

Open Systems & Information Dynamics
Vol. 19, No. 1 (2012) 1–28
DOI: xxx
© World Scientific Publishing Company



1 The Group of Dyadic Unitary Matrices

2 Alexis De Vos, Raphaël Van Laer, and Steven Vandenbrande

3 *Vakgroep elektronica en informatiesystemen*

4 *Universiteit Gent*

5 *Sint Pietersnieuwstraat 41, B-9000 Gent, Belgium*

6 (Received: September 2, 2011)

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

15 1. Introduction

16 Basically, there exist three kinds of groups:

- 17 • finite groups, i.e. groups with a finite order,
- 18 • infinite but nevertheless discrete groups, i.e. groups with a countably
19 infinite order, and
- 20 • Lie groups, i.e. groups with an uncountably infinite order.

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

24 The most basic example of a countably infinite nonabelian group is the
25 discrete group $SL_2(\mathbb{Z})$, i.e. the special linear group of 2×2 matrices with in-
26 teger entries. Conrad [1] demonstrates that the group can be generated with
27 merely two generators and shows how to decompose an arbitrary group mem-
28 ber into a finite product of factors, each equal to one of these two building
29 blocks. In the present paper, we follow a basically similar approach for de-
30 scribing the group of rational unitary matrices where all matrix elements have
31 a denominator of the form 2^p . The motivation to study this group is inspired
32 by its importance in computer theory. Whereas classical reversible computa-
33 tion is described by finite groups and quantum computation is represented by

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

40 2. The Group $\text{DU}(m)$

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

44 Next, we consider, within the group $\text{U}(m)$, the matrices which have ex-
 45 clusively Gaussian entries. This means that the matrix entries are Gaussian
 46 rationals

$$47 \quad \frac{a}{A} + i \frac{b}{B}, \quad \frac{c}{C} + i \frac{d}{D}, \quad \dots,$$

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

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

$$58 \quad \frac{a}{2^p} + i \frac{b}{2^p},$$

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

$$65 \quad \begin{pmatrix} \frac{5}{2} & 1 \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}^{-1} = \begin{pmatrix} \frac{2}{3} & -\frac{4}{3} \\ -\frac{2}{3} & \frac{10}{3} \end{pmatrix},$$

66 the inverse of a dyadic matrix is not necessarily a dyadic matrix. The inverse
 67 of dyadic unitary matrix, however, is a dyadic unitary matrix (with the same
 68 level), for the simple reason that the inverse of a unitary matrix is its Hermi-
 69 tian transpose. The product of a dyadic matrix with level equal to 2^{p_1} and a

70 dyadic matrix with level equal to 2^{p_2} is a dyadic matrix with level lower than
 71 or equal to $2^{p_1+p_2}$. We thus may conclude that the dyadic unitary matrices
 72 form a group. We call this group the dyadic unitary group $\text{DU}(m)$.

73 3. Two Subgroups of $\text{DU}(m)$

74 In the present section, we discuss two (out of the many) subgroups of $\text{DU}(m)$.

75 An $m \times m$ matrix has $2m$ lines, i.e. m rows and m columns. We consider
 76 the matrices whose line sums are all equal. If the matrix is unitary, then
 77 the constant line sum is on the unit circle (See Appendix A). If the matrix is
 78 dyadic, then the constant line sum is a dyadic rational. Now, on the unit circle
 79 there exist only four such Gaussian rationals $\frac{x}{2^p} + i \frac{y}{2^p}$. Indeed, the condition
 80 $(\frac{x}{2^p})^2 + (\frac{y}{2^p})^2 = 1$ leads to $x^2 + y^2 = (2^p)^2$, which implies that $\{x, y, 2^p\}$ forms
 81 a Pythagorean triple. However, there exist no primitive Pythagorean triples
 82 where the greatest number is even. We conclude that either x or y has to
 83 be zero. Therefore, if the matrix is both unitary and dyadic, the constant
 84 line sum equals one of the four complex numbers $1, i, -1,$ and $-i$, known
 85 as the four Gaussian units. The product of a matrix with constant line sum
 86 equal to s and a matrix with constant line sum equal to t is a matrix with
 87 constant line sum st . Proof is provided in [4, p. 239]. Therefore, matrices
 88 with constant line sum equal to 1 form a group. The members of $\text{DU}(m)$ that
 89 have constant line sum equal to 1, thus form a subgroup of $\text{DU}(m)$; we will
 90 call this subgroup $\text{XDU}(m)$. Their study is interesting in the framework of
 91 quantum computing. The groups $\text{XDU}(2^w)$ naturally appear when studying
 92 quantum circuits built with the gate called ‘the square root of NOT’, see below
 93 in Sections 8 to 11. Matrices belonging to $\text{XDU}(m)$ may be considered as
 94 a ‘complex generalization’ of doubly stochastic (or bistochastic) matrices,
 95 where equally well all line sums equal 1, but where all entries are restricted
 96 to real non-negative numbers.

97 The matrices of $\text{DU}(m)$ with $p = 0$, i.e. the $\text{DU}(m)$ matrices of level 1,
 98 form a finite subgroup, isomorphic to the semi-direct product $(\text{DU}(1) \times$
 99 $\text{DU}(1) \times \dots \times \text{DU}(1)) : \mathcal{S}_m = \text{DU}(1)^m : \mathcal{S}_m$, where \mathcal{S}_m denotes the sym-
 100 metric group of degree m (and thus order $m!$). We will call the subgroup the
 101 monomial dyadic unitary group $\text{MDU}(m)$, as all its members are matrices
 102 with exactly one non-zero entry in each row and each column. The group
 103 $\text{P}(m)$ of all $m \times m$ permutation matrices, in turn, is a subgroup of $\text{MDU}(m)$:

$$104 \quad \text{P}(m) \subset \text{MDU}(m) \subset \text{DU}(m) \subset \text{U}(m).$$

105 The subgroup $\text{MDU}(m)$ partitions the supergroup $\text{DU}(m)$ into double cosets,
 106 each containing matrices of a same level 2^p . These double cosets can be
 107 regarded as equivalence classes. Any element of a double coset can act as
 108 its representative. Here, two matrices are considered equivalent iff they can

109 be converted into one another by applying a combination of the following
110 operations:

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

113 This equivalence is analogous to the one used in investigating real and com-
114 plex Hadamard matrices. See e.g. the equivalence relation \approx by Haagerup [5].

