A unified approach to quantum computation and classical reversible computation

Alexis De Vos[1] and Stijn De Baerdemacker[2]

Universiteit Gent, B - 9000 Gent, Belgium
[1] Cmst, vakgroep elektronica en informatiesystemen,
alexis.devos@ugent.be
[2] vakgroep fysica en sterrenkunde

Abstract. The design of a quantum computer and the design of a classical computer can be based on quite similar circuit designs. The former is based on the subgroup structure of the infinite group of unitary matrices, whereas the latter is based on the subgroup structure of the finite group of permutation matrices. Because these two groups display similarities as well as differences, the corresponding circuit designs are comparable but not identical.

1 Introduction

Quantum computation [1] acting on w qubits is described by $n \times n$ unitary matrices, where n equals 2^w. The $n \times n$ unitary matrices form an infinite group $\mathrm{U}(n)$. This continuous group fills a curved and compact n^2-dimensional space. In contrast, classical reversible computation [2] acting on w bits is described by an $n \times n$ permutation matrix, where n again equals 2^w. The $n \times n$ permutation matrices form a finite group $\mathrm{P}(n)$. As permutation matrices are unitary, this group can be visualized as $n!$ discrete points within the n^2-dimensional space of $\mathrm{U}(n)$.

In the present paper, we will discuss subgroups of both $\mathrm{U}(n)$ and $\mathrm{P}(n)$. The subgroups of $\mathrm{U}(n)$ are infinite and therefore their dimension (smaller than n^2) will be important; the subgroups of $\mathrm{P}(n)$ are finite and therefore their order (smaller than $n!$) will be important. In both cases, subgroups will be chosen such that an arbitrary group element can be decomposed into three simpler group elements. This approach leads to the synthesis of arbitrary quantum circuits and arbitrary classical reversible circuits [3].

2 Group hierarchy of the unitary matrices

We consider an arbitrary $n \times n$ unitary matrix U. It has $2n$ line sums: n row sums and n column sums. If n is even, we can consider the matrix built up from four $n/2 \times n/2$ blocks:

$$U = \begin{pmatrix} U_{11}\, U_{12} \\ U_{21}\, U_{22} \end{pmatrix} ,$$

where U_{jk} are $n/2 \times n/2$ matrices, not necessarily unitary. We call the matrices $U_{11} + U_{12}$ and $U_{21} + U_{22}$ the block-row sums and $U_{11} + U_{21}$ and $U_{12} + U_{22}$ the block-column sums. Both a block-row sum and a block-column sum is called a block-line sum.

The group $\mathrm{U}(n)$ of $n \times n$ unitary matrices has dimension n^2. Limiting ourselves to the case where n is even, we consider the following subgroups of $\mathrm{U}(n)$:

- the group $\mathrm{XU}(n)$ of $\mathrm{U}(n)$ matrices with all $2n$ line sums equal to 1,
- the group $\mathrm{bXU}(n)$ of $\mathrm{XU}(n)$ matrices with all four block-line sums equal to the $n/2 \times n/2$ unit matrix,
- the group $\mathrm{cXU}(n)$ of circulant $\mathrm{XU}(n)$ matrices,
- the group $\mathrm{aZU}(n)$ of $\mathrm{U}(n)$ matrices with upper-left entry equal to 1,
- the group $\mathrm{bZU}(n)$ of $\mathrm{U}(n)$ matrices with the upper-left block equal to the $n/2 \times n/2$ unit matrix,
- the group $\mathrm{ZU}(n)$ of diagonal $\mathrm{aZU}(n)$ matrices, and
- the trivial group $\mathbf{1}(n)$ consisting of the $n \times n$ unit matrix.

