


Near-optimal quantum circuit construction via Cartan decomposition

Maximilian Balthasar Mansky,^{*} Santiago Londoño Castillo[✉], Victor Ramos Puigvert, and Claudia Linnhoff-Popien
Department of Informatics, LMU Munich, 80538 Munich, Germany

 (Received 10 January 2023; revised 30 May 2023; accepted 2 August 2023; published 15 November 2023)

We show the applicability of the Cartan decomposition of Lie algebras to quantum circuits. This approach can be used to synthesize circuits that can efficiently implement any desired unitary operation. Our method finds explicit quantum circuit representations of the algebraic generators of the relevant Lie algebras allowing the direct implementation of a Cartan decomposition on a quantum computer. The construction is recursive and allows us to expand any circuit down to generators and rotation matrices on individual qubits, where through our recursive algorithm we find that the generators themselves can be expressed with controlled-NOT (CNOT) and SWAP gates explicitly. Our approach is independent of the standard CNOT implementation and can be easily adapted to other cross-qubit circuit elements. In addition to its versatility, we also achieve near-optimal counts when working with CNOT gates, achieving an asymptotic CNOT cost of $\frac{21}{16}4^n$ for n qubits.

DOI: [10.1103/PhysRevA.108.052607](https://doi.org/10.1103/PhysRevA.108.052607)

I. INTRODUCTION

Quantum computing relies on a quantum circuit to translate an algorithm to work on a quantum computer. The circuit expresses the physical actions that are necessary to create a particular quantum-mechanical state and whose measurement provides the output of the calculation. Every circuit is equivalent to a unitary transformation in $SU(2^n)$, where n refers to the number of qubits. The mapping is injective, in the sense that two different circuits can perform the same calculation and correspond to the same transformation U [1]. Consequently, circuits of different lengths can perform the same circuit. In most cases, the shorter circuit is preferable, since it reduces the execution time, imprecision due to hardware limitations, or, on noisy systems, reductions of noise due to fewer actual operations. Various methods can be employed to optimize circuits [2–4]; however, before optimization, the circuit must first be constructed.

There are several ways to construct quantum circuits. One can construct an algorithm along a schema—the well-known algorithms of Shor [5] and Grover [6] work in this way and can be scaled to the required system size by following the schema. Finding new schematic algorithms and showing their speed-up compared with classical methods is its own field of research. So far, the number of discovered algorithms is limited [7,8].

An alternative is to use a parametrized circuit and modify the parameters until the circuit fits the desired output. The approach is called quantum machine learning [9–11]. Similar to classical machine learning, some quantum circuit ansatz

is chosen, often with distinct layers of repeated subcircuits, which is then trained with some classical feedback loop to approximate a desired solution.

In our work, we provide a solution to a third approach, decomposing a known unitary matrix into its corresponding quantum circuit. We can build circuits for any arbitrary target, not just the ones for which we have schemas, and also with known performance, as we know the number of required CNOT gates. Our approach provides a direct method for translating a unitary operation U to an explicit quantum circuit.

The developed algorithm generalizes the unstructured circuit decomposition of a three-qubit unitary, done in [12], to an n -qubit unitary by using a recursive method. The mathematics upon which this recursive algorithm is constructed is based on the work of Khaneja and Glaser [13]. Underlying our construction is the Cartan decomposition of a unitary $U \in SU(2^n)$ into four terms $K_1 \exp(z_1) K_2 \exp(y) K_3 \exp(z_2) K_4$, where all K_i are part of the next-lower dimension group $K_i \in SU(2^{n-1}) \otimes U(1)$, and z_i and y are algebra elements belonging to certain Cartan subalgebras. We show that this argument is recursive and allows us to decompose any unitary into components that can be easily represented in a quantum circuit. This is described in Sec. III A.

The orthogonal elements $\exp(z_i)$ and $\exp(y)$ in the Cartan decomposition are created through the generators of the Lie subalgebras and will ultimately contain the only cross-qubit elements in the circuit. To express them in terms of circuit elements, we make use of a block-diagonal decomposition to the elements of the algebra. This form is easily expressible in terms of CNOTs and elementary rotations, described in detail in Sec. IV.

We also assess the performance of our algorithm as expressed by the number of CNOTs that an arbitrary circuit requires in the worst case. The number of gates can be determined analytically; see Sec. VI. There we also compare our CNOT count to other methods decomposing a unitary [3,14–17], and we also provide an outlook of future work in Sec. VII.

^{*}maximilian-balthasar.mansky@ifi.lmu.de

Published by the American Physical Society under the terms of the Creative Commons Attribution 4.0 International license. Further distribution of this work must maintain attribution to the author(s) and the published article's title, journal citation, and DOI.

II. RELATED WORK

We provide a general overview of some of the most relevant algorithms for the synthesis of general multiqubit gates: cosine-sine decomposition [16], optimized quantum Shannon decomposition (QSD) [17], and Khaneja-Glaser decomposition [13]. The theory behind the Khaneja-Glaser decomposition is discussed in more detail, as our work relies on the mathematical structure and extends their work to an arbitrary number of qubits.

A. Cosine-sine decomposition

One way to realize a general $SU(2^n)$ matrix on a quantum computer is via matrix factorization, where the initial matrix is separated into a product of matrices which can be more easily implemented as a quantum circuit. Such a factorization can be recursively achieved by using the cosine-sine decomposition (CSD) [18]. In general, the CSD of a $SU(2^n)$ matrix U can be written as follows:

$$U = U_1^1 A_1^1 \tilde{U}_2^1 = \begin{pmatrix} u_{11}^1 & 0 \\ 0 & u_{12}^1 \end{pmatrix} \begin{pmatrix} c_{11}^1 & s_{11}^1 \\ -s_{11}^1 & c_{11}^1 \end{pmatrix} \begin{pmatrix} \tilde{u}_{21}^1 & 0 \\ 0 & \tilde{u}_{22}^1 \end{pmatrix}. \tag{1}$$

This decomposition can be applied recursively to the submatrices U_j^i until a 2×2 block-diagonal form is obtained.

In [18], it is shown that the matrices resulting from the above decomposition can be attained as a product of uniformly controlled rotations. After canceling some of the occurring CNOT gates using reflection symmetries of the circuit, and using a method for implementing uniformly controlled gates described in the paper, the authors show that a general CSD of a $SU(2^n)$ matrix, as shown in Eq. (1), can be implemented using $4^n - 2^{n+1}$ CNOT gates and 4^n one-qubit gates.

B. Optimized quantum Shannon decomposition

Another way to decompose a generic unitary matrix is by generalizing the concepts of Boolean algebra and logic conditionals to quantum circuits. By interpreting the qubits as the predicates and requiring the action of clauses to be unitary, operations in a quantum circuit can then be interpreted as quantum conditionals. In [17], the authors introduce *quantum multiplexors* as quantum circuit blocks implementing quantum conditionals, e.g., the CNOT gate is the simplest two-qubit multiplexor. To perform the decomposition of a unitary matrix, the authors provide a generalization to quantum circuits of the classical Shannon decomposition theorem, which allows any Boolean function F to be factorized as $F = xF_x + \bar{x}F_{\bar{x}}$, where x is a variable and \bar{x} is its complement. The proposed quantum Shannon decomposition (QSD) theorem states that an arbitrary n -qubit operator can be implemented by a circuit containing three multiplexed rotations and four generic $(n - 1)$ -qubit operators. This provides a method to recursively decompose a generic $SU(2^n)$ operator. Applying this theorem to the previously discussed CSD, see Sec. II A, and by providing a method to implement multiplexed- R_y rotations using Controlled-Z gates, the authors showed that the number of CNOT gates required to decompose an $SU(2^n)$ matrix can be

TABLE I. Comparison of different methods for the number of CNOT gates necessary for synthesizing an n -qubit unitary. The Khaneja-Glaser decomposition of a unitary is a factor of 5 from the lower theoretical bound.

Algorithm	CNOT gate count
Original decomp. [14]	$O(n^3 4^n)$
Asymptotic decomp. [3]	$O(n 4^n)$
Gray codes [15]	$O(4^n)$
Cosine-Sine decomp. [16]	$4^n - 2^{n+1}$
Optimized QSD [17]	$\frac{23}{48} 4^n - \frac{3}{2} 2^n + \frac{4}{3}$
KG Cartan decomposition	$\frac{21}{16} 4^n - 3(n 2^{n-2} + 2^n)$
Theoretical lower bound [24]	$\lceil \frac{1}{4}(4^n - 3n - 1) \rceil$

reduced to $\frac{23}{48} 4^n - \frac{3}{2} 2^n + \frac{4}{3}$, a significant improvement from the previously discussed CSD.

Both approaches use post-circuit creation optimization to improve their count of operations. We compare the achieved CNOT counts with our own in Table I.

III. CARTAN DECOMPOSITION

The Cartan decomposition method is a powerful tool in the realm of Lie group decomposition. It allows us to break down a given Lie group into smaller, simpler subgroups, which can be much easier to work with. This method has found numerous applications in a variety of fields, including physics, engineering, and computer science. Building upon the work of Khaneja and Glaser, we have extended their method, which uses the Cartan decomposition of a Lie group, to be applicable to an arbitrary system size.

A. Khaneja-Glaser decomposition

The underlying mathematics here relies on the work of Cartan [19,20] in French and is by now part of the standard knowledge of physics and mathematics. For an English language introduction to Lie groups and algebras, see, e.g., [21]. Throughout this paper, let G be a compact semisimple Lie group with identity e , and let \mathfrak{g} denote its Lie algebra. Moreover, let K denote a compact closed subgroup of G . Note that, given that \mathfrak{g} is a semisimple algebra there exists, due to Cartan’s criterion, a nondegenerate Killing form inducing a bi-invariant metric $\langle \cdot, \cdot \rangle_G$ on G , which allows the sum decomposition of \mathfrak{g} into subalgebras.

Throughout this paper, capital letters identify groups. Capital letters with subscripts identify elements of the group. The algebras are denoted by lowercase fraktur letters, and elements thereof by lowercase letters. Pauli matrices are referenced by their standard σ_i . We also make use of the following notation for generalized Pauli matrices:

$$x_k \equiv \mathbb{1} \otimes \dots \otimes \mathbb{1} \otimes \sigma_x \otimes \mathbb{1} \otimes \dots \otimes \mathbb{1},$$

where the Pauli matrix σ_x acts on the k th qubit. Matrices for the rotations around σ_y and σ_z are constructed similarly and denoted y_k and z_k , respectively.

Definition III.1 (Cartan decomposition of \mathfrak{g}). Let \mathfrak{g} and \mathfrak{l} be the two real semisimple Lie algebras of G and K , respectively. Then, $(\mathfrak{g}, \mathfrak{l})$ is called an *orthogonal symmetric Lie algebra pair*

if the decomposition $\mathfrak{g} = \mathfrak{m} \oplus \mathfrak{l}$, where $\mathfrak{m} = \mathfrak{l}^\perp$, satisfies the following commutation relations:

- (i) $[\mathfrak{l}, \mathfrak{l}] \subset \mathfrak{l}$.
- (ii) $[\mathfrak{m}, \mathfrak{l}] = \mathfrak{m}$.
- (iii) $[\mathfrak{m}, \mathfrak{m}] \subset \mathfrak{l}$.

The direct sum decomposition $\mathfrak{g} = \mathfrak{m} \oplus \mathfrak{l}$ is then called a Cartan decomposition of the Lie algebra \mathfrak{g} .

Definition III.2 (Cartan subalgebra). Let $(\mathfrak{g}, \mathfrak{l})$ be an orthogonal symmetric Lie algebra pair of the groups G and K . A maximal subalgebra \mathfrak{h} of \mathfrak{m} is called a *Cartan subalgebra* of $(\mathfrak{g}, \mathfrak{l})$.

In [13] it is shown that the Lie algebra $\mathfrak{su}(2^n)$ defined by

$$\mathfrak{su}(2^n) = \text{span}\{a \otimes \sigma_x, b \otimes \sigma_y, c \otimes \sigma_z, d \otimes \mathbb{1}, ix_n, iy_n, iz_n | a, b, c, d \in \mathfrak{su}(2^{n-1})\}$$

has a Cartan decomposition $\mathfrak{su}(2^n) = \mathfrak{su}_m(2^n) \oplus \mathfrak{su}_l(2^n)$, where

$$\begin{aligned} \mathfrak{su}_m(2^n) &= \text{span}\{a \otimes \sigma_x, b \otimes \sigma_y, ix_n, iy_n | a, b \in \mathfrak{su}(2^{n-1})\} \\ \mathfrak{su}_l(2^n) &= \text{span}\{c \otimes \sigma_z, d \otimes \mathbb{1}, iz_n | c, d \in \mathfrak{su}(2^{n-1})\}. \end{aligned}$$

Theorem III.1 (Cartan decomposition of G). Let \mathfrak{g} be a semisimple Lie algebra of the group G and let $\mathfrak{g} = \mathfrak{m} \oplus \mathfrak{l}$ be its Cartan decomposition. Moreover, let \mathfrak{h} be a Cartan subalgebra of $(\mathfrak{g}, \mathfrak{l})$ and let K be a compact closed subgroup of G . Then,

$$G = K \exp(\mathfrak{h})K, \tag{2}$$

where $\exp(\mathfrak{h}) \subset G$. This decomposition is then called the *Cartan decomposition* of the Lie group G .

The decomposition of the Lie group G into two groups K linked by a determinable element of the algebra is the heart of our algorithm. In terms of the actual elements of the group, we obtain a structure as below.

Corollary III.1. Let $U \in \text{SU}(2^n)$ be an n -qubit unitary operator. Then it has a decomposition

$$U = K_1 \exp(y)K_2 \tag{3}$$

where $K_i \in \exp(\mathfrak{su}_l(2^n))$ and for some $y \in \mathfrak{h}$, where \mathfrak{h} is a Cartan subalgebra of $(\mathfrak{su}(2^n), \mathfrak{su}_l(2^n))$.

In [13] it is proven that $K_i \in \exp(\mathfrak{su}_l(2^n)) \cong \text{SU}(2^{n-1}) \otimes \text{SU}(2^{n-1}) \otimes \text{U}(1)$ so that the unitaries K_i have again a Cartan decomposition. This provides a recursive algorithm for determining a unitary $U \in \text{SU}(2^n)$ by successive decompositions.

Theorem III.2. The direct sum decomposition

$$\mathfrak{su}_l(2^n) = \mathfrak{su}_{l_0}(2^n) \oplus \mathfrak{su}_{l_1}(2^n), \tag{4}$$

where

$$\begin{aligned} \mathfrak{su}_{l_0}(2^n) &= \text{span}\{c \otimes \sigma_z | c \in \mathfrak{su}(2^{n-1})\}, \\ \mathfrak{su}_{l_1}(2^n) &= \text{span}\{d \otimes \mathbb{1}, iz_n | d \in \mathfrak{su}(2^{n-1})\} \end{aligned}$$

is a Cartan decomposition of the Lie algebra $\mathfrak{su}_l(2^n)$.

The proof of this theorem can also be found in [13].

Corollary III.2. Let $V \in \exp(\mathfrak{su}_l(2^n))$ be an n -qubit operator. Then it has a unique decomposition

$$V = K_1 \exp(z)K_2, \tag{5}$$

where $K_i \in \text{SU}(2^{n-1}) \otimes \text{U}(1)$ and for some $z \in \mathfrak{f}$, where \mathfrak{f} is a Cartan subalgebra of $(\mathfrak{su}_l(2^n), \mathfrak{su}_{l_0}(2^n))$.

Corollary III.3. Let $U \in \text{SU}(2^n)$ be an n -qubit unitary operator. Then it has a decomposition

$$U = K_1 \exp(z_1)K_2 \exp(y)K_3 \exp(z_2)K_4, \tag{6}$$

where $K_i \equiv A_i \otimes B_i \in \text{SU}(2^{n-1}) \otimes \text{U}(1)$, $y \in \mathfrak{h}$, and $z_i \in \mathfrak{f}$, where \mathfrak{h} is a Cartan subalgebra of $(\mathfrak{su}(2^n), \mathfrak{su}_l(2^n))$ and \mathfrak{f} is a Cartan subalgebra of $(\mathfrak{su}_l(2^n), \mathfrak{su}_{l_0}(2^n))$.

To define a Cartan subalgebra in the product operator basis for the pairs $(\mathfrak{su}(2^n), \mathfrak{su}_l(2^n))$ and $(\mathfrak{su}_l(2^n), \mathfrak{su}_{l_0}(2^n))$, we proceed analogously as in [13]. The elements of the Cartan

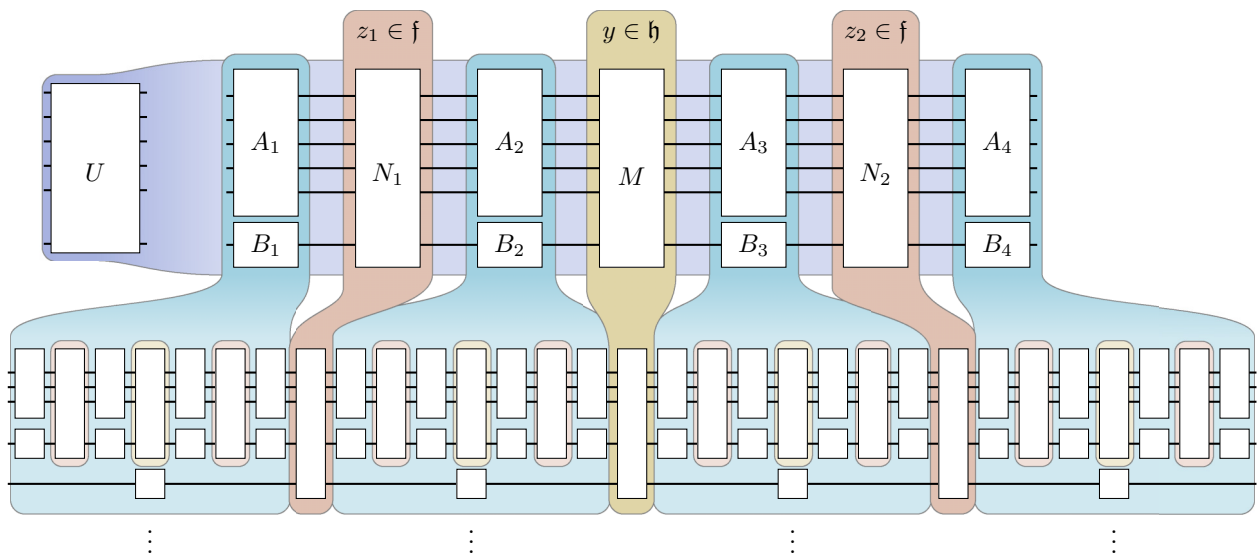


FIG. 1. Graphical representation of our work. We establish a structure from an arbitrary unitary U into circuit elements of lower dimension [$K_i = A_i \otimes B_i$, $A_i \in \text{SU}(2^{n-1})$, $B_i \in \text{U}(1)$] and n -qubit elements that generate from the algebras \mathfrak{f} and \mathfrak{h} . The algorithm is recursive for all A_i and detailed in Sec. III A. Between the recursive elements are the $(n - k)$ -qubit elements, where k refers to the number of recursions. The elements can be expressed explicitly as CNOT and SWAP elements through the block-diagonal decomposition explained in Sec. IV.

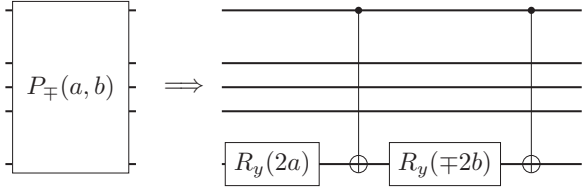


FIG. 2. Quantum circuit decomposing the unitary block-form $P_{\mp}(a, b)$ up to phase. The block-diagonal matrices $P_{\mp}(a, b)$ can always be decomposed up to a global phase by a dimensionally adapted quantum circuit, where the one-qubit gates and the target qubits have to be adjusted accordingly.

subalgebra can be generated recursively by the following equations:

$$\begin{aligned}
 \mathfrak{a}(2) &= i\{x_1x_2, y_1y_2, z_1z_2\}, & \mathfrak{b}(2) &= \emptyset, \\
 \mathfrak{s}(k) &= \bigcup_{i=2}^k \mathfrak{a}(i) \otimes \mathbb{1}^{k-i}, \\
 \mathfrak{a}(n) &= \{\alpha \otimes \sigma_x, ix_n | \alpha \in \mathfrak{s}(n-1)\}, & (7) \\
 \mathfrak{b}(n) &= \{\alpha \otimes \sigma_z | \alpha \in \mathfrak{s}(n-1)\}, \\
 \mathfrak{h}(n) &= \text{span}\{\mathfrak{a}(n)\}, \\
 \mathfrak{f}(n) &= \text{span}\{\mathfrak{b}(n)\}.
 \end{aligned}$$

This decomposition structure allows us to express any n -qubit unitary in terms of $(n - 1)$ -qubit unitaries and elements of orthogonal algebras. The circuit structure is visualized in Fig. 1. Recursively it follows that each of the A_i shown in the figure can itself be decomposed in the same way. This decomposition method of an n -qubit unitary works all the way down to $SU(4)$, the space of two-qubit operations, which can be further decomposed by $K_1 \exp(y)K_2$, where $K_i \in SU(2)$ and $y \in \mathfrak{h}(2)$ since $\mathfrak{f}(2) = \emptyset$.

It is important to note that x_1x_2 and so on are elements of the algebra, not elements of the group such as $X_1 \otimes X_2$. The corresponding group element $\exp(x_1x_2)$ is not the direct product of two X rotations but rather a two-qubit operation. Moreover, note that, for $\alpha \in \mathfrak{s}(n - 1)$, $\alpha \otimes \sigma_x$ and $\alpha \sigma_{nx}$ represent the same element, where $\sigma_{xn} \equiv x_n$.

IV. BLOCK-DIAGONAL DECOMPOSITION

By employing a recursive method, the developed algorithm extends the unstructured circuit decomposition of a three-qubit unitary, as demonstrated in [12], to an n -qubit unitary. This algorithm determines a decomposition for the generators $y \in \mathfrak{h}(n)$ and $z \in \mathfrak{f}(n)$ of the relevant Lie subalgebras ($\mathfrak{su}(2^n)$, $\mathfrak{su}_l(2^n)$) and ($\mathfrak{su}_r(2^n)$, $\mathfrak{su}_{l0}(2^n)$) using a block-diagonal matrix.

It is important to note that within these Lie subalgebras, there are always two generators constructed through the recursive equations in (7) that are proportional to each other,

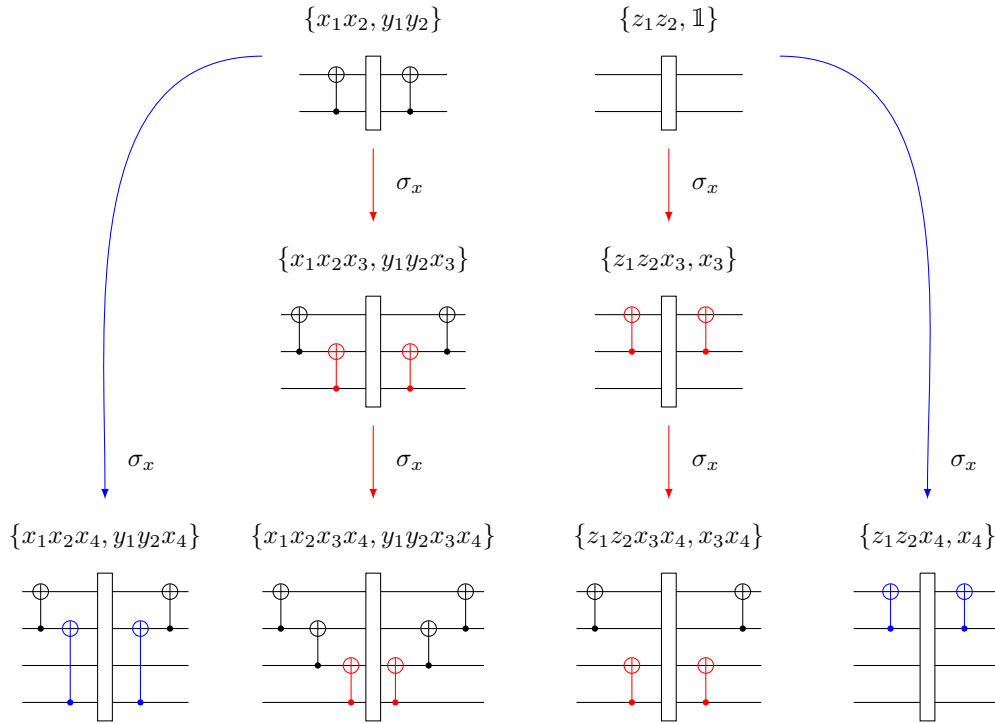


FIG. 3. Recursive algorithm showing the decomposition of the exponential operator $M = e^y$, $y \in \mathfrak{h}(4)$, where $\mathfrak{h}(4)$ is a Cartan subalgebra of ($\mathfrak{su}(16)$, $\mathfrak{su}_l(16)$). Each of the exponential operators $M_i(a_i, b_i)$ is decomposed through a circuit including a block-diagonal matrix $P_{\mp}(a_i, b_i)$, displayed as a block in the center of each diagram, which can always be synthesized by two CNOT gates and two one-qubit gates; see Fig. 2. For each $\otimes \sigma_x$, two CNOT gates are added, where the control qubit is always the n th dimension and the target qubit is given by the i th dimension of the subalgebra $\mathfrak{h}(i)$ from which it gets generated. The control qubits of the rest of the CNOT gates enlarge up to the respective n th dimension, with the exception of the outermost CNOT gates, which remain unaltered since they serve as a final permutation.

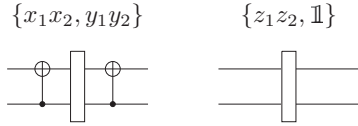


FIG. 4. Quantum circuits generating the exponentials of the generators of the Lie subalgebra $\mathfrak{h}(2)$ by using a block-diagonal form. Each of the central blocks contains an instance of the dimensionally adapted circuit shown in Fig. 2.

since x_1x_2 is proportional to y_1y_2 , and z_1z_2 is proportional to the identity. Consequently, in order to decompose the Cartan subalgebras $M = e^y$ and $N = e^z$, where $y \in \mathfrak{h}(n)$ and $z \in \mathfrak{f}(n)$ represent, respectively, the generators of the Cartan subalgebras ($\mathfrak{su}(2^n)$, $\mathfrak{su}_l(2^n)$) and ($\mathfrak{su}_l(2^n)$, $\mathfrak{su}_{l_0}(2^n)$), we group the proportional generators together and separate the exponential terms into 2^{n-2} different components $M_i(a_i, b_i)$ and $N_i(a_i, b_i)$:

$$M = e^y \equiv M_1(a_1, b_1) \cdots M_{2^{n-2}}(a_{2^{n-2}}, b_{2^{n-2}}), \quad (8)$$

$$N = e^z \equiv N_1(a_1)N_2(a_2, b_2) \cdots N_{2^{n-2}}(a_{2^{n-2}}, b_{2^{n-2}}). \quad (9)$$

An efficient way of mapping the generators to circuit elements is by means of a particular block-diagonal form:

$$P_{\mp}(a_i, b_i) = \text{diag}(p_{\mp}, \dots, p_{\mp}, p_{\pm}, \dots, p_{\pm}) \quad (10)$$

with entries

$$p_- = \begin{pmatrix} \cos(a_i - b_i) & i \sin(a_i - b_i) \\ i \sin(a_i - b_i) & \cos(a_i - b_i) \end{pmatrix}, \quad (11)$$

$$p_+ = \begin{pmatrix} \cos(a_i + b_i) & i \sin(a_i + b_i) \\ i \sin(a_i + b_i) & \cos(a_i + b_i) \end{pmatrix}.$$

The block-diagonal structure can be implemented on a quantum circuit in a straightforward way, visualized in Fig. 2. The two parameters are implemented as rotation gates on the n th wire and controlled via CNOTs from the first. The method we employ to decompose the exponential terms $M_i(a_i, b_i)$ and $N_i(a_i, b_i)$ is through a block-diagonal matrix $P_{\mp}(a, b)$. The method we found, based on the recursive algorithm (7), starts by grouping the generator $\mathfrak{a}(2)$ into its proportional terms

$$\mathfrak{a}(2) = i\{x_1x_2, y_1y_2\} \cup i\{z_1z_2, \mathbb{1}\}. \quad (12)$$

This recursive structure is illustrated in Fig. 3. The circuits corresponding to these algebra elements are shown in Fig. 4, which decomposes the block-diagonal matrix P_{\mp} . Expansion to larger elements and therefore higher-dimensional structures can be done recursively through adding more terms in the algebra. The central P_{\mp} element expands correspondingly.

We can differentiate expansion into higher dimensions along σ_x and σ_z . We find that there is a direct correspondence between enlarging the algebra and the circuit construction. Adding a σ_x to the algebra corresponds to adding a CNOT gate from the n th to the $(n-1)$ th quantum gate. For σ_z , the corresponding gate is a fermionic SWAP gate, see Fig. 5, between the same wires. This gives a circuit construction as shown in Fig. 6 for $SU(16)$. Higher dimensions work in a similar fashion and exhibit a branching structure depending on which algebra dimensions are added. This is shown in more detail in Figs. 3 and 7. The structure is also relevant for the

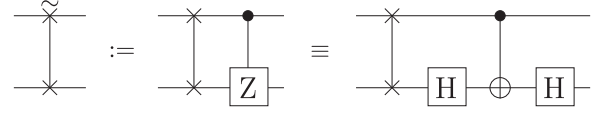


FIG. 5. Quantum circuit decomposing a fermionic SWAP gate. A fermionic SWAP can be decomposed at worst through four CNOT gates.

CNOT count, where each fermionic SWAP will count in the end as one CNOT gate; see Fig. 5. In addition to these structures, on every dimension $n \geq 3$, there is one generator $z_1z_2z_n$ of the Cartan subalgebra $\mathfrak{f}(n)$ which is more efficient to treat separately. We found that such an exponential term depending on one parameter can always be decomposed, regardless of the dimension, with a single rotation gate surrounded by four dimensionally adapted CNOT gates; see Fig. 8.

These constructions are sufficient to implement all possible algebra generators since they cover the whole subalgebra given in Definition III.2. Hence all possible unitaries $U \in SU(2^n)$ can be covered by the construction.

V. EXAMPLE

We now apply the decomposition method described above to an operator $U \in SU(8)$. Using the Cartan decomposition (6), the following decomposition is obtained:

$$U = K_1 \exp(z_1)K_2 \exp(y)K_3 \exp(z_3)K_4,$$

where $K_i \in SU(4) \otimes U(1)$, and $z \in \mathfrak{h}(3)$ and $y \in \mathfrak{f}(3)$, where $\mathfrak{h}(3)$ is a Cartan subalgebra of ($\mathfrak{su}(8)$, $\mathfrak{su}_l(8)$) and $\mathfrak{f}(3)$ is a Cartan subalgebra of ($\mathfrak{su}_l(8)$, $\mathfrak{su}_{l_0}(8)$). The elements of the Lie subalgebra are generated by (7) and thus given by

$$\mathfrak{h}(3) = \text{span } i\{x_1x_2x_3, y_1y_2x_3\} \cup i\{z_1z_2x_3, x_3\},$$

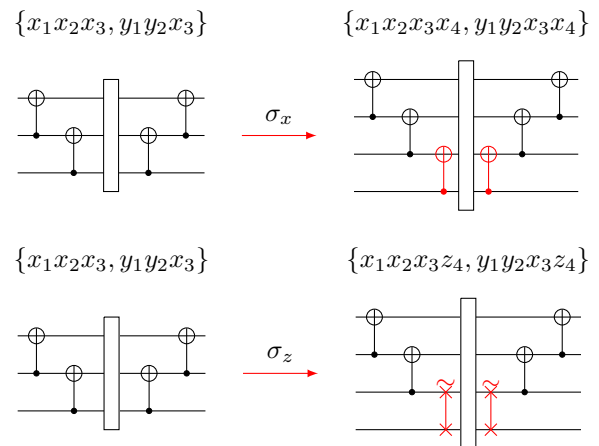


FIG. 6. Quantum circuits decomposing the exponential terms $M_1(a_1, b_1) = e^{i(a_1x_1x_2x_3x_4 + b_1y_1y_2x_3x_4)}$ (top) and $N_2(a_2, b_2) = e^{i(a_2x_1x_2x_3z_4 + b_2y_1y_2x_3z_4)}$ (bottom). The action of $\otimes\sigma_x$ introduces two additional CNOT gates, and the action of $\otimes\sigma_z$ adds two additional SWAP gates, whose target qubits are given by the subalgebra $\mathfrak{h}(3)$. The rest of the control qubits in $\mathfrak{h}(4)$ enlarge up to the fourth dimension with the exception of the outermost CNOT gates, which serve only as a final diagonal permutation.

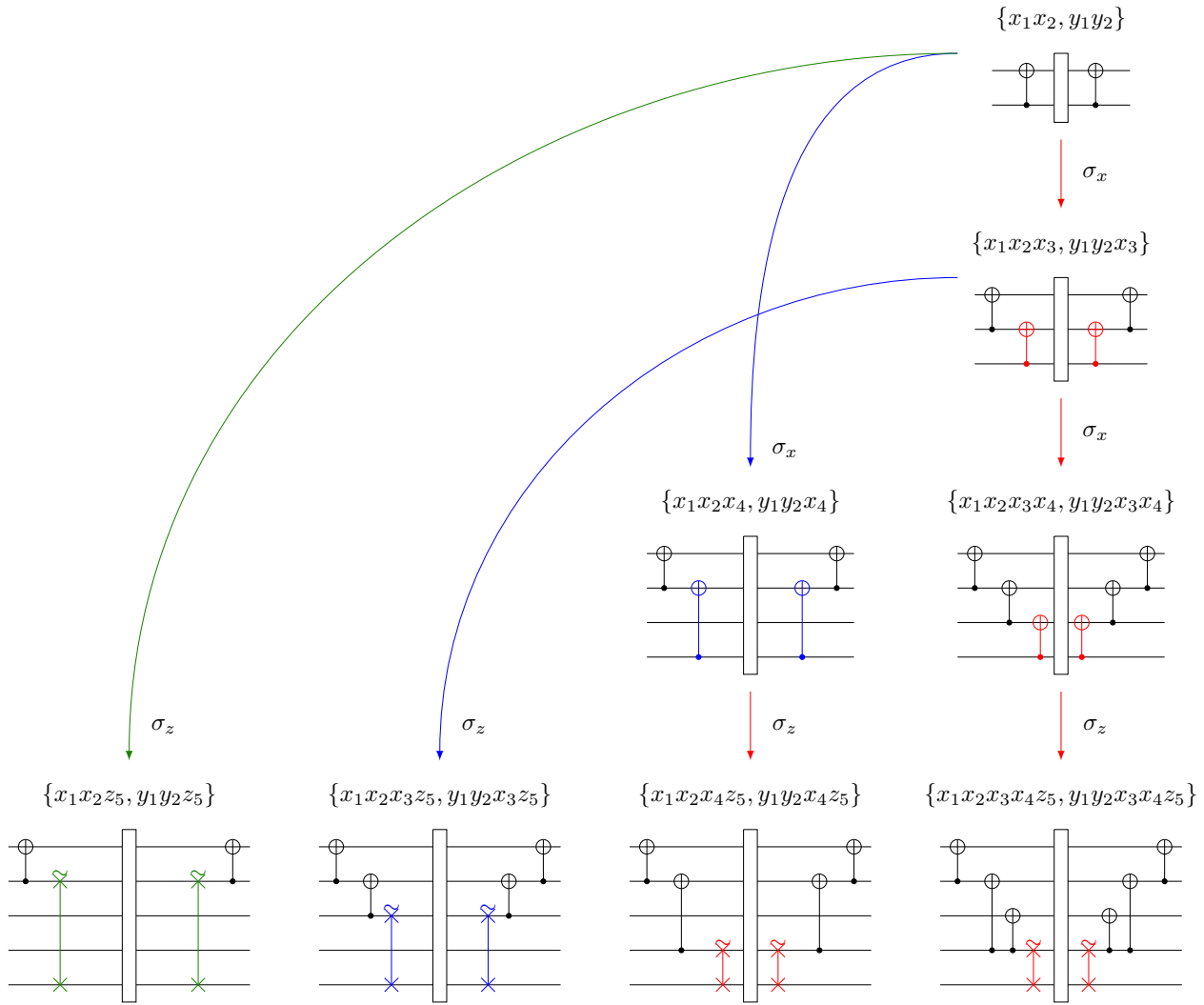


FIG. 7. Recursive algorithm displaying how a part of the Cartan subalgebra $\mathfrak{f}(5)$ gets generated. For each $\otimes\sigma_x$, two CNOT gates are added, while for each $\otimes\sigma_z$ two SWAP gates are added. The control qubit of the additional gates is always the n th dimension, while the target qubit is given by the i th dimension of the subalgebra $\mathfrak{h}(i)$ from which it is generated, with the exception of the outermost always unaltered CNOT gates, which serve only as a final diagonal permutation. Moreover, for each $\otimes\sigma_x$ the control qubit of the rest of the CNOT gates enlarges up to the respective n th dimension.

$$\mathfrak{f}(3) = \text{span } i\{x_1x_2z_3, y_1y_2z_3\} \cup i\{z_1z_2z_3\},$$

where we have already grouped the proportional terms.

By means of the recursive algorithm introduced previously, we decompose the exponential terms of the generators of

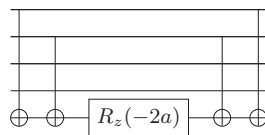


FIG. 8. Quantum circuit decomposing the exponential term $N(a) = e^{iaz_1z_2z_5} \equiv \text{diag}(z_1z_2z_5) \in \text{SU}(32)$. This quantum circuit appears for all $n \geq 3$ dimensions, where the target qubits and the one-qubit gate have to be adjusted according to the dimension of the quantum circuit.

this subalgebra through a quantum circuit including a block-diagonal form $P_{\mp}(a, b)$. For instance, the unitary $M_1(a_1, b_1)$ defined by

$$M_1(a_1, b_1) = e^{i(a_1x_1x_2x_3 + b_1y_1y_2x_3)}, \tag{13}$$

which denotes the exponential of the generators $\{x_1x_2x_3, y_1y_2x_3\}$, is decomposed through the quantum circuit shown in Fig. 9 below, where the white box denotes the block-diagonal operator $P_{\mp}(a_1, b_1)$.

The rest of the generators can be decomposed by following the same algorithm introduced in the previous section; see Figs. 9 and 10. The exponential term involving the generator $\{z_1z_2z_3\}$ can always be generated by an analogous quantum circuit such as the one shown in Fig. 8 involving four CNOT gates and one one-qubit gate. The entire construction can be seen in Fig. 1.

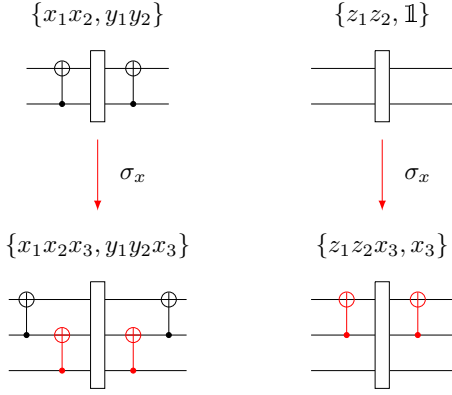


FIG. 9. Recursive algorithm showing how to decompose the unitaries $M_1(a_1, b_1) = e^{i(a_1x_1x_2x_3+b_1y_1y_2x_3)}$ and $M_2(a_2, b_2) = e^{i(a_2z_1z_2x_3+b_2x_3)}$ generated from the respective subalgebra elements $\{x_1x_2, y_1y_2\}$ and $\{z_1z_2, \mathbb{1}\}$ of $\mathfrak{a}(2)$ by tensoring with σ_x . For every tensor product with a σ_x matrix, there is an additional CNOT gate on each side whose target qubit is given by $\mathfrak{h}(2)$, with the exception of the outer CNOT gates since they serve only as a final diagonal permutation.

By just counting, we can see that there are six CNOT gates and two block-diagonal P_{\mp} matrices decomposing the exponential terms $M_1(a_1, b_1) = e^{i(a_1x_1x_2x_3+b_1y_1y_2x_3)}$ and $M_2(a_2, b_2) = e^{i(a_2z_1z_2x_3+b_2x_3)}$. To decompose the exponential terms $N_1(c_1, d_1) = e^{i(c_1x_1x_2z_3+d_1y_1y_2z_3)}$ and $N_2(c_2) = e^{ic_2z_1z_2z_3}$ there are six CNOT gates, two fermionic SWAP gates, and one block-diagonal P_{\mp} matrix. Therefore, to decompose a unitary U in $SU(8)$ we need a total of 54 CNOT gates, where we have assumed that every two-qubit circuit can be decomposed at most by three CNOT gates and every fermionic SWAP gate by at most three CNOT gates. It is possible to get rid of the SWAP gates by interchanging the roles of the second and the third qubit and thus reduce the number of CNOT gates to 42.

Although this is slightly worse than the previous unstructured Cartan decomposition method [12] of a three-qubit unitary, which required a total of 40 CNOT gates, it is possible

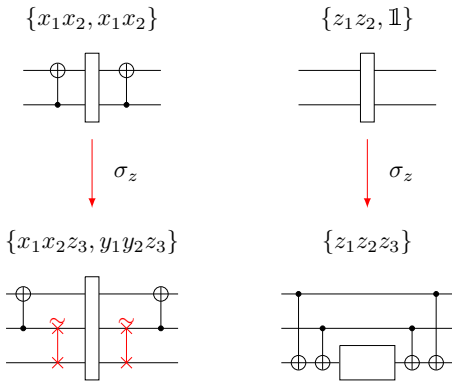


FIG. 10. Recursive algorithm showing how the exponential elements coming from the terms in the subalgebra $\mathfrak{h}(2)$ by tensoring with σ_z are generated by adding a fermionic SWAP gate on each side. However, the exponential term which comes from $\{z_1z_2z_3\}$ and depends only on one parameter has to be treated separately; see Fig. 8.

to further improve the cost to 38 CNOT gates by absorbing some of the CNOT gates by the neighboring $A_i \in SU(4)$ unitaries, which can be seen represented in Fig. 1.

VI. NUMBER OF CNOT GATES

To determine the amount of CNOT gates required, let C_n denote the number of CNOT gates coming directly from the diagram decomposition for $SU(2^n)$, where $C_{\mathfrak{h}(n)}$ specifies the number of CNOT gates required to synthesize the exponential operator $M = e^v$, and $C_{\mathfrak{f}(n)}$ specifies the number of CNOT gates required to synthesize the exponential operator $N_i = e^{z_i}$. From Corollary III.3 follows then $C_n = C_{\mathfrak{h}(n)} + 2C_{\mathfrak{f}(n)}$. Since the amount of CNOT gates in the recursive algorithm of the Cartan subalgebra $\mathfrak{h}(n)$ follows the same structure as Pascal's triangle, $C_{\mathfrak{h}(n)}$ is given by the following equation:

$$C_{\mathfrak{h}(n)} = \sum_{k=0}^{n-2} \binom{n-2}{k} 2(k+1)\text{CNOT} + 2^{n-2}P_{\mp}, \quad (14)$$

where P_{\mp} denotes the block-diagonal matrices, which always consist of two CNOT gates and two one-qubit gates; see Fig. 2. To count the number of CNOT gates for $C_{\mathfrak{f}(n)}$, note that the FSWAP gate consists of a SWAP gate followed by two Hadamard gates and one CNOT. Note that all occurring FSWAPs are adjacent to the block-diagonal matrix P_{\mp} and therefore we can get rid of the internal SWAPs by manually adjusting the one-qubit and the dimension of the target qubits of the block-diagonal matrix. Thus, in terms of CNOTs, adding a pair of FSWAPs effectively introduces two CNOTs. Moreover, the number of CNOT gates in the recursive algorithm of $\mathfrak{f}(n)$ also follows the structure of Pascal's triangle,

$$C_{\mathfrak{f}(n)} = \sum_{k=1}^{n-2} \binom{n-2}{k} 2(k+1)\text{CNOT} + (2^{n-2} - 1)P_{\mp} + \text{diag}(z_1z_2z_n), \quad (15)$$

where $\text{diag}(z_1z_2z_n)$ denotes the generator $z_1z_2z_n$ that is not proportional to any other generator and which always consists, regardless of the dimension, of four CNOT gates and one-qubit gate; see Fig. 8.

Hence, the number of CNOT gates C_n required to synthesize the exponential operators is

$$C_n = 6 \sum_{k=0}^{n-2} \binom{n-2}{k} (k+1)\text{CNOT} + 3 \left(2^{n-2} - \frac{2}{3} \right) P_{\mp} + 2 \text{diag}(z_1z_2z_n) - 4 = 6 \sum_{k=0}^{n-2} \binom{n-2}{k} (k+1) + \frac{3}{2} 2^n, \quad (16)$$

where we used the fact that every block-diagonal matrix P_{\mp} can be decomposed by two CNOT gates; see Fig. 2. This binomial sum can be determined by means of the following identities:

$$\sum_{k=0}^n \binom{n}{k} = 2^n, \quad \sum_{k=0}^n k \binom{n}{k} = n2^{n-1}. \quad (17)$$

Therefore, C_n is given by

$$C_n = 3 \times (2^{n-1} + n2^{n-2}). \quad (18)$$

To determine the entire number of CNOT gates for a unitary $U \in \text{SU}(2^n)$, we also need to take into consideration the CNOT gates that recursively come from lower dimensions; see Eq. (6) and its corresponding Fig. 1. To that end, let T_n denote the total number of CNOT gates for a unitary $U \in \text{SU}(2^n)$. By Corollary III.3, which follows from the decomposition of a unitary, we have that the total number of CNOT gates for a unitary U in $\text{SU}(2^n)$ is given by

$$\begin{aligned} T_n &= C_n + 4C_{n-1} + 4^2C_{n-2} + \dots = \sum_{i=2}^n 4^{n-i}C_i \\ &= 4^{n-2}C_2 + 3 \times 2^{n-3}[3 \times 2^n - 2n - 8], \end{aligned} \quad (19)$$

which was determined by using Eq. (18) and where we have explicitly separated C_2 since our $n = 2$ base case does not work recursively. In [22–24] it was proven that a two-qubit quantum circuit could usually be synthesized with at most three CNOT gates. Therefore, the total number of CNOT gates required to decompose a unitary U in $\text{SU}(2^n)$ by means of the Khaneja-Glaser decomposition algorithm is

$$T_n = \frac{3}{16}4^n + \frac{9}{8}4^n - 3(n2^{n-2} + 2^n) = \frac{21}{16}4^n - O(n2^n), \quad (20)$$

which is roughly a factor of 5 away from the best-known theoretical lower bound for synthesizing an n -qubit unitary [24]. As our method is recursive and creates unitaries of any $(n - k)$ qubit size, more optimal unitary decompositions for a particular number of qubits can be taken into account and inserted at that size.

VII. DISCUSSION

We have implemented the algorithm in rudimentary form and provide it in the supplemental material [25]. