Creating subgroups of $U(2^w)$ for quantum-minus computers

To cite this article: Alexis De Vos and Michiel Boes 2011 J. Phys.: Conf. Ser. 284 012021

View the article online for updates and enhancements.
Creating subgroups of $U(2^w)$
for quantum-minus computers

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

Abstract. Classical reversible computers on $w$ bits are isomorphic to the (finite) symmetric group $S_{2^w}$; quantum computers on $w$ qubits are isomorphic to the (Lie) unitary group $U(2^w)$. We investigate and classify groups $X$ which represent computers intermediate between classical reversible computers and quantum computers. Such intermediate groups $X$ may exist in three flavours:

- finite groups of order larger than $(2^w)!$,
- infinite but discrete groups, and
- Lie groups of dimension smaller than $(2^w)^2$.

The larger the group, the more powerful the computer may be, but the smaller the group, the easier it can be to build the computer hardware. In the present paper, we investigate the first two flavours only.

For our purpose, we start from 1-qubit transformations, represented by $2 \times 2$ unitary matrices. We call this group the creator. Its members are called gates and act on one qubit. Controlled gates are quantum circuits acting on $w$ qubits, such that the 1-qubit transformation (applied to a particular qubit) depends on the state of the $w-1$ other qubits. The controlled gates generate the group $X$ of $2^w \times 2^w$ matrices, called the creation.

We discuss all creators of order up to 8. Additionally a creator of order 16 and one of order 192 are discussed.

1. Introduction
Reversible logic circuits, acting on $w$ bits, form a group, isomorphic to the symmetric group $S_m$ of degree $m$ and order $m!$, where $m$ is equal to $2^w$. For $w = 1$, the group $S_2$ consists of two $2 \times 2$ matrices:

\[ e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad n = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \]

where $e$ is called the IDENTITY gate and $n$ is called the NOT gate. The group may be generated by a single generator, i.e. by $n$. We note that $n^2 = e$.

We now enlarge this matrix group, either by replacing the generator $n$ by another generator or by adding extra generator(s). In the former case, we make sure that the NOT gate $n$ is member of the group. The resulting new group of $2 \times 2$ unitary matrices, we denote by $X_2$. We have

\[ S_2 \subset X_2 \subset U(2). \]
As the two matrices $e$ and $n$ form a subgroup of $X_2$, Lagrange’s theorem tells us that the order of $X_2$ is even. We denote this number by $p$.

Logic circuits of $w$ qubits are described by $2^w \times 2^w$ unitary matrices, which form a group isomorphic to the Lie group $U(2^w)$. Within this group we define a particular set, represented by $2^w \times 2^w$ matrices with all matrix entries equal to 0, except for $2^{w-1}$ submatrices of size $2 \times 2$, each member of $U(2)$. We impose that those submatrices are either equal to $e$ or equal to some given unitary matrix $v$, element of $X_2$:

$$v = \begin{pmatrix} v_{11} & v_{12} \\ v_{21} & v_{22} \end{pmatrix},$$

Such logic gates are called controlled Vs. One qubit $k$ is called the controlled qubit; the others are called the controlling qubits. The matrices with equal $k$ form a group isomorphic to the direct product $X_2 \times X_2 \times \ldots \times X_2 = X_{2^w}$, of order $2^{2w}$. The figure shows an arbitrary example of a group element: a controlled $V$ with $w = 3$ and $k = 2$. The 1-qubit transformation $v$ is applied to qubit $A_2$, if a given Boolean function $f(A_1, A_3)$ equals 1. We call this function $f$ the control function of the gate. If e.g. $f$ is the OR function $A_1 \lor A_3$, then the circuit is represented by the transformation matrix

$$A_1 \quad A_2 \quad A_3 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & v_{11} & 0 & v_{12} & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & v_{21} & 0 & v_{22} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & v_{11} & 0 & v_{12} & 0 \\ 0 & 0 & 0 & 0 & 0 & v_{11} & 0 & v_{12} \\ 0 & 0 & 0 & 0 & v_{21} & 0 & v_{22} & 0 \\ 0 & 0 & 0 & 0 & 0 & v_{21} & 0 & v_{22} \end{pmatrix},$$

with the four submatrices bold-faced (one equal to $e$, the three others to $v$).

The four generators of the group with arbitrary $f(A_1, A_3)$ are

$$V, \quad \overline{V}, \quad \overline{V}, \quad \overline{V}, \quad \text{and} \quad V.$$

These gates have control functions $f$ equal to $\overline{A_1} \overline{A_3}$, $A_1 A_3$, $A_1 \overline{A_3}$, and $A_1 A_3$, respectively. Here $\overline{A}$ is a short-hand notation for $\overline{NOT \ A}$. In order to decompose an arbitrary control gate into generators, it suffices to decompose its control function $f$ into minterms.