These groups have following dimensions:

$$\begin{aligned} \dim[\ \mathrm{U}(n)\ ] &= n^2 \\ \dim[\ \mathrm{XU}(n)\ ] = \dim[\ \mathrm{aZU}(n)\ ] &= (n-1)^2 \\ \dim[\ \mathrm{bXU}(n)\ ] = \dim[\ \mathrm{bZU}(n)\ ] &= (n/2)^2 \\ \dim[\ \mathrm{cXU}(n)\ ] = \dim[\ \mathrm{ZU}(n)\ ] &= n-1 \\ \dim[\ \mathbf{1}(n)\ ] &= 0\ . \end{aligned}$$

The group hierarchy is shown in Figure 1. From top to bottom of the graph, we recognize:

- the group $\mathrm{U}(n)$,
- the groups $\mathrm{XU}(n)$ and $\mathrm{aZU}(n)$, each other's Fourier conjugate,
- the groups $\mathrm{bXU}(n)$ and $\mathrm{bZU}(n)$, each other's Hadamard conjugate,
- the groups $\mathrm{cXU}(n)$ and $\mathrm{ZU}(n)$, each other's Fourier conjugate, and
- the group $\mathbf{1}(n)$.

We indeed have

$$\begin{aligned} \mathrm{XU} &= F\ \mathrm{aZU}\ F^{-1} \\ \mathrm{bXU} &= G\ \mathrm{bZU}\ G^{-1} \\ \mathrm{cXU} &= F\ \mathrm{ZU}\ F^{-1}\ , \end{aligned} \tag{1}$$

with F the $n \times n$ Fourier matrix and $G = G^{-1}$ given by

$$G = H \otimes I = \frac{1}{\sqrt{2}} \begin{pmatrix} I & I \\ I & -I \end{pmatrix}\ ,$$

where I is the $n/2 \times n/2$ unit matrix and H is the 2×2 Hadamard matrix:

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\ .$$

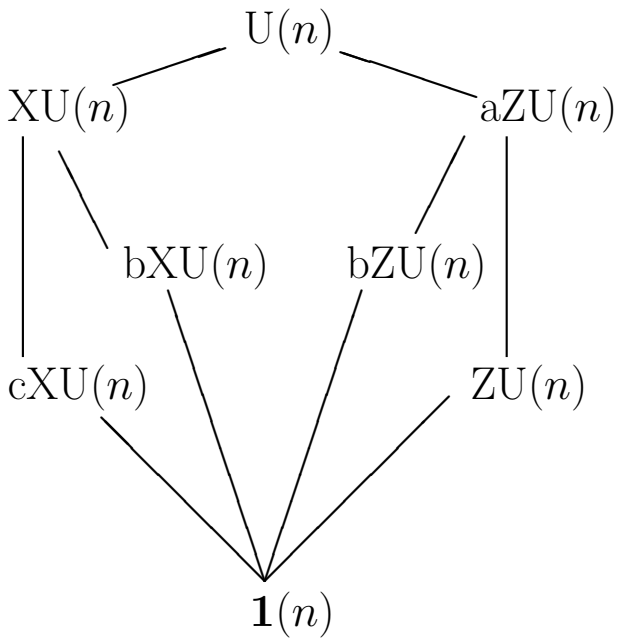


Fig. 1. Hierarchy of the infinite groups U(n), XU(n), bXU(n), cXU(n), ZU(n), aZU(n), and bZU(n) and the finite group $\mathbf{1}(n)$.

The groups XU(n), bXU(n), cXU(n), aZU(n), bZU(n), and ZU(n) give rise to four different decompositions of an arbitrary U(n) matrix U:

– Thanks to the groups XU(n) and ZU(n), we have the ZXZ decomposition [4] [5]

$$U = e^{i\delta} Z_1 X Z_2 \ , \tag{2}$$

where
- Z_1 and Z_2 are both members of ZU(n),
- X is a member of XU(n), and
- $e^{i\delta}$ is a unit-modulus scalar (i.e. a diagonal unitary matrix with all entries equal).

– Thanks to the groups cXU(n) and aZU(n), we have the CAC decomposition

$$U = e^{i\delta} C_1 A C_2 \ , \tag{3}$$

where
- C_1 and C_2 are both members of cXU(n),
- A is a member of aZU(n), and
- $e^{i\delta}$ is a unit-modulus scalar (i.e. a diagonal unitary matrix with all entries equal).

Proof is by applying (2) not to U but to FUF^{-1} instead.

– Thanks to the groups bXU(n) and bZU(n), we have two decompositions: the primal bZbXbZ decomposition [6] and the dual bXbZbX decomposition [7]

$$U = DZ_1XZ_2 \tag{4}$$
$$= X_1DZX_2 \ , \tag{5}$$

where
- Z_1, Z_2, and Z are members of bZU(n),
- X, X_1, and X_2 are members of bXU(n), and
- D is a block-diagonal matrix with two identical $n/2 \times n/2$ blocks.

The four decompositions are of the type called three-sandwiches [8]. The proof that an arbitrary unitary matrix U always can be decomposed as (2) and as (3) is non-constructive and based on symplective topology [5]; the proof that an arbitrary unitary matrix U always can be decomposed as (4) and as (5) is constructive and based on linear algebra (in particular on the polar decomposition of a square matrix) [7] [9]. The ZXZ decomposition (2) is also known as the matrix scaling into Sinkhorn normal form and decomposition (4) is known as block scaling.

We note that all four decompositions are optimally efficient, as the number of degrees of freedom in the decomposition exactly matches the dimension of the group U(n). In case of the ZXZ and CAC decompositions, we indeed have

$$1 + (n-1) + (n-1)^2 + (n-1) = n^2 \ .$$

In case of the bZbXbZ and bXbZbX decompositions, we have

$$\left(\frac{n}{2}\right)^2 + \left(\frac{n}{2}\right)^2 + \left(\frac{n}{2}\right)^2 + \left(\frac{n}{2}\right)^2 = n^2 \ .$$

The decomposition efficiency is mainly due to the fact that the conjugate subgroups overlap little:

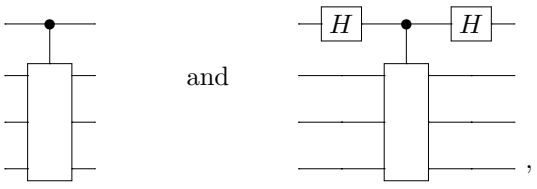
$$\mathrm{XU}(n) \cap \mathrm{ZU}(n) = \mathrm{cXU}(n) \cap \mathrm{aZU}(n) = \mathrm{bXU}(n) \cap \mathrm{bZU}(n) = \mathbf{1}(n)$$

and collaborate well:

$$\mathrm{Closure}[\mathrm{XU}(n), \mathrm{ZU}(n)] = \mathrm{Closure}[\mathrm{cXU}(n), \mathrm{aZU}(n)] = \mathrm{Closure}[\mathrm{bXU}(n), \mathrm{bZU}(n)] = \mathrm{U}(n) \ .$$

3 Quantum circuit synthesis

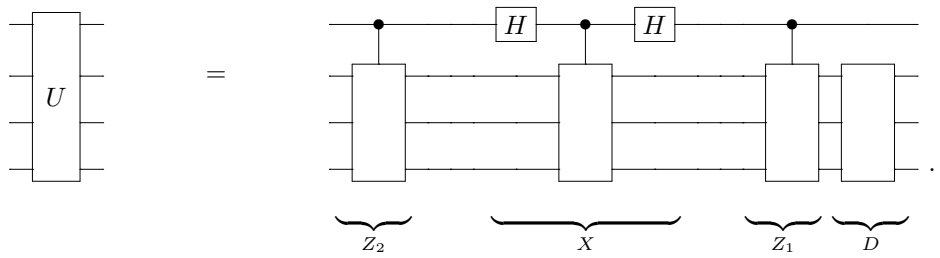
Limiting ourselves to the case where the even number n equals a power of two (say $n = 2^w$), the bZU(n) and bXU(n) matrices represent quantum circuits of the following form:



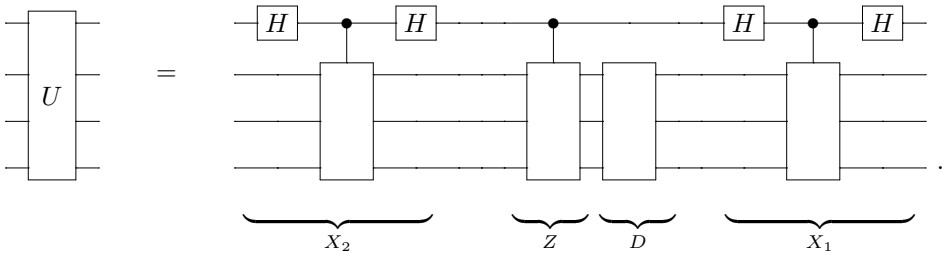
,

respectively. One recognizes here the relationship (1).

The primal bZbXbZ decomposition (4) by Führ and Rzeszotnik [6] of an arbitrary member U of $\mathrm{U}(n)$ looks like



The dual bXbZbX decomposition (5) by De Vos and De Baerdemacker [7] of an arbitrary member U of $\mathrm{U}(n)$ looks like



We now can apply to each of the four subcircuits (either to D, Z_1, X, and Z_2 or to X_1, D, Z, and X_2) again either the primal or the dual decomposition. By acting so again and again, we ultimately obtain a circuit decomposition into $\frac{5}{12}\ 4^w - \frac{2}{3}$ single-qubit gates (either controlled or not). Each such gate is one of the 4-dimensional infinity of U(2) gates. Finally, each single-qubit gate can be decomposed as a cascade of two `NEGATOR` gates and three `PHASOR` gates [3]. It can also be approximated with the help of Clifford gates and the `T` gate [10].

Example

As an example, we give the primal decomposition of the U(4) matrix:

$$U = \frac{1}{12} \begin{pmatrix} 8 & 0 & 4+8i & 0 \\ 2+i & 3-9i & -2i & -3-6i \\ 1-7i & 6 & -6+2i & -3+3i \\ 3+4i & 3-3i & 2-4i & 9i \end{pmatrix} .$$

We find:

$$D = \begin{pmatrix} 0.67+0.72i & -0.19+0.03i & & \\ 0.18+0.06i & 0.80-0.57i & & \\ & & 0.67+0.72i & -0.19+0.03i \\ & & 0.18+0.06i & 0.80-0.57i \end{pmatrix} ,$$

$$Z_1 = \begin{pmatrix} 1 & 0 & & \\ 0 & 1 & & \\ & & -0.56 - 0.24i & -0.09 - 0.78i \\ & & 0.60 + 0.52i & 0.13 - 0.60i \end{pmatrix} ,$$

$$X = \begin{pmatrix} 0.48 - 0.48i & 0.00 - 0.15i & 0.52 + 0.48i & 0.01 + 0.15i \\ -0.04 - 0.15i & 0.63 - 0.46i & 0.04 + 0.15i & 0.38 + 0.46i \\ 0.52 + 0.48i & 0.00 + 0.15i & 0.48 - 0.48i & -0.01 - 0.15i \\ 0.04 + 0.15i & 0.38 + 0.46i & -0.04 - 0.15i & 0.63 - 0.46i \end{pmatrix} , \text{ and}$$

$$Z_2 = \begin{pmatrix} 1 & 0 & & \\ 0 & 1 & & \\ & & 0.87 - 0.43i & -0.15 + 0.20i \\ & & -0.08 - 0.24i & -0.68 - 0.68i \end{pmatrix} .$$

The decomposition is numerical, as the procedure starts by performing the polar decomposition of each of the four blocks U_{11}, U_{12}, U_{21}, and U_{22} of U. We have performed these four decompositions applying Heron's iterative method. E.g.

$$\begin{aligned} U_{11} &= \frac{1}{12} \begin{pmatrix} 8 & 0 \\ 2 + i & 3 - 9i \end{pmatrix} \\ &= \begin{pmatrix} 0.66 + 0.00i & 0.08 - 0.04i \\ 0.08 + 0.04i & 0.81 - 0.00i \end{pmatrix} \begin{pmatrix} 0.99 - 0.00i & 0.02 + 0.13i \\ 0.11 + 0.06i & 0.31 - 0.94i \end{pmatrix} , \end{aligned}$$

the left factor being a positive semidefinite matrix, the right factor being a unitary matrix.

4 Group hierarchy of the permutation matrices

The group $\mathrm{P}(n)$ of $n \times n$ permutation matrices has order $n!$. Again limiting ourselves to even n, we consider the intersections of $\mathrm{P}(n)$ with each of the subgroups of $\mathrm{U}(n)$ in Section 2:

$$\begin{aligned} \mathrm{U}(n) \cap \mathrm{P}(n) = \mathrm{XU}(n) \cap \mathrm{P}(n) &= \mathrm{P}(n) \\ \mathrm{aZU}(n) \cap \mathrm{P}(n) &= \mathrm{aP}(n) \\ \mathrm{bXU}(n) \cap \mathrm{P}(n) &= \mathrm{XP}(n) \\ \mathrm{bZU}(n) \cap \mathrm{P}(n) &= \mathrm{ZP}(n) \\ \mathrm{cXU}(n) \cap \mathrm{P}(n) &= \mathrm{cP}(n) \\ \mathrm{ZU}(n) \cap \mathrm{P}(n) = \mathbf{1}(n) \cap \mathrm{P}(n) &= \mathbf{1}(n) . \end{aligned}$$

This way, Figure 1 gives rise to Figure 2. These groups have following orders:

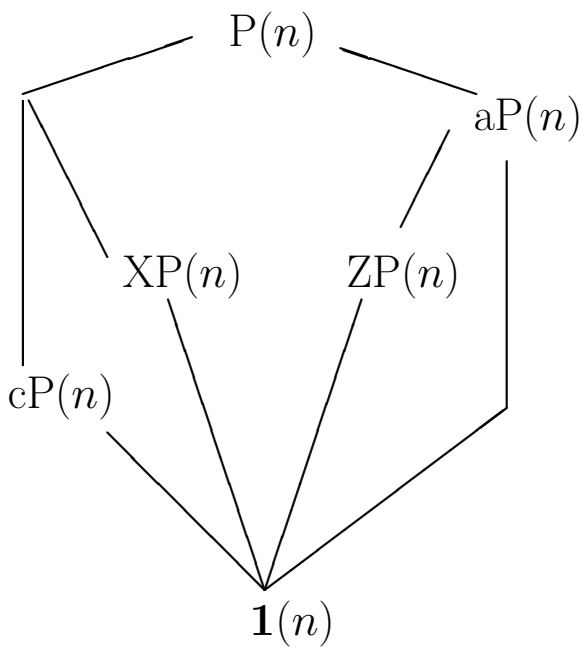


Fig. 2. Hierarchy of the finite groups P(n), XP(n), cP(n), aP(n), ZP(n) and $\mathbf{1}(n)$.

$$\begin{aligned}
\text{order}[\ \mathrm{P}(n)\ ] &= n! \\
\text{order}[\ \mathrm{aP}(n)\ ] &= (n-1)! \\
\text{order}[\ \mathrm{XP}(n)\ ] &= 2^{n/2} \\
\text{order}[\ \mathrm{ZP}(n)\ ] &= (n/2)! \\
\text{order}[\ \mathrm{cP}(n)\ ] &= n \\
\text{order}[\ \mathbf{1}(n)\ ] &= 1\ .
\end{aligned}$$

The groups can be interpreted as follows:

- the group XP(n) consists of the P(n) matrices with all four $n/2 \times n/2$ sub-blocks diagonal,
- the group cP(n) consists of the circulant P(n) matrices,
- the group aP(n) consists of P(n) matrices with upper-left entry equal to 1,
- the group ZP(n) consists of P(n) matrices with the upper-left $n/2 \times n/2$ block equal to the $n/2 \times n/2$ unit matrix, and
- the trivial group $\mathbf{1}(n)$ consists of the $n \times n$ unit matrix.

The four decompositions of a U(n) matrix in Section 2 lead to four decompositions of a P(n) matrix into three unitary matrices. However, because the intersections XU(n)$\cap$P(n) and ZU(n)$\cap$P(n) are the trivial subgroups P(n) and $\mathbf{1}(n)$ of P(n), the first decomposition of an arbitrary P(n) matrix is trivial. There

thus remain only three non-trivial decompositions of an arbitrary $\mathrm{P}(n)$ matrix P. In all three cases, we can guarantee that the factors of the decomposition are permutation matrices themselves:

- Thanks to the groups $\mathrm{cP}(n)$ and $\mathrm{aP}(n)$, we have the CA decomposition [11] into two permutation matrices:

$$P = CA \ ,$$

  where
  - C is a member of $\mathrm{cP}(n)$ and
  - A is a member of $\mathrm{aP}(n)$.
- Thanks to the groups $\mathrm{XP}(n)$ and $\mathrm{ZP}(n)$, we have two decompositions [12] [13]:

$$\begin{aligned} P &= DZ_1XZ_2 && (6)\\ &= X_1DZX_2 \ , && (7) \end{aligned}$$

  where
  - Z_1, Z_2 and Z are members of $\mathrm{ZP}(n)$,
  - X, X_1, and X_2 are members of $\mathrm{XP}(n)$, and
  - D is a block-diagonal matrix with two identical $n/2 \times n/2$ blocks.

The last two decompositions are of the type three-sandwiches [8]. Both profit from the advantageous properties

$$\begin{aligned} \mathrm{XP}(n) \cap \mathrm{ZP}(n) &= \mathbf{1}(n) \\ \mathrm{Closure}[\mathrm{XP}(n), \mathrm{ZP}(n)] &= \mathrm{P}(n) \ . \end{aligned}$$

However, whereas $\mathrm{bXU}(n)$ and $\mathrm{bZU}(n)$ are each other's Hadamard conjugate, the corresponding groups $\mathrm{XP}(n)$ and $\mathrm{ZP}(n)$ are not each other's conjugate. They even have different orders: $2^{n/2}$ and $(n/2)!$, respectively. As a consequence the resulting classical ZXZ and XZX decompositions are not equally efficient. Neither is optimal. In both cases, the number of possible products in the decomposition exceeds the order of the group $\mathrm{P}(n)$. In case of the ZXZ decomposition, we have a large overhead:

$$\left(\frac{n}{2}\right)! \ 2^{n/2} \ \left(\frac{n}{2}\right)! \ \left(\frac{n}{2}\right)! \gg n! \ .$$

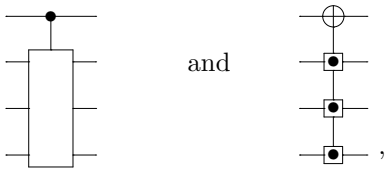
In case of the XZX decomposition, we have a moderate overhead:

$$2^{n/2-1} \ \left(\frac{n}{2}\right)! \ \left(\frac{n}{2}\right)! \ 2^{n/2} > n! \ .$$

As a result, the classical ZXZ decomposition is far from optimal, whereas the classical XZX decomposition is almost optimal.

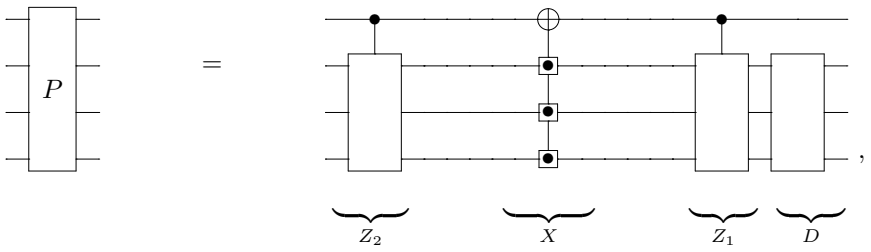
5 Reversible circuit synthesis

Limiting ourselves to the case where the even number n equals a power of two, the $\mathrm{ZP}(n)$ and $\mathrm{XP}(n)$ matrices represent classical reversible circuits of the following form:



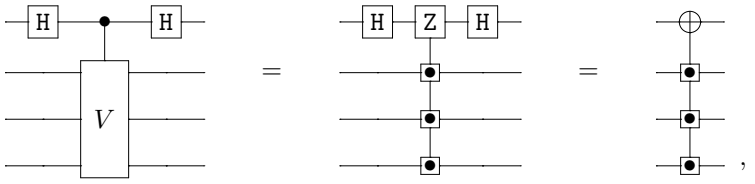
respectively. The latter is a `NOT` gate acting on the first bit, controlled by some Boolean control function f of the remaining bits [14].

Interesting is the fact that, if U happens to be a permutation matrix P, then the decomposition (4) recovers the decomposition (6) and hence, the primal quantum synthesis method by Führ and Rzeszotnik [6] recovers the primal synthesis method of a classical reversible circuit by De Vos and Van Rentergem [12] [13]:



where the `NOT` is controlled by an appropriate Boolean function x. The classical proof that such decomposition is always possible is based on combinatorics, in particular on the integer version [15] [16] of Birkhoff's theorem [17] on doubly stochastic matrices.

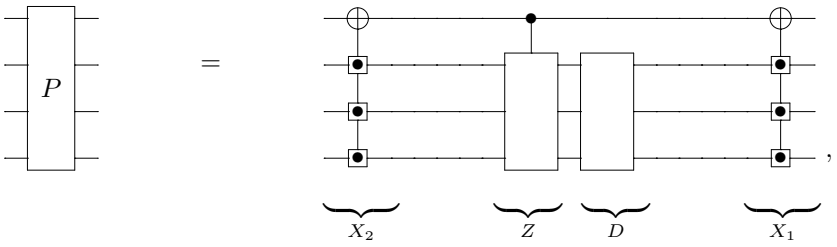
The fact that the primal quantum synthesis becomes the primal classical synthesis is thanked to the following identities, valid if circuit V is described by a diagonal matrix with exclusively ± 1 entries:



where `Z` is the 1-qubit gate fulfilling the transformation $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

The dual decomposition (5) often, but unfortunately not always, recovers the decomposition (7) and hence, the dual quantum synthesis method by De Vos and

De Baerdemacker [7], often but not always [3] leads to the dual synthesis method of a classical reversible circuit by De Vos and Van Rentergem [12] [13]:



where the NOTs are controlled by appropriate Boolean functions x_1 and x_2. The classical proof that such dual decomposition is always possible is equally based on combinatorics, in particular on the integer version of the Birkhoff theorem.

We now can apply to both subcircuits (Z and D) again the dual decomposition. By acting so again and again, we finally obtain a circuit decomposition into $\frac{3}{2}\ 2^w - 2$ single-bit gates (either controlled or not). Each such gate is one of the only two P(2) circuits, i.e. either the IDENTITY gate or the NOT gate. Both the controlled and the uncontrolled IDENTITY gates can be deleted.

Example

As an example, we give the decomposition of the P(4) matrix:

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

We find:

$$D = \begin{pmatrix} 0&1&&\\ 1&0&&\\ &&0&1\\ &&1&0 \end{pmatrix} ,\ Z_1 = \begin{pmatrix} 1&0&&\\ 0&1&&\\ &&0&1\\ &&1&0 \end{pmatrix} ,$$

$$X = \begin{pmatrix} 0&&1&\\ &1&&0\\ 1&&0&\\ &0&&1 \end{pmatrix} ,\ \text{and}\ Z_2 = \begin{pmatrix} 1&0&&\\ 0&1&&\\ &&0&1\\ &&1&0 \end{pmatrix} .$$

6 Conclusion

We introduced six infinite subgroups of the unitary group U(n) with even n. These lead us to four equally efficient matrix decompositions. Two of them enable optimally efficient synthesis of a w-qubit quantum circuit. Both the primal and the dual synthesis method lead to a circuit with $\frac{5}{12}\ 4^w - \frac{2}{3}$ or less quantum gates.

The same approach to the finite group $\mathrm{P}(n)$ with even n, leads to a less symmetrical group hierarchy and to only three matrix decompositions. Two of them enable reversible circuit synthesis, the dual synthesis method being more efficient than the primal one and leading to a w-bit circuit with $\frac{3}{2}\ 2^w - 2$ or less classical gates.

Acknowledgement

The authors thank the European COST Action IC 1405 'Reversible computation' for its valuable support.

References

1. M. Nielsen and I. Chuang, *Quantum computation and quantum information*, Cambridge University Press, Cambridge, 2000.
2. A. De Vos, *Reversible computing*, Wiley - VCH, Weinheim, 2010.
3. A. De Vos, S. De Baerdemacker, and Y. Van Rentergem, *Synthesis of quantum circuits versus synthesis of classical reversible circuits*, Morgan & Claypool, La Porte, 2018.
4. A. De Vos and S. De Baerdemacker, "Scaling a unitary matrix", *Open Systems & Information Dynamics*, vol. 21, 1450013, 2014.
5. M. Idel and M. Wolf, "Sinkhorn normal form for unitary matrices", *Linear Algebra and its Applications*, vol. 471, 76-84, 2015.
6. H. Führ and Z. Rzeszotnik, "On biunimodular vectors for unitary matrices", *Linear Algebra and its Applications*, vol. 484, 86-129, 2015.
7. A. De Vos and S. De Baerdemacker, "Block-ZXZ synthesis of an arbitrary quantum circuit", *Physical Review A*, vol. 94, 052317, 2016.
8. L. Chen and L. Yu, "Decomposition of bipartite and multipartite unitary gates", *Physical Review A*, vol. 91, 032308, 2015.
9. H. Führ and Z. Rzeszotnik, "A note on factoring unitary matrices", *Linear Algebra and its Applications*, vol. 547, 32-44, 2018.
10. P. Selinger, "Efficient Clifford+T approximations of single-qubit operators", *Quantum Information & Computation*, vol. 15, 159-180, 2015.
11. A. De Vos and S. De Baerdemacker, "The group zoo of classical reversible computing and quantum computing", In: A. Adamatzky, *Advances in unconventional computing*, Springer, Cham, 2017, pp. 455-474.
12. A. De Vos and Y. Van Rentergem, "Synthesis of reversible logic for nanoelectronic circuits", *International Journal of Circuit Theory and Applications*, vol. 35, 325-341, 2007.
13. A. De Vos and Y. Van Rentergem, "Young subgroups for reversible computers", *Advances in Mathematics of Communications*, vol. 2, 183-200, 2008.
14. A. De Vos, B. Raa, and L. Storme, "Generating the group of reversible logic gates", *Journal of Physics A: Mathematical and General*, vol. 35, 7063-7078, 2002.
15. D. de Werra, "Path coloring in bipartite graphs", *European Journal of Operational Research*, vol. 164, 575-584, 2005.
16. C. Peng, G. Bochman, and T. Hall, "Quick Birkhoff-von Neumann decomposition algorithm for agile all-photonic network cores", *Proceedings of the IEEE International Conference on Communications*, Istanbul (June 2006), pp. 2593-2598.
17. G. Birkhoff, "Tres observaciones sobre el algebra lineal", *Universidad Nacional de Tucumán: Revista Matemáticas y Física Teórica*, vol. 5, 147-151, 1946.