefore, matrices with constant line sum equal to 1 form a group. The members of DU(m) that have constant line sum equal to 1, thus form a subgroup of DU(m); we will call this subgroup XDU(m). Their study is interesting in the framework of quantum computing. The groups XDU(2^w) naturally appear when studying quantum circuits built with the gate called 'the square root of `NOT`', see below in Sections 8 to 11. Matrices belonging to XDU(m) may be considered as a 'complex generalization' of doubly stochastic (or bistochastic) matrices, where equally well all line sums equal 1, but where all entries are restricted to real non-negative numbers.

The matrices of DU(m) with $p = 0$, i.e. the DU(m) matrices of level 1, form a finite subgroup, isomorphic to the semi-direct product (DU(1) $\times$ DU(1) $\times \ldots \times$ DU(1)): $\boldsymbol{S}_m$ = DU$(1)^m$: $\boldsymbol{S}_m$, where $\boldsymbol{S}_m$ denotes the symmetric group of degree m (and thus order $m!$). We will call the subgroup the monomial dyadic unitary group MDU(m), as all its members are matrices with exactly one non-zero entry in each row and each column. The group P(m) of all $m \times m$ permutation matrices, in turn, is a subgroup of MDU(m):

$$\mathrm{P}(m) \subset \mathrm{MDU}(m) \subset \mathrm{DU}(m) \subset \mathrm{U}(m)\,.$$

The subgroup MDU(m) partitions the supergroup DU(m) into double cosets, each containing matrices of a same level 2^p. These double cosets can be regarded as equivalence classes. Any element of a double coset can act as its representative. Here, two matrices are considered equivalent iff they can be converted into one another by applying a combination of the following operations:

- permutation of two rows or two columns and
- multiplication of a row or a column by i.

This equivalence is analogous to the one used in investigating real and complex Hadamard matrices. See e.g. the equivalence relation $\approx$ by Haagerup [5].

4. The Group DU(1) and its subgroup XDU(1)

The group DU(1) is the group of Gaussian numbers $\frac{a}{2^p} + i\frac{b}{2^p}$, such that $(\frac{a}{2^p})^2 + (\frac{b}{2^p})^2 = 1$. As demonstrated in the previous section, only the numbers ± 1 and $\pm i$ satisfy this condition. Thus DU(1) is isomorphic to the finite group of the four complex numbers 1, i, -1, and $-i$. This group has order 4 and is isomorphic to the cyclic group $\boldsymbol{Z}_4$.

The subgroup MDU(1) is identical to DU(1). The subgroup XDU(1) has order 1 and is isomorphic to $\boldsymbol{Z}_1$.

5. The Group DU(2) and its Subgroup XDU(2)

We consider the unitary matrices of the form

$$\begin{pmatrix} \frac{a}{2^p} + i\,\frac{b}{2^p} & \frac{c}{2^p} + i\,\frac{d}{2^p} \\ \frac{e}{2^p} + i\,\frac{f}{2^p} & \frac{g}{2^p} + i\,\frac{h}{2^p} \end{pmatrix},$$

where at least one of the eight integers $a, b, c, \ldots, h$ is odd. For the sake of convenience, we assume that $\{a, b, c, d\}$ contains an odd number. We have

$$a^2 + b^2 + c^2 + d^2 \;=\; 4^p\,. \tag{1}$$

According to Lagrange's theorem each natural number can be written as the sum of four squares. So can 4^p.

If $p = 0$, then only one partition into four squares exists:

$$1 \;=\; 1^2 + 0^2 + 0^2 + 0^2\,. \tag{2}$$

If $p > 0$, then (1) implies that $a^2 + b^2 + c^2 + d^2$ has to be a multiple of 4. Therefore, either all four numbers a, b, c, and d are even or all are odd. If $p = 1$, then both kinds of partition exist:

$$\begin{aligned} 4 \;&=\; 1^2 + 1^2 + 1^2 + 1^2 \\ &=\; 2^2 + 0^2 + 0^2 + 0^2\,. \end{aligned} \tag{3}$$

If $p > 1$, then the four numbers are necessarily even:

$$\begin{aligned} 4^p &= (2^{p-1})^2 + (2^{p-1})^2 + (2^{p-1})^2 + (2^{p-1})^2 \\ &= (2^p)^2 + 0^2 + 0^2 + 0^2 . \end{aligned}$$

We denote by $p_s(n)$ the number of partitions of a number n into s squares. In contrast to this number of partitions, the total number of representations of the number n as a sum of s squares takes into account order and sign of the parts, thus e.g. considering $4 = 2^2+0^2+0^2+0^2$, $4 = 0^2+2^2+0^2+0^2$, and $4 = (-2)^2+0^2+0^2+0^2$ as three different solutions of $a^2+b^2+c^2+d^2 = 4$. This number of 'lattice on the hypersphere with radius $\sqrt{n}$' traditionally is denoted $r_s(n)$. We have (for $n > 0$ and $s > 3$) that $r_s(n) \gg p_s(n)$. Thanks to Jacobi [6], explicit expressions [7, 8, 9] exist for $r_2(n)$, $r_4(n)$, $r_6(n)$, $r_8(n)$, and $r_{12}(2n)$. In particular, we have

$$r_4(n) = 8 \sum_{4 \not| d \,|\, n} d ,$$

yielding

$$r_4(4^p) = \begin{cases} 8 & \text{if} \quad p = 0 \\ 24 & \text{if} \quad p > 0 . \end{cases} \qquad (4)$$

As a result, we have

$$p_4(4^p) = \begin{cases} 1 & \text{if} \quad p = 0 \\ 2 & \text{if} \quad p > 0 . \end{cases}$$

Thus there exist no other partitions of 4^p than those mentioned above. As a result, there exists no partition $a^2+b^2+c^2+d^2$ of 4^p (with $p > 1$) with at least one odd number a, b, c, or d. That is the reason why there do not exist any dyadic unitary 2×2 matrices with $p \geq 2$. The fact that neither $p_4(4^p)$ nor $r_4(4^p)$ increase for increasing p, once $p \geq 1$, explains why no dyadic unitary 2×2 matrices with $p > 1$ exist.

We conclude that the group DU(2) consists of matrices with level equal to either 1 or 2. As a consequence, the group is finite. It consists of the Gaussian unitary matrices where either all denominators are 1 (and numerators are based on (2)) or all denominators are 2 (and numerators are based on (3)):

$$\begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} \text{ or } \begin{pmatrix} 0 & \alpha \\ \beta & 0 \end{pmatrix} \text{ or } \frac{1}{2}\begin{pmatrix} a+ib & c+id \\ e+if & g+ih \end{pmatrix} ,$$

where α and β are 1, i, -1, or $-i$ and $a, b, \ldots$, and h are 1 or -1. This yields a group of order 96. Its most notorious members are

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

representing, in quantum computation, the dummy gate, the `NOT` gate [10, 4], and the square root of `NOT` gate [2, 10, 4, 11, 12, 13], respectively. The group is isomorphic to the group `[96, 67]` of the `GAP` library. It consists of 32 matrices with $p = 0$ and 64 matrices with $p = 1$. The former constitute the subgroup MDU(2), isomorphic to (DU(1) $\times$ DU(1)) : $\boldsymbol{S}_2$ and thus to $\boldsymbol{Z}_4^2 : \boldsymbol{Z}_2$. The subgroup MDU(2) partitions the supergroup DU(2) into two double cosets, one containing all the matrices with $p = 0$, the other all the matrices with $p = 1$.

Besides the permutation group P(2), also the Pauli group [14, 15] $\boldsymbol{P}$ is a subgroup of MDU(2):

$$\mathrm{P}(2) \ \subset \ \boldsymbol{P} \ \subset \ \mathrm{MDU}(2) \ \subset \ \mathrm{DU}(2) \ \subset \ \mathrm{U}(2)\,,$$

with successive orders

$$4 \ < \ 16 \ < \ 32 \ < \ 96 \ < \ \infty^4\,.$$

According to the definition in Sect. 3, the members of DU(2) with all four line sums equal to 1, form the subgroup XDU(2) of DU(2). The subgroup has order 4. Only two of the four matrices of XDU(2) belong to MDU(2). The subgroup XDU(2) partitions its supergroup DU(2) into nine double cosets, five of size 16 and four of size 4.

6. The Group DU(3)

For the case $m = 3$, we have to investigate a partition into six squares:

$$a^2 + b^2 + c^2 + d^2 + e^2 + f^2 \ = \ 4^p$$

with at least one of the integers $\{a, b, c, d, e, f\}$ odd. Whatever the value of p, such partition is possible. Suffice it to successively

- choose an arbitrary odd number a such that $a^2 \leq 4^p$,
- choose an arbitrary number b such that $b^2 \leq 4^p - a^2$, and
- apply Lagrange's four-square theorem to the number $4^p - a^2 - b^2$.

There always exists at least one partition of the form

$$4^p \ = \ 1^2 + 0^2 + c^2 + d^2 + e^2 + f^2\,.$$

As p can have any value from $\{0, 1, 2, \ldots\}$, this yields a (countably) infinite number of possibilities. This fact constitutes the underlying reason why DU(3) (in contrast to DU(2)) is a (countably) infinite group. An actual proof of the infinitude of DU(3) is given in Appendix B.

The numbers $p_6(4^p)$ and $r_6(4^p)$ grow fast with increasing p. Indeed, according to Jacobi, we have

$$r_6(n) \;=\; 4 \sum_{2\not{|}\, d\,|\,n} (-1)^{(d-1)/2} \left(\frac{4n^2}{d^2} - d^2 \right) .$$

For $n = 4^p$ this yields

$$r_6(4^p) \;=\; 4\,(4 \times 16^p - 1)\,,$$

i.e. an exponentially increasing function of p, in strong contrast to (4).

Within the infinite group DU(3), the matrices with $p = 0$ form the finite subgroup MDU(3), isomorphic to (DU(1) $\times$ DU(1) $\times$ DU(1)) : $\boldsymbol{S}_3$, of order $4^3 \times 3! = 384$. It partitions the whole group into an infinite number of double cosets. All elements of such a double coset have a same value of p. However, two matrices with a same p may be member of two different double cosets. E.g. the two matrices

$$\frac{1}{2^2} \begin{pmatrix} 1 & 1+2i & 3-i \\ -3-2i & 1 & 1+i \\ 1-i & -1-3i & 2 \end{pmatrix} \;\;\text{and}\;\; \frac{1}{2^2} \begin{pmatrix} -3+i & 1+i & 2 \\ 1+i & -3+i & 2 \\ 2 & 2 & 2+2i \end{pmatrix}$$

sit in two different double cosets, both with $p = 2$. The former double coset contains matrices, where all lines (i.e. rows and columns) are based on the partition $16 = 3^2 + 2^2 + 1^2 + 1^2 + 1^2 + 0^2$. The latter double coset contains matrices where four lines are based on this partition, but two other lines are based on $16 = 2^2 + 2^2 + 2^2 + 2^2 + 0^2 + 0^2$. The two double cosets have different size: the former contains $36{,}864 = 96 \times 384$ elements, whereas the latter contains only $18{,}432 = 48 \times 384$ elements.

For large values of n, we have

$$p_s(n) \;\approx\; \frac{r_s(n)}{s!\,2^s}\,,$$

such that, for sufficiently large p, we have

$$p_6(4^p) \;\approx\; \frac{1}{2880}\,16^p\,.$$

The fact that $p_6(4^p)$ grows so rapidly with increasing p leads to a fast growing number of double cosets as a function of the level 2^p. For $p = 1$, we have two double cosets; for $p = 2$, we have six double cosets; and for $p = 3$, we have at least seven double cosets. The two double cosets with $p = 1$ have e.g. the following representatives:

$$r_1 \;=\; \frac{1}{2} \begin{pmatrix} 2 & 0 & 0 \\ 0 & 1+i & 1-i \\ 0 & 1-i & 1+i \end{pmatrix} \quad\text{and}\quad r_2 \;=\; \frac{1}{2} \begin{pmatrix} 0 & 1-i & 1+i \\ 1+i & 1 & -i \\ 1-i & i & 1 \end{pmatrix},$$

Table 1: Number of DU(m) matrices.

		$m=1$	$m=2$	$m=3$	$m=4$	...
$p=0$	$q=0$	4	32	384	6,144	
$p=1$	$q=1$	0	64	2,304	147,456	
$p=1$	$q=2$	0	0	9,216	5,701,632	
$p=2$	$q=3$	0	0	36,864		
$p=2$	$q=4$	0	0	147,456		
$p=3$	$q=5$	0	0	589,824		
$p=3$	$q=6$	0	0	2,359,296		
...						
total		4	96	$\aleph_0$	$\aleph_0$	

respectively.

It turns out to be advantageous to decompose the number 2 into the irreducible elements of the Gaussian integers,

$$2 \;=\; -i(1+i)^2\,,$$

where $-i$ is one of the four Gaussian units (i.e. $1, i, -1$, and $-i$) and $1+i$ is a Gaussian prime. We thus obtain

$$r_1 = \frac{1}{1+i}\left(\begin{array}{ccc} 1+i & 0 & 0 \\ 0 & i & 1 \\ 0 & 1 & i \end{array}\right)\,, \quad r_2 = \frac{1}{(1+i)^2}\left(\begin{array}{ccc} 0 & 1+i & i(1+i) \\ i(1+i) & i & 1 \\ 1+i & -1 & i \end{array}\right)\,.$$

We may say that r_1 is of level $1+i$, whereas r_2 is of level $(1+i)^2$. In this sense, the matrices of level 2^p consist of the union of the matrices of level $(1+i)^{2p-1}$ and the matrices of level $(1+i)^{2p}$. We may say that the Gaussian prime $1+i$ plays a role like 'some kind of rational square root of 2', thus allowing levels resembling a 'halfinteger power of 2'. We will use χ as a short-hand notation for $1+i$. We will make use of the following property of the number χ: any Gaussian integer is either 0 mod χ or 1 mod χ. A Gaussian number $a+ib$ is 0 mod χ iff either both a and b are even or both a and b are odd.

The number of DU(3) matrices of different levels χ^q are given in Table 1. All matrices of level χ^0 are members of MDU(3), a group isomorphic to $\mathrm{DU}(1)^3 : \boldsymbol{S}_3$ of order $4^3{\times}3! = 384$. All $3{\times}3$ matrices of level χ^1 consist of a $1\times$

1 DU(1) block (4 possible contents) and a 2×2 DU(2) block (64 possibilities), with 9 possible block placings: indeed we have $9 \times (4 \times 64) = 2,304$. All matrices of level χ^2 or higher do not fall apart into blocks. Table 1 reveals that, for $q > 0$, the number of DU(3) matrices with level χ^q equals 576×4^q. Appendix C explains why. For $p > 0$, the DU(3) matrices of level 2^p consist of the matrices of levels χ^{2p-1} and χ^{2p}. Thus (for $p > 0$) there are 720×16^p such matrices.

An arbitrary matrix A of DU(3) of level χ^q looks like

$$A \; = \; \frac{1}{\chi^q} \begin{pmatrix} a+ib & c+id & e+if \\ g+ih & j+ik & l+im \\ n+io & p+iq & r+is \end{pmatrix} \tag{5}$$

with at least one of the nine entries $a+ib, c+id, \ldots$, or $r+is$ not divisible by χ. We now introduce the matrix $R_n(A)$, where n is a Gaussian integer. It is obtained by multiplying A by its level χ^q and subsequently computing the remainder when dividing each matrix entry by n:

$$R_n(A) \; = \; (\chi^q A) \bmod n \, .$$

E.g.

$$R_\chi \left[\frac{1}{(1+i)^5} \begin{pmatrix} 4+2i & 1-3i & -1-i \\ -1+3i & -3 & -3+2i \\ 1-i & 2+3i & -4-i \end{pmatrix} \right] \; = \; \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

$$R_2 \left[\frac{1}{(1+i)^5} \begin{pmatrix} 4+2i & 1-3i & -1-i \\ -1+3i & -3 & -3+2i \\ 1-i & 2+3i & -4-i \end{pmatrix} \right] \; = \; \begin{pmatrix} 0 & 1+i & 1+i \\ 1+i & 1 & 1 \\ 1+i & i & i \end{pmatrix} .$$

Note that all entries of an R_χ matrix are either 0 or 1 and all entries of an R_2 matrix are 0, 1, i, or $1+i$.

For any Gaussian integer n, we have $n\overline{n} \bmod \chi = n \bmod \chi$. Therefore, the unitarity condition

$$a^2+b^2+c^2+d^2+e^2+f^2 \; = \; 2^q \, ,$$

in case $q > 0$, leads to

$$(a+ib) \bmod \chi + (c+id) \bmod \chi + (e+if) \bmod \chi \; = \; 0$$

and similar for the remaining two rows, as well as for the three columns. Taking also orthogonalities into account, we can conclude that the R_χ matrix of a DU(3) matrix (of level higher than 1) always is of the type

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix} \tag{6}$$

or equivalent, i.e. of this type after permutation of rows or permutation of columns. One can similarly demonstrate that the R_2 matrix of a DU(3) matrix (of level higher than χ^1) always is of the following type or equivalent:

$$\begin{pmatrix} 0 & 1+i & 1+i \\ 1+i & \multicolumn{2}{c}{\multirow{2}{*}{M}} \\ 1+i & & \end{pmatrix}, \tag{7}$$

where the lower-right submatrix M exists in five flavours:

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

They correspond to the five 2×2 matrices $G_1, G_2, \ldots$, and G_5 discussed in Appendix D.

By multiplying the DU(3) matrix of level χ^q by an appropriate DU(3) matrix of level χ, it always is possible to obtain a matrix of level χ^{q-1} (instead of level χ^{q+1}, as one would expect normally). By performing such a multiplication again and again, we can thus lower the level of the matrix from χ^q to χ^{q-1}, to χ^{q-2}, ..., to χ^0. It suffices to proceed, at each of the q stages, in *three steps*:

- First, one multiplies by an appropriate permutation matrix (automatically of level 1), such that the original R_χ matrix is converted into the standard form (6).
- Next, one either or not multiplies by the diagonal matrix (of level 1)

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

  Detailed study [16] demonstrates that the b matrix has to be applied if the R_2 matrix (7) contains the submatrix

  $$\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ i & i \end{pmatrix} \text{ or } \begin{pmatrix} i & i \\ i & i \end{pmatrix}$$

  and the b matrix should not be applied if the submatrix is

  $$\text{either } \begin{pmatrix} 1 & i \\ 1 & i \end{pmatrix} \text{ or } \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}.$$

- Finally, one right-multiplies by the matrix (of level χ)

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

The second and the third step of the procedure are illustrated by an example where we lower the level of a given matrix from χ^5 to χ^4:

$$\frac{1}{(1+i)^5}\begin{pmatrix} 4+2i & 1-3i & -1-i \\ -1+3i & -3 & -3+2i \\ 1-i & 2+3i & -4-i \end{pmatrix} b\,a \;=\; \frac{1}{(1+i)^4}\begin{pmatrix} 3-i & -1+i & -2 \\ 1+2i & i & 1+3i \\ -i & -3-2i & 1+i \end{pmatrix},$$

what, expressed in dyadic form, looks like

$$\frac{1}{8}\begin{pmatrix} -6+2i & 2+4i & 2 \\ -2-4i & 3-3i & 1-5i \\ 2i & -5-i & 5-3i \end{pmatrix} b\,a \;=\; \frac{1}{4}\begin{pmatrix} -3+i & 1-i & 2 \\ -1-2i & -i & -1-3i \\ i & 3+2i & -1-i \end{pmatrix}.$$

The underlying reason why the 3-step procedure always works, is explained in Appendix D: it suffices to choose the appropriate matrix

$$c \;=\; \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix},$$

equal either to

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

in order to guarantee that the product of two R_2 matrices

$$\begin{pmatrix} 0 & 1+i & 1+i \\ 1+i & g_{11} & g_{12} \\ 1+i & g_{21} & g_{22} \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 \\ 0 & c_{11} & c_{12} \\ 0 & c_{21} & c_{22} \end{pmatrix}$$

is the 3×3 zero matrix (modulo 2). Now, if an $R_2(A)$ matrix is the zero matrix, then all entries of matrix A are divisible by 2 (and therefore by χ^2).

By applying the procedure again and again, we eventually obtain a decomposition of an arbitrary matrix into

- q matrices $a^{-1} = \frac{1}{2}\begin{pmatrix} 2 & 0 & 0 \\ 0 & 1+i & 1-i \\ 0 & 1-i & 1+i \end{pmatrix}$,
- q or less matrices $b^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & i & 0 \\ 0 & 0 & 1 \end{pmatrix}$,
- $q+1$ permutation matrices, and
- one diagonal matrix,

e.g.

$$\frac{1}{8}\begin{pmatrix} -6+2i & 2+4i & 2 \\ -2-4i & 3-3i & 1-5i \\ 2i & -5-i & 5-3i \end{pmatrix}$$

$$= \begin{pmatrix} -i & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} a^{-1}b^{-1} \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} a^{-1}b^{-1}$$

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} a^{-1} \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} a^{-1} \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} a^{-1}b^{-1} .$$

No procedure for shorter decomposition into matrices of levels 1 and χ is possible. Multiplication by a level-χ matrix indeed cannot convert an arbitrary matrix of level χ^q into a matrix of level χ^{q-2}.

7. The Subgroup XDU(3)

The members of DU(3) with all six line sums equal to 1 form the infinite subgroup XDU(3) of DU(3). Any line of an XDU(3) matrix is, just like any line of a DU(3) matrix, based on a partition into six squares:

$$a^2 + b^2 + c^2 + d^2 + e^2 + f^2 \ = \ 4^p ,$$

however with the two additional restrictions:

$$\begin{aligned} a + c + e &= 2^p \\ b + d + f &= 0 . \end{aligned}$$

The number of integer solutions therefore is much smaller than $r_6(4^p)$. Finding the exact number of solutions is no easy problem. It turns out to be equal to $3(2 \times 4^p - 1)$, according to [17].

Just like DU(3), we subdivide XDU(3) either into classes of different level 2^p or into classes of different level $(1+i)^q$. The matrices of level 1 form a subgroup: the 3! permutation matrices. This subgroup P(3) divides the supergroup XDU(3) into double cosets. There exist two double cosets of level 2, with representatives r_1 and

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

and with sizes 18 and 36, respectively. The former is of level $(1+i)^1$, the latter of level $(1+i)^2$. See Table 2. We note that, for $q > 1$, the number of double cosets equals 2^{q-2}, each set being of size 36, such that the number of matrices equals 9×2^q. This is demonstrated in Appendix C.1. The XDU(3) matrices of level 2^p consist of the matrices of levels $(1+i)^{2p-1}$ and $(1+i)^{2p}$. Therefore, there are $\frac{27}{2}\, 4^p$ such matrices.