115 4. The Group $\text{DU}(1)$ and its subgroup $\text{XDU}(1)$

116 The group $\text{DU}(1)$ is the group of Gaussian numbers $\frac{a}{2^p} + i\frac{b}{2^p}$, such that
117 $(\frac{a}{2^p})^2 + (\frac{b}{2^p})^2 = 1$. As demonstrated in the previous section, only the numbers
118 ± 1 and $\pm i$ satisfy this condition. Thus $\text{DU}(1)$ is isomorphic to the finite group
119 of the four complex numbers $1, i, -1,$ and $-i$. This group has order 4 and is
120 isomorphic to the cyclic group \mathbf{Z}_4 .

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

123 5. The Group $\text{DU}(2)$ and its Subgroup $\text{XDU}(2)$

124 We consider the unitary matrices of the form

$$125 \begin{pmatrix} \frac{a}{2^p} + i\frac{b}{2^p} & \frac{c}{2^p} + i\frac{d}{2^p} \\ \frac{e}{2^p} + i\frac{f}{2^p} & \frac{g}{2^p} + i\frac{h}{2^p} \end{pmatrix},$$

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

$$128 a^2 + b^2 + c^2 + d^2 = 4^p. \quad (1)$$

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

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

$$132 1 = 1^2 + 0^2 + 0^2 + 0^2. \quad (2)$$

133 If $p > 0$, then (1) implies that $a^2 + b^2 + c^2 + d^2$ has to be a multiple of 4.
134 Therefore, either all four numbers $a, b, c,$ and d are even or all are odd. If
135 $p = 1$, then both kinds of partition exist:

$$136 \begin{aligned} 4 &= 1^2 + 1^2 + 1^2 + 1^2 \\ &= 2^2 + 0^2 + 0^2 + 0^2. \end{aligned} \quad (3)$$

137

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

$$139 \quad 4^p = (2^{p-1})^2 + (2^{p-1})^2 + (2^{p-1})^2 + (2^{p-1})^2$$

$$140 \quad = (2^p)^2 + 0^2 + 0^2 + 0^2.$$

141 We denote by $p_s(n)$ the number of partitions of a number n into s squares.
 142 In contrast to this number of partitions, the total number of representations
 143 of the number n as a sum of s squares takes into account order and sign of
 144 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
 145 $4 = (-2)^2 + 0^2 + 0^2 + 0^2$ as three different solutions of $a^2 + b^2 + c^2 + d^2 = 4$.
 146 This number of 'lattice on the hypersphere with radius \sqrt{n} ' traditionally is
 147 denoted $r_s(n)$. We have (for $n > 0$ and $s > 3$) that $r_s(n) \gg p_s(n)$. Thanks
 148 to Jacobi [6], explicit expressions [7, 8, 9] exist for $r_2(n)$, $r_4(n)$, $r_6(n)$, $r_8(n)$,
 149 and $r_{12}(2n)$. In particular, we have

$$150 \quad r_4(n) = 8 \sum_{4 \nmid d | n} d,$$

151 yielding

$$152 \quad r_4(4^p) = \begin{cases} 8 & \text{if } p = 0 \\ 24 & \text{if } p > 0. \end{cases} \quad (4)$$

153 As a result, we have

$$154 \quad p_4(4^p) = \begin{cases} 1 & \text{if } p = 0 \\ 2 & \text{if } p > 0. \end{cases}$$

155 Thus there exist no other partitions of 4^p than those mentioned above. As a
 156 result, there exists no partition $a^2 + b^2 + c^2 + d^2$ of 4^p (with $p > 1$) with at
 157 least one odd number a , b , c , or d . That is the reason why there do not exist
 158 any dyadic unitary 2×2 matrices with $p \geq 2$. The fact that neither $p_4(4^p)$ nor
 159 $r_4(4^p)$ increase for increasing p , once $p \geq 1$, explains why no dyadic unitary
 160 2×2 matrices with $p > 1$ exist.

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

$$165 \quad \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} \text{ or } \begin{pmatrix} 0 & \alpha \\ \beta & 0 \end{pmatrix} \text{ or } \frac{1}{2} \begin{pmatrix} a + ib & c + id \\ e + if & g + ih \end{pmatrix},$$

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

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

166 representing, in quantum computation, the dummy gate, the NOT gate [10, 4],
 167 and the square root of NOT gate [2, 10, 4, 11, 12, 13], respectively. The group
 168 is isomorphic to the group [96, 67] of the GAP library. It consists of 32
 169 matrices with $p = 0$ and 64 matrices with $p = 1$. The former constitute
 170 the subgroup MDU(2), isomorphic to $(DU(1) \times DU(1)) : \mathbf{S}_2$ and thus to
 171 $\mathbf{Z}_4^2 : \mathbf{Z}_2$. The subgroup MDU(2) partitions the supergroup DU(2) into two
 172 double cosets, one containing all the matrices with $p = 0$, the other all the
 173 matrices with $p = 1$.

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

$$176 \quad \mathrm{P}(2) \subset \mathbf{P} \subset \mathrm{MDU}(2) \subset \mathrm{DU}(2) \subset \mathrm{U}(2),$$

177 with successive orders

$$178 \quad 4 < 16 < 32 < 96 < \infty^4.$$

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

184 6. The Group DU(3)

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

$$186 \quad a^2 + b^2 + c^2 + d^2 + e^2 + f^2 = 4^p$$

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

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

192 There always exists at least one partition of the form

$$193 \quad 4^p = 1^2 + 0^2 + c^2 + d^2 + e^2 + f^2.$$

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

198 The numbers $p_6(4^p)$ and $r_6(4^p)$ grow fast with increasing p . Indeed, ac-
 199 cording to Jacobi, we have

$$200 \quad r_6(n) = 4 \sum_{2/d|n} (-1)^{(d-1)/2} \left(\frac{4n^2}{d^2} - d^2 \right).$$

