Serdica J. Computing **3** (2009), 359–370

Serdica
Journal of Computing

Bulgarian Academy of Sciences
Institute of Mathematics and Informatics

COMPUTING WITH THE SQUARE ROOT OF NOT

Alexis De Vos, Jan De Beule, Leo Storme

Abstract. To the two classical reversible 1-bit logic gates, i.e. the identity gate (a.k.a. the follower) and the NOT gate (a.k.a. the inverter), we add an extra gate, the square root of NOT. Similarly, we add to the 24 classical reversible 2-bit circuits, both the square root of NOT and the controlled square root of NOT. This leads to a new kind of calculus, situated between classical reversible computing and quantum computing.

1. Introduction. Reversible logic circuits, acting on m bits, form a group, isomorphic to the symmetric group $\mathbf{S}_n$ of degree n and order $n!$, where n is a short-hand notation for 2^m. Quantum circuits, acting on m qubits, form a group, isomorphic to the unitary group $\mathrm{U}(n)$. Whereas $\mathbf{S}_n$ is finite, $\mathrm{U}(n)$ is an infinite group, i.e. a Lie group (with an uncountably infinite order, i.e. ∞^{n^2}) with dimension n^2.

Although $\mathbf{S}_n$ is a subgroup of $\mathrm{U}(n)$, the step from $\mathbf{S}_n$ to $\mathrm{U}(n)$ is huge. Therefore, the question arises whether groups X exist that are simultaneously a subgroup of $\mathrm{U}(n)$ and a supergroup of $\mathbf{S}_n$:

$$\mathbf{S}_n \subset \mathrm{X} \subset \mathrm{U}(n). \tag{1}$$

ACM Computing Classification System (1998): B6.1, F1.1, G2.1.
Key words: Reversible computing, square root of NOT, discrete group.

Such group may exist in three different kinds:

- either a finite group with order $> n!$,
- or a discrete group with a countable infinity as order,
- or a Lie group (i.e. a group with an uncountable infinity as order) with dimension $< n^2$.

Each of these possibilities deserves our attention. The larger the group X, the more difficult it is to implement it into hardware, but the more powerful is the resulting computer. Assuming that for a lot of interesting problems the quantum computer, based on the whole group $\mathrm{U}(n)$, is an 'overkill', we have to look for a satisfactory compromise between simplicity (found close to $\mathbf{S}_n$) and computational power (found close to $\mathrm{U}(n)$). Such a computer we may refer to as 'reversible plus' or 'quantum light'.

We may tackle this problem in two ways: either bottom-up or top-down. For bottom-up we start from the symmetric group and add some extra group generators. For top-down we start from the unitary group and impose some restrictions. In the present paper, we apply the former approach. We limit ourselves to the cases $m = 1$ (thus $n = 2$) and $m = 2$ (thus $n = 4$).

2. One-(qu)bit calculations. A qubit can be in a state $a_0\Psi_0 + a_1\Psi_1$, where Ψ_0 and Ψ_1 are its two eigenstates. The complex coefficients a_0 and a_1 are the two amplitudes. In quantum computing they can have any value, as long as $a_0\overline{a_0} + a_1\overline{a_1} = 1$.

The classical reversible gates on one bit are represented by the two 2×2 permutation matrices $\varphi = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ (i.e. the follower) and $\nu = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ (i.e. the inverter or `NOT` gate), which form a group isomorphic to the symmetric group $\mathbf{S}_2$. We may enlarge the group by adding generators. In the literature [1, 2], the 2×2 Pauli matrices $\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}$ have been proposed, leading to the Pauli group (of order 16). In the present paper, on the contrary, we investigate what happens if we introduce the generator

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

which satisfies $\sigma^2 = \nu$. Thus, σ is the notorious square root of NOT [3, 4, 5, 6]. It generates a group of order four with elements

$$\varphi = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma = \begin{pmatrix} \omega & \overline{\omega} \\ \overline{\omega} & \omega \end{pmatrix}, \quad \nu = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \text{and} \quad \overline{\sigma} = \begin{pmatrix} \overline{\omega} & \omega \\ \omega & \overline{\omega} \end{pmatrix},$$

where the number ω is given by

$$\omega = \frac{1}{2} + i\,\frac{1}{2}$$

and $\overline{\omega}$ is its complex conjugate:

$$\overline{\omega} = \frac{1}{2} - i\,\frac{1}{2}\,.$$

The matrix $\overline{\sigma}$ obeys $\overline{\sigma}^2 = \nu$ and thus is the 'other' square root of NOT. Together, the four matrices form a group with respect to the operation of ordinary matrix multiplication, isomorphic to the cyclic group of order 4, i.e. to $\mathbf{Z}_4$. Indeed, we have $\sigma^2 = \nu$, $\sigma^3 = \overline{\sigma}$, and $\sigma^4 = \varphi$. Each of the four matrices has all line sums (i.e. row sums and column sums) equal to 1.

Any of the four matrices transforms the input state $a_0\Psi_0 + a_1\Psi_1$ into an output state $p_0\Psi_0 + p_1\Psi_1$:

$$\begin{pmatrix} p_0 \\ p_1 \end{pmatrix} = \begin{pmatrix} U_{11} & U_{12} \\ U_{21} & U_{22} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \end{pmatrix}.$$

Because the matrix U is unitary, we automatically have $p_0\overline{p_0} + p_1\overline{p_1} = 1$. If the input is in an eigenstate (either $(a_0, a_1) = (1, 0)$ or $(a_0, a_1) = (0, 1)$), then the output is in a superposition. E.g.

$$\begin{pmatrix} p_0 \\ p_1 \end{pmatrix} = \begin{pmatrix} \omega & \overline{\omega} \\ \overline{\omega} & \omega \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \omega \\ \overline{\omega} \end{pmatrix}.$$

But, as the output of one circuit may be the input of a subsequent circuit, we have to consider the possibility of (a_0, a_1) being in such a superposition of eigenstates. In fact, we have to consider all possible values of (a_0, a_1) and (p_0, p_1), which may be transformed into one another. These values turn out to be either a column or a row of one of the four matrices. Thus, in total, four states have to be considered: $(1, 0)$, $(0, 1)$, $(\omega, \overline{\omega})$, and $(\overline{\omega}, \omega)$. Such an object, which may be in four different states, we can call a squabit, in order to distinguish it from a qubit, which can be in as many as ∞^3 different states, and from a bit, which can be in only two different states.

We see that, besides $a_0\overline{a_0} + a_1\overline{a_1} = 1$, the amplitudes a_0 and a_1 fulfil one more restriction, namely $a_0 + a_1 = 1$. Because each of the four transformation matrices has constant line sum equal to 1, the property $a_0 + a_1 = 1$ automatically induces $p_0 + p_1 = 1$. Table 1 displays how each of the matrices acts on the column matrix $(a_0, a_1)^T$. The tables constitute the truth tables of the four reversible transformations. Each of these tables expresses a permutation of the four objects $(1, 0)$, $(0, 1)$, $(\omega, \overline{\omega})$, and $(\overline{\omega}, \omega)$. Together they therefore form a permutation group which is a subgroup of the symmetric group $\mathbf{S}_4$.

Table 1. The members of the group with $m = 1$: (a) follower, (b) square root of `NOT`, (c) `NOT`, and (d) square root of `NOT`

a_0a_1	p_0p_1
1 0	1 0
0 1	0 1
ω $\overline{\omega}$	ω $\overline{\omega}$
$\overline{\omega}$ ω	$\overline{\omega}$ ω

(a)

a_0a_1	p_0p_1
1 0	ω $\overline{\omega}$
0 1	$\overline{\omega}$ ω
ω $\overline{\omega}$	0 1
$\overline{\omega}$ ω	1 0

(b)

a_0a_1	p_0p_1
1 0	0 1
0 1	1 0
ω $\overline{\omega}$	$\overline{\omega}$ ω
$\overline{\omega}$ ω	ω $\overline{\omega}$

(c)

a_0a_1	p_0p_1
1 0	$\overline{\omega}$ ω
0 1	ω $\overline{\omega}$
ω $\overline{\omega}$	1 0
$\overline{\omega}$ ω	0 1

(d)

3. Two-(qu)bit calculations

Two qubits exist in a superposition $a_{00}\Psi_{00} + a_{01}\Psi_{01} + a_{10}\Psi_{10} + a_{11}\Psi_{11}$ with $\sum a_{kl}\overline{a_{kl}} = 1$. Here, additionally we have $\sum a_{kl} = 1$. The subset of 2-qubit circuits we investigate has to comprise the circuit calculating the square root of `NOT` of qubit # 2. This circuit is represented by the matrix

$$\sigma_2 = \begin{pmatrix} \omega & \overline{\omega} & 0 & 0 \\ \overline{\omega} & \omega & 0 & 0 \\ 0 & 0 & \omega & \overline{\omega} \\ 0 & 0 & \overline{\omega} & \omega \end{pmatrix}. \tag{2}$$

This matrix is the generator of a group isomorphic to $\mathbf{Z}_4$. The wanted set of 2-qubit circuits should also contain all classical reversible 2-bit circuits. Those are generated by two generators

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

generating a group isomorphic to $\mathbf{S}_4$.

Straightforward calculations (with the help of the computer algebra package GAP [7]) reveal that the group generated by the three generators $\{\sigma_2, a, b\}$ has order 192. It constitutes the closure of the group (isomorphic to $\mathbf{Z}_4$) generated by the first generator and the group (isomorphic to $\mathbf{S}_4$) generated by the two other generators. We call this closure $\boldsymbol{\Upsilon}$. All 192 different 4×4 unitary matrices of $\boldsymbol{\Upsilon}$ have entries from the set $\left\{0, 1, \overline{\omega}, \omega, -\frac{1}{2}, \frac{1}{2}, -\frac{i}{2}, \frac{i}{2}\right\}$ and all have line sums equal to 1. We have

- 24 matrices with entries from $\{0, 1\}$,
- 72 matrices with entries from $\{0, \overline{\omega}, \omega\}$,
- 72 matrices with entries from $\left\{\frac{1}{2}, -\frac{i}{2}, \frac{i}{2}\right\}$, and
- 24 matrices with entries from $\left\{-\frac{1}{2}, \frac{1}{2}\right\}$.

The four classes of matrices are the four double cosets in which the group $\boldsymbol{\Upsilon}$ is partitioned by its $\mathbf{S}_4$-subgroup. Representatives of these double cosets are e.g.

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

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

Figure 1 shows the four representative circuits.

We may note that the number 192 is really an 'ordinary order' for a finite group. Indeed, according to Conway et al. [8], there are 6013 different groups with order smaller than 200. Among them, not fewer than 1543 (i.e. about 26%) have an order precisely equal to 192. With the GAP command `IdGroup()`, we find that the group $\boldsymbol{\Upsilon}$ has the GAP library number `[192, 944]`. The group is isomorphic to $(\mathbf{Z}_4 \times \mathbf{Z}_4 \times \mathbf{Z}_2) : \mathbf{S}_3$, where $\times$ denotes the direct product and :

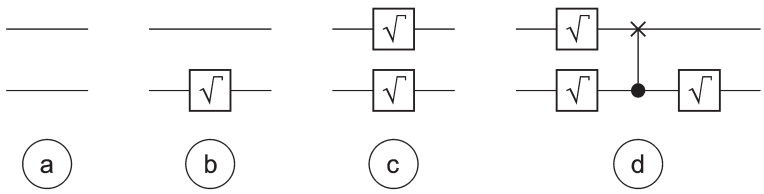

Fig. 1. Four representative circuits: (a) follower, (b) square root of NOT, (c) double square root of NOT, and (d) a more complicated circuit

denotes the semidirect product of two groups. Its subgroup isomorphic to $\mathbf{Z}_4\times \mathbf{Z}_4\times \mathbf{Z}_2$ is generated by the three generators

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

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

Noteworthy is the fact that a matrix like

$$c = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \omega & \overline{\omega} \\ 0 & 0 & \overline{\omega} & \omega \end{pmatrix}, \tag{3}$$

which may be interpreted as a 'controlled square root of NOT' (or as a 'square root of controlled NOT'), is not a member of the group $\boldsymbol{\Upsilon}$. In contrast, the 'controlled NOT', i.e.

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

is a member of $\boldsymbol{\Upsilon}$. Also automatically a member is the circuit calculating the square root of NOT of qubit # 1:

$$\sigma_1 = \begin{pmatrix} \omega & 0 & \overline{\omega} & 0 \\ 0 & \omega & 0 & \overline{\omega} \\ \overline{\omega} & 0 & \omega & 0 \\ 0 & \overline{\omega} & 0 & \omega \end{pmatrix}.$$

The group $\boldsymbol{\Upsilon}$ may be regarded as a permutation group, provided we introduce the necessary number of quantum superpositions. These states, again, correspond to rows/columns of the matrices. E.g. Table 2 shows an example of a truth table. Both this permutation table and the matrix (2) constitute a representation of the same circuit in Figure 1b.

We see that, in order to guarantee that the set of input words $(a_{00}, a_{01}, a_{10}, a_{11})$ equals the set of output words $(p_{00}, p_{01}, p_{10}, p_{11})$, we need to consider not fewer than 32 different words. Therefore, the group of circuits generated by the three generators will be a subgroup of $\mathbf{S}_{32}$. This group $\boldsymbol{\Upsilon}$ of 2-qubit circuits can thus be represented by a subset of the 32! different 32×32 permutation matrices. We may summarize that the 192 matrices of the group $\boldsymbol{\Upsilon}$ simultaneously form a supergroup of the symmetric group $\mathbf{S}_4$ and a subgroup of the symmetric group $\mathbf{S}_{32}$:

$$\mathbf{S}_4 \subset \boldsymbol{\Upsilon} \subset \mathbf{S}_{32}.$$

With the `GAP` command `SmallerDegreePermutationRepresentation(Image (RegularActionHomomorphism()))` we find that the matrix group is isomorphic to a particular group of even permutations of twelve objects:

$$\mathbf{S}_4 \subset \boldsymbol{\Upsilon} \subset \mathbf{A}_{12},$$

where $\mathbf{A}_n$ denotes the alternating group of degree n (with order $n!/2$).

If we add the matrix (3) as a fourth generator, the group $\boldsymbol{\Upsilon}$ is enlarged to a new group $\boldsymbol{\Omega}$ (i.e. the closure of $\boldsymbol{\Upsilon}$ and c), which, according to `GAP`, has infinite order. However, this result seems to be only a warning [9] that the order of one of its elements 'must be larger than 1000'. We thus will explicitly prove that the new group has order equal to the countable infinity $\aleph_0$. For this purpose, below we will

- first demonstrate that the order is smaller than or equal to $\aleph_0$ and
- then demonstrate that the order is greater than or equal to $\aleph_0$.

First, we note that each element of $\boldsymbol{\Omega}$ is a matrix with 16 entries, all of the form $a + bi$, with both a and b rational numbers. The non-singular matrices with such entries form a group. The latter group has order equal to $\aleph_0^{32} - \aleph_0^{30}$, i.e. order $\aleph_0$. Our group $\boldsymbol{\Omega}$ is a subgroup of it and therefore has an order smaller than or equal to $\aleph_0$.

Next, we note that the group generated by the four generators $\{\sigma_2, a, b, c\}$ equals the group generated by the three generators $\{a, b, c\}$. Indeed, gate σ_2 can be realized by combining two gates c with two `NOT` gates. See Figure 2. Then we