Each of the $w$ choices of the number $k$ gives rise to $g2^{w-1}$ generators, where $g$ is the number of $2 \times 2$ matrices necessary to generate $X_2$. The complete set of $gw2^{w-1}$ generators generates the group $X$. If $X_2$ is $S_2$, then $X$ is nothing else but $S_{2w}$. If $X_2$ is not $S_2$, then $X$ is not necessarily $S_{2w}$. We call the group $X$ the creation of $X_2$; we call the group $X_2$ the creator of $X$. Above, we have seen that $S_2$ is the creator of $S_{2w}$. Below, we investigate which groups are created by groups $X_2$. Because of (1), we automatically have

$$S_{2w} \subset X \subset U(2^w).$$

2. Results for small creators

Here follows a full classification of creations $X$, created by small creators $X_2$, i.e. creators of order $p$ smaller than 10.
Table 1. The orders of small creator groups \((w = 1)\) and the orders of the corresponding creation groups (where \(m\) stands for \(2^w\) with \(w > 1\)).

| \(p = \text{order of creator}\) | 2    | 4    | 4    | 6    | 6    | 6    | 8    | 8    | 8    | 8    |
|----------------------------------|------|------|------|------|------|------|------|------|------|------|
| isomorphism of creator           | \(\mathbb{Z}_2\) | \(\mathbb{Z}_2 \times \mathbb{Z}_2\) | \(\mathbb{Z}_4\) | \(S_3\) | \(\mathbb{Z}_6\) | \(S_3\) | \(D_4\) | \(D_4\) | \(\mathbb{Z}_2 \times \mathbb{Z}_4\) | \(\mathbb{Z}_8\) |
| order of creation                | \(m!\) | \(\frac{m!2^m}{2}\) | \(N_0\) | \(\frac{m!3^m}{3}\) | \(m!3^m\) | \(N_0\) | \(m!2^m\) | \(\frac{m!4^m}{4}\) | \(\frac{m!4^m}{2}\) | \(N_0\) |

2.1. Creator of order 2
The case \(p = 2\) is trivial. The creator \(X_2\) is generated by a single generator, i.e. \(n\), and consists of two \(2 \times 2\) matrices: \(e\) and \(n\). The creations \(X\) are the groups of \(2^w \times 2^w\) permutation matrices and thus are isomorphic to the symmetric groups \(S_{2^w}\), of order \((2^w)!\). This constitutes the case of reversible classical computers.

2.2. Creators of order 4
There exist three groups of \(2 \times 2\) unitary matrices, containing the \textsc{not} matrix \(n\) and being of order 4.

The first creator of order 4 is generated by two generators: \(-e\) and \(n\). It consists of the matrices \(e\), \(-e\), \(n\), and \(-n\) and is isomorphic to \(\mathbb{Z}_2 \times \mathbb{Z}_2\). Its creations consist of \(2^w \times 2^w\) matrices with all entries from \(\{0, 1, -1\}\), such that the number of \(-1\)s is even. The order of the creation is \((2^w)!2^{2^w-1}\).

The second one is generated by a single generator, i.e.

\[
s = \frac{1}{2} \begin{pmatrix} 1 + i & 1 - i \\ 1 - i & 1 + i \end{pmatrix}.
\]

We call this matrix the ‘square root of \textsc{not}’ \cite{1} \cite{2} \cite{3}. It generates a group isomorphic to the cyclic group \(\mathbb{Z}_4\). The members of the group are \(s\), \(s^2 = n\), \(s^3 = \overline{n}\), and \(s^4 = e\). This creator gives rise to creations of a countably infinite order \cite{4}.

The third order-4 group is generated by \(-s\) and consists of the four matrices \(-s\), \(n\), \(-\overline{n}\), and \(e\). This creator behaves similar to the previous one.

2.3. Creators of order 6
There exist four abelian groups of \(2 \times 2\) unitary matrices, containing the \textsc{not} matrix \(n\) and being of order 6. All are isomorphic to the cyclic group \(\mathbb{Z}_6\). They are generated by a single generator, respectively

\[
\begin{array}{c}
\frac{1}{4} \begin{pmatrix} 3 + \lambda & 1 - \lambda \\ 1 - \lambda & 3 + \lambda \end{pmatrix}, \\
\frac{1}{4} \begin{pmatrix} -3 + \lambda & 1 + \lambda \\ 1 + \lambda & -3 + \lambda \end{pmatrix}, \\
\frac{1}{2} \begin{pmatrix} \lambda & -1 \\ -1 & \lambda \end{pmatrix}, \\
\frac{1}{2} \begin{pmatrix} 0 & -1 + \lambda \\ -1 + \lambda & 0 \end{pmatrix},
\end{array}
\]

where \(\lambda\) is a short-hand notation for \(i\sqrt{3}\). The fourth creator creates groups of order \((2^w)!3^{2^w}\) (the formula however not holding in the trivial case \(w = 1\)), consisting of \(2^w \times 2^w\) matrices with all entries from \(\{0, 1, (-1 + \lambda)/2, (-1 - \lambda)/2\}\). The three other creators create infinite creations.