201 For $n = 4^p$ this yields

$$202 \quad r_6(4^p) = 4(4 \times 16^p - 1),$$

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

204 Within the infinite group $\text{DU}(3)$, the matrices with $p = 0$ form the finite
 205 subgroup $\text{MDU}(3)$, isomorphic to $(\text{DU}(1) \times \text{DU}(1) \times \text{DU}(1)) : \mathbf{S}_3$, of order
 206 $4^3 \times 3! = 384$. It partitions the whole group into an infinite number of double
 207 cosets. All elements of such a double coset have a same value of p . However,
 208 two matrices with a same p may be member of two different double cosets.
 209 E.g. the two matrices

$$210 \quad \frac{1}{2^2} \begin{pmatrix} 1 & 1+2i & 3-i \\ -3-2i & 1 & 1+i \\ 1-i & -1-3i & 2 \end{pmatrix} \quad \text{and} \quad \frac{1}{2^2} \begin{pmatrix} -3+i & 1+i & 2 \\ 1+i & -3+i & 2 \\ 2 & 2 & 2+2i \end{pmatrix}$$

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

218 For large values of n , we have

$$219 \quad p_s(n) \approx \frac{r_s(n)}{s! 2^s},$$

220 such that, for sufficiently large p , we have

$$221 \quad p_6(4^p) \approx \frac{1}{2880} 16^p.$$

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

$$227 \quad r_1 = \frac{1}{2} \begin{pmatrix} 2 & 0 & 0 \\ 0 & 1+i & 1-i \\ 0 & 1-i & 1+i \end{pmatrix} \quad \text{and} \quad r_2 = \frac{1}{2} \begin{pmatrix} 0 & 1-i & 1+i \\ 1+i & 1 & -i \\ 1-i & i & 1 \end{pmatrix},$$

Table 1: Number of $\text{DU}(m)$ matrices.

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

228 respectively.

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

$$231 \quad 2 = -i(1+i)^2,$$

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

$$234 \quad r_1 = \frac{1}{1+i} \begin{pmatrix} 1+i & 0 & 0 \\ 0 & i & 1 \\ 0 & 1 & i \end{pmatrix}, \quad r_2 = \frac{1}{(1+i)^2} \begin{pmatrix} 0 & 1+i & i(1+i) \\ i(1+i) & i & 1 \\ 1+i & -1 & i \end{pmatrix}.$$

235 We may say that r_1 is of level $1+i$, whereas r_2 is of level $(1+i)^2$. In this sense,
 236 the matrices of level 2^p consist of the union of the matrices of level $(1+i)^{2p-1}$
 237 and the matrices of level $(1+i)^{2p}$. We may say that the Gaussian prime $1+i$
 238 plays a role like ‘some kind of rational square root of 2’, thus allowing levels
 239 resembling a ‘halfinteger power of 2’. We will use χ as a short-hand notation
 240 for $1+i$. We will make use of the following property of the number χ : any
 241 Gaussian integer is either $0 \pmod{\chi}$ or $1 \pmod{\chi}$. A Gaussian number $a+ib$ is
 242 $0 \pmod{\chi}$ iff either both a and b are even or both a and b are odd.

243 The number of $\text{DU}(3)$ matrices of different levels χ^q are given in Table 1.
 244 All matrices of level χ^0 are members of $\text{MDU}(3)$, a group isomorphic to
 245 $\text{DU}(1)^3 : \mathcal{S}_3$ of order $4^3 \times 3! = 384$. All 3×3 matrices of level χ^1 consist of a $1 \times$

246 1 DU(1) block (4 possible contents) and a 2×2 DU(2) block (64 possibilities),
 247 with 9 possible block placings: indeed we have $9 \times (4 \times 64) = 2,304$. All
 248 matrices of level χ^2 or higher do not fall apart into blocks. Table 1 reveals
 249 that, for $q > 0$, the number of DU(3) matrices with level χ^q equals 576×4^q .
 250 Appendix C explains why. For $p > 0$, the DU(3) matrices of level 2^p consist
 251 of the matrices of levels $\chi^{2^{p-1}}$ and χ^{2^p} . Thus (for $p > 0$) there are 720×16^p
 252 such matrices.

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

$$254 \quad A = \frac{1}{\chi^q} \begin{pmatrix} a + ib & c + id & e + if \\ g + ih & j + ik & l + im \\ n + io & p + iq & r + is \end{pmatrix} \quad (5)$$

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

$$259 \quad R_n(A) = (\chi^q A) \bmod n.$$

260 E.g.

$$261 \quad R_\chi \left[\frac{1}{(1+i)^5} \begin{pmatrix} 4+2i & 1-3i & -1-i \\ -1+3i & -3 & -3+2i \\ 1-i & 2+3i & -4-i \end{pmatrix} \right] = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

$$262 \quad R_2 \left[\frac{1}{(1+i)^5} \begin{pmatrix} 4+2i & 1-3i & -1-i \\ -1+3i & -3 & -3+2i \\ 1-i & 2+3i & -4-i \end{pmatrix} \right] = \begin{pmatrix} 0 & 1+i & 1+i \\ 1+i & 1 & 1 \\ 1+i & i & i \end{pmatrix}.$$

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

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

$$267 \quad a^2 + b^2 + c^2 + d^2 + e^2 + f^2 = 2^q,$$

268 in case $q > 0$, leads to

$$269 \quad (a + ib) \bmod \chi + (c + id) \bmod \chi + (e + if) \bmod \chi = 0$$

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

$$273 \quad \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix} \quad (6)$$

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

$$277 \quad \begin{pmatrix} 0 & 1+i & 1+i \\ 1+i & & M \\ 1+i & & \end{pmatrix}, \quad (7)$$

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

$$279 \quad \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ i & i \end{pmatrix}, \begin{pmatrix} 1 & i \\ 1 & i \end{pmatrix}, \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix} \text{ and } \begin{pmatrix} i & i \\ i & i \end{pmatrix}.$$

280 They correspond to the five 2×2 matrices G_1, G_2, \dots , and G_5 discussed in
 281 Appendix D.

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

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

$$292 \quad b = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -i & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

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

$$295 \quad \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ i & i \end{pmatrix} \text{ or } \begin{pmatrix} i & i \\ i & i \end{pmatrix}$$

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

$$297 \quad \text{either } \begin{pmatrix} 1 & i \\ 1 & i \end{pmatrix} \text{ or } \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}.$$