While applying the 3-step DU(3) matrix decomposition method to an XDU(3) matrix, one automatically obtains a product without any diagonal

Table 2: Number of XDU(m) matrices.

		$m=1$	$m=2$	$m=3$	$m=4$	$\dots$
$p=0$	$q=0$	1	2	6	24	
$p=1$	$q=1$	0	2	18	216	
$p=1$	$q=2$	0	0	36	2,256	
$p=2$	$q=3$	0	0	72	16,320	
$p=2$	$q=4$	0	0	144	57,600	
$p=3$	$q=5$	0	0	288	230,400	
$p=3$	$q=6$	0	0	576	921,600	
$p=4$	$q=7$	0	0	1,152		
$p=4$	$q=8$	0	0	2,304		
$\dots$						
total		1	4	$\aleph_0$	$\aleph_0$	

matrices: the second step of the 3-step procedure thus is absent, such that all factors of the decomposition belong to XDU(3). The underlying reason is given at the end of Appendix D. As an example, we have

$$\frac{1}{8}\begin{pmatrix} 1-3i & 1+4i & 6-i \\ 6+4i & 1-i & 1-3i \\ 1-i & 6-3i & 1+4i \end{pmatrix} = p_1a^{-1}p_2a^{-1}p_3a^{-1}p_3a^{-1}p_3a^{-1}p_3a^{-1}$$

where the 3×3 matrices a and a^{-1} are defined in Sect. 6 and where

$$p_1 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad p_2 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad p_3 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

Because the group P(3) of permutations can be generated by two generators, e.g.

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

and because

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} = (a^{-1})^2,$$

we may conclude that the group XDU(3) can be generated by two generators, e.g.

$$g_1 \;=\; \frac{1}{2}\begin{pmatrix} 2 & 0 & 0 \\ 0 & 1+i & 1-i \\ 0 & 1-i & 1+i \end{pmatrix} \quad \text{and} \quad g_2 \;=\; \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

Finally, because

$$\begin{aligned} g_2 \;=\; & \frac{1}{2}\begin{pmatrix} 1+i & 0 & 1-i \\ 0 & 2 & 0 \\ 1-i & 0 & 1+i \end{pmatrix} \frac{1}{2}\begin{pmatrix} 1+i & 0 & 1-i \\ 0 & 2 & 0 \\ 1-i & 0 & 1+i \end{pmatrix} \\ & \times \frac{1}{2}\begin{pmatrix} 2 & 0 & 0 \\ 0 & 1+i & 1-i \\ 0 & 1-i & 1+i \end{pmatrix} \frac{1}{2}\begin{pmatrix} 2 & 0 & 0 \\ 0 & 1+i & 1-i \\ 0 & 1-i & 1+i \end{pmatrix}, \end{aligned}$$

XDU(3) can also be generated by the following two generators:

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

Thus any member of XDU(3) can be written as a product of square roots of 3×3 permutation matrices.

8. The Group DU(4)

Jacobi's formula

$$r_8(n) \;=\; 16\,(-1)^n \sum_{d\,|\,n} (-1)^d\, d^3$$

yields

$$r_8(4^p) \;=\; \begin{cases} 16 & \text{if} \quad p = 0 \\ \frac{16}{7}\,(8 \times 64^p - 15) & \text{if} \quad p > 0\,, \end{cases}$$

such that it is no surprise DU(4) is infinite.

We consider within the infinite group DU(4), the subgroup MDU(4) of monomial matrices. It is isomorphic to $\mathrm{DU}(1)^4 : \boldsymbol{S}_4$, of order $4^4 \times 4! = 6,144$. Twenty-four of its members are permutation matrices and thus represent the 24 classical reversible logic circuits acting on two bits. The monomial subgroup partitions the total group into an infinite number of double cosets.

All matrices of $m = 4$ and $p = 1$ have at least one line based on the partition $4 = 1^2 + 1^2 + 1^2 + 1^2 + 0^2 + 0^2 + 0^2 + 0^2$, the remaining lines being based on $4 = 2^2 + 0^2 + 0^2 + 0^2 + 0^2 + 0^2 + 0^2 + 0^2$. One of the double cosets contains the two square roots of `NOT`, such as

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

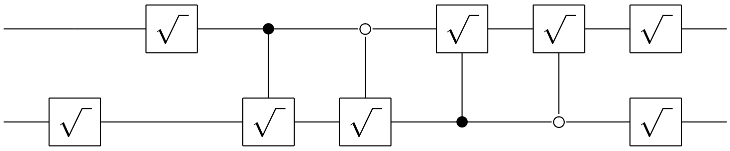


Fig. 1: From left to right: two square roots of NOT, four controlled square roots of NOT, and the twin square roots of NOT.

Its size is 73,728. Another double coset (equally of size 73,728) contains the four controlled square roots of NOT, such as[a]

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

See Fig. 1. All six circuits belong to XDU(4). Both double cosets have level $1+i$.

There exist 393,216 unitary matrices where all entries are from the set of the 4 numbers $\frac{1}{2}\{1, i, -1, -i\}$. These matrices are of the form $\frac{1}{2}\ H(4,4)$, where $H(4,4)$ denotes the 4×4 complex (or: generalized) Hadamard matrices [18]. They fall apart into two equivalence classes: 294,912 are represented by the dephased matrix

$$\frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}, \tag{8}$$

i.e. 1/2 times the 4-point Fourier transform F_4; the 98,304 remaining matrices being represented by the dephased matrix

$$\frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}, \tag{9}$$

i.e. the tensor product of two 2-point Fourier transforms F_2:

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

To the latter double coset belongs the matrix representing the twin square

[a] A 'controlled square root of NOT' may also be called a 'square root of controlled NOT', as well as a 'square root of Feynman gate'.

roots of `NOT`:

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

All matrices of the form $\frac{1}{2}\,H(4,4)$ are of level $(1+i)^2$.

The above-mentioned four double cosets (containing a total of 540,672 matrices) do not exhaust all unitary dyadic matrices with $p=1$, as is illustrated by the existence of e.g.

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

There are in fact nine classes [16] with level 2^1.

All matrices of level $(1+i)^0$ fall apart in four 1×1 blocks and are member of the MDU(4) subgroup of DU(4): we have $24\times 4^4 = 6,144$ such matrices. All matrices of level $(1+i)^1$ either consist of two DU(1) blocks and one DU(2) block or consist of two DU(2) blocks. We have $72\times(4^2\times 64)+18\times 64^2 = 147,456$ such matrices. Among the 5,701,632 matrices of level $(1+i)^2$, there are $16\times(4\times 9,216) = 589,824$ ones, which consist of one DU(1) block and one DU(3) block. All the matrices of level $(1+i)^3$ or higher do not have a block structure. Finally, Table 1 gives the number of DU(4) matrices for some levels.