Besides this finite number of abelian creators, there exist a (non-countable) infinity of non-abelian creators of order 6. They are isomorphic to the symmetric group \(S_3\). They are generated
by two generators: $n$ and
\[
\begin{pmatrix}
\cos(\theta) & \sin(\theta) \exp(i\alpha) \\
\sin(\theta) \exp(-i\alpha) & -\cos(\theta)
\end{pmatrix},
\]
where $\alpha$ is an arbitrary angle (different from $\pm \pi/2$), but $\theta$ obeys
\[
\sin(\theta) = -\frac{1}{2\cos(\alpha)}.
\]
These order-6 creators yield infinite creations, except if $\alpha = \pm \pi/3$, in which case the creations have merely order $(2^w)!3^{2^w-1}$.

2.4. Creators of order 8

There exist eight different creator groups isomorphic to $\mathbb{Z}_8$, each one generated by a matrix of the form
\[
\frac{1}{4} \begin{pmatrix}
\lambda_1 + \lambda_2 & \lambda_1 - \lambda_2 \\
\lambda_1 - \lambda_2 & \lambda_1 + \lambda_2
\end{pmatrix},
\]
where $\lambda_1 = 2i^k$ with an integer $k$ and $\lambda_2$ is $\sqrt{7} \pm i\sqrt{2}$. All eight creators yield infinite creations.

There exist three different creators isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_4$: one is generated by the two matrices $-i$ and $s$, one by the generators $n$ and $is$, and one by the two generators $ie$ and $n$. The last creator yields groups of order $(2^w)!4^{2^w-1/2}$ (consisting of matrices with entries from \{0, 1, -1, i, -i\}, with the restriction that the number of entries equal to ±i is even), the other two yielding creations of infinite order.

Finally, there exist $\infty$ matrix groups isomorphic to the dihedral group $D_4$, generated by the two generators $n$ and
\[
\begin{pmatrix}
\cos(\theta) & -i\sin(\theta) \\
 i \sin(\theta) & -\cos(\theta)
\end{pmatrix}.
\]
All create infinite creations, except in the cases $\theta = 0$ (in which case the order is $(2^w)!2^{2^w}$) and $\theta = \pi/2$ (in which case the order is $(2^w)!4^{2^w-1}$).

3. Results for a few larger creators

Below, some creators of order $p$ higher than 9 are discussed, because they are well-known in quantum computer theory.

3.1. A creator with $p = 16$

The notorious Pauli group $[5] [6]$ consists of the sixteen matrices $\pm e, \pm n, \pm \sigma_2, \pm \sigma_3, \pm ie, \pm in, \pm i\sigma_2, \pm i\sigma_3$, where $\sigma_2$ and $\sigma_3$ stand for the Pauli matrices$^1$
\[
\begin{pmatrix}
0 & -i \\
i & 0
\end{pmatrix}
\quad \text{and} \quad
\begin{pmatrix}
1 & 0 \\
0 & -1
\end{pmatrix},
\]
respectively. The group is generated by the three generators $n$, $\sigma_2$, and $\sigma_3$. It creates finite creations (of order $(2^w)!4^{2^w-1/2}$), consisting of the same $2^w \times 2^w$ matrices with entries from \{0, 1, -1, i, -i\}, created by the order-8 creator generated by $ie$ and $n$ (see Section 2.4).

We note that the creations are much larger than the $w$-qubit Pauli group (of order $4 \times 4^w$), consisting of the tensor products of the one-qubit Pauli matrices.

$^1$ Sometimes $n$, i.e. the $\text{NOT}$ matrix, is also called a Pauli matrix and then denoted $\sigma_1$. 

3.2. A creator with \( p = 192 \)

The notorious Clifford group [6] [7] [8] consists of the 192 matrices generated by the two generators

\[
\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix},
\]

known as the HADAMARD gate and the PHASE gate, respectively. The group creates infinite creations. Again, the creations are much larger than the \( w \)-qubit Clifford groups (of order \( 2^{w^2 + 2w + 3} \prod_{j=1}^{w} 4^j - 1 \)), consisting of the tensor products of the one-qubit Clifford matrices.

