Almost-Classical Quantum Computers

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

Abstract

By means of a subgroup of the $2 \times 2$ unitary matrices, i.e. a subgroup $Q$ of $U(2)$, acting on a single qubit, we create a group $X$, acting on $w$ qubits. If $Q$ equals the group of order 2 consisting of the follower and the inverter, we recover $S_{2^w}$, i.e. the permutation matrices describing a classical reversible computer acting on $w$ bits. If $Q$ is another group of two $2 \times 2$ matrices, then a new kind of computing appears.

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:

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

where $y$ 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 $n^2 = y$.

We now replace $n$ by another unitary matrix $q$, such that $q^2 = y$ still holds. It generates a new group of order 2:

$$y = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad q = \begin{pmatrix} q_{11} & q_{12} \\ q_{21} & q_{22} \end{pmatrix}.$$

Quantum circuits of $w$ qubits are described by $2^w \times 2^w$ unitary matrices [1], 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 $y$ or equal to $q$. Such logic gates are called controlled $Q$s or control gates. 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 $S_2 \times S_2 \times \ldots \times S_2 = S_2^{2^w-1}$, of order $2^{2w-1}$. The figure below shows an arbitrary example of a group element: a control $Q$ with $w = 3$ and $k = 2$. The $1$-qubit transformation $q$ 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

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & q_{11} & 0 & q_{12} & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & q_{21} & 0 & q_{22} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & q_{11} & q_{12} & 0 \\ 0 & 0 & 0 & 0 & q_{21} & 0 & q_{22} \\ 0 & 0 & 0 & 0 & 0 & q_{21} & 0 \end{pmatrix}.$$
with the submatrices bold-faced (one equal to \( y \), the three others to \( q \)). If \( f \) is the \textsc{and} function \( A_1A_3 \) and \( q \) is the \( 2 \times 2 \) \textsc{not} matrix \( n \), then the control gate corresponds to the classical \textsc{toffoli} gate.

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

\[
\begin{align*}
&Q, & & Q, & & Q, & & 2,
\end{align*}
\]

These gates have control functions \( f \) equal to \( A_1A_3 \), \( A_1A_3 \), \( A_1A_3 \), and \( A_1A_3 \), respectively. In order to decompose an arbitrary control gate into generators, it thus suffices to decompose its control function into minterms.

Each of the \( w \) choices of the number \( k \) gives rise to \( 2^{w-1} \) generators. The complete set of \( w2^{w-1} \) generators generates the group \( X \). If \( Q \) is \( S_2 \), then \( X \) is nothing else but \( S_{2^w} \). Thanks to the Birkhoff theorem, we know that an arbitrary element of \( S_{2^w} \) can be synthesized by cascading no more than \( 2w - 1 \) control gates [2] [3]. E.g. for \( w = 3 \), five control gates suffice:

\[
\begin{align*}
&Q, & & Q, & & Q, & & Q, & & Q,
\end{align*}
\]

If \( Q \) is not \( S_2 \), then \( X \) is not necessarily \( S_{2^w} \). We call the group \( X \) the creation of \( Q \); we call the group \( Q \) the creator of \( X \). Above, we have seen that \( S_2 \) is the creator of \( S_{2^w} \). Below, we investigate which groups are created by order-2 groups \( Q \) other than \( S_2 \).

## 2 Theory

We only investigate groups \( Q \) of order 2. They thus consist of only two \( 2 \times 2 \) unitary matrices: the matrix \( q \) and the \textsc{identity} matrix \( y \), with \( q^2 = y \). Matrices \( q \) satisfying \( q^2 = y \) are sometimes called involutary matrices. They are self-inverse. Matrices, which are both unitary and involutary, are necessarily also Hermitian. The reader may easily verify that such unitary–involuntary–Hermitian \( 2 \times 2 \) matrices exist only in two flavours:

- the set of two matrices \( y \) and \( -y \), both with determinant equal to 1,
- the \( 2 \)-dimensional space of matrices

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

all with determinant equal to \(-1\).

The former flavour we call the ‘special case’, as the matrices are members of \( SU(2) \); the latter flavour we call the ‘non-special case’, as the matrices are not members of \( SU(2) \).

