Beyond quantum Shannon decomposition

Circuit construction for n -qubit gates based on block- ZXZ decomposition

Krol, Anna M.; Al-Ars, Zaid

DOI
10.1103/PhysRevApplied.22.034019

Publication date
2024

Document Version
Final published version

Published in
Physical Review Applied

Beyond quantum Shannon decomposition: Circuit construction for *n*-qubit gates based on block-*ZXZ* decomposition

Anna M. Krol* and Zaid Al-Ars
Quantum & Computer Engineering Department, Delft University of Technology, Delft, Netherlands

(Received 2 April 2024; revised 24 July 2024; accepted 25 July 2024; published 9 September 2024)

This paper proposes an optimized quantum block-*ZXZ* decomposition method that results in more optimal quantum circuits than the quantum Shannon decomposition, which was presented in 2005 by M. Möttönen, and J. J. Vartiainen [in *Trends in quantum computing research*, edited by S. Shannon (Nova Science Publishers, 2006) Chap. 7, p. 149, arXiv:quant-ph/0504100]. The decomposition is applied recursively to generic quantum gates, and can take advantage of existing and future small-circuit optimizations. Because our method uses only single-qubit gates and uniformly controlled rotation-Z gates, it can easily be adapted to use other types of multi-qubit gates. With the proposed decomposition, a general three-qubit gate can be decomposed using 19 CNOT gates (rather than 20). For general *n*-qubit gates, the proposed decomposition generates circuits that have $\frac{22}{48}4^n - \frac{3}{2}2^n + \frac{5}{3}$ CNOT gates, which is less than the best-known exact decomposition algorithm by $(4^{n-2} - 1)/3$ CNOT gates.

DOI: 10.1103/PhysRevApplied.22.034019

I. INTRODUCTION

To execute a quantum algorithm, a series of unitary operations (gates) and nonunitary operations (measurements) are applied to quantum bits (qubits) in a quantum circuit. The complexity of a quantum algorithm can be described as the number of gates, the number of qubits or the length of the critical path (depth) of the circuit.

Physically, a qubit is a quantum mechanical system that can store quantum information, such as superconducting qubits [1], trapped ions [2], or spin qubits [3]. Applying a quantum gate means manipulating the state of the qubit in a controlled way. Exactly which gate operations are possible depends on the qubit technology and the implementation [4].

To run arbitrary quantum operations on real quantum hardware, the unitary operator (matrix) needs to be translated into elementary (native) gate operations. This is by no means a trivial task, and the focus of much research over the years into methods for performing such translation using quantum gate decomposition.

A target of gate-decomposition methods is to minimize the number of two-qubit gates required to implement a given unitary matrix. This is essential, because the two-qubit gates require qubit connectivity and mapping, and the execution time and error rates of two-qubit gates are an order of magnitude worse than for single-qubit gates in current quantum hardware [4].

It has been proven that any exact decomposition of an arbitrary *n*-qubit gate requires at least $\frac{1}{4}(4^n - 3n - 1)$ CNOT gates [5].

Approximate decomposition algorithms such as Refs. [6–8] can be used to decompose arbitrary quantum gates with (almost) the minimum number of CNOT gates and little accuracy loss, at the cost of excessive runtime of the search algorithm: decomposition of a five-qubit gate can take at least several hours. These methods are therefore not suitable for bigger gates or for applications where classical compile time is relevant for the performance of the algorithm [9].

In contrast, exact decomposition methods are much faster, and for one- and two-qubit gates also achieve the minimum CNOT count. One-qubit gates do not require any CNOTs and can be decomposed into a sequence of three rotation gates [10]. Arbitrary two-qubit gates can be decomposed into three CNOTs using the methods described in Refs. [5,11–13], which also show that fewer CNOTs are necessary when the gate meets certain conditions. For arbitrary three-qubit gates, there is no algorithm that results in the minimum 14 CNOTs, but algorithms do exist that can decompose them into 64 [14], 40 [15], 26 [16], or 20 [17,18] CNOTs.

For quantum gates of arbitrary size, the decomposition methods have drastically improved since 1995, when Barenco *et al.* [10] showed that any unitary operator on *n* qubits can be constructed using at most $O(n^3 4^n)$ two-qubit gates. This decomposition method used the standard QR decomposition based on Givens rotations [19], and the CNOT count has been improved over the years by use

*Contact author: annerietkrol@gmail.com

of Gray codes and gate cancellations to $O(\frac{1}{2} \times 4^n)$ CNOT gates [14,18,20]. Another approach to unitary decomposition has been to use cosine sine decomposition (CSD) [21–24]. This was combined with diagonalization and separate handling of quantum multiplexors (using the method from Ref. [24]) in 2004 to construct the NQ decomposition, which requires $O(\frac{1}{2} \times 4^n)$ CNOTs [25]. The NQ decomposition was optimized in 2005 by Möttönen and Vartiainen to produce a decomposition that requires at most $(23/48) \times 4^n - (3/2) \times 2^n + (4/3)$ CNOT gates [17]. This decomposition is more widely known as the quantum Shannon decomposition (QSD) [18]. More recently, the Khaneja-Glaser decomposition [26] was used in Ref. [27] to construct a decomposition method that can decompose unitary operations using $(21/16) \times 4^n - 3(n \times 2^{n-2} + 2^n)$ CNOT gates.

In this paper, we show the design and construction of an alternative unitary decomposition method based on block-*ZXZ* decomposition [28–30], that uses demultiplexing and optimizations similar to quantum Shannon decomposition [17,18]. The contributions of this paper are as follows:

(1) We show how to decompose an arbitrary n-qubit gate into at most $(22/48) \times 4^n - (3/2) \times 2^n + (5/3)$ CNOT gates. This is $(4^{n-2} - 1)/3$ less than the best previously published work [17,18].

(2) More specifically, we can construct a general three-qubit operator with at most 19 qubits, which is currently the least known for any exact decomposition method.

An overview of the CNOT count for the proposed method compared to previously published unitary decomposition algorithms is given in Table I.

The rest of the paper is organized as follows. We start with the notation and gate definitions in Sec. II. Then in Sec. III, we show the decomposition of uniformly controlled rotations. Section IV continues with the full decomposition. The optimizations and the resulting gate count are shown in Sec. V. The paper ends with the conclusion in Sec. VI.

II. NOTATION AND GATE DEFINITIONS

This section introduces the mathematical notation and gate definitions used in this paper.

A. Mathematical operations

The conjugate transpose of a matrix is represented with † (i.e., the conjugate transpose of matrix U is $U^\dagger$). Reversible quantum operations (gates) can be fully represented as unitary matrices, for which $U^\dagger = U^{-1}, UU^\dagger = I$, where I is the identity matrix.

The Kronecker product of two matrices is written as $\otimes$. The Kronecker product of $(n \times m)$ matrix A and $(p \times q)$ matrix B is the $(pm \times qn)$ block matrix:

$$A \otimes B = \begin{bmatrix} a_{11}B & \cdots & a_{1n}B \\ \vdots & \ddots & \vdots \\ a_{m1}B & \cdots & a_{mn}B \end{bmatrix}.$$

The Kronecker sum of two matrices is written as $\oplus$. The Kronecker sum of $(n \times m)$ matrix A and $(p \times q)$ matrix B is the $((m+p) \times (n+q))$ block matrix:

$$A \oplus B = \begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix},$$

where the zeros are zero matrices.

TABLE I. Number of CNOT gates resulting from unitary decomposition by the proposed decomposition compared to previously published algorithms and the theoretical lower bound. The results of this paper are shown in bold.

Number of qubits	1	2	3	4	5	6	n
Original QR decomp. [10,19]							$O(n^3 \times 4^n)$
Improved QR decomp. [31]							$O(n \times 4^n)$
Palindrome transform [18,20]							$O(n \times 4^n)$
Givens rotations (QR) [14]	0	4	64	536	4156	22618	$\approx 8.7 \times 4^n$
Original CSD [23,32]	0	14	92	504	2544	12256	$(1/2) \times n \times 4^n - (1/2) \times 2^n$
Iterative disentangling (QR) [18]	0	8	62	344	1642	7244	$2 \times 4^n - (2n+3) \times 2^n + 2^n$
KG Cartan decomp. [27]	0	3	42	240	1128	4896	$(21/16) \times 4^n - 3(n \times 2^{n-2} + 2^n)$
CSD [24]	0	8	48	224	960	3968	$4^n - 2 \times 2^n$
QSD (base) [18]	0	6	36	168	720	2976	$(3/4) \times 4^n - (3/2) \times 2^n$
Block-*ZXZ* [28]	0	6	36	168	720	2976	$(3/4) \times 4^n - (3/2) \times 2^n$
CSD (optimized) [17]	0	4	26	118	494	2014	$(1/2) \times 4^n - (1/2) \times 2^n - 2$
NQ [25]	0	3	21	105	465	1953	$(1/2) \times 4^n - (3/2) \times 2^n + 1$
QSD (optimized) [17,18]	0	3	20	100	444	1868	$(23/48) \times 4^n - (3/2) \times 2^n + (4/3)$
Proposed decomposition	**0**	**3**	**19**	**95**	**423**	**1783**	$\mathbf{(22/48) \times 4^n - (3/2) \times 2^n + (5/3)}$
Theoretical lower bounds	0	3	14	61	252	1020	$(1/4) \times (4^n - 3n - 1)$

B. Generic gates

The elementary quantum operations used in this paper are part of the well-established and widely used set presented in Ref. [10].

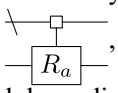
The following generic gates are used in the decomposition and their circuit representation are listed below.

(1) Generic single-qubit unitary gate:
$U(2) =$

(2) Generic multiqubit unitary gate:
$U(n) =$ where the backslash is used to show that the wire carries an arbitrary number of qubits.

(3) Controlled arbitrary (multiqubit) gates:
 $= \begin{bmatrix} I & 0 \\ 0 & U \end{bmatrix}$, gate U is only applied if the control qubit is in state $|1\rangle$.

(4) Quantum multiplexor:  $= U_1 \oplus U_2 = \begin{bmatrix} U_1 & 0 \\ 0 & U_2 \end{bmatrix}$, gate U_1 is applied if the control qubit is in state $|0\rangle$, gate U_2 is applied if the control qubit is in state $|1\rangle$.

(5) Uniformly controlled rotation gate:
 , a different rotation around axis a is applied depending on the state of the control qubits.

III. DECOMPOSING UNIFORMLY CONTROLLED ROTATIONS

This section shows the decomposition for one of the main building blocks resulting from our method; the uniformly controlled rotation gates. These gates will be decomposed using the method from Ref. [24].

The uniformly controlled rotation gates that are used in our decomposition method are always uniformly controlled R_z gates applied to the first qubit. The matrix representation of such a gate follows from the general matrix representation of a uniformly controlled R_z gate with k controlling qubits, and is $(D \oplus D^\dagger)$, where D is a $(2^k \times 2^k)$ diagonal matrix.

This gate can be implemented by an alternating sequence consisting of 2^k CNOTs and 2^k single-qubit rotation gates applied to the target qubit. The CNOT controls are determined using a sequence based on the binary reflected Gray code [33]. The 2^k rotation gates in the circuit each apply a rotation by some angle θ_j to the target qubit, which can be calculated in such a way that the complete circuit is equivalent to $(D \oplus D^\dagger)$ [24].

The structure of the decomposition of a uniformly controlled R_z gate with three control qubits is shown in Fig. 1.

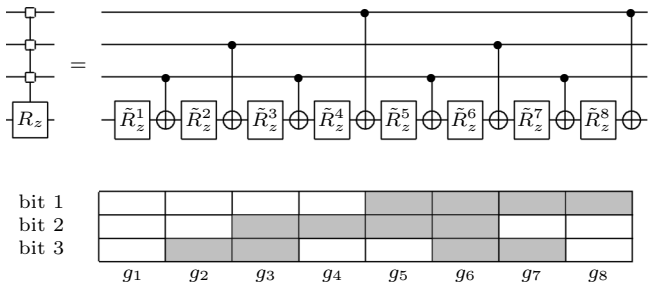


FIG. 1. Decomposition of a uniformly controlled R_z gate with $(k = 3)$ control qubits with the three-bit Gray code that is used to find the control nodes of the CNOTs. In this figure $\tilde{R}_z^j$ is used to mean $R_z(\theta_j)$, where $j = 1, \cdots, 2^k$.

IV. FULL DECOMPOSITION

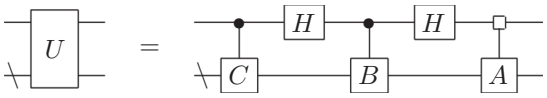
In this section, we first introduce the basis of our decomposition: the block-*ZXZ* decomposition [28]. Then we show how to decompose the circuit into elementary gates. This decomposition method results in the same number of CNOT gates as the unoptimized quantum Shannon decomposition [28].

A. Block-*ZXZ* decomposition

The proposed decomposition is based on the block-*ZXZ* decomposition presented in Ref. [28], which shows how the method presented in Ref. [30] can be used to decompose a general unitary gate into the following structure:

$$\begin{aligned} U &= \frac{1}{2}\begin{bmatrix} A_1 & 0 \\ 0 & A_2 \end{bmatrix}\begin{bmatrix} I+B & I-B \\ I-B & I+B \end{bmatrix}\begin{bmatrix} I & 0 \\ 0 & C \end{bmatrix} \\ &= \frac{1}{2}\begin{bmatrix} A_1 & 0 \\ 0 & A_2 \end{bmatrix}(H \otimes I)\begin{bmatrix} I & 0 \\ 0 & B \end{bmatrix}(H \otimes I)\begin{bmatrix} I & 0 \\ 0 & C \end{bmatrix}. \end{aligned} \tag{1}$$

This can be represented as the following quantum circuit:



To construct this circuit, we need to solve Eq. (1), which requires that [30]:

$$U\begin{bmatrix} I \\ C^\dagger \end{bmatrix} = \begin{bmatrix} A_1 \\ A_2 \end{bmatrix}. \tag{2}$$

To find matrices A_1, A_2, and C, we first divide the starting matrix U into four equal blocks. We call the upper left block X, the upper right block Y and the lower two

blocks U_{21} and U_{22}. This makes $U = \left[\begin{smallmatrix} X & Y \\ U_{21} & U_{22} \end{smallmatrix}\right]$ and then use singular value decomposition to decompose X and Y.

For X, with singular value decomposition we get $X = V_X \Sigma W_X^\dagger$ with unitary matrices $V_X, W_X \in U$, and Σ is a diagonal matrix with non-negative real numbers on the diagonal. We define $S_X = V_X \Sigma V_X^\dagger$, a positive semidefinite matrix and unitary matrix $U_X = V_X W_X^\dagger$. Then we have the polar decomposition of $X = S_X U_X$. The same method can be used to find S_Y and U_Y so that $Y = S_Y U_Y$.

Then we can write

$$U = \begin{bmatrix} S_X U_X & S_Y U_Y \\ U_{21} & U_{22} \end{bmatrix} \tag{3}$$

and define $C^\dagger = iU_Y^\dagger U_X$ so that Eq. (2) becomes

$$U \begin{bmatrix} I \\ iU_Y^\dagger U_X \end{bmatrix} = \begin{bmatrix} A_1 \\ A_2 \end{bmatrix}. \tag{4}$$

We can find $A_1 = (S_X + iS_Y)U_X$ and $A_2 = U_{21} + U_{22}(iU_Y^\dagger U_X)$. Finally, we rewrite Eq. (1) and solve for the upper left corner to get $B = 2A_1^\dagger X - I$.

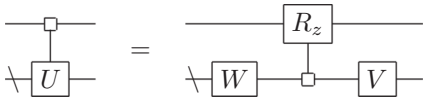
B. Demultiplexing

A gate $U = U_1 \oplus U_2$ can be decomposed into unitary matrices V and W and a unitary diagonal matrix D so that $U = (I \otimes V)(D \oplus D^\dagger)(I \otimes W)$ using the method described in theorem 12 of [18]

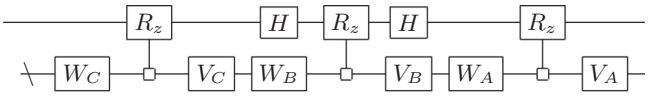
$$\begin{bmatrix} U_1 & 0 \\ 0 & U_2 \end{bmatrix} = \begin{bmatrix} V & 0 \\ 0 & V \end{bmatrix} \begin{bmatrix} D & 0 \\ 0 & D^\dagger \end{bmatrix} \begin{bmatrix} W & 0 \\ 0 & W \end{bmatrix}. \tag{5}$$

To find the values for V, D, and W, we first use diagonalization of $U_1 U_2^\dagger$ to get $U_1 U_2^\dagger = VD^2V^\dagger$, where V is a square matrix with columns representing the eigenvalues of $U_1 U_2^\dagger$ and D a diagonal matrix whose diagonal entries are the corresponding eigenvalues. Then we can find W as $W = DV^\dagger U_2$. The matrix $D \oplus D^\dagger$ corresponds to a multiplexed R_z gate acting on the most significant qubit in the circuit.

In a quantum circuit, demultiplexing looks like this:



We can use this method to demultiplex gates A, B, and C from the circuit in Sec. IV A, which gives the following circuit:



It is clear from the circuit that gate V_C can be merged with W_B, and that V_B can be merged with W_A. This means we now have a circuit decomposition of an initial n-qubit gate into four $(n-1)$-qubit gates, three uniformly controlled R_z gates and two Hadamard gates. The uniformly controlled R_z gates can be decomposed as in Sec. III. The decomposition is applied recursively to each $(n-1)$-qubit gate until only one-qubit gates are left, which can be decomposed using ZYZ decomposition [10].

This leads to a total CNOT count that is the same as the unoptimized quantum Shannon decomposition [18]: $(3/4) \times 4^n - (3/2) \times 2^n$.