Table 2. The truth table of member σ_2 of the group $\mathbf{\Upsilon}$

a_{00}	a_{01}	a_{10}	a_{11}	p_{00}	p_{01}	p_{10}	p_{11}
0	0	0	1	0	0	$\overline{\omega}$	ω
0	0	1	0	0	0	ω	$\overline{\omega}$
0	1	0	0	$\overline{\omega}$	ω	0	0
1	0	0	0	ω	$\overline{\omega}$	0	0
0	0	$\overline{\omega}$	ω	0	0	1	0
0	0	ω	$\overline{\omega}$	0	0	0	1
0	$\overline{\omega}$	0	ω	$\frac{-i}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{i}{2}$
0	$\overline{\omega}$	ω	0	$\frac{-i}{2}$	$\frac{1}{2}$	$\frac{i}{2}$	$\frac{1}{2}$
0	ω	0	$\overline{\omega}$	$\frac{1}{2}$	$\frac{i}{2}$	$\frac{-i}{2}$	$\frac{1}{2}$
0	ω	$\overline{\omega}$	0	$\frac{1}{2}$	$\frac{i}{2}$	$\frac{1}{2}$	$\frac{-i}{2}$
$\overline{\omega}$	0	0	ω	$\frac{1}{2}$	$\frac{-i}{2}$	$\frac{1}{2}$	$\frac{i}{2}$
$\overline{\omega}$	0	ω	0	$\frac{1}{2}$	$\frac{-i}{2}$	$\frac{i}{2}$	$\frac{1}{2}$
$\overline{\omega}$	ω	0	0	1	0	0	0
ω	0	0	$\overline{\omega}$	$\frac{i}{2}$	$\frac{1}{2}$	$\frac{-i}{2}$	$\frac{1}{2}$
ω	0	$\overline{\omega}$	0	$\frac{i}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{-i}{2}$
ω	$\overline{\omega}$	0	0	0	1	0	0
$\frac{1}{2}$	$\frac{1}{2}$	$\frac{-i}{2}$	$\frac{i}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{-1}{2}$
$\frac{1}{2}$	$\frac{1}{2}$	$\frac{i}{2}$	$\frac{-i}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{-1}{2}$	$\frac{1}{2}$
$\frac{1}{2}$	$\frac{-i}{2}$	$\frac{1}{2}$	$\frac{i}{2}$	0	$\overline{\omega}$	ω	0
$\frac{1}{2}$	$\frac{i}{2}$	$\frac{1}{2}$	$\frac{-i}{2}$	ω	0	0	$\overline{\omega}$
$\frac{1}{2}$	$\frac{-i}{2}$	$\frac{i}{2}$	$\frac{1}{2}$	0	$\overline{\omega}$	0	ω
$\frac{1}{2}$	$\frac{i}{2}$	$\frac{-i}{2}$	$\frac{1}{2}$	ω	0	$\overline{\omega}$	0
$\frac{-i}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{i}{2}$	$\overline{\omega}$	0	ω	0
$\frac{i}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{-i}{2}$	0	ω	0	$\overline{\omega}$
$\frac{-i}{2}$	$\frac{1}{2}$	$\frac{i}{2}$	$\frac{1}{2}$	$\overline{\omega}$	0	0	ω
$\frac{i}{2}$	$\frac{1}{2}$	$\frac{-i}{2}$	$\frac{1}{2}$	0	ω	$\overline{\omega}$	0
$\frac{-i}{2}$	$\frac{i}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{-1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$
$\frac{i}{2}$	$\frac{-i}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{-1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$
$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{-1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{i}{2}$	$\frac{-i}{2}$
$\frac{1}{2}$	$\frac{1}{2}$	$\frac{-1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{-i}{2}$	$\frac{i}{2}$
$\frac{1}{2}$	$\frac{-1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{i}{2}$	$\frac{-i}{2}$	$\frac{1}{2}$	$\frac{1}{2}$
$\frac{-1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{-i}{2}$	$\frac{i}{2}$	$\frac{1}{2}$	$\frac{1}{2}$

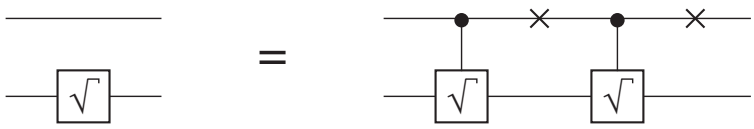

Fig. 2. An uncontrolled gate as a sequence of two controlled gates

note that, in order to prove that the order of a matrix group is infinite, it suffices to demonstrate that one of its elements has infinite order. We chose the element

$$y = abc = \begin{pmatrix} 0 & 0 & \omega & \overline{\omega} \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \overline{\omega} & \omega \\ 1 & 0 & 0 & 0 \end{pmatrix}. \tag{4}$$

The proof that matrix y has infinite order is given in the Appendices: Appendix A treats the case of an arbitrary unitary matrix x, whereas Appendix B treats the particular case of the matrix y defined by equation (4). Thus the group $\{1, y, y^2, y^3, \dots\}$ has an order equal to $\aleph_0$. Our group $\mathbf{\Omega}$ is a supergroup of it and therefore has an order greater than or equal to $\aleph_0$.