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

$$299 \quad a = \frac{1}{2} \begin{pmatrix} 2 & 0 & 0 \\ 0 & 1-i & 1+i \\ 0 & 1+i & 1-i \end{pmatrix} = \frac{1}{1+i} \begin{pmatrix} 1+i & 0 & 0 \\ 0 & -i & 1 \\ 0 & 1 & -i \end{pmatrix}.$$

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

$$302 \quad \frac{1}{(1+i)^5} \begin{pmatrix} 4+2i & 1-3i & -1-i \\ -1+3i & -3 & -3+2i \\ 1-i & 2+3i & -4-i \end{pmatrix} b a = \frac{1}{(1+i)^4} \begin{pmatrix} 3-i & -1+i & -2 \\ 1+2i & i & 1+3i \\ -i & -3-2i & 1+i \end{pmatrix},$$

303 what, expressed in dyadic form, looks like

$$304 \quad \frac{1}{8} \begin{pmatrix} -6+2i & 2+4i & 2 \\ -2-4i & 3-3i & 1-5i \\ 2i & -5-i & 5-3i \end{pmatrix} b a = \frac{1}{4} \begin{pmatrix} -3+i & 1-i & 2 \\ -1-2i & -i & -1-3i \\ i & 3+2i & -1-i \end{pmatrix}.$$

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

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

305 in order to guarantee that the product of two R_2 matrices

$$306 \quad \begin{pmatrix} 0 & 1+i & 1+i \\ 1+i & g_{11} & g_{12} \\ 1+i & g_{21} & g_{22} \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & c_{11} & c_{12} \\ 0 & c_{21} & c_{22} \end{pmatrix}$$

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

309 By applying the procedure again and again, we eventually obtain a de-
 310 composition of an arbitrary matrix into

$$311 \quad \bullet \text{ } q \text{ matrices } a^{-1} = \frac{1}{2} \begin{pmatrix} 2 & 0 & 0 \\ 0 & 1+i & 1-i \\ 0 & 1-i & 1+i \end{pmatrix},$$

$$312 \quad \bullet \text{ } q \text{ or less matrices } b^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & i & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

313 \bullet $q + 1$ permutation matrices, and

314 \bullet one diagonal matrix,

315 e.g.

$$316 \quad \frac{1}{8} \begin{pmatrix} -6+2i & 2+4i & 2 \\ -2-4i & 3-3i & 1-5i \\ 2i & -5-i & 5-3i \end{pmatrix}$$

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

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.

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

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

$$350 \quad \frac{1}{8} \begin{pmatrix} 1-3i & 1+4i & 6-i \\ 6+4i & 1-i & 1-3i \\ 1-i & 6-3i & 1+4i \end{pmatrix} = p_1 a^{-1} p_2 a^{-1} p_3 a^{-1} p_3 a^{-1} p_3 a^{-1} p_3 a^{-1}$$

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

$$352 \quad p_1 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad p_2 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad p_3 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

353 Because the group P(3) of permutations can be generated by two gener-
 354 ators, e.g.

$$355 \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix},$$

356 and because

$$357 \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} = (a^{-1})^2,$$

we may conclude that the group $\text{XDU}(3)$ 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

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

$\text{XDU}(3)$ 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 $\text{XDU}(3)$ can be written as a product of square roots of 3×3 permutation matrices.

8. The Group $\text{DU}(4)$

Jacobi's formula

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

yields

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

such that it is no surprise $\text{DU}(4)$ is infinite.

We consider within the infinite group $\text{DU}(4)$, the subgroup $\text{MDU}(4)$ of monomial matrices. It is isomorphic to $\text{DU}(1)^4 : \mathcal{S}_4$, 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

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

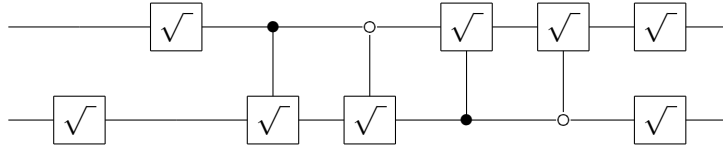


Fig. 1: From left to right: two square roots of NOT, four controlled square roots of NOT, and the twin square roots of NOT.

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

386
$$\frac{1}{2} \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 1+i & 1-i \\ 0 & 0 & 1-i & 1+i \end{pmatrix}.$$

387 See Fig. 1. All six circuits belong to XDU(4). Both double cosets have level
 388 $1+i$.

389 There exist 393,216 unitary matrices where all entries are from the set
 390 of the 4 numbers $\frac{1}{2} \{1, i, -1, -i\}$. These matrices are of the form $\frac{1}{2} H(4, 4)$,
 391 where $H(4, 4)$ denotes the 4×4 complex (or: generalized) Hadamard matrices
 392 [18]. They fall apart into two equivalence classes: 294,912 are represented by
 393 the dephased matrix

394
$$\frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}, \tag{8}$$

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

397
$$\frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}, \tag{9}$$

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

399
$$\frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

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

^aA ‘controlled square root of NOT’ may also be called a ‘square root of controlled NOT’, as well as a ‘square root of Feynman gate’.

401 roots of NOT:

$$402 \quad \frac{1}{2} \begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix} \otimes \frac{1}{2} \begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix} = \frac{1}{2} \begin{pmatrix} i & 1 & 1 & -i \\ 1 & i & -i & 1 \\ 1 & -i & i & 1 \\ -i & 1 & 1 & i \end{pmatrix}.$$

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

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

$$407 \quad \frac{1}{2} \begin{pmatrix} 1+i & 1 & 1 & 0 \\ 1+i & -1 & -1 & 0 \\ 0 & 1 & -1 & 1+i \\ 0 & -1 & 1 & 1+i \end{pmatrix}.$$

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

409 All matrices of level $(1+i)^0$ fall apart in four 1×1 blocks and are member
410 of the MDU(4) subgroup of DU(4): we have $24 \times 4^4 = 6,144$ such matrices.
411 All matrices of level $(1+i)^1$ either consist of two DU(1) blocks and one
412 DU(2) block or consist of two DU(2) blocks. We have $72 \times (4^2 \times 64) + 18 \times 64^2 =$
413 $147,456$ such matrices. Among the 5,701,632 matrices of level $(1+i)^2$, there
414 are $16 \times (4 \times 9,216) = 589,824$ ones, which consist of one DU(1) block and
415 one DU(3) block. All the matrices of level $(1+i)^3$ or higher do not have
416 a block structure. Finally, Table 1 gives the number of DU(4) matrices for
417 some levels.