We note that the particular case \( \alpha = 0 \) and \( \theta = \pi/2 \) gives rise to classical logic: \( q = n \). For \( \alpha = 0 \) but \( \theta \neq \pi/2 \), other interesting matrices [4] appear: \( -n \) for \( \theta = -\pi/2 \), the Hadamard transformation \( H = (1/\sqrt{2}) \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \) for \( \theta = \pi/4 \), and its negation \( -H \), for \( \theta = 5\pi/4 \). The Pauli matrix \( \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \) pops up for \( \alpha = -\pi/2 \) and \( \theta = \pi/2 \) (or \( \alpha = \pi/2 \) and \( \theta = -\pi/2 \)), and its negation \( -\sigma_2 \) for \( \alpha = \theta = \pi/2 \) (or \( \alpha = \theta = -\pi/2 \)). The Pauli matrix \( \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \) appears for \( \theta = 0 \), its negation \( -\sigma_3 \) for \( \theta = \pi \).
Because $Q$ is unitary–involutary–Hermitian, the controlled $Q$ gates are also unitary–involutary–Hermitian. Nevertheless, the group $X$ generated by these controlled $Q$s (i.e. created by $Q$) are not necessarily involutary and not necessarily Hermitian.

2.1 The Special Case

Although the matrix $y$ is unitary, involutary, and Hermitian, we will not consider this trivial case, as, in fact, $y$ is not of order 2, but of order 1. We thus proceed with the case $q = -y$ : the creator $Q$ consisting of

$$y = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad -y = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$$ 

One may easily verify that the group $Q$ creates a group $X$, consisting of $2^w \times 2^w$ diagonal matrices, with all diagonal elements equal to $\pm 1$, such that the number of $-1$s is even. These matrices form a group isomorphic to $S_{2^w}^{2^w-1}$ of order $2^{2^w-1}$. This group is smaller than $S_{2^w}$ of order $(2^w)!$. The group created by the group $\{y, -y\}$ has only one element in common with the permutation group created by the group $\{y, n\}$ and that is the $2^w \times 2^w$ identity matrix. As the creation of $\{y, -y\}$ is smaller than the creation of $\{y, n\}$, it is no surprise that an arbitrary element of the creation of $\{y, -y\}$ can be synthesized with a shorter cascade than an arbitrary element of $S_{2^w}$. Indeed, a cascade of no more than $w$ controlled $Q$s is sufficient.

2.2 The Non-Special Case

We now proceed to the latter flavour. We investigate two particular elements of the created group with $w = 2$, both consisting of a cascade of only two control gates:

$$Q \quad \text{and} \quad Q,$$

i.e.

$$g = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & c & se \\ 0 & 0 & s/e & -c \end{pmatrix} \quad \begin{pmatrix} c & 0 & se & 0 \\ 0 & c & 0 & se \\ s/e & 0 & -c & 0 \\ 0 & s/e & 0 & -c \end{pmatrix} = \begin{pmatrix} c & 0 & se & 0 \\ 0 & c & 0 & se \\ cs/e & s^2 & -c^2 & -cs/e \\ s^2/c^2 & cs/e & -cs/e & c^2 \end{pmatrix},$$

and $h = \begin{pmatrix} c & se & 0 & 0 \\ 0 & c & 0 & se \\ 0 & c se & 0 & 0 \\ 0 & s/e & 0 & -c \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & s/e & 0 & -c \end{pmatrix} = \begin{pmatrix} c & cse & 0 & s^2e^2 \\ s/e & -c^2 & 0 & -cs/e \\ s/e & -cs/e & 0 & -cse \\ 0 & 0 & 1 & 0 \end{pmatrix},$

where $c$ is a short-hand notation for $\cos(\theta)$, $s$ for $\sin(\theta)$, and $e$ for $\exp(i\alpha)$. The eigenvalues $\lambda$ of $g$ and $\mu$ of $h$ obey the equations

$$(\lambda - 1)(\lambda + 1)(\lambda^2 - 2c\lambda + 1) = 0 \quad \text{and} \quad (\mu - 1)^2 \left[ \mu^2 + (1 + c^2)\mu + 1 \right] = 0,$$

respectively. Their values are

$\lambda_1 = 1, \ \lambda_2 = -1, \ \lambda_3 = \exp(i\theta), \ \lambda_4 = \exp(-i\theta) \quad \text{and} \quad \mu_1 = 1, \ \mu_2 = 1, \ \mu_3 = \exp(i\varphi), \ \mu_4 = \exp(-i\varphi),$
where $\varphi$ is the angle satisfying
\[
2 \cos\left(\frac{\varphi}{2}\right) + \cos\left(\frac{\pi}{2} - \theta\right) = 0.
\]

