The synthesis of a quantum circuit

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

Stijn De Baerdemacker*
Center for Molecular Modeling, Vakgroep fysica en sterrenkunde
Universiteit Gent
Technologiepark 903, B - 9052 Gent, Belgium
e-mail: Stijn.DeBaerdemacker@UGent.be

Abstract
As two basic building blocks for any quantum circuit, we consider the 1-qubit NEGATOR ($\theta$) circuit and the 1-qubit PHASOR ($\theta$) circuit, extensions of the NOT gate and PHASE gate, respectively: $\text{NEGATOR}(\pi) = \text{NOT}$ and $\text{PHASOR}(\pi) = \text{PHASE}$. Quantum circuits (acting on $w$ qubits) consisting of controlled NEGATORs are represented by matrices from $\text{XU}(2^w)$; quantum circuits (acting on $w$ qubits) consisting of controlled PHASORs are represented by matrices from $\text{ZU}(2^w)$. Here, $\text{XU}(n)$ and $\text{ZU}(n)$ are subgroups of the unitary group $\text{U}(n)$: the group $\text{XU}(n)$ consists of all $n \times n$ unitary matrices with all line sums equal to 1 and the group $\text{ZU}(n)$ consists of all $n \times n$ unitary diagonal matrices with first entry equal to 1. We conjecture that any $\text{U}(n)$ matrix can be decomposed into four parts: $U = e^{i\alpha}Z_1XZ_2$, where both $Z_1$ and $Z_2$ are $\text{ZU}(n)$ matrices and $X$ is an $\text{XU}(n)$ matrix. For $n = 2^w$, this leads to a decomposition of a quantum computer into simpler blocks.

1 Introduction

A classical reversible logic circuit, acting on $w$ bits, is represented by a permutation matrix, i.e. a member of the finite matrix group $\text{P}(2^w)$. A quantum circuit, acting on $w$ qubits, is represented by a unitary matrix, i.e. a member of the infinite matrix group $\text{U}(2^w)$. The classical reversible circuits form a subgroup of the quantum circuits. This is a consequence of the group hierarchy $\text{P}(n) \subset \text{U}(n)$, where $n$ is allowed to have any (positive) integer value.

Below, we will construct an arbitrary quantum circuit according to a bottom-up approach. For this purpose, we start from the simplest logic operation possible on a single (qu)bit (i.e. $w = 1$ and thus $n = 2^w = 2$), being the IDENTITY operation $u = \left(\begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array}\right)$. Next, we consider two different square roots of that $2 \times 2$ matrix:

$m = (1 - t)u + tq$

The former is a permutation matrix and thus represents a classical logic gate, i.e. the NOT gate; the latter is not a permutation matrix, but is a unitary matrix and therefore represents a quantum logic gate, called the PHASE gate.

Next, we interpolate between the IDENTITY $u$ and an as of yet arbitrary unitary matrix $q$:

$m = (1 - t)u + tq$

where $t$ is a parameter interpolating between $u$ (for $t = 0$) and $q$ (for $t = 1$). We impose that $m$ is a unitary matrix. If $q^2 = u$, then this leads to the condition that $t$ is complex and of the form

$t = \frac{1}{2} \left(1 - e^{i\theta}\right)$.

* SDB is an ‘FWO-Vlaanderen’ post-doctoral fellow.
where \( \theta \) is a real parameter [1]. Note that \( t = 0 \) for \( \theta = 0 \) and \( t = 1 \) for \( \theta = \pi \). For \( \theta = 2\pi \), the value of \( t \) has returned to 0. Now, by choosing \( q = \text{NOT} \) and \( q = \text{PHASE} \), respectively, this leads to two different 1-parameter single-qubit operations:

\[
\begin{pmatrix}
\cos(\theta/2)e^{-i\theta/2} & i\sin(\theta/2)e^{-i\theta/2} \\
i\sin(\theta/2)e^{-i\theta/2} & \cos(\theta/2)e^{-i\theta/2}
\end{pmatrix}
\text{ and }
\begin{pmatrix}
1 & 0 \\
0 & e^{i\theta}
\end{pmatrix}.
\]