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

$$420 \quad \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix},$$

$$421 \quad \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}. \quad (10)$$

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

$$426 \quad a^{-1} = \frac{1}{2} \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 1+i & 1-i \\ 0 & 0 & 1-i & 1+i \end{pmatrix} \quad \text{and} \quad b^{-1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & i & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

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

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

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

428 9. The Subgroup XDU(4)

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

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

$$440 \quad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix},$$

441 and because

$$442 \quad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = (a^{-1})^2,$$

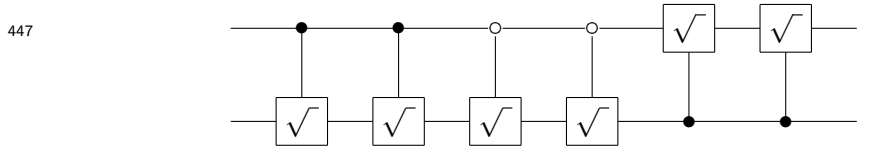
443 we may conclude that the group XDU(4) can be generated by two generators,

^bOnce 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.

444 e.g.

$$445 \quad g_1 = \frac{1}{2} \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 1+i & 1-i \\ 0 & 0 & 1-i & 1+i \end{pmatrix} \quad \text{and} \quad g_2 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

446 Finally, because g_2 can be decomposed as



448 we can conclude that the whole group $\text{XDU}(4)$ can be generated by three
449 different controlled square roots of NOT:

$$450 \quad \frac{1}{2} \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 1+i & 1-i \\ 0 & 0 & 1-i & 1+i \end{pmatrix}, \quad \frac{1}{2} \begin{pmatrix} 1+i & 1-i & 0 & 0 \\ 1-i & 1+i & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix},$$

$$451 \quad \frac{1}{2} \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 1+i & 0 & 1-i \\ 0 & 0 & 2 & 0 \\ 0 & 1-i & 0 & 1+i \end{pmatrix}.$$

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

$$457 \quad \begin{pmatrix} 1 & \mathbb{O} \\ \mathbb{O} & y \end{pmatrix},$$

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

460 We summarize the present section by concluding that any matrix in
461 $\text{XDU}(4)$ can be written as a product of controlled square roots of NOT.

462 10. The Group $\text{DU}(m)$, with $m > 4$

463 Each $\text{DU}(m)$ matrix of level 1 consists of lines of the form $[X, 0, 0, \dots, 0]$
464 (up to permutation of its vector components), where X is a number from
465 $\{1, i, -1, -i\}$. There are $m! 4^m$ such matrices. They all are member of one
466 of the $m!$ subgroups of $\text{DU}(m)$ isomorphic to $\text{DU}(1)^m$.

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 $[X, 0, 0, \dots, 0]$ or $[Y, Y, 0, 0, \dots, 0]$, where Y is a number from $\{1/\chi, i/\chi, -1/\chi, -i/\chi\}$. Orthonormality implies that the matrix consists of merely

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

467 blocks. As a result, there exist

$$468 \quad m! 4^m \left[m! \sum_{k=0}^{\lfloor m/2 \rfloor} \frac{1}{k! (m-2k)!} - 1 \right]$$

469 such matrices. This amount can be written as $m! 4^m (\kappa_m - 1)$, where κ_m may
 470 be expressed in terms of the confluent hypergeometric series ${}_1F_1(-j, k/2, -l/4)$,
 471 which in turn can be expressed in terms of the Gamma function and the La-
 472 guerre polynomials. Additionally, κ_m is a number sequenced by Sloane [19]
 473 and applied e.g. by Khruzin [20] and Proctor [21]. All these $m! 4^m (\kappa_m -$
 474 $1)$ matrices belong to one of the subgroups of $DU(m)$ isomorphic to some
 475 group $DU(2)^k \times DU(1)^{m-2k}$ (with $0 \leq k \leq \lfloor m/2 \rfloor$). The number of these
 476 subgroups amounts to $m! (\lambda_m/2^m - 1)$, where the number λ_m is another
 477 hypergeometric series (also expressable in terms of the Gamma function and
 478 Laguerre polynomials) as well as another integer sequence [22]. Taking into
 479 account the asymptotic behaviour [23] of the Laguerre polynomials for large
 480 degree into account, as well as Stirling's formula, we find for $m \gg 1$:

$$481 \quad \kappa_m \approx \frac{1}{\sqrt{2}} (m-1)^{m/2} \exp \left[-\frac{m}{2} + \frac{\sqrt{2m+1}}{2} + \frac{3}{8} \right]$$

$$482 \quad \lambda_m \approx \frac{1}{\sqrt{2}} (m-1)^{m/2} \exp \left[-\frac{m}{2} + \sqrt{2m+1} \right].$$

483 The set of $DU(m)$ matrices of level χ^2 is much richer, as they do also
 484 display lines of the form $[Y, Z, Z, 0, 0, \dots, 0]$ and $[Z, Z, Z, Z, 0, 0, \dots, 0]$, where
 485 Z is one of the complex numbers $\{\pm 1/2, \pm i/2\}$. such that, besides the single
 486 1×1 block type, the single 2×2 block type, and the single 3×3 block type,
 487 i.e.

$$488 \quad \begin{pmatrix} X \end{pmatrix}, \quad \begin{pmatrix} Y & Y \\ Y & Y \end{pmatrix}, \quad \text{and} \quad \begin{pmatrix} Y & Z & Z \\ Y & Z & Z \\ 0 & Y & Y \end{pmatrix},$$

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

$$490 \quad \begin{pmatrix} 0 & Y & Z & Z \\ Y & 0 & Z & Z \\ Z & Z & Z & Z \\ Z & Z & Z & Z \end{pmatrix}, \quad \begin{pmatrix} 0 & Y & Z & Z \\ Y & 0 & Z & Z \\ Z & Z & 0 & Y \\ Z & Z & Y & 0 \end{pmatrix}, \quad \begin{pmatrix} Y & 0 & Z & Z \\ 0 & Y & Z & Z \\ Y & 0 & Z & Z \\ 0 & Y & Z & Z \end{pmatrix},$$

$$491 \quad \begin{pmatrix} Y & 0 & Y & 0 \\ 0 & Y & 0 & Y \\ Z & Z & Z & Z \\ Z & Z & Z & Z \end{pmatrix}, \quad \text{and} \quad \begin{pmatrix} Z & Z & Z & Z \\ Z & Z & Z & Z \\ Z & Z & Z & Z \\ Z & Z & Z & Z \end{pmatrix},$$

492 etcetera. Results by Severini and Szöllősi [24] on unitary (though not neces-
493 sarily dyadic) matrices demonstrate how the number of different $k \times k$ block
494 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.

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

495 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

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

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

$$500 \quad a^{-1} = \frac{1}{2} \begin{pmatrix} 2 \cdot \mathbb{1} & \mathbb{O} & \mathbb{O} \\ \mathbb{O} & 1+i & 1-i \\ \mathbb{O} & 1-i & 1+i \end{pmatrix} \quad \text{and} \quad b^{-1} = \begin{pmatrix} \mathbb{1} & \mathbb{O} & \mathbb{O} \\ \mathbb{O} & i & 0 \\ \mathbb{O} & 0 & 1 \end{pmatrix},$$

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

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

$$511 \quad m \frac{1}{2^q} = 1.$$

512 Therefore, we define the critical number Q :

$$513 \quad Q(m) = \log_2(m).$$

514 All matrices with $q < Q$ have, in each row and in each column, at least one
 515 zero. In fact, in each line, they have at least $m - 2^q = 2^Q - 2^q$ and at most
 516 $m - 1 = 2^Q - 1$ zeroes. Only matrices with $q \geq Q$ may have all entries
 517 non-zero. In particular, if Q happens to be an integer, then matrices may
 518 be of the Hadamard style, iff $q = Q$. The condition that Q is an integer, is
 519 equivalent to m being of the form 2^w . All matrices representing a quantum
 520 circuit (acting on w qubits) fulfil this condition. Therefore we investigate
 521 this case in particular.

522 In case $m = 2^w$, matrices with $q = Q = w$ may be of the Hadamard style
 523 [5, 18]. These $2^w \times 2^w$ matrices look like

$$524 \quad \frac{1}{\chi^w} \begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & & & \\ \vdots & & & \\ 1 & & & \end{pmatrix},$$

525 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
 526 Fourier transforms.

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

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

$$530 \quad m! (\mu_m - 1),$$

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

$$533 \quad \mu_m \approx \frac{1}{\sqrt{2}} (m-1)^{m/2} \exp \left[-\frac{m}{2} + \frac{\sqrt{2m+1}}{\sqrt{2}} + \frac{1}{4} \right].$$

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

537 12. Conclusion

538 We have introduced the dyadic unitary matrix groups DU(m). The matrix
 539 entries consist of Gaussian rationals with denominator 2^p . We have investi-
 540 gated into detail the cases DU(1), DU(2), DU(3), and DU(4). Whereas DU(1)
 541 is isomorphic to the cyclic group \mathbf{Z}_4 of order 4, the group DU(2) is a finite
 542 group of order 96, and all groups DU(m) with $m \geq 3$ are (countably) infinite.
 543 We propose a simple algorithm to decompose an arbitrary member of DU(3)
 544 into a product of DU(3) matrices with exclusively denominators 2^0 and 2^1 .
 545 A similar, though somewhat more complicated, algorithm is introduced for
 546 $m > 3$. In case m is a power of 2, say equals 2^w , such decomposition is useful
 547 for the synthesis of a quantum computer acting on w qubits, by applying
 548 merely building blocks known as ‘controlled square roots of NOT’.

549

Appendix A

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

552 Let M be an $m \times m$ unitary matrix, where the m row sums are de-
553 noted $\sigma_1, \sigma_2, \dots, \sigma_m$. We compute

$$\begin{aligned}
 554 \quad \sum_k \sigma_k \overline{\sigma_k} &= \sum_k \left[\left(\sum_l M_{kl} \right) \overline{\left(\sum_n M_{kn} \right)} \right] \\
 555 &= \sum_k \left[\left(\sum_l M_{kl} \right) \left(\sum_n \overline{M_{kn}} \right) \right] \\
 556 &= \sum_k \sum_l \sum_n M_{kl} \overline{M_{kn}} \\
 557 &= \sum_k \sum_l \left(\sum_{n \neq l} M_{kl} \overline{M_{kn}} + M_{kl} \overline{M_{kl}} \right) \\
 558 &= \sum_l \sum_{n \neq l} \sum_k M_{kl} \overline{M_{kn}} + \sum_k \sum_l M_{kl} \overline{M_{kl}} \\
 559 &= \sum_l \sum_{n \neq l} 0 + \sum_k 1 \\
 560 &= 0 + \sum_k 1 \\
 561 &= m.
 \end{aligned}$$

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

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

567 Finally, if a unitary matrix has all row sums equal (say, σ) and all column
568 sums equal (say, τ), then these two sums are equal. The proof is trivial: it
569 suffices to compute, in two different ways, the sum of all matrix elements,
570 $\sum_j \sum_k M_{jk} = \sum_j \sigma = m\sigma$ and $\sum_k \sum_j M_{jk} = \sum_k \tau = m\tau$.

571

Appendix B

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

$$574 \quad y = \frac{1}{2} \begin{pmatrix} 1-i & 1 & i \\ 1+i & -i & 1 \\ 0 & 1+i & 1-i \end{pmatrix}.$$

575 Its three eigenvalues are 1, $\exp(i\theta_1)$, and $\exp(i\theta_2)$, with $\theta_1 = -\frac{\pi}{2} - \theta$ and
 576 $\theta_2 = -\frac{\pi}{2} + \theta$, where θ is $\text{Arccos}(3/4) \approx 41^\circ 24' 35''$.

