

# 1 The Synthesis of a Quantum Circuit

ALEXIS DE VOS

STIJN DE BAERDEMACKER

## 1.1 Quantum Computation

A quantum computation [1], acting on  $w$  qubits, is described by a unitary  $2^w \times 2^w$  matrix  $U$ . The synthesis problem of quantum computing consists of decomposing a particular matrix  $U$  into ‘simpler’ matrices. Many decompositions have been proposed in the literature. Most of them are based on basic unitary transformations, well-known from elementary particle, nuclear, atomic or molecular physics. Thus the quantum circuit is decomposed into building blocks called controlled ROTATORS, where a ROTATOR is a single-qubit gate represented by a  $2 \times 2$  unitary matrix

$$\cos(\theta/2) \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} - i \sin(\theta/2) \left[ n_1 \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + n_2 \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} + n_3 \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right],$$

associated with the physical rotation of a spinor around the unit vector  $n_1\vec{e}_x + n_2\vec{e}_y + n_3\vec{e}_z$  over an angle  $\theta$ . Well-known are the rotations around the  $x$ -axis,  $y$ -axis, and  $z$ -axis:

$$R_x = \begin{pmatrix} \cos(\theta/2) & -i \sin(\theta/2) \\ -i \sin(\theta/2) & \cos(\theta/2) \end{pmatrix}, \quad R_y = \begin{pmatrix} \cos(\theta/2) & -\sin(\theta/2) \\ \sin(\theta/2) & \cos(\theta/2) \end{pmatrix},$$

$$\text{and } R_z = \begin{pmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{pmatrix}.$$

This approach leads to powerful synthesis methods [1] [2]. Its major drawback however is that it does not illuminate the relation with classical computing.

It is well established that the intermediate step between conventional classical computing and quantum computing is made up by classical reversible computing [3]. A classical reversible computer, acting on  $w$  bits, is described by a  $2^w \times 2^w$  permutation matrix. The synthesis of such reversible circuit is based on controlled NOTs, i.e. on the single-bit gate represented by the  $2 \times 2$  permutation matrix

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

As this matrix is neither an  $R_x$  matrix, nor an  $R_y$  matrix, nor an  $R_z$  matrix, the relation between classical reversible computing and quantum computing is obscured. For this reason, it is natural to introduce controlled NEGATORS and controlled PHASORS, rather than controlled ROTATORS.

## 1.2 Building Blocks

A classical reversible logic circuit, acting on  $w$  bits, is represented by a permutation matrix, i.e. a member of the finite matrix group  $P(2^w)$ . A quantum circuit, acting on  $w$  qubits, is represented by a unitary matrix, i.e. a member of the infinite matrix group  $U(2^w)$ . The classical reversible circuits form a subgroup of the quantum circuits. This is a consequence of the group hierarchy

$$P(n) \subset U(n),$$

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  $u = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ . Next, we consider two different square roots of that  $2 \times 2$  matrix:

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

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

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

where  $\theta$  is a real parameter [4]. 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:

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

We denote them with the schematics

$$\boxed{N(\theta)} \quad \text{and} \quad \boxed{\Phi(\theta)} ,$$

respectively. The former operation, we call the **NEGATOR** gate [5]; the latter, we call the **PHASOR** gate. Each of these two sets of matrices constitutes a continuous group, i.e. a 1-dimensional Lie group. Both groups contain the **IDENTITY** circuit. Indeed:  $\text{NEGATOR}(0) = \text{PHASOR}(0) = \text{IDENTITY}$ . Additionally, by construction, the **NOT** gate is a **NEGATOR** and the **PHASE** gate is a **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 [6]. For  $\theta = \pi/2$ , we have the square root of **NOT** and the square root of **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 [7] [8], while the latter is sometimes called the **S** gate [9]. 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 [8] and the **T** gate [9] [10], respectively.

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

$$\begin{pmatrix} \mathbf{1}_{6 \times 6} & & & \\ & \cos(\theta/2)e^{-i\theta/2} & i \sin(\theta/2)e^{-i\theta/2} & \\ & i \sin(\theta/2)e^{-i\theta/2} & \cos(\theta/2)e^{-i\theta/2} & \\ & & & \end{pmatrix} = \begin{array}{c} \text{---} \bullet \text{---} \\ \text{---} \bullet \text{---} \\ \boxed{N(\theta)} \end{array} ,$$

where  $\mathbf{1}_{a \times a}$  denotes the  $a \times a$  unit matrix. Of course, we equally introduce controlled **PHASORS**, negative-polarity controls, a target on a higher-positioned wire, etc...

It turns out [11] that all possible **NEGATORS** and controlled **NEGATORS** together generate a group  $\text{XU}(2^w)$ , subgroup of the unitary group  $\text{U}(2^w)$ . They cannot generate the full  $\text{U}(2^w)$  group, because the matrix representing a (controlled) **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) **NEGATORS** cannot synthesize a unitary matrix with one or more line sums different from unity. Whereas the unitary group  $\text{U}(n)$  has  $n^2$  dimensions, the group  $\text{XU}(n)$  has only  $(n-1)^2$  dimensions and is isomorphic to  $\text{U}(n-1)$  [11] [12] [13]. Analogously, a quantum circuit composed exclusively of (controlled) **PHASORS** 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 [13].

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

- $XU(n)$ , i.e. all  $n \times n$  unitary matrices with all of their  $2n$  line sums equal to 1;
- $ZU(n)$ , 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  $P(n)$ :

$$P(n) \subset XU(n) \subset U(n) \quad (1)$$

$$ZU(n) \subset U(n) . \quad (2)$$

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

### 1.3 First Decomposition of a Unitary Matrix

In Reference [4], the following theorem is proved: any  $U(n)$  matrix  $U$  can be decomposed as

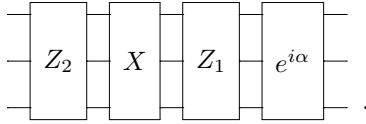
$$U = e^{i\alpha} Z_1 X_1 Z_2 X_2 Z_3 \dots Z_{p-1} X_{p-1} Z_p ,$$

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 [13], it is proved that a shorter decomposition exists: with  $p \leq n$ . Finally, in Reference [14], it is conjectured that an again shorter decomposition exists: with  $p \leq 2$ . Idel and Wolf [15] have provided a non-constructive proof.

In the present paper, we investigate the consequences of the decomposition

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

Reference [14] 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 [16]. According to the theorem, a quantum schematic (here for  $w = 3$  and thus  $n = 8$ ) looks like



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

$$\text{diag}(a, a, a, a, a, \dots, a, a) = P_0 \text{diag}(1, a, 1, a, 1, \dots, 1, a) P_0^{-1} \text{diag}(1, a, 1, a, 1, \dots, 1, a) ,$$

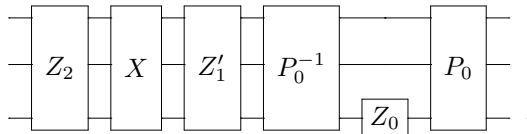
where  $a$  is a short-hand notation for  $e^{i\alpha}$  and  $P_0$  is the (circulant) permutation matrix

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

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 [3] [17]). 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  $Z_0 = \text{diag}(1, a, 1, a, 1, \dots, 1, a)$  is a  $ZU$  matrix which can be implemented by a single (uncontrolled) PHASOR gate and where  $Z'_1$  is the product  $Z_0 Z_1$ :



## 1.4 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  $XU(n)$ . As a member of the  $(n-1)^2$ -dimensional group  $XU(n)$ ,  $X_n$  has the following form [11]:

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

where  $U_{n-1}$  is a member of  $U(n-1)$  and  $T_n$  is an  $n \times n$  generalized Hadamard matrix. Reference [11] provides the algorithm to find the  $U_{n-1}$  matrix corresponding to a given  $XU(n)$  matrix  $X_n$ .

Again according to (3),  $U_{n-1}$  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  $XU(n-1)$  matrix, and a second  $ZU(n-1)$  matrix. We thus obtain for  $X_n$  the product  $T_n L_{n-1} X_{n-1} R_{n-1} T_n^{-1}$ , where

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

Hence, we have  $U = e^{i\alpha_n} L_n T_n (L_{n-1} X_{n-1} R_{n-1}) T_n^{-1} R_n$ . By applying such decomposition again and again, we find a decomposition

$$e^{i\alpha_n} L_n T_n L_{n-1} T_{n-1} L_{n-2} \dots T_2 L_1 X_1 R_1 T_2^{-1} R_2 \dots R_{n-2} T_{n-1}^{-1} R_{n-1} T_n^{-1} R_n$$

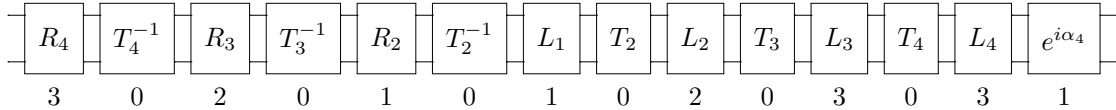
of an arbitrary member of  $XU(n)$ . As automatically  $X_1$  and  $R_1$  equal the unit matrix  $\mathbf{1}_{n \times n}$ , we thus obtain

$$U = e^{i\alpha_n} L_n T_n L_{n-1} T_{n-1} L_{n-2} \dots T_2 L_1 T_2^{-1} R_2 \dots R_{n-2} T_{n-1}^{-1} R_{n-1} T_n^{-1} R_n , \quad (4)$$

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  $\mathbf{1}_{(n-j) \times (n-j)}$  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:



where the  $T_j$  blocks represent the  $n-1$  constant matrices

$$T_2 = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & 1/\sqrt{2} & 1/\sqrt{2} & \\ & 1/\sqrt{2} & -1/\sqrt{2} & \end{pmatrix} , \quad T_3 = \begin{pmatrix} 1 & & & \\ & 1/\sqrt{3} & 1/\sqrt{3} & 1/\sqrt{3} \\ & 1/\sqrt{3} & \omega/\sqrt{3} & \omega^2/\sqrt{3} \\ & 1/\sqrt{3} & \omega^2/\sqrt{3} & \omega/\sqrt{3} \end{pmatrix} ,$$

$$\text{and} \quad T_4 = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix} ,$$

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  $U(n)$ .

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  $T_j$ . See next

subsection. 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 subsection on  $ZU$  circuits.

We close the present subsection by deriving from (4) a dual decomposition. By introducing the matrices  $L'_j = T_{j+1}L_jT_{j+1}^{-1}$  and  $R'_j = T_{j+1}R_jT_{j+1}^{-1}$ , for  $j < n$ , as well as  $L'_n = T_nL_nT_n^{-1}$  and  $R'_n = T_nR_nT_n^{-1}$ , we indeed find

$$U = e^{i\alpha_n} T_n^{-1} L'_n T_n L'_{n-1} T_{n-1} L'_{n-2} T_{n-2} \dots T_3 L'_1 T_3^{-1} R'_2 \dots T_{n-1}^{-1} R'_{n-2} T_{n-2}^{-1} R'_{n-1} T_{n-1}^{-1} R'_n T_n ,$$

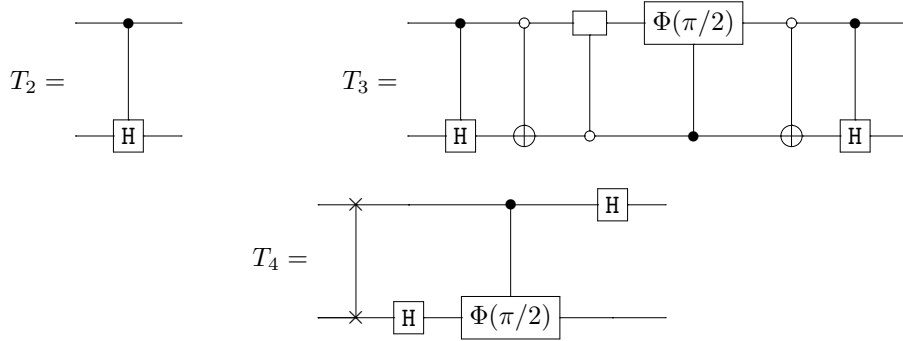
where all matrices  $L'_j$  and  $R'_j$  belong to a  $(j-1)$ -dimensional subgroup of  $XU(n)$ . If, in particular, each  $T_j$  is composed of the  $(n-j) \times (n-j)$  unit block combined with the  $j \times j$  discrete Fourier transform, then this subgroup consists of block-diagonal matrices with an  $(n-j) \times (n-j)$  unit block and a  $j \times j$  circulant matrix from  $XU(j)$  [17] [18].