4. Conclusion

In the above examples, the finite creators lead to creations, which can be subdivided into two different classes:

- either finite creations
- or (countably) infinite creations.

We shortly discuss both categories.

4.1. Finite creations

Whenever all generators (and thus automatically all elements) of the creator are unitary \( 2 \times 2 \) matrices with two zero entries, then the creations are groups of \( 2^w \times 2^w \) matrices with all entries equal zero, except one entry in each row and one entry in each column, with a modulus equal to 1 (and a phase angle equal to some rational multiple of \( \pi \)). Such matrices are monomial and thus strongly resemble permutation matrices. Creation group orders turn out to be of the form \( (2^w)! c^{2^w} / d \), with both \( c \) and \( d \) appropriate integer constants.

Such matrices lead to computational power hardly exceeding the power of classical computers. Indeed, any such matrix transforms a classical input pattern into a classical output pattern, up to a phase factor, as illustrated by a \( w = 2 \) example:

\[
\begin{pmatrix}
0 & \exp(i\varphi_1) & 0 & 0 \\
0 & 0 & \exp(i\varphi_2) & 0 \\
\exp(i\varphi_3) & 0 & 0 & 0 \\
0 & 0 & \exp(i\varphi_4) & 0
\end{pmatrix}
\begin{pmatrix}
0 \\
0 \\
1 \\
0
\end{pmatrix}
= \exp(i\varphi_4)
\begin{pmatrix}
0 \\
0 \\
0 \\
1
\end{pmatrix}.
\]

In passing, we mention that also infinite groups of such matrices (displaying \( \varphi \) angles which are not rational multiples of \( \pi \)) have such low computational power.

4.2. Infinite creations

In all above examples, as soon as one generator of the creator is a \( 2 \times 2 \) unitary matrix \( u \) with all four entries different from zero, the creations are of infinite order. We conjecture that this result is generally valid. There exists a proof [9] for the case where \( u \) is of the form

\[
\begin{pmatrix}
\cos(\theta) & \sin(\theta) \exp(i\alpha) \\
\sin(\theta) \exp(-i\alpha) & -\cos(\theta)
\end{pmatrix},
\]

with both non-zero \( \cos(\theta) \) and non-zero \( \sin(\theta) \). There also exists a proof [4] if \( u \) is the matrix \( s \), i.e. the \( \sqrt{\text{NOT}} \) gate. This very same proof remains valid for all \( u \) of the form

\[
\frac{1}{2}
\begin{pmatrix}
(1 + i) \exp(i\eta) & 1 - i \\
1 - i & (1 + i) \exp(-i\eta)
\end{pmatrix}.
\]
The infinite (but discrete) creations are computationally more powerful than classical reversible computers. Their extra power is e.g. illustrated by the fact that the 3-bit Toffoli gate is not decomposable into simpler parts within the framework of classical computing, but is decomposable into 2-qubit gates if the creator is the order-4 group with the square root of NOT [10] [11] [12]. Nevertheless, they do not have the full computational power of quantum computing. Therefore, any creation of order $\aleph_0$, we call quantum-minus computers.

References
[1] Deutsch D 1992 Physics World 5 57–61
[2] Deutsch D, Ekert A and Lupacchini A 2000 The Bulletin of Symbolic Logic 3 265–83
[3] Galindo A and Martín-Delgado M 2002 Review of Modern Physics 74 347–423
[4] De Vos A, De Beule J and Storme L 2009 Serdica Journal of Computing 3 359–70
[5] Nielsen M and Chuang I 2000 “Quantum computation and quantum information”, Cambridge University Press, pp 65, 454, and 611
[6] Planat M 2010 Invertis Journal of Science and Technology 3 1–4
[7] Planat M and Solé P 2009 Journal of Physics A: Mathematical and Theoretical 42 042003
[8] Sloane N http://public.research.att.com/~njas/sequences/?id%3A003956
[9] Boes M, De Vos A and De Beule J 2010 Proc. 9 th Int. Workshop on Boolean Problems, Freiberg (September 2010), pp 51–6
[10] Barenco A, Bennett C, Cleve R, DiVincenzo D, Margolus N, Shor S, Sleator T, Smolin J and Weinfurter H 1995 Physical Review C 52 3457–67
[11] Wille R, Saeedi M and Drechsler R 2009 Proc. 18 th Int. Workshop on Logic and Synthesis, Berkeley (July 2009) pp 43–9
[12] Miller M and Sasanian Z 2010 Proc. 9 th Int. Workshop on Boolean Problems, Freiberg (September 2010), pp 37–41