Whereas $m=3$ leads to only one matrix type modulo χ, i.e. the matrix type (6), the case $m=4$ leads to six different R_χ types:

$$\begin{pmatrix} 0&0&0&0\\0&0&0&0\\0&0&1&1\\0&0&1&1 \end{pmatrix},\quad \begin{pmatrix} 1&1&0&0\\1&1&0&0\\0&0&1&1\\0&0&1&1 \end{pmatrix},\quad \begin{pmatrix} 1&1&0&0\\1&1&0&0\\1&1&0&0\\1&1&0&0 \end{pmatrix},$$
$$\begin{pmatrix} 1&1&1&1\\1&1&1&1\\0&0&0&0\\0&0&0&0 \end{pmatrix},\quad \begin{pmatrix} 1&1&0&0\\1&1&0&0\\1&1&1&1\\1&1&1&1 \end{pmatrix},\quad \begin{pmatrix} 1&1&1&1\\1&1&1&1\\1&1&1&1\\1&1&1&1 \end{pmatrix}. \qquad (10)$$

Detailed study [16] reveals that nevertheless an arbitrary DU(4) matrix can be decomposed into a string of permutation matrices, a^{-1} matrices, and b^{-1} matrices, where a^{-1} is a controlled square root of `NOT` and b^{-1} is a controlled phase gate, e.g.

$$a^{-1} = \frac{1}{2}\begin{pmatrix} 2&0&0&0\\0&2&0&0\\0&0&1+i&1-i\\0&0&1-i&1+i \end{pmatrix} \quad \text{and} \quad b^{-1} = \begin{pmatrix} 1&0&0&0\\0&1&0&0\\0&0&i&0\\0&0&0&1 \end{pmatrix} .$$

However, for a given 4×4 matrix, in order to lower its level from χ^q to χ^{q-1}, it may be necessary to apply the 3-step procedure of Sect. 6 not just once but once, twice, or three times[b]. To further lower the level (from χ^{q-1} to χ^{q-2}, χ^{q-3}, ...), the 3-step procedure needs to be applied, each time, either once or twice. As a result, the number of a^{-1} factors in the decomposition is $2q+1$ at most. One of the underlying reasons why a procedure similar to the DU(3) procedure is applicable, is the fact that all six matrix types (10) consist of 2×2 blocks, either equal to

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \quad \text{or equal to} \quad \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} ,$$

such that Appendix D can again be applied [16].

9. The Subgroup XDU(4)

The members of DU(4) where all eigth line sums are equal to 1, form the infinite subgroup XDU(4) of DU(4). The XDU(4) matrices of level 1 form the subgroup P(4) of the $4! = 24$ permutation matrices. This subgroup P(4) divides the supergroup XDU(4) into double cosets. E.g., there are eleven double cosets of level 2, i.e. two of level $1+i$ plus nine of level $(1+i)^2$, comprising a total of 2,472 matrices. Numbers for higher levels are given in Table 2. The table suggests that the number of matrices grows like 225×4^q, for $q > 3$.

An arbitrary member of XDU(4) can be factorized without phase gates. Because the permutation group P(4) can be generated by two generators, e.g.

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

and because

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = (a^{-1})^2 ,$$

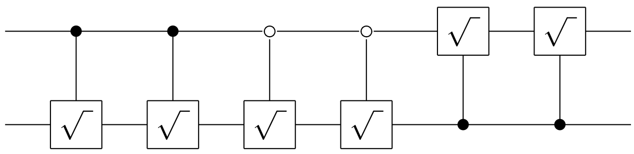
we may conclude that the group XDU(4) can be generated by two generators,

[b] Once if the R_χ type (10) contains a zero row or column; twice if the R_χ type contains zero entries but neither a zero row nor a zero column; either twice or three times if the R_χ type contains no zero entries.

e.g.

$$g_1 = \frac{1}{2}\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 1+i & 1-i \\ 0 & 0 & 1-i & 1+i \end{pmatrix} \quad \text{and} \quad g_2 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

Finally, because g_2 can be decomposed as



,

we can conclude that the whole group XDU(4) can be generated by three different controlled square roots of `NOT`:

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

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

Two of them control a same qubit, the third controls the other qubit. Two of them are controlled by a signal of same polarity, the remaining one is controlled by a signal of opposite polarity. We note that the first and third generator together generate a subgroup of XDU(4) isomorphic to XDU(3), i.e. all 4×4 matrices of the form

$$\begin{pmatrix} 1 & \mathbb{O} \\ \mathbb{O} & y \end{pmatrix},$$

where $\mathbb{O}$ denotes either the 1×3 zero matrix or the 3×1 zero matrix, and y is a member of XDU(3).

We summarize the present section by concluding that any matrix in XDU(4) can be written as a product of controlled square roots of `NOT`.

10. The Group DU(m), with $m > 4$

Each DU(m) matrix of level 1 consists of lines of the form $[X, 0, 0, \ldots, 0]$ (up to permutation of its vector components), where X is a number from $\{1, i, -1, -i\}$. There are $m!\,4^m$ such matrices. They all are member of one of the $m!$ subgroups of DU(m) isomorphic to DU$(1)^m$.

We now consider a DU(m) matrix of level χ^1. Because we have to guarantee the unit norm of each matrix line, a line can only exist (up to ordering) in two different forms: either $[X, 0, 0, \ldots, 0]$ or $[Y, Y, 0, 0, \ldots, 0]$, where Y is a number from $\{1/\chi, i/\chi, -1/\chi, -i/\chi\}$. Orthonormality implies that the matrix consists of merely

$$\begin{pmatrix} X \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} Y & Y \\ Y & Y \end{pmatrix}$$

blocks. As a result, there exist

$$m!\, 4^m \left[m! \sum_{k=0}^{\lfloor m/2 \rfloor} \frac{1}{k!\,(m-2k)!} - 1 \right]$$

such matrices. This amount can be written as $m!\,4^m\,(\kappa_m - 1)$, where κ_m may be expressed in terms of the confluent hypergeometric series ${}_1F_1(-j, k/2, -l/4)$, which in turn can be expressed in terms of the Gamma function and the Laguerre polynomials. Additionally, κ_m is a number sequenced by Sloane [19] and applied e.g. by Khruzin [20] and Proctor [21]. All these $m!\,4^m\,(\kappa_m - 1)$ matrices belong to one of the subgroups of DU(m) isomorphic to some group DU$(2)^k\times$ DU$(1)^{m-2k}$ (with $0 \leq k \leq \lfloor m/2 \rfloor$). The number of these subgroups amounts to $m!\,(\lambda_m/2^m - 1)$, where the number λ_m is another hypergeometric series (also expressable in terms of the Gamma function and Laguerre polynomials) as well as another integer sequence [22]. Taking into account the asymptotic behaviour [23] of the Laguerre polynomials for large degree into account, as well as Stirling's formula, we find for $m \gg 1$:

$$\begin{aligned}
\kappa_m &\approx \frac{1}{\sqrt{2}}\,(m-1)^{m/2} \exp\left[-\frac{m}{2} + \frac{\sqrt{2m+1}}{2} + \frac{3}{8}\right] \\
\lambda_m &\approx \frac{1}{\sqrt{2}}\,(m-1)^{m/2} \exp\left[-\frac{m}{2} + \sqrt{2m+1}\right].
\end{aligned}$$

The set of DU(m) matrices of level χ^2 is much richer, as they do also display lines of the form $[Y, Z, Z, 0, 0, \ldots, 0]$ and $[Z, Z, Z, Z, 0, 0, \ldots, 0]$, where Z is one of the complex numbers $\{\pm 1/2, \pm i/2\}$. such that, besides the single 1×1 block type, the single 2×2 block type, and the single 3×3 block type, i.e.

$$\begin{pmatrix} X \end{pmatrix}, \quad \begin{pmatrix} Y & Y \\ Y & Y \end{pmatrix}, \quad \text{and} \quad \begin{pmatrix} Y & Z & Z \\ Y & Z & Z \\ 0 & Y & Y \end{pmatrix},$$

they also may display five different 4×4 block types:

$$\begin{pmatrix} 0 & Y & Z & Z \\ Y & 0 & Z & Z \\ Z & Z & Z & Z \\ Z & Z & Z & Z \end{pmatrix}, \quad \begin{pmatrix} 0 & Y & Z & Z \\ Y & 0 & Z & Z \\ Z & Z & 0 & Y \\ Z & Z & Y & 0 \end{pmatrix}, \quad \begin{pmatrix} Y & 0 & Z & Z \\ 0 & Y & Z & Z \\ Y & 0 & Z & Z \\ 0 & Y & Z & Z \end{pmatrix},$$

$$\begin{pmatrix} Y & 0 & Y & 0 \\ 0 & Y & 0 & Y \\ Z & Z & Z & Z \\ Z & Z & Z & Z \end{pmatrix}, \quad \text{and} \quad \begin{pmatrix} Z & Z & Z & Z \\ Z & Z & Z & Z \\ Z & Z & Z & Z \\ Z & Z & Z & Z \end{pmatrix},$$

etcetera. Results by Severini and Szöllősi [24] on unitary (though not necessarily dyadic) matrices demonstrate how the number of different $k \times k$ block types increases fast with increasing k.

We recall here some results of Sects. 4, 5, 6, and 8. For $m = 1$, we have only one level (i.e. level 1) with only one R_χ remainder class, i.e. the 1×1 matrix (1). For $m = 2$, we have only two levels: level 1 with only one remainder class, i.e.

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

and level χ with only one remainder class, i.e.

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

For $m = 3$, we have $\aleph_0$ levels: level 1 with only one remainder class, i.e.

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

and levels χ^q (with $q > 0$) with only one remainder class, i.e.

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

For $m = 4$, we have $\aleph_0$ levels: level 1 with only one remainder class, i.e.

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

level χ with two remainder classes, i.e.

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

and levels χ^q (with $q > 1$) with six remainder classes, i.e. the classes (10).

We now conjecture that also in the case of arbitrary dimension m and arbitrary level (higher than χ^0), the R_χ types consist exclusively of 2×2 blocks

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

2×2 blocks

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

and (in case m is odd) a zero row and a zero column. We checked that this hypothesis is true for all matrices with $m < 7$. If the conjecture is generally true, then Appendix D may be applied once again, the role of the building blocks a^{-1} and b^{-1} being played by

$$a^{-1} \;=\; \frac{1}{2} \begin{pmatrix} 2 \cdot \mathbb{1} & \mathbb{O} & \mathbb{O} \\ \mathbb{O} & 1+i & 1-i \\ \mathbb{O} & 1-i & 1+i \end{pmatrix} \quad \text{and} \quad b^{-1} \;=\; \begin{pmatrix} \mathbb{1} & \mathbb{O} & \mathbb{O} \\ \mathbb{O} & i & 0 \\ \mathbb{O} & 0 & 1 \end{pmatrix},$$

where $2 \cdot \mathbb{1}$ denotes twice the $(m-2) \times (m-2)$ unit matrix $\mathbb{1}$ and where $\mathbb{O}$ denotes either the $(m-2) \times 1$ zero matrix or the $1 \times (m-2)$ zero matrix. For more details, the reader is referred to [16]. The procedure results in a decomposition of an arbitrary DU(m) matrix into a finite number of exclusively controlled square root of `NOT` gates, controlled phase gates and classical reversible gates.

We close the present section by drawing attention to matrices of one particular level. Apart from zero, the smallest norm a unitary dyadic matrix entry can have, is $1/2^q$. If, in a line, all m entries have this minimum non-zero norm, then

$$m \, \frac{1}{2^q} \;=\; 1\,.$$

Therefore, we define the critical number Q :

$$Q(m) \;=\; \log_2(m)\,.$$

All matrices with $q < Q$ have, in each row and in each column, at least one zero. In fact, in each line, they have at least $m - 2^q = 2^Q - 2^q$ and at most $m - 1 = 2^Q - 1$ zeroes. Only matrices with $q \geq Q$ may have all entries non-zero. In particular, if Q happens to be an integer, then matrices may be of the Hadamard style, iff $q = Q$. The condition that Q is an integer, is equivalent to m being of the form 2^w. All matrices representing a quantum circuit (acting on w qubits) fulfil this condition. Therefore we investigate this case in particular.

In case $m = 2^w$, matrices with $q = Q = w$ may be of the Hadamard style [5, 18]. These $2^w \times 2^w$ matrices look like

$$\frac{1}{\chi^w}\begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & & & \\ \vdots & & & \\ 1 & & & \end{pmatrix},$$

i.e. χ^{-w} times a tensor product $F_2 \otimes F_2 \otimes \dots \otimes F_2 \otimes F_4 \otimes F_4 \otimes \dots \otimes F_4$ of Fourier transforms.

11. The Subgroup XDU(m), with $m > 4$

The number of XDU(m) matrices of level χ^0 is $m!$, whereas the number of XDU(m) matrices of level χ^1 is given by

$$m!\,(\mu_m - 1)\,,$$

where μ_m is given either by the appropriate ${}_1F_1(-j, k/2, -l/4)$ series or by the appropriate Sloane sequence [25]. For $m \gg 1$, we have

$$\mu_m \;\approx\; \frac{1}{\sqrt{2}}(m-1)^{m/2}\exp\Big[-\frac{m}{2} + \frac{\sqrt{2m+1}}{\sqrt{2}} + \frac{1}{4}\Big]\,.$$

For an XDU(m) of arbitrary level χ^q, we conjecture a decomposition without b^{-1} phase matrices. If $m = 2^w$, then the a^{-1} building block is the controlled square root of `NOT` with $w-1$ controlling lines.

12. Conclusion

We have introduced the dyadic unitary matrix groups DU(m). The matrix entries consist of Gaussian rationals with denominator 2^p. We have investigated into detail the cases DU(1), DU(2), DU(3), and DU(4). Whereas DU(1) is isomorphic to the cyclic group $\boldsymbol{Z}_4$ of order 4, the group DU(2) is a finite group of order 96, and all groups DU(m) with $m \geq 3$ are (countably) infinite. We propose a simple algorithm to decompose an arbitrary member of DU(3) into a product of DU(3) matrices with exclusively denominators 2^0 and 2^1. A similar, though somewhat more complicated, algorithm is introduced for $m > 3$. In case m is a power of 2, say equals 2^w, such decomposition is useful for the synthesis of a quantum computer acting on w qubits, by applying merely building blocks known as 'controlled square roots of `NOT`'.

Appendix A

In this appendix we prove the following theorem: if a unitary $m \times m$ matrix has m identical row sums, then that row sum is on the unit circle.

Let M be an $m \times m$ unitary matrix, where the m row sums are denoted $\sigma_1, \sigma_2, \ldots, \sigma_m$. We compute

$$\begin{aligned}
\sum_k \sigma_k \, \overline{\sigma_k} &= \sum_k \Big[\Big(\sum_l M_{kl}\Big) \overline{\Big(\sum_n M_{kn}\Big)} \Big] \\
&= \sum_k \Big[\Big(\sum_l M_{kl}\Big) \Big(\sum_n \overline{M_{kn}}\Big) \Big] \\
&= \sum_k \sum_l \sum_n \; M_{kl} \overline{M_{kn}} \\
&= \sum_k \sum_l \Big(\sum_{n \neq l} \; M_{kl} \overline{M_{kn}} + M_{kl} \overline{M_{kl}} \Big) \\
&= \sum_l \sum_{n \neq l} \sum_k M_{kl} \overline{M_{kn}} + \sum_k \sum_l M_{kl} \overline{M_{kl}} \\
&= \sum_l \sum_{n \neq l} 0 + \sum_k 1 \\
&= 0 + \sum_k 1 \\
&= m \, .
\end{aligned}$$

If all σ_k are equal to σ, this yields $m\sigma\,\overline{\sigma} = m$ and thus $\sigma\,\overline{\sigma} = 1$. The matrix M can thus be written as the product of a matrix M' with contant row sum 1 and a scalar σ that merely is a complex phase.