577 Because the only rational multiples of π with a rational cosine [26] are
 578 $0 = \text{Arccos}(1)$, $\pi/3 = \text{Arccos}(1/2)$, $\pi/2 = \text{Arccos}(0)$, $2\pi/3 = \text{Arccos}(-1/2)$,
 579 $\pi = \text{Arccos}(-1)$, $5\pi/3 = \text{arccos}(-1/2)$, $3\pi/2 = \text{arccos}(0)$, and $5\pi/3 = \text{arc}$ -
 580 $\text{cos}(1/2)$, neither θ_1 nor θ_2 is a rational multiple of π . Therefore, the power
 581 sequence $\{y, y^2, y^3, \dots\}$ is not periodic. Therefore the sequence $\{\dots, y^{-2}, y^{-1},$
 582 $y^0, y^1, y^2, \dots\}$ forms a countably infinite group. As it is a cyclic subgroup of
 583 $\text{DU}(3)$, this proves that $\text{DU}(3)$ is at least countably infinite.

584 As an immediate consequence, $\text{DU}(m)$ with m larger than 3 also is infi-
 585 nite. Suffice it to note that the $m \times m$ square matrix

$$586 \quad \begin{pmatrix} \mathbb{1} & \mathbb{O} \\ \mathbb{O} & y \end{pmatrix},$$

587 where $\mathbb{1}$ represents the $(m-3) \times (m-3)$ unit matrix and \mathbb{O} either the
 588 $(m-3) \times 3$ zero matrix or the $3 \times (m-3)$ zero matrix, is a member of $\text{DU}(m)$
 589 and has infinite order.

590 Appendix C

591 C.1 NUMBER OF $\text{XDU}(3)$ MATRICES

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

$$594 \quad V_1 = \frac{1}{\chi^{q+1}} \begin{bmatrix} (a_1 - b_1) + i(a_1 + b_1) & (a_2 - b_2) + i(a_2 + b_2) & (a_3 - b_3) + i(a_3 + b_3) \end{bmatrix}$$

$$595 \quad V_2 = \frac{1}{\chi^{q+1}} \begin{bmatrix} (a_2 - b_2) + i(a_3 + b_3) & (a_3 - b_3) + i(a_1 + b_1) & (a_1 - b_1) + i(a_2 + b_2) \end{bmatrix}$$

$$596 \quad V_3 = \frac{1}{\chi^{q+1}} \begin{bmatrix} (a_3 - b_3) + i(a_2 + b_2) & (a_1 - b_1) + i(a_3 + b_3) & (a_2 - b_2) + i(a_1 + b_1) \end{bmatrix}.$$

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

$$599 \quad (a_1 - b_1) + i(a_1 + b_1) = (a_1 + ib_1)(1 + i) \text{ etc.}$$

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

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

$$605 \quad \frac{1}{\chi^{q+1}} [(a_1 + a_2 + a_3 - b_1 - b_2 - b_3) + i(a_1 + a_2 + a_3 + b_1 + b_2 + b_3)]$$

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

608 They also have the same norm,

$$\begin{aligned}
609 \quad &\frac{1}{2^{q+1}}(2a_1^2+2b_1^2+2a_2^2+2b_2^2+2a_3^2+2b_3^2) \\
610 \quad &= \frac{1}{2^q}(a_1^2+a_2^2+a_3^2+b_1^2+b_2^2+b_3^2).
\end{aligned}$$

611 We assume that this norm is equal to 1,

$$612 \quad (a_1^2+a_2^2+a_3^2+b_1^2+b_2^2+b_3^2)/2^q = 1.$$

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

$$615 \quad [(a_1+a_2+a_3)^2+(b_1+b_2+b_3)^2]/2^q = 1.$$

616 Subtracting the former result from the latter result yields that $a_1a_2+a_2a_3+$
617 $a_3a_1+b_1b_2+b_2b_3+b_3b_1$ equals zero. Because straightforward calculation of the
618 inner product $V_1\bar{V}_2$ leads to the value $(a_1a_2+a_2a_3+a_3a_1+b_1b_2+b_2b_3+b_3b_1)/2^q$,
619 we can conclude that V_1 and V_2 are orthogonal to each other. Similarly, we
620 find that all three vectors V_1, V_2 , and V_3 are orthogonal to one another. Thus
621 the triple $\{V_1, V_2, V_3\}$ gives rise to an XDU(3) matrix of level χ^{q+1} . In fact,
622 because of permutation of matrix lines, it actually gives rise to six different
623 XDU(3) matrices of level χ^{q+1} .

624 We now consider different triples $\{V_1, V_2, V_3\}, \{V'_1, V'_2, V'_3\}, \{V''_1, V''_2, V''_3\},$
625 \dots , where V_1, V'_1, V''_1, \dots all are vectors of level χ^q . Then V_1 is orthogonal
626 to V_2 and V_3 , but not to $V'_2, V'_3, V''_2, V''_3, V'''_2, \dots$ [17]. Thus only the triples
627 $\{V_1, V_2, V_3\}, \{V'_1, V'_2, V'_3\}, \dots$ can give rise to an XDU(3) matrix of level χ^{q+1} .
628 As each such triple gives rise to six XDU(3) matrices, for any $q \geq 0$, there
629 are 6 times as many XDU(3) matrices of level χ^{q+1} as there are vectors of
630 level χ^q . Because with each vector V_1 of level χ^q correspond two vectors (V_2
631 and V_3) of level χ^{q+1} , the number of vectors with a same level χ^q increases
632 like 2^q . Therefore, the number of matrices similarly increases as 2^q and thus
633 equals $c \times 2^q$, with c some appropriate constant. The coefficient c is identified
634 by remarking that there are eighteen XDU(3) matrices of level χ^1 (Table 2).
635 One thus finds $c = 9$. We conclude: for any $q \geq 1$, there exist 9×2^q XDU(3)
636 matrices of level χ^q .

637 C.2 NUMBER OF DU(3) MATRICES

638 A similar reasoning as in Subappendix C.1 exists for the DU(3) matrices [17].
639 Again we assume vectors V_1, V'_1, V''_1, \dots of level χ^q . With each vector V_1

Table 3: The five R_2 remainder matrices G_j .

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

640 of level χ^q now correspond four vectors ($V_2, V_3, V_4,$ and V_5) of level χ^{q+1} ,
641 such that the number of vectors with a same level χ^q grows like 4^q . With
642 each quintuple $\{V_1, V_2, V_3, V_4, V_5\}$ correspond two triples, i.e. $\{V_1, V_2, V_3\}$ and
643 $\{V_1, V_4, V_5\}$ and therefore twice six matrices of $\text{DU}(3)$. The number of ma-
644 trices grows like the number of vectors, i.e. equals $c \times 4^q$. We identify the
645 coefficient c by remarking that there are 2,304 $\text{DU}(3)$ matrices of level χ^1
646 (Table 1). One thus finds $c = 576$. We conclude: for any $q \geq 1$, there exist
647 576×4^q $\text{DU}(3)$ matrices of level χ^q .

648

Appendix D

Applying Gaussian primes to Sect. 5 leads to the conclusion that the group $\text{DU}(2)$ 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

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

649 but can have five and only five different remainder matrices $R_2(g)$ (up to
650 equivalence by row or column swapping). We call these 2×2 matrices
651 $G_1, G_2, \dots,$ and G_5 , respectively, see Table 3.

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

$$654 \quad a = \frac{1}{\chi} \begin{pmatrix} -i & 1 \\ 1 & -i \end{pmatrix} \quad \text{and} \quad b = \begin{pmatrix} -i & 0 \\ 0 & 1 \end{pmatrix}.$$

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

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

655 this yields Table 3. We see that in two cases multiplication by $R_2(a)$ leads to
656 the 2×2 zero matrix and that in the remaining three cases multiplication by
657 $R_2(ba)$ leads to the zero matrix. A zero $R_2(g)R_2(a)$ matrix reveals that the
658 product ga is not of level χ^2 but instead of level 1, whereas a zero $R_2(g)R_2(ba)$
659 matrix reveals that the product gba is of level 1. We thus may conclude that
660 each of the sixty-four DU(2) matrices g of level χ can be lowered to level 1
661 either through multiplication by a or through multiplication by ba .

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

664 Acknowledgment

665 Alexis De Vos thanks Fred Brackx (Vakgroep wiskundige analyse, Univer-
666 siteit Gent) for valuable discussions concerning the hypergeometric series.

667 Bibliography

- 668 [1] K. Conrad, “SL₂(Z)”, <http://www.math.uconn.edu/~kconrad/blurbs/>.
- 669 [2] A. De Vos, J. De Beule, and L. Storme, *Computing with the square root of NOT*, *Serdica*
670 *Journal of Computing* **3**, 359 (2009).
- 671 [3] W. Wang and C. Xu, *An excluding algorithm for testing whether a family of graphs*
672 *are determined by their generalized spectra*, *Lin. Alg. Appl.* **418**, 62 (2006).
- 673 [4] A. De Vos, *Reversible computing*, Wiley–VCH, Weinheim, 2010.
- 674 [5] U. Haagerup, *Orthogonal maximal abelian *-subalgebras of the $n \times n$ matrices and cyclic*
675 *n -roots*, in: *Operator algebras and quantum field theory*, S. Doplicher, R. Longo, J.
676 Roberts, and L. Zsidó, eds., International Press, Cambridge, 1996, pp. 296–322.
- 677 [6] C. Jacobi, *Fundamenta nova theoriae functionum ellipticarum*, Borntäger, Re-
678 giomonti, 1829, pp. 103–108.
- 679 [7] E. Grosswald, *Representations of integers as sums of squares*, Springer, New York,
680 1985, pp. 121–123.
- 681 [8] B. Berndt, *Fragments by Ramanujan on Lambert series*, in: *Number theory and its ap-*
682 *plications*, S. Kanemutsi and K. Györy, eds., Kluwer Academic Publishers, Dordrecht,
683 1999, pp. 35–49.
- 684 [9] K. Williams, *Number theory in the spirit of Liouville*, Cambridge University Press,
685 Cambridge, 2011, pp. 77–99 and 251–261.

- 686 [10] R. Wille and R. Drechsler, *Towards a design flow for reversible logic*, Springer, Dor-
687 drecht, 2010.
- 688 [11] D. Deutsch, *Quantum computation*, Physics World **5**, 57 (1992).
- 689 [12] D. Deutsch, A. Ekert, and R. Lupacchini, *Machines, logic and quantum physics*, Bul-
690 letin of Symbolic Logic **3**, 265 (2000).
- 691 [13] A. Galindo and M. Martín-Delgado, *Information and computation: classical and quan-*
692 *tum aspects*, Rev. Mod. Phys. **74**, 347 (2002).
- 693 [14] M. Nielsen and I. Chuang, *Quantum computation and quantum information*, Cam-
694 bridge University Press, Cambridge, 2000, pp. 65, 454, and 611.
- 695 [15] M. Planat, *Clifford quantum computer and the Mathieu groups*, Invertis Journal of
696 Science and Technology **3**, 1 (2010).
- 697 [16] R. Van Laer, *Dyadic quantum computers*, MSc. Thesis Universiteit Gent, Gent, 2011.
- 698 [17] S. Vandenbrande, *Reversibele digitale schakelingen*, MSc. Thesis Universiteit Gent,
699 Gent, 2011.
- 700 [18] W. Tadej and K. Życzkowski, *A concise guide to complex Hadamard matrices*, Open
701 Sys. Information Dyn. **13**, 133 (2006).
- 702 [19] N. Sloane, *The on-line encyclopedia of integer sequences*, sequence A047974,
703 <http://oeis.org/A047974>.
- 704 [20] A. Khruzin, *Enumeration of chord diagrams*, arXiv:math/0008209.
- 705 [21] R. Proctor, *Let's expand Rota's twelvefold way for counting partitions!*,
706 arXiv:math/0606404.
- 707 [22] N. Sloane, *The on-line encyclopedia of integer sequences*, sequence A000898,
708 <http://oeis.org/A000898>.
- 709 [23] *Laguerre polynomials*, Wikipedia, the free encyclopedia,
710 http://en.wikipedia.org/wiki/Laguerre_polynomial.
- 711 [24] S. Severini and F. Szöllösi, *A further look into combinatorial orthogonality*, Electronic
712 Journal of Linear Algebra **17**, 376 (2008).
- 713 [25] N. Sloane, *The on-line encyclopedia of integer sequences*, sequence A000085,
714 <http://oeis.org/A000085>.
- 715 [26] J. Jahnel, *When is the (co)sine of a rational angle equal to a rational number?*,
716 <http://www.uni-math.gwdg.de/jahnel/Preprints/cos.pdf> (2006).