We denote them with the schematics

\[
N(\theta) \quad \text{and} \quad \Phi(\theta)
\]

respectively. The former operation, we call the \textsc{negator} gate [2]; the latter, we call the \textsc{phasor} gate. Each of these two sets of matrices constitutes a continuous group, i.e. a 1-dimensional Lie group. Both groups contain the \textsc{identity} circuit. Indeed: \textsc{negator}(0) = \textsc{phasor}(0) = \textsc{identity}. Additionally, by construction, the \textsc{not} gate is a \textsc{negator} and the \textsc{phase} gate is a \textsc{phasor}. Indeed:

\[
\text{negator}(\pi) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad \text{phasor}(\pi) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},
\]

sometimes abbreviated to \( X \) and \( Z \) gate, respectively [4]. For \( \theta = \pi/2 \), we have the square root of \textsc{not} and the square root of \textsc{phase}:

\[
\text{negator}(\pi/2) = \frac{1}{2} \begin{pmatrix} 1 + i & 1 - i \\ 1 - i & 1 + i \end{pmatrix} \quad \text{and} \quad \text{phasor}(\pi/2) = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}.
\]

The former is sometimes referred to as the \( V \) gate [3] [5], the latter is sometimes called the \( S \) gate [6]. Finally, for \( \theta = \pi/4 \), we have the quartic roots

\[
\text{negator}(\pi/4) = \frac{1}{2\sqrt{2}} \begin{pmatrix} \sqrt{2} + 1 + i & \sqrt{2} - 1 - i \\ \sqrt{2} - 1 - i & \sqrt{2} + 1 + i \end{pmatrix} \quad \text{and} \quad \text{phasor}(\pi/4) = \frac{1}{\sqrt{2}} \begin{pmatrix} \sqrt{2} & 0 \\ 0 & 1 + i \end{pmatrix},
\]

sometimes called the \( W \) gate [5] and the \( T \) gate [6] [7], respectively.

Now, we consider multiple-qubit (say, \( w \)-qubit) circuits. For this purpose, we introduce both the controlled \textsc{negator} gates and the controlled \textsc{phasor} gates. As an example, we give here the \( w = 3 \) schematic of the positive-polarity twice-controlled \textsc{negator} (the lowermost quantum wire being the target line), represented by the block-diagonal matrix

\[
\begin{pmatrix}
1_{6 \times 6} & \cos(\theta/2)e^{-i\theta/2} & i\sin(\theta/2)e^{-i\theta/2} \\
i\sin(\theta/2)e^{-i\theta/2} & \cos(\theta/2)e^{-i\theta/2} & 0 \\
0 & 0 & 1
\end{pmatrix} = \begin{pmatrix}
N(\theta)
\end{pmatrix},
\]

where \( 1_{a \times a} \) denotes the \( a \times a \) unit matrix. Of course, we equally introduce controlled \textsc{phasors}, negative-polarity controls, a target on a higher-positioned wire, etc...

It turns out [9] that all possible \textsc{negator}s and controlled \textsc{negator}s together generate a group \( \text{XU}(2^w) \), subgroup of the unitary group \( U(2^w) \). They cannot generate the full \( U(2^w) \) group, because the matrix representing a (controlled) \textsc{negator} has all line sums (i.e. all row sums and all column sums) equal to 1. The multiplication of two matrices with all line sums equal to 1 yields again a unit-line-sum matrix. Therefore a quantum circuit composed exclusively of (controlled) \textsc{negator}s cannot synthesize a unitary matrix with one or more line sums different from unity. Whereas the unitary group \( U(n) \) has \( n^2 \) dimensions, the group \( \text{XU}(n) \) has only \( (n - 1)^2 \) dimensions and is isomorphic to \( U(n - 1) \) [8] [9] [10]. Analogously, a quantum circuit composed exclusively of (controlled) \textsc{phasor}s can only generate matrices from \( \text{ZU}(2^w) \), where \( \text{ZU}(n) \) is the group of diagonal unitary matrices with unit entry at the upper-left corner. The group \( \text{ZU}(n) \) has only \( (n - 1) \) dimensions [10].

We can summarize as follows: we find two subgroups of the unitary group \( U(n) \):

- \( \text{XU}(n) \), i.e. all \( n \times n \) unitary matrices with all of their \( 2n \) line sums equal to 1;
- \( \text{ZU}(n) \), i.e. all \( n \times n \) diagonal unitary matrices with upper-left entry equal to 1.
Whereas the infinite unitary group $U(n)$ describes quantum computing, the finite permutation group $P(n)$ describes classical reversible computing. Whereas $XU(n)$ is both supergroup of $P(n)$ and subgroup of $U(n)$, in contrast, $ZU(n)$ is a subgroup of $U(n)$ but not a supergroup of $P(n)$:

\begin{align}
P(n) & \subset XU(n) \subset U(n) \quad (1) \\
ZU(n) & \subset U(n) \quad (2)
\end{align}

The XU circuits therefore can be considered as circuits ‘between’ classical and quantum circuits, whereas the ZU circuits are truly non-classical circuits.

2 First decomposition of a unitary matrix

In Reference [1], the following theorem is proved: any $U(n)$ matrix $U$ can be decomposed as

\[ U = e^{i\alpha} Z_1 X_1 Z_2 X_2 Z_3 \ldots Z_{p-1} X_{p-1} Z_p , \]

with $p \leq n(n - 1)/2 + 1$ and where all $Z_j$ are $ZU(n)$ matrices and all $X_j$ are $XU(n)$ matrices. In Reference [10], it is proved that a shorter decomposition exists: with $p \leq n$. Finally, in Reference [11], it is conjectured that an again shorter decomposition exists: with $p \leq 2$.

In the present paper, we investigate what would be the consequences of the conjecture that each $U(n)$ matrix can be decomposed as

\[ U = e^{i\alpha} Z_1 X Z_2 . \quad (3) \]

Reference [11] provides a numerical algorithm to find the number $\alpha$ and the matrices $Z_1$, $X$, and $Z_2$ for a given matrix $U$, based on a Sinkhorn-like approach. According to the conjecture, a quantum schematic (here for $w = 3$ and thus $n = 8$) looks like

\[ Z_2 \quad X \quad Z_1 \quad e^{i\alpha} \]

If $n$ is even, then we note the identity

\[ \text{diag}(a, a, a, a, ..., a, a) = P_0 \text{diag}(1, a, 1, a, 1, ..., 1, a) P_0^{-1} \text{diag}(1, a, 1, a, 1, ..., 1, a) , \]

where $a$ is a short-hand notation for $e^{i\alpha}$ and $P_0$ is the (circulant) permutation matrix

\[ \begin{pmatrix}
0 & 1 & 0 & 0 & \ldots & 0 & 0 \\
0 & 0 & 1 & 0 & \ldots & 0 & 0 \\
0 & 0 & 0 & 1 & \ldots & 0 & 0 \\
\vdots & & & & & & \\
0 & 0 & 0 & 0 & \ldots & 0 & 1 \\
1 & 0 & 0 & 0 & \ldots & 0 & 0 \\
\end{pmatrix} , \]

i.e. the P matrix called the cyclic-shift matrix, which can be implemented with classical reversible gates (i.e. one NOT and $w - 1$ controlled NOTs [12] [13]). We thus can transform (3) into a decomposition containing exclusively XU and ZU matrices:

\[ U = P_0 Z_0 P_0^{-1} Z_1' X Z_2 , \]

where $Z_0 = \text{diag}(1, a, 1, a, 1, ..., 1, a)$ is a ZU matrix which can be implemented by a single (uncontrolled) PHASOR gate and where $Z_1'$ is the product $Z_0 Z_1$: 

\[ Z_2 \quad X \quad Z_1' \quad P_0^{-1} \quad P_0 \quad Z_0 . \]
3 Further decomposition of a unitary matrix

For convenience, we rewrite eqn (3) as

\[ U = e^{i\alpha_n} L_n X_n R_n, \]

where the left matrix \( L_n \) and the right matrix \( R_n \) are members of \( ZU(n) \) and \( X_n \) belongs to \( \text{XU}(n) \). As a member of the \((n - 1)^2\)-dimensional group \( \text{XU}(n) \), \( X_n \) has the following form [9]:

\[ X_n = T_n \begin{pmatrix} 1 & 0 \\ U_{n-1} & T_n^{-1} \end{pmatrix}, \]

where \( U_{n-1} \) is a member of \( \text{U}(n-1) \) and \( T_n \) is an \( n \times n \) generalized Hadamard matrix. Reference [9] provides the algorithm to find the \( U_{n-1} \) matrix corresponding to a given \( \text{XU}(n) \) matrix \( X_n \).

Again according to the De Vos–De Baerdemacker conjecture [11], \( U_{n-1} \) can be decomposed as \( e^{i\alpha_{n-1}} l_{n-1} x_{n-1} r_{n-1} \), a product of a scalar, a \( ZU(n-1) \) matrix, an \( \text{XU}(n-1) \) matrix, and a second \( ZU(n-1) \) matrix. We thus obtain for \( X_n \) the product \( T_n L_n X_n R_n T_n^{-1} \), where

\[ L_{n-1} = \begin{pmatrix} 1 & 0 \\ e^{i\alpha_{n-1}} l_{n-1} & 1 \end{pmatrix}, \quad X_{n-1} = \begin{pmatrix} 1 \\ x_{n-1} \end{pmatrix}, \quad \text{and} \quad R_{n-1} = \begin{pmatrix} 1 \\ r_{n-1} \end{pmatrix}. \]

Hence, we have \( U = e^{i\alpha_n} L_n T_n L_{n-1} X_{n-1} R_{n-1} T_n^{-1} \). By applying such decomposition again and again, we find a decomposition \( e^{i\alpha_n} L_n T_n L_{n-1} T_{n-1} L_{n-2} \ldots T_2 L_1 X_1 R_1 T_1^{-1} R_2 \ldots R_{n-2} T_{n-2}^{-1} R_{n-1} T_{n-1}^{-1} R_n \)

of an arbitrary member of \( \text{XU}(n) \). As automatically \( X_1 \) and \( R_1 \) equal the unit matrix \( I_{n \times n} \), we thus obtain

\[ U = e^{i\alpha_n} L_n T_n L_{n-1} T_{n-1} L_{n-2} \ldots T_2 L_1 X_1 R_1 T_1^{-1} R_2 \ldots R_{n-2} T_{n-2}^{-1} R_{n-1} T_{n-1}^{-1} R_n, \]

(4)

where all \( n \) matrices \( L_j \) and all \( n-1 \) matrices \( R_j \) belong to the \((n-1)\)-dimensional group \( ZU(n) \). The \( n-1 \) matrices \( T_j \) are block-diagonal matrices of the form

\[ T_j = \begin{pmatrix} A \\ S_j \end{pmatrix}, \]

where \( A \) is an arbitrary \((n-j) \times (n-j)\) unitary matrix and \( S_j \) is a \( j \times j \) generalized Hadamard matrix. An obvious choice consists of \( A \) equal to \( I_{(n-j) \times (n-j)} \) and \( S_j \) equal to the \( j \times j \) discrete Fourier transform. For \( w = 2 \) (and thus \( n = 4 \)), eqn (4) thus looks like the following cascade of six constant matrices, seven \( ZU \) circuits, and one overall phase:

\[
\begin{array}{cccccccc}
  & R_4 & T_4^{-1} & R_3 & T_3^{-1} & R_2 & T_2^{-1} & L_1 & T_2 & L_2 & T_3 & L_3 & T_4 & L_4 & e^{i\alpha_4} \\
 3 & 0 & 2 & 0 & 1 & 0 & 1 & 3 & 0 & 3 & 0 & 3 & 1 & ,
\end{array}
\]

where the \( T_j \) blocks represent the \( n-1 \) constant matrices

\[ T_2 = \begin{pmatrix} 1 \\ 1/\sqrt{2} \\ 1/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix}, \quad T_3 = \begin{pmatrix} 1 \\ 1/\sqrt{3} \\ 1/\sqrt{3} \\ 1/\sqrt{3} \\ \omega/\sqrt{3} \\ \omega^2/\sqrt{3} \\ \omega/\sqrt{3} \end{pmatrix}, \]

and

\[ T_4 = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}, \]

with \( \omega \) equal to the cubic root of unity (\( \omega = e^{i2\pi/3} = -1/2 + i\sqrt{3}/2 \)). Beneath each of the \( 4n-2 \) blocks is displayed the number of real parameters of the block. These numbers sum to 16, i.e., exactly \( n^2 \), the dimensionality of \( \text{U}(n) \).

Hence, the synthesis problem of an arbitrary \( U(2^w) \) matrix is reduced to two smaller problems. First, for the given value of \( w \), we have to synthesize the \( 2^w - 1 \) circuits \( T_j \). Then, for the particular matrix \( U \), we have to synthesize the \( 2^{w+1} - 1 \) circuits of type \( ZU(2^w) \). The synthesis of an arbitrary \( ZU(2^w) \) circuit is discussed in the next section.
We close the present section by deriving from (4) a dual decomposition. By introducing the matrices $L'_j = T_{j+1} L'_j T_{j+1}^{-1}$ and $R'_j = T_{j+1} R'_j T_{j+1}^{-1}$, for $j < n$, as well as $L'_n = T_n L_n T_n^{-1}$ and $R'_n = T_n R_n T_n^{-1}$, we indeed find

$$U = e^{\alpha n} T_n^{-1} L_n' T_n L_n^{-1} T_{n-1} L_{n-1}^T T_{n-1}^{-1} T_n^{-1} R_n' T_n R_n^{-1} T_n',$$

where all matrices $L'_j$ and $R'_j$ belong to an $(j-1)$-dimensional subgroup of $XU(n)$. If, in particular, each $T_j$ is composed of the $(n-j) \times (n-j)$ unit block combined with the $j \times j$ discrete Fourier transform, then this subgroup consists of block-diagonal matrices with an $(n-j) \times (n-j)$ unit block and a $j \times j$ circular matrix from $XU(j)$ [12] [14].

4 Synthesizing a ZU circuit

The decomposition of a matrix $Z$, arbitrary member of $ZU(n)$, is straightforward. Indeed, for even $n$, the matrix can be written as the following product of four matrices:

$$\text{diag}(1, a_2, a_3, a_4, a_5, a_6, ..., a_n) = \text{diag}(1, a_2, 1, a_4, 1, a_6, ..., 1, a_n) P_0 \text{ diag}(1, 1, 1, a_3, 1, a_5, ..., 1, a_{n-1}) P_0^{-1},$$

where $a_j$ is a short-hand notation for $e^{a_j}$. If $n$ equals $2^w$, then the diagonal matrix $\text{diag}(1, a_2, 1, a_4, 1, a_6, ..., a_n)$ represents $2^{w-1}$ PHASORS, controlled $(w-1)$ times, and the diagonal matrix $\text{diag}(1, 1, 1, a_3, 1, a_5, ..., 1, a_{n-1})$ represents $2^{w-1} - 1$ PHASORS, controlled $(w-1)$ times. E.g. for $w = 3$, we obtain

![Diagram](image)

We thus have a total of $2^w - 1$ controlled PHASORS. According to Lemma 7.5 of Barenco et al. [15], each multiply-controlled gate $\Phi(\alpha)$ can be replaced by classical gates and three singly-controlled PHASORS $\Phi(\pm \alpha/2)$. According to De Vos and De Baerdemacker [10], each singly-controlled PHASOR $\Phi(\beta)$ can be decomposed into two controlled NOTs and three uncontrolled PHASORS $\Phi(\pm \beta/2)$. We thus obtain a circuit with a total of $9(2^w - 1)$ uncontrolled PHASORS.

5 Conclusion

We have demonstrated that, provided the $ZXZ$-conjecture of De Vos and De Baerdemacker is true, an arbitrary quantum circuit, acting on $w$ qubits, can be decomposed into $2^{w+1} - 1$ blocks, each described by a $2^w \times 2^w$ matrix from the $(2^w - 1)$-dimensional Lie group $ZU(2^w)$, subgroup of $U(2^w)$, separated by $2(2^w - 1)$ FOURIER circuits. The ZU blocks can be further decomposed into classical gates and a total of $9(2^{w+1} - 1)(2^w - 1)$ uncontrolled PHASE gates. As $\Phi(\theta) = H N(\theta) H$, each uncontrolled PHASE gate can be substituted by two HADAMARD gates and one uncontrolled NEGATOR gate. Taking into account that the HADAMARD gate is a FOURIER circuit, we thus have provided two synthesis algorithms, based on two different (dual) gate libraries:

- classical gates + FOURIER circuits + PHASE gate and
- classical gates + FOURIER circuits + NEGATOR gate.

References


[10] A. De Vos and S. De Baerdemacker: “The decomposition of $U(n)$ into $XU(n)$ and $ZU(n)$”, accepted for the 44th International Symposium on Multiple-Valued Logic, Bremen, 19 - 21 May 2014.