4. Conclusions. There exist 2 reversible logic circuits acting on 1 bit (forming a group isomorphic to $\mathbf{S}_2$); there exist 24 reversible logic circuits acting on 2 bits (forming a group isomorphic to $\mathbf{S}_4$). Adding to the former set the logic gate called the 'square root of NOT' leads to a group of four circuits (isomorphic to $\mathbf{Z}_4$). Adding the same square root of NOT to the latter set leads to a group $\mathbf{\Upsilon}$ of 192 circuits. Additionally adding the 'controlled square root of NOT' leads to a group $\mathbf{\Omega}$ with a (countable) infinity of circuits. This suggests that there might be limited room for groups X satisfying (1), in contrast to what one would expect from the huge difference between Order($\mathbf{S}_n$) and Order(U(n)).

REFERENCES

[1] Gottesman D. The Heisenberg representation of quantum computers. arXiv:quant-ph/9807006v1 (1998).

[2] Aaronson S. Improved simulation of stabilizer circuits. *Physical Review A*, **70** (2004), 052328.

[3] Deutsch D. Quantum computation. *Physics World*, **5** (1992), 57–61.

[4] Deutsch D., A. Ekert, R. Lupacchini. Machines, logic and quantum physics. *The Bulletin of Symbolic Logic*, **3** (2000), 265–283.

[5] Galindo A., M. Martín-Delgado. Information and computation: classical and quantum aspects. *Review of Modern Physics*, **74** (2002), 347–423.

[6] Miller D. Decision diagram techniques for reversible and quantum circuits. In: Proc. 8th Int. Workshop on Boolean Problems, Freiberg, (September 2008), 1–15.

[7] Schönert M. GAP. *Computer Algebra Nederland Nieuwsbrief*, **9** (1992), 19–28.

[8] Conway J., H. Dietrich, E. O'Brien. Counting groups: gnus, moas, and other exotica. *The Mathematical Intelligencer*, **30** (2008), 6–15.

[9] Schönert M. et al. GAP manual 3.4, Section 34.11.
`http://www-groups.dcs.st-and.ac.uk/~gap/Gap3/Manual3/C034S011.htm`

[10] Jahnel J. When is the (co)sine of a rational angle equal to a rational number?
`http://www.uni-math.gwdg.de/jahnel/linkstopapers.html`, 2004.

[11] Calcut J. Rationality and the tangent function.
`http://www.ma.utexas.edu/users/jack/tanpap.pdf`, 2008.

Alexis De Vos
Imec v.z.w. and Vakgroep elektronika en informatiesystemen
Universiteit Gent
Sint Pietersnieuwstraat 41
B-9000 Gent, Belgium
e-mail: `alex@elis.ugent.be`

Jan De Beule, Leo Storme
Vakgroep zuivere wiskunde en computeralgebra
Universiteit Gent
Krijgslaan 281 (S22)
B-9000 Gent, Belgium
e-mail: `jdebeule@cage.ugent.be`
e-mail: `ls@cage.ugent.be`

Received July 3, 2009
Final Accepted September 26, 2009

A. Order of an arbitrary unitary matrix x. We consider an $n \times n$ unitary matrix x. The matrix x has infinite order if the sequence $\{x^0, x^1, x^2, \dots\}$ is not periodic, i.e. if all x^j with $j > 0$ are different from $x^0 = 1$. The matrix recursion equation $x^j = x^{j-1}x$ yields n^2 scalar recursion equations. These fall apart into n sets of n equations. Within a set the row number k is fixed and the column number q takes all values from 1 to n :

$$(x^j)_{kq} = \sum_p (x^{j-1})_{kp}\, x_{pq}.$$

Let X be the Z-transform of the matrix sequence x^0, x^1, x^2, ... Then:

$$X_{kq} = \sum_p \frac{X_{kp}}{z}\, x_{pq}$$

or

$$\sum_p x_{pq} X_{kp} - z X_{kq} = 0,$$

a set of n homogeneous equations, which has a non-zero solution iff

$$\det(x - z) = 0\ .$$

The solutions z of this equation are the eigenvalues of the given matrix x. Thus the n poles z_k of the Z-transform of the matrix sequence $\{x^j\}$ are the n eigenvalues of x itself. Thus, if all eigenvalues z_k of x are different, then

$$x^j = \sum_{k=0}^{n-1} x_k z_k^j, \tag{5}$$

with n appropriate matrices x_k, each to be determined as a linear superposition of the n initial conditions $x^0 = 1$, x^1, ..., and x^{n-1}. This result is strongly related to the Cayley–Hamilton theorem. Because of (5), x^j can only be periodic if all the eigenvalues z_k are located on the unit circle with rational phase angles. Here, we call an angle rational iff it is a rational multiple of π.