We distinguish different possibilities:

- Either $\theta$ is not a rational multiple of $\pi$. Then the numbers $\lambda_3$ and $\lambda_4$ have infinite order. Thus the matrix $g$ has infinite order.
- Or $\theta$ is a rational multiple of $\pi$.
  - Either $\varphi$ is not a rational multiple of $\pi$. Then the numbers $\mu_3$ and $\mu_4$ have infinite order. Thus the matrix $h$ has infinite order.
  - Or also $\varphi$ is a rational multiple of $\pi$. Then, a theorem by Crosby [5] on the solutions of the equation $\cos(\theta_1) + \cos(\theta_2) + \cos(\theta_3) = 0$, teaches that $\theta$ is necessarily one of the following angles: $0$, $\pi/2$, $\pi$, or $3\pi/2$.

Thus, the order of the created group $X$ is always infinity, except for the cases where $\theta$ is an integer multiple of $\pi/2$.

2.2.1 Subcase $\theta = 0$

If $\theta = 0$, then $c = 1$ and $s = 0$, such that the creator is the group consisting of
\[
y = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.
\]

All generators are $2^w \times 2^w$ diagonal matrices with diagonal elements equal to 1, except for one diagonal element that is equal to $-1$. They generate the group of $2^{2^w-1}$ diagonal matrices with all diagonal elements equal to $\pm 1$, except the first one which is equal to 1. An arbitrary element of the group can be decomposed into a cascade of $2w$ control gates or less.

2.2.2 Subcase $\theta = \pi$

This case is equivalent with the previous case, $\sigma_3$ being replaced by $-\sigma_3$.

2.2.3 Subcase $\theta = \pi/2$

If $\theta = \pi/2$, then $c = 0$ and $s = 1$, such that the creator is the group consisting of
\[
y = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad u = \begin{pmatrix} 0 & e \\ e^{-1} & 0 \end{pmatrix},
\]

where again $e$ denotes $\exp(i\alpha)$. It creates the group of unitary $2^w \times 2^w$ matrices $M$ where all entries $M_{ik}$ are either equal to 0 or equal to $e^{\psi(k-1) - \psi(j-1)}$, where $\psi(b)$ denotes the number of 1s in the binary notation of $b$.

Such matrices $M$ strongly resemble permutation matrices, however with particular powers of $e$ in place of 1s. They form a group of order $(2^w)!$. In fact, they are conjugate to the group of $m \times m$ permutation matrices $P$:
\[
M = C^{-1}PC,
\]

where $C$ is a constant $m \times m$ diagonal matrix with diagonal entries $e^{\psi(0)}, e^{\psi(1)}, e^{\psi(2)}, \ldots, e^{\psi(m-2)}$, and $e^{\psi(m-1)}$. E.g.
\[
\begin{pmatrix}
e^0 & 0 & 0 & 0 \\
0 & e^{-1} & 0 & 0 \\
0 & 0 & e^{-1} & 0 \\
0 & 0 & 0 & e^{-2}
\end{pmatrix}
\begin{pmatrix}
1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 \\
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0
\end{pmatrix}
\begin{pmatrix}
e^0 & 0 & 0 & 0 \\
0 & e^1 & 0 & 0 \\
0 & 0 & e^1 & 0 \\
0 & 0 & 0 & e^2
\end{pmatrix}
= \begin{pmatrix}
e^0 & 0 & 0 & 0 \\
0 & e^0 & 0 & e^1 \\
0 & e^0 & 0 & e^2 \\
0 & 0 & e^{-1} & 0
\end{pmatrix}.
\]

It is thus no surprise that (just like any permutation matrix) an arbitrary element $M$ of the group can be decomposed into a cascade of $2w - 1$ control gates or less.
Table 1: The number of different reversible-minus circuits, reversible circuits, and reversible-plus circuits, as a function of the circuit width $w$

<table>
<thead>
<tr>
<th>$w$</th>
<th>reversible$^{-}$</th>
<th>reversible</th>
<th>reversible$^{+}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>8</td>
<td>24</td>
<td>$\infty$</td>
</tr>
<tr>
<td>3</td>
<td>128</td>
<td>40,320</td>
<td>$\infty$</td>
</tr>
<tr>
<td>4</td>
<td>32,768</td>
<td>20,922,789,888,000</td>
<td>$\infty$</td>
</tr>
</tbody>
</table>

2.2.4 Subcase $\theta = 3\pi/2$

This case is equivalent with the previous case, $u$ being replaced by $-u$.