Analogously, if a unitary matrix has all identical column sums, then that column sum is on the unit circle.

Finally, if a unitary matrix has all row sums equal (say, σ) and all column sums equal (say, τ), then these two sums are equal. The proof is trivial: it suffices to compute, in two different ways, the sum of all matrix elements, $\sum_j \sum_k \; M_{jk} = \sum_j \sigma = m\sigma$ and $\sum_k \sum_j \; M_{jk} = \sum_k \tau = m\tau$.

Appendix B

An example of a dyadic unitary matrix with dimension m equal to 3 and level equal to 2 is given by

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

Its three eigenvalues are 1, $\exp(i\theta_1)$, and $\exp(i\theta_2)$, with $\theta_1 = -\frac{\pi}{2} - \theta$ and $\theta_2 = -\frac{\pi}{2} + \theta$, where θ is Arccos(3/4) $\approx$ 41°24'35".

Because the only rational multiples of π with a rational cosine [26] are $0 = \text{Arccos}(1)$, $\pi/3 = \text{Arccos}(1/2)$, $\pi/2 = \text{Arccos}(0)$, $2\pi/3 = \text{Arccos}(-1/2)$, $\pi = \text{Arccos}(-1)$, $5\pi/3 = \text{arccos}(-1/2)$, $3\pi/2 = \text{arccos}(0)$, and $5\pi/3 =$ arccos(1/2), neither θ_1 nor θ_2 is a rational multiple of π. Therefore, the power sequence $\{y, y^2, y^3, \ldots\}$ is not periodic. Therefore the sequence $\{\ldots, y^{-2}, y^{-1}, y^0, y^1, y^2, \ldots\}$ forms a countably infinite group. As it is a cyclic subgroup of DU(3), this proves that DU(3) is at least countably infinite.

As an immediate consequence, DU(m) with m larger than 3 also is infinite. Suffice it to note that the $m \times m$ square matrix

$$\begin{pmatrix} \mathbb{1} & \mathbb{O} \\ \mathbb{O} & y \end{pmatrix},$$

where $\mathbb{1}$ represents the $(m-3) \times (m-3)$ unit matrix and $\mathbb{O}$ either the $(m-3) \times 3$ zero matrix or the $3 \times (m-3)$ zero matrix, is a member of DU(m) and has infinite order.

Appendix C

C.1 Number of XDU(3) matrices

We assume six arbitrary integers a_1, a_2, a_3, b_1, b_2, and b_3 (not all zero). With their help, we construct the following three vectors:

$$\begin{aligned}
V_1 &= \frac{1}{\chi^{q+1}}\Big[(a_1-b_1)+i(a_1+b_1) \quad (a_2-b_2)+i(a_2+b_2) \quad (a_3-b_3)+i(a_3+b_3)\Big] \\
V_2 &= \frac{1}{\chi^{q+1}}\Big[(a_2-b_2)+i(a_3+b_3) \quad (a_3-b_3)+i(a_1+b_1) \quad (a_1-b_1)+i(a_2+b_2)\Big] \\
V_3 &= \frac{1}{\chi^{q+1}}\Big[(a_3-b_3)+i(a_2+b_2) \quad (a_1-b_1)+i(a_3+b_3) \quad (a_2-b_2)+i(a_1+b_1)\Big].
\end{aligned}$$

The numbers $(a_1-b_1)+i(a_1+b_1)$, $(a_2-b_2)+i(a_2+b_2)$, and $(a_3-b_3)+i(a_3+b_3)$ are divisible by $1+i$,

$$(a_1-b_1)+i(a_1+b_1) = (a_1+ib_1)(1+i) \text{ etc.}$$

Thus the vector V_1 is of level χ^q at most. We assume that the vector V_1 has exactly level χ^q, i.e. that at least one of the three numbers a_1+ib_1, a_2+ib_2, and a_3+ib_3 is not divisible by χ. Detailed analysis [17] then demonstrates that the vectors V_2 and V_3 are not divisible by χ and thus have level χ^{q+1}.

The three vectors V_1, V_2, and V_3 all have the same line sum,

$$\frac{1}{\chi^{q+1}}[\,(a_1+a_2+a_3-b_1-b_2-b_3)+i(a_1+a_2+a_3+b_1+b_2+b_3)\,]$$

$$= \frac{1}{\chi^{q+1}}(1+i)[\,(a_1+a_2+a_3)+i(b_1+b_2+b_3)\,]$$

$$= \frac{1}{\chi^{q}}[\,(a_1+a_2+a_3)+i(b_1+b_2+b_3)\,]\,.$$

They also have the same norm,

$$\frac{1}{2^{q+1}}\;(\,2a_1^2+2b_1^2+2a_2^2+2b_2^2+2a_3^2+2b_3^2\,)$$

$$= \frac{1}{2^q}\;(a_1^2+a_2^2+a_3^2+b_1^2+b_2^2+b_3^2)\,.$$

We assume that this norm is equal to 1,

$$(a_1^2+a_2^2+a_3^2+b_1^2+b_2^2+b_3^2)\;/\;2^q \;=\; 1\,.$$

We also assume that the line sum equals 1. Therefore the norm of the line sum is equal to 1,

$$[(a_1+a_2+a_3)^2+(b_1+b_2+b_3)^2]\;/\;2^q \;=\; 1\,.$$

Subtracting the former result from the latter result yields that $a_1a_2+a_2a_3+a_3a_1+b_1b_2+b_2b_3+b_3b_1$ equals zero. Because straightforward calculation of the inner product $V_1\overline{V_2}$ leads to the value $(a_1a_2+a_2a_3+a_3a_1+b_1b_2+b_2b_3+b_3b_1)/2^q$, we can conclude that V_1 and V_2 are orthogonal to each other. Similarly, we find that all three vectors V_1, V_2, and V_3 are orthogonal to one another. Thus the triple $\{V_1,V_2,V_3\}$ gives rise to an XDU(3) matrix of level χ^{q+1}. In fact, because of permutation of matrix lines, it actually gives rise to six different XDU(3) matrices of level χ^{q+1}.

We now consider different triples $\{V_1,V_2,V_3\}$, $\{V_1',V_2',V_3'\}$, $\{V_1'',V_2'',V_3''\}$, $\ldots$, where V_1, V_1', V_1'', $\ldots$ all are vectors of level χ^q. Then V_1 is orthogonal to V_2 and V_3, but not to V_2', V_3', V_2'', V_3'', V_2''', $\ldots$ [17]. Thus only the triples $\{V_1,V_2,V_3\}$, $\{V_1',V_2',V_3'\}$, $\ldots$ can give rise to an XDU(3) matrix of level χ^{q+1}. As each such triple gives rise to six XDU(3) matrices, for any $q\geq 0$, there are 6 times as many XDU(3) matrices of level χ^{q+1} as there are vectors of level χ^q. Because with each vector V_1 of level χ^q correspond two vectors (V_2 and V_3) of level χ^{q+1}, the number of vectors with a same level χ^q increases like 2^q. Therefore, the number of matrices similarly increases as 2^q and thus equals $c\times 2^q$, with c some appropriate constant. The coefficient c is identified by remarking that there are eighteen XDU(3) matrices of level χ^1 (Table 2). One thus finds $c=9$. We conclude: for any $q\geq 1$, there exist 9×2^q XDU(3) matrices of level χ^q.

C.2 Number of DU(3) matrices

A similar reasoning as in Subappendix C.1 exists for the DU(3) matrices [17]. Again we assume vectors V_1, V_1', V_1'', $\ldots$ of level χ^q. With each vector V_1

Table 3: The five R_2 remainder matrices G_j.

$R_2(g) = G_j$	$R_2(g\,a) = G_jR_2(a)$	$R_2(g\,b\,a) = G_jR_2(b\,a)$
$\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$	$\begin{pmatrix} 1+i & 1+i \\ 1+i & 1+i \end{pmatrix}$	$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$
$\begin{pmatrix} 1 & 1 \\ i & i \end{pmatrix}$	$\begin{pmatrix} 1+i & 1+i \\ 1+i & 1+i \end{pmatrix}$	$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$
$\begin{pmatrix} 1 & i \\ 1 & i \end{pmatrix}$	$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 1+i & 1+i \\ 1+i & 1+i \end{pmatrix}$
$\begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}$	$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 1+i & 1+i \\ 1+i & 1+i \end{pmatrix}$
$\begin{pmatrix} i & i \\ i & i \end{pmatrix}$	$\begin{pmatrix} 1+i & 1+i \\ 1+i & 1+i \end{pmatrix}$	$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

of level χ^q now correspond four vectors (V_2, V_3, V_4, and V_5) of level χ^{q+1}, such that the number of vectors with a same level χ^q grows like 4^q. With each quintuple $\{V_1, V_2, V_3, V_4, V_5\}$ correspond two triples, i.e. $\{V_1, V_2, V_3\}$ and $\{V_1, V_4, V_5\}$ and therefore twice six matrices of DU(3). The number of matrices grows like the number of vectors, i.e. equals $c \times 4^q$. We identify the coefficient c by remarking that there are 2,304 DU(3) matrices of level χ^1 (Table 1). One thus finds $c = 576$. We conclude: for any $q \geq 1$, there exist 576×4^q DU(3) matrices of level χ^q.

Appendix D

Applying Gaussian primes to Sect. 5 leads to the conclusion that the group DU(2) consists of 32 matrices of level 1 and 64 matrices g of level χ. The latter all have the same remainder matrix $R_\chi(g)$ equal to

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

but can have five and only five different remainder matrices $R_2(g)$ (up to equivalence by row or column swapping). We call these 2×2 matrices $G_1, G_2, \ldots$, and G_5, respectively, see Table 3.

We now introduce two particular DU(2) matrices: a of level χ and b of level 1,

$$a \;=\; \frac{1}{\chi}\begin{pmatrix} -i & 1 \\ 1 & -i \end{pmatrix} \quad \text{and} \quad b \;=\; \begin{pmatrix} -i & 0 \\ 0 & 1 \end{pmatrix}.$$

We compute the matrices $R_2(ga) = G_j R_2(a)$ and $R_2(gba) = G_j R_2(b\,a)$. With

$$R_2(a) \;=\; \begin{pmatrix} i & 1 \\ 1 & i \end{pmatrix} \quad \text{and} \quad R_2(ba) \;=\; \begin{pmatrix} 1 & i \\ 1 & i \end{pmatrix},$$

this yields Table 3. We see that in two cases multiplication by $R_2(a)$ leads to the 2×2 zero matrix and that in the remaining three cases multiplication by $R_2(b\,a)$ leads to the zero matrix. A zero $R_2(g)R_2(a)$ matrix reveals that the product ga is not of level χ^2 but instead of level 1, whereas a zero $R_2(g)R_2(b\,a)$ matrix reveals that the product gba is of level 1. We thus may conclude that each of the sixty-four DU(2) matrices g of level χ can be lowered to level 1 either through multiplication by a or through multiplication by $b\,a$.

Only 2 of the 64 matrices g belong to XDU(2). They both lead to type G_4, such that $R_2(ga)$ is the zero matrix.

Acknowledgment

Alexis De Vos thanks Fred Brackx (Vakgroep wiskundige analyse, Universiteit Gent) for valuable discussions concerning the hypergeometric series.

Bibliography

[1] K. Conrad, "$SL_2(\mathbb{Z})$", http://www.math.uconn.edu/~kconrad/ blurbs/.

[2] A. De Vos, J. De Beule, and L. Storme, *Computing with the square root of* `NOT`, Serdica Journal of Computing **3**, 359 (2009).

[3] W. Wang and C. Xu, *An excluding algorithm for testing whether a family of graphs are determined by their generalized spectra*, Lin. Alg. Appl. **418**, 62 (2006).

[4] A. De Vos, *Reversible computing*, Wiley–VCH, Weinheim, 2010.

[5] U. Haagerup, *Orthogonal maximal abelian $*$-subalgebras of the $n\times n$ matrices and cyclic n-roots*, in: *Operator algebras and quantum field theory*, S. Doplicher, R. Longo, J. Roberts, and L. Zsidó, eds., International Press, Cambridge, 1996, pp. 296–322.

[6] C. Jacobi, *Fundamenta nova theoriae functionum ellipticarum*, Bornträger, Regiomonti, 1829, pp. 103–108.

[7] E. Grosswald, *Representations of integers as sums of squares*, Springer, New York, 1985, pp. 121–123.

[8] B. Berndt, *Fragments by Ramanujan on Lambert series*, in: *Number theory and its applications*, S. Kanemutsi and K. Györy, eds., Kluwer Academic Publishers, Dordrecht, 1999, pp. 35–49.

[9] K. Williams, *Number theory in the spirit of Liouville*, Cambridge University Press, Cambridge, 2011, pp. 77–99 and 251–261.

[10] R. Wille and R. Drechsler, *Towards a design flow for reversible logic*, Springer, Dordrecht, 2010.

[11] D. Deutsch, *Quantum computation*, Physics World **5**, 57 (1992).

[12] D. Deutsch, A. Ekert, and R. Lupacchini, *Machines, logic and quantum physics*, Bulletin of Symbolic Logic **3**, 265 (2000).

[13] A. Galindo and M. Martín-Delgado, *Information and computation: classical and quantum aspects*, Rev. Mod. Phys. **74**, 347 (2002).

[14] M. Nielsen and I. Chuang, *Quantum computation and quantum information*, Cambridge University Press, Cambridge, 2000, pp. 65, 454, and 611.

[15] M. Planat, *Clifford quantum computer and the Mathieu groups*, Invertis Journal of Science and Technology **3**, 1 (2010).

[16] R. Van Laer, *Dyadic quantum computers*, MSc. Thesis Universiteit Gent, Gent, 2011.

[17] S. Vandenbrande, *Reversibele digitale schakelingen*, MSc. Thesis Universiteit Gent, Gent, 2011.

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

[19] N. Sloane, *The on-line encyclopedia of integer sequences*, sequence A047974, http://oeis.org/A047974.

[20] A. Khruzin, *Enumeration of chord diagrams*, arXiv:math/0008209.

[21] R. Proctor, *Let's expand Rota's twelvefold way for counting partitions!*, arXiv:math/0606404.

[22] N. Sloane, *The on-line encyclopedia of integer sequences*, sequence A000898, http://oeis.org/A000898.

[23] *Laguerre polynomials*, Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/Laguerre_polynomial.

[24] S. Severini and F. Szöllősi, *A further look into combinatorial orthogonality*, Electronic Journal of Linear Algebra **17**, 376 (2008).

[25] N. Sloane, *The on-line encyclopedia of integer sequences*, sequence A000085, http://oeis.org/A000085.

[26] J. Jahnel, *When is the (co)sine of a rational angle equal to a rational number?*, http://www.uni-math.gwdg.de/jahnel/Preprints/ cos.pdf (2006).