Because x is unitary, automatically all its eigenvalues are on the unit circle, so that we only have to check the n phase angles. If x has an eigenvalue z_k with multiplicity s, then, beside a term proportional to z_k^j, also terms proportional to jz_k^j, to $j^2 z_k^j$, ..., $j^{s-1} z_k^j$ appear and x^j is not periodic, even if z_k has a rational phase angle (unless the starting values x, x^2, ..., x^{n-1} of the sequence $\{x^j\}$ are such that all the coefficients of jz_k^j, $j^2 z_k^j$, ..., $j^{s-1} z_k^j$ turn out to be equal to the zero matrix).

B. Order of the unitary matrix y. The power sequence $\{y^j\}$ of the 4×4 matrix (4) is of the form

$$y^j = c_0 z_0^j + d_0 j z_0^j + c_1 z_1^j + c_2 z_2^j,$$

with z_0, z_1, and z_2 the three solutions of the eigenvalue equation

$$(z-1)^2(z^2 + \omega z + i) = 0$$

and with appropriate matrices c_0, d_0, c_1, and c_2, determined* by the initial conditions $y^0 = 1$, y^1, y^2, and y^3. We have $z_0 = 1$ (with multiplicity 2), $z_1 = -\frac{\sqrt{7}+1}{4} + i\,\frac{\sqrt{7}-1}{4}$, and $z_2 = \frac{\sqrt{7}-1}{4} - i\,\frac{\sqrt{7}+1}{4}$. As expected, all three numbers z_0, z_1, and z_2 lie on the unit circle of the complex plane. Their phase angles are $\theta_0 = 0$, $\theta_1 = \pi/2 - \theta$, and $\theta_2 = \pi + \theta$, where $\theta = \text{Arccos}\left(\frac{\sqrt{7}-1}{4}\right) = \text{Arctan}(\sqrt{7}) - \pi/4 \approx 24°17'43''$.

Neither z_1^j nor z_2^j is periodic, because the angle θ is not a so-called rational angle, i.e. an angle which is a rational multiple of π. Indeed, according to Jahnel [10], the only rational angles (between 0° and 90°) with a cosine equal to a quadratic irrational are 30°, 36°, 45°, and 72° (with cosines equal to respectively $\sqrt{3}/2$, $\sqrt{5}/4+1/4$, $\sqrt{2}/2$, and $\sqrt{5}/4-1/4$). Similarly, according to Calcut [11], the only rational angles (between 0° and 90°) with a tangent equal to a quadratic irrational are 15°, 22°30′, 30°, 60°, 67°30′, and 75° (with tangent equal to respectively $2-\sqrt{3}$, $\sqrt{2}-1$, $\sqrt{3}/3$, $\sqrt{3}$, $\sqrt{2}+1$, and $2+\sqrt{3}$).

*Straightforward but lengthy calculations (involving the solution of 16 sets each of four equations in four unknowns) leads to $c_0 = \frac{1}{3}\,G$, $d_0 = 0$, $c_1 = \frac{1}{6}\,H + \frac{\sqrt{7}}{21}\,J + i\,\frac{\sqrt{7}}{14}\,K$, and $c_2 = \frac{1}{6}\,H - \frac{\sqrt{7}}{21}\,J - i\,\frac{\sqrt{7}}{14}\,K$, where

$$G = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 3 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}, \quad H = \begin{pmatrix} 2 & 0 & -1 & -1 \\ 0 & 0 & 0 & 0 \\ -1 & 0 & 2 & -1 \\ -1 & 0 & -1 & 2 \end{pmatrix},$$

$$J = \begin{pmatrix} -1 & 0 & -1 & 2 \\ 0 & 0 & 0 & 0 \\ -1 & 0 & 2 & -1 \\ 2 & 0 & -1 & -1 \end{pmatrix}, \text{ and } K = \begin{pmatrix} 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 1 \\ 1 & 0 & -1 & 0 \end{pmatrix}.$$