## 1.5 Synthesizing a Fourier Circuit

We have the following decomposition:

$$T_3 = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1/\sqrt{2} & 1/\sqrt{2} \\ & & 1/\sqrt{2} & -1/\sqrt{2} \end{pmatrix} \begin{pmatrix} 1 & & & \\ & 1/\sqrt{3} & \sqrt{2}/\sqrt{3} & \\ & \sqrt{2}/\sqrt{3} & -1/\sqrt{3} & \\ & & & i \end{pmatrix} \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1/\sqrt{2} & 1/\sqrt{2} \\ & & 1/\sqrt{2} & -1/\sqrt{2} \end{pmatrix}$$

On the other hand, reference [17] provides a circuit for  $T_4$ . Thus we have:



The boxes filled with the letter H are either uncontrolled or controlled HADAMARD gates, performing the  $\begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{pmatrix}$ -transformation. The empty box in the schematic of the  $T_3$  circuit is a controlled  $\begin{pmatrix} 1/\sqrt{3} & \sqrt{2}/\sqrt{3} \\ \sqrt{2}/\sqrt{3} & -1/\sqrt{3} \end{pmatrix}$ -gate. Its synthesis may benefit from the following decomposition:

$$\begin{aligned} \begin{pmatrix} 1/\sqrt{3} & \sqrt{2}/\sqrt{3} \\ \sqrt{2}/\sqrt{3} & -1/\sqrt{3} \end{pmatrix} &= \begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix} \begin{pmatrix} \cos(\varphi) & i \sin(\varphi) \\ i \sin(\varphi) & \cos(\varphi) \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix} \\ &= e^{i\varphi} \Phi(-\pi/2) N(2\varphi) \Phi(-\pi/2) , \end{aligned}$$

where  $\varphi$  equals  $\text{Atan}(\sqrt{2})$ . Also the Hadamard gate H has an  $e^{i\alpha}ZXZ$  decomposition in closed form:

$$\begin{aligned} H &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1-i}{\sqrt{2}} \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \begin{pmatrix} (1+i)/2 & (1-i)/2 \\ (1-i)/2 & (1+i)/2 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \\ &= e^{-i\pi/4} \Phi(\pi/2) N(\pi/2) \Phi(\pi/2) \\ &= N(\pi) \Phi(7\pi/4) N(\pi) \Phi(\pi/4) N(\pi/2) \Phi(\pi/2) = XZSTXTVS . \end{aligned}$$

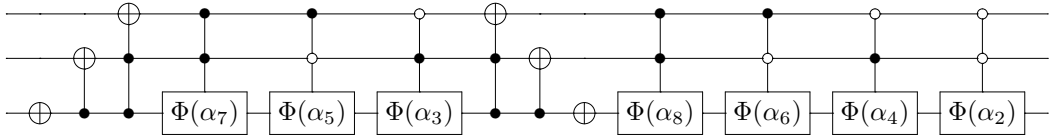
## 1.6 Synthesizing a ZU Circuit

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:

$$\text{diag}(1, a_2, a_3, a_4, a_5, a_6, \dots, a_n) =$$

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

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



We thus have a total of  $2^w - 1$  controlled PHASORS. According to Lemma 7.5 of Barenco et al. [2], 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 [13], 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.

The computer thus is built from uncontrolled PHASORS as basic blocks. The precision of the quantum computer is thus directly related to the precision of the PHASOR gate  $\Phi(\theta)$ . Above, we assumed that the angle  $\theta$  can be chosen arbitrarily, with arbitrary precision. Probably, in future quantum computer hardware, this will not be possible and only angles  $\theta$  which are a multiple of some basic angle  $2\pi/k$  (with  $k$  integer) will be available (e.g.  $k = 8$  if the basic building block is the T gate). Determining the precision of the computer, for a given value of  $k$ , remains a challenge for future research.

## 1.7 Summary

We have demonstrated that, thanks to the  $ZXZ$ -theorem, 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  $\Phi(\theta) = \mathbb{H}N(\theta)\mathbb{H}$ , 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

- [1] M. Nielsen and I. Chuang. *Quantum computation and quantum information*. Cambridge University Press, 2000.
- [2] A. Barenco, C. Bennett, R. Cleve, D. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. Smolin, and H. Weinfurter. Elementary gates for quantum computing. *Physical Review A*, 52:3457–3467, 1995.
- [3] A. De Vos. *Reversible computing*. Wiley-VCH, Weinheim, 2010.
- [4] A. De Vos and S. De Baerdemacker. Matrix calculus for classical and quantum circuits. *A.C.M. Journal on Emerging Technologies in Computing Systems*, 11:9, 2014.
- [5] A. De Vos and S. De Baerdemacker. The roots of the NOT gate. In *Proceedings of the 42 nd International Symposium on Multiple-Valued Logic*, pages 167–172, May 2012. Victoria.
- [6] M. Soeken, D. Miller, and R. Drechsler. Quantum circuits employing roots of the Pauli matrices. *Physical Review A*, 88:04322, 2013.
- [7] R. Wille and R. Drechsler. *Towards a design flow for reversible logic*. Springer, 2010.

- [8] Z. Sasanian and D. Miller. Transforming MCT circuits to NCVW circuits. In *Proceedings of the 3rd International Workshop on Reversible Computation*, pages 163–174, July 2011. Gent.
- [9] P. Selinger. Efficient Clifford+ $T$  approximations of single-qubit operators. *Quantum Information & Computation*, 15:159–180, 2015.
- [10] M. Amy, D. Maslov, and M. Mosca. Polynomial-time  $T$ -depth optimization of Clifford+ $T$  circuits via matroid partitioning. *I.E.E.E. Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 33:1476–1489, 2014.
- [11] A. De Vos and S. De Baerdemacker. The NEGATOR as a basic building block for quantum circuits. *Open Systems & Information Dynamics*, 20:1350004, 2013.
- [12] A. De Vos and S. De Baerdemacker. Logics between classical reversible logic and quantum logic. In *Proceedings of the 9th International Workshop on Quantum Physics and Logic*, pages 123–128, October 2012. Bruxelles.
- [13] A. De Vos and S. De Baerdemacker. The decomposition of  $U(n)$  into  $XU(n)$  and  $ZU(n)$ . In *Proceedings of the 44th International Symposium on Multiple-Valued Logic*, pages 173–177, May 2014. Bremen.
- [14] A. De Vos and S. De Baerdemacker. Scaling a unitary matrix. *Open Systems & Information Dynamics*, 21:1450013, 2014.
- [15] M. Idel and M. Wolf. Sinkhorn normal form for unitary matrices. 2014. [arXiv:math-ph 1408.5728](https://arxiv.org/abs/1408.5728).
- [16] R. Sinkhorn. A relationship between arbitrary positive matrices and doubly stochastic matrices. *The Annals of Mathematical Statistics*, 35:876–879, 1964.
- [17] T. Beth and M. Rötteler. Quantum algorithms: applicable algebra and quantum physics. In G. Alber, T. Beth, M. Horodecki, P. Horodecki, R. Horodecki, M. Rötteler, H. Weinfurter, R. Werner, and A. Zeilinger, editors, *Quantum information*, pages 96–150. Springer Verlag, 2001.
- [18] M. Combescure. Circulant matrices, Gauss sums and mutually unbiased bases, I. The prime number case. *CUBO Mathematical Journal*, 11:73–86, 2009.