2.2.5 Subcase $\theta$ not an integer multiple of $\pi/2$

If $\theta$ is not an integer multiple of $\pi/2$, then the creator $Q$ consists of

$$y = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad v = \begin{pmatrix} \cos(\theta) & \sin(\theta) \exp(i\alpha) \\ \sin(\theta) \exp(-i\alpha) & -\cos(\theta) \end{pmatrix}.$$ 

We stress that $\theta$ and $\alpha$ are two arbitrary, but fixed real numbers. In this subcase, the theorem of Crosby proves that the creator creates a group of infinite order. Infinite groups have either a countable or an uncountable order [6]. The Appendix demonstrates that, in the present case, the infinity is countable.

Because there are an infinite number of different group elements, an arbitrary element of the group cannot be decomposed into a cascade of a finite number of building blocks, each from the finite generator set of $w2^{w-1}$ different controlled $Q$s. Indeed, the chains of length $p$ can yield no more than $(w2^{w-1})^p$ different circuits.

3 Conclusion

Replacing the $2 \times 2$ NOT matrix by another unitary and involutary $2 \times 2$ matrix creates computing schemes on $w$ qubits, consisting of

- either a group isomorphic to $S_{2w}$ and thus of order $(2^w)!$
- or a group isomorphic to $S_{2w-1}^2$ and thus of order $2^{2w-1}$
- or a group of infinite order.

We call these computational worlds ‘reversible’, ‘reversible minus’, and ‘reversible plus’, respectively. See Table 1. Both ‘reversible$^{-}$’ and ‘reversible$^{+}$’ circuits are quantum circuits, but nevertheless they resemble a lot classical reversible circuits. The ‘reversible minus’ circuits are computationally less strong than the full set of classical reversible circuits, as they are isomorphic to a (Sylow) subgroup of the symmetric group. The ‘reversible plus’ circuits are computationally stronger than the classical reversible circuits. Whether they can approximate an arbitrary quantum computer depends on how the discrete matrices are distributed within the continuous $(2^{2w}$-dimensional) Lie space $U(2^w)$.

References


Appendix

We make a product of \( p \) matrices, with the help of a finite number of generators, each an \( m \times m \) matrix with entries from \{0, 1, se, \( \frac{s}{e} \), c, \( -c \)\}. The result is an \( m \times m \) matrix with all \( m^2 \) entries a polynomial in \( se, \frac{s}{e}, \) and \( c \), of degree \( p \), with exclusively integer coefficients. Because the generators are constructed with \( 2 \times 2 \) submatrices, either \(
\begin{pmatrix}
1 & 0 \\
0 & 1
\end{pmatrix}
\) or \(
\begin{pmatrix}
c & se \\
\frac{s}{e} & -c
\end{pmatrix}
\), in particular places on the diagonal, the polynomial may be written

\[ P(s, c) e^t, \]

where \( t \) is an integer, only dependent on the row number and the column number of the matrix entry. Because of \( c^2 + s^2 = 1 \), in the polynomial we can replace each occurrence of \( c^2 \) by \( 1 - s^2 \), such that each matrix entry may be written as

\[ Q(s) e^t + R(s) ce^t, \]

where both \( Q \) and \( R \) are polynomials with integer coefficients, \( Q(s) \) being of degree \( p \) or lower, \( R(s) \) of degree \( p - 1 \) or lower. It has been demonstrated by Cantor [7] that the number of polynomials with integer coefficients is countable. Therefore, each matrix element can have only a countable infinity of values. Thus the number of different \( m \times m \) matrices is countable.

In the case the creator is the order-2 group generated by the \textsc{hadamard} gate \( (s = c = 1/\sqrt{2} \) and \( e = 1) \), the \( m^2 \) entries of the \( m \times m \) matrix belong to \( Q(\sqrt{2}) \).