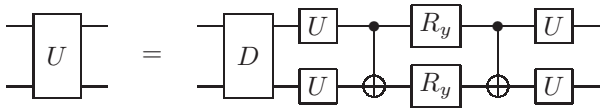
V. OPTIMIZATION

Because the circuit resulting from the block-ZXZ decomposition is very similar to that of the quantum Shannon decomposition [17,18], it can be optimized using the same methods. But where QSD can merge one CNOT gate from the central R_y gate, we can merge two CNOT gates into the central multiplexor. This results in a total CNOT count of $\frac{22}{48}4^n - \frac{3}{2}2^n + \frac{5}{3} = \frac{11}{24}4^n - \frac{3}{2}2^n + \frac{5}{3}$ CNOT gates for decomposing an n-qubit unitary gate.

A. Decomposition of two-qubit operators

The decomposition can be applied recursively until the biggest blocks are the generic two-qubit unitary gates. These can be decomposed using the optimal three-CNOT circuit, which can be done using one of several methods [5,13,34]. This reduces the CNOT count to $(9/16) \times 4^n - (3/2) \times 2^n$ [18].

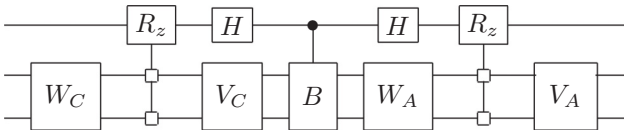
The CNOT count can be further reduced using the technique described in Ref. [25]. The right-most two-qubit gate can be decomposed up to the diagonal into the following circuit, which requires only two qubits [34]:



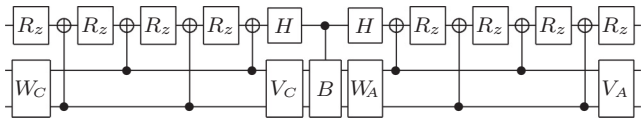
The diagonal matrix can be migrated through the circuit and merged with the next two-qubit gate, which can then be decomposed and its diagonal joined with the next, until only one two-qubit gate is left. This reduces the CNOT count by $4^{n-2} - 1$ gates to $(8/16) \times 4^n - (3/2) \times 2^n - 1$.

B. Merging two CNOT gates into the central multiplexor

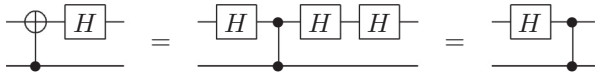
After the block-*ZXZ* decomposition, we first decompose only the left and right multiplexors (A and C). We now have a circuit with two uniformly controlled R_z gates. Using the decomposition of a three-qubit unitary as an example, the circuit now looks like this:



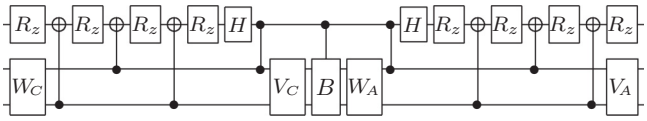
When decomposing the uniformly controlled R_z gates (see Sec. IV B), we can modify one of the decompositions so that both of the Hadamard gates are next to a CNOT:



The Hadamard gates can be moved to the other side of two CNOTs, making them into CZ gates:



This makes the circuit:

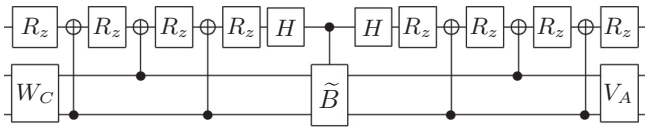


The two CZ gates can be merged into the middle controlled gate (B) together with the two $(n-1)$-qubit gates V_C and W_A, similar to the optimization introduced in Ref. [17].

The central gate $\widetilde{B}$ can be calculated as

$$\widetilde{B} = (CZ \otimes I)\begin{bmatrix} W_A & 0 \\ 0 & W_A \end{bmatrix}\begin{bmatrix} I & 0 \\ 0 & B \end{bmatrix}\begin{bmatrix} V_C & 0 \\ 0 & V_C \end{bmatrix}(CZ \otimes I)$$
$$= \begin{bmatrix} W_A V_C & 0 \\ 0 & (Z \otimes I) W_A B V_C (Z \otimes I) \end{bmatrix} \quad (6)$$

and decomposed as a regular multiplexor, using the method described in Sec. IV B.



This saves two CNOTs for every step of the recursion, for a total savings of $2 \times (4^{n-2} - 1)/3$ CNOT gates when stopping the recursion at generic two-qubit gates.

C. Gate count

Figure 2 shows the structure of the circuit after the decomposition of a generic three-qubit gate. For a three-qubit unitary, the decomposition results in four generic two-qubit gates. Three of these require two CNOTs to implement, while the last one requires three CNOTs. The left and right controlled R_z gates both need three CNOTs and the middle uniformly controlled R_z gate requires four CNOTs to decompose. That makes the total CNOT count for the decomposition of a three-qubit unitary: $3 \times 2 + 3 + 2 \times 3 + 4 = 19$ CNOT gates.

To find the number of CNOT gates required for implementing bigger operators, we start with the recursive relation below. An n-qubit unitary requires c_n CNOTs, which are at most:

$$c_n \leq 4 \times c_{n-1} - 3 + 3 \times 2^{n-1} - 2$$
$$\leq 4 \times c_{n-1} + 3 \times 2^{n-1} - 5.$$

This breaks down as follows: at each level of the recursion, the CNOT count is the sum of the CNOTs required for the decompositions of the four smaller unitaries (c_{n-1}) and the CNOTs required by the three quantum multiplexors (2^{n-1}). Three of the smaller unitaries can be implemented using one CNOT less by applying the optimization presented in Sec. V A, and two of the multiplexors can be implemented using one less CNOT using the method in Sec. V B.

A two-qubit unitary operator can be decomposed using at most three CNOTs ($c_2 \leq 3$), the recursive relations for three, four, and five qubit unitary operators are given

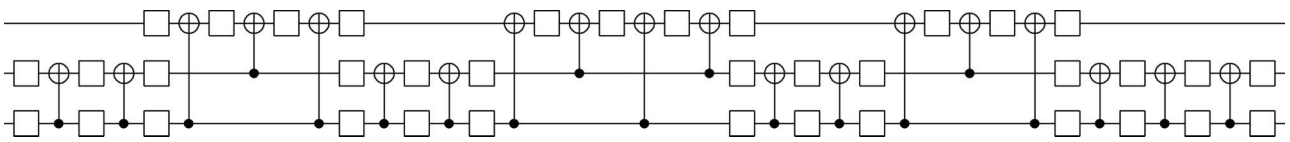


FIG. 2. Decomposition of a three-qubit gate using 19 CNOTs and 37 single-qubit gates.

below.

$$
\begin{aligned}
c_3 &\leq 4 \times c_2 + 3 \times 2^{3-1} - 5 \\
c_4 &\leq 4 \times c_3 + 3 \times 2^{4-1} - 5 \\
&\leq 4 \times 4 \times c_2 + 4 \times 3 \times 2^{4-2} - 4 \times 5 + 3 \times 2^{4-1} - 5 \\
&\leq 4^2 \times c_2 + 3 \times 2^{4-1}(4 \times 2^{-1} + 1) - 5 \times (4+1) \\
c_5 &\leq 4^3 \times c_2 + 3 \times 2^{5-1}(4^2 \times 2^{-2} + 4 \times 2^{-1} + 1) \\
&\quad - 5 \times (4^2 + 4 + 1) \\
&\leq 4^3 \times c_2 + 3 \times 2^{5-1}(2^2 + 2^1 + 1) \\
&\quad - 5 \times (4^2 + 4 + 1).
\end{aligned}
$$

We can recognize the following structure [35]:

$$
1 + x + x^2 + \cdots + x^n = \frac{x^{n+1} - 1}{x - 1}.
$$

We can use this to derive the following relation for the CNOT count for the decomposition of an n-qubit unitary gate:

$$
\begin{aligned}
c_n &\leq 4^{n-2} \times c_2 + 3 \times 2^{n-1}\left(\frac{2^{(n-3)+1} - 1}{2 - 1}\right) \\
&\quad - 5\left(\frac{4^{(n-3)+1} - 1}{4 - 1}\right) \\
c_n &\leq 4^{n-2} \times c_2 + 3 \times 2^{n-1}(2^{n-2} - 1) - \frac{5}{3}(4^{n-2} - 1) \\
c_n &\leq \left(4^{-2} \times c_2 + 3 \times 2^{-3} - \frac{5}{3} \times 4^{-2}\right) \\
&\quad \times 4^n - 3 \times 2^{-1} \times 2^n + \frac{5}{3}.
\end{aligned}
$$

With $c_2 \leq 3$, we get the following CNOT count for the decomposition of an n-qubit unitary gate:

$$
\begin{aligned}
c_n &\leq \left(\frac{3}{16} + \frac{3}{8} - \frac{5}{48}\right) \times 4^n - \frac{3}{2} \times 2^n + \frac{5}{3} \\
c_n &\leq \frac{22}{48} \times 4^n - \frac{3}{2} \times 2^n + \frac{5}{3}.
\end{aligned}
$$

VI. CONCLUSION

In this paper, we presented an alternative quantum decomposition method that is able to produce circuits with a gate count that is lower than existing state-of-the-art quantum decomposition methods. We used the optimizations presented by Refs. [17] and [18], gate commutation and gate merging to optimize the block-ZXZ decomposition [28]. The decomposition follows the same structure of the well-known quantum Shannon decomposition, and has the same benefit of using recursion on generic quantum gates. This means that the decomposition can take advantage of the known optimal decompositions for two-qubit unitary gates, and other small-circuit optimizations, heuristic methods or optimal decompositions for three or more qubit gates when these become available.

Other than general unitary gates, the decomposition uses only single-qubit gates and diagonal gates. This simplifies the structure and presents further opportunity for optimizations, such as accounting for specific hardware constraints like connectivity.

The circuit output of the decomposition can be compiled to any universal gateset. The resulting circuit will have the same overall structure with an equal number of two-qubit gates when the gateset includes a two-qubit gate that is equivalent to the CNOT gate up to single-qubit gates. This is the case for, among others, the CZ gate (part of the native gateset of the IBM Heron) [10], the ECR gate (IBM Eagle) [36], and the XX gate (trapped ions) [2]. The compilation to a different type of two-qubit gate will add additional single-qubit gates, but many of these can be merged into neighboring (generic) gates.

If these circuits are executed on a quantum execution platform, which has a more permissive gateset, the diagonal gates can also be implemented with uniformly controlled Z gates [37] instead of CNOTs. QR, QSD, and Cartan decompositions have also been generalized to higher-dimensional quantum systems [38], which may offer practical advantage over two-level qubits [39]. If our decomposition is also generalizable to multilevel quantum systems, it may result in more optimal gate counts for these types of systems as well.

As can be seen in Table I, our approach improves upon the previous record holder by $(4^{n-2} - 1)/3$ CNOT gates to achieve the best-known CNOT count for any generic quantum gate of size three or more qubits.

[1] M. Kjaergaard, M. E. Schwartz, J. Braumüller, P. Krantz, J. I.-J. Wang, S. Gustavsson, and W. D. Oliver, Superconducting qubits: Current state of play, Annu. Rev. Condens. Matter Phys. **11**, 369 (2020).

[2] C. D. Bruzewicz, J. Chiaverini, R. McConnell, and J. M. Sage, Trapped-ion quantum computing: Progress and challenges, Appl. Phys. Rev. **6**, 021314 (2019).

[3] M. V. G. Dutt, L. Childress, L. Jiang, E. Togan, J. Maze, F. Jelezko, A. S. Zibrov, P. R. Hemmer, and M. D. Lukin, Quantum register based on individual electronic and nuclear spin qubits in diamond, Science **316**, 1312 (2007).

[4] N. M. Linke, D. Maslov, M. Roetteler, S. Debnath, C. Figgatt, K. A. Landsman, K. Wright, and C. Monroe, Experimental comparison of two quantum computing architectures, Proc. Natl. Acad. Sci. **114**, 3305 (2017).

[5] V. V. Shende, I. L. Markov, and S. S. Bullock, Minimal universal two-qubit controlled-not-based circuits, Phys. Rev. A **69**, 062321 (2004).

[6] P. Rakyta and Z. Zimborás, Approaching the theoretical limit in quantum gate decomposition, Quantum **6**, 710 (2022).

[7] S. Ashhab, N. Yamamoto, F. Yoshihara, and K. Semba, Numerical analysis of quantum circuits for state preparation and unitary operator synthesis, Phys. Rev. A **106**, 022426 (2022).

[8] E. Younis, K. Sen, K. Yelick, and C. Iancu, Qfast: Quantum synthesis using a hierarchical continuous circuit space, arXiv:2003.04462.

[9] A. M. Krol, K. Mesman, A. Sarkar, and Z. Al-Ars, in *2023 IEEE International Conference on Quantum Computing and Engineering (QCE)* (IEEE Computer Society, Bellevue, WA, USA, 2023), Vol. 2, p. 103.

[10] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter, Elementary gates for quantum computation, Phys. Rev. A **52**, 3457 (1995).

[11] F. Vatan and C. Williams, Optimal quantum circuits for general two-qubit gates, Phys. Rev. A **69**, 032315 (2004).

[12] G. Vidal and C. M. Dawson, Universal quantum circuit for two-qubit transformations with three controlled-not gates, Phys. Rev. A **69**, 010301(R) (2004).

[13] P. B. M. Sousa and R. V. Ramos, Universal quantum circuit for N-qubit quantum gate: A programmable quantum gate, Quantum Inf. Comput. **7**, 228 (2007).

[14] J. J. Vartiainen, M. Möttönen, and M. M. Salomaa, Efficient decomposition of quantum gates, Phys. Rev. Lett. **92**, 177902 (2004).

[15] F. Vatan and C. P. Williams, Realization of a general three-qubit quantum gate, arXiv:quant-ph/0401178.

[16] W. Hai-Rui, D. Yao-Min, Zhang-Jie, Modified Khaneja–Glaser decomposition and realization of three-qubit quantum gate, Chin. Phys. Lett. **25**, 3107 (2008).

[17] M. Möttönen and J. J. Vartiainen, in *Trends in quantum computing research*, edited by S. Shannon (Nova Science Publishers, New York, NY, USA, 2006) Chap. 7, p. 149.

[18] V. Shende, S. Bullock, and I. Markov, Synthesis of quantum-logic circuits, IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst. **25**, 1000 (2006).

[19] G. Cybenko, Reducing quantum computations to elementary unitary operations, Comput. Sci. Eng. **3**, 27 (2001).

[20] A. V. Aho and K. M. Svore, Compiling quantum circuits using the palindrome transform, arXiv:quant-ph/0311008.

[21] C. Paige and M. Wei, History and generality of the CS decomposition, Linear Algebra Appl. **208-209**, 303 (1994).

[22] G. Golub and C. van Loan, *Matrix Computations* (Johns Hopkins University Press, Baltimore, MD, USA, 2013), 4th ed.

[23] R. R. Tucci, A rudimentary quantum compiler(2cnd ed.), arXiv:quant-ph/9902062.

[24] M. Möttönen, J. J. Vartiainen, V. Bergholm, and M. M. Salomaa, Quantum circuits for general multiqubit gates, Phys. Rev. Lett. **93**, 130502 (2004).

[25] V. V. Shende, S. S. Bullock, and I. L. Markov, A practical top-down approach to quantum circuit synthesis, arXiv:quant-ph/0406176v3.

[26] N. Khaneja and S. J. Glaser, Cartan decomposition of $Su(2^n)$ and control of spin systems, Chem. Phys. **267**, 11 (2001).

[27] M. B. Mansky, S. L. n. Castillo, V. R. Puigvert, and C. Linnhoff-Popien, Near-optimal quantum circuit construction via Cartan decomposition, Phys. Rev. A **108**, 052607 (2023).

[28] A. De Vos and S. De Baerdemacker, Block-ZXZ synthesis of an arbitrary quantum circuit, Phys. Rev. A **94**, 052317 (2016).

[29] A. De Vos and S. De Baerdemacker, in *Reversible Computation*, edited by J. Kari and I. Ulidowski (Springer International Publishing, Cham, 2018), p. 133.

[30] H. Führ and Z. Rzeszotnik, On biunimodular vectors for unitary matrices, Linear Algebra Appl. **484**, 86 (2015).

[31] E. Knill, Approximation by quantum circuits, arXiv:quant-ph/9508006.

[32] A. M. Krol, A. Sarkar, I. Ashraf, Z. Al-Ars, and K. Bertels, Efficient decomposition of unitary matrices in quantum circuit compilers, Appl. Sci. **12**, 759 (2022).

[33] F. Gray, Pulse code communication, U.S. Patent no. 2,632,058 (1953).

[34] V. V. Shende, I. L. Markov, and S. S. Bullock, in *Proceedings Design, Automation and Test in Europe Conference and Exhibition* (IEEE, Paris, France, 2004), Vol. 2, p. 980.

[35] J. M. Cargal, in *Discrete Mathematics for Neophytes: Number Theory, Probability, Algorithms, and Other Stuff* (cargalmathbooks.com, 1991) Chap. 31, http://www.cargalmathbooks.com/lectures.htm.

[36] P. Jurcevic, *et al.*, Demonstration of quantum volume 64 on a superconducting quantum computing system, Quantum Sci. Technol. **6**, 025020 (2021).

[37] K. M. Nakanishi, T. Satoh, and S. Todo, Quantum-gate decomposer, arXiv:2109.13223.

[38] G.-L. Jiang, W.-Q. Liu, and H.-R. Wei, Optimal quantum circuits for general multi-qutrit quantum computation, Adv. Quantum Technol. **7**, 2400033 (2024).

[39] B. P. Lanyon, M. Barbieri, M. P. Almeida, T. Jennewein, T. C. Ralph, K. J. Resch, G. J. Pryde, J. L. O'brien, A. Gilchrist, and A. G. White, Simplifying quantum logic using higher-dimensional Hilbert spaces, Nat. Phys. **5**, 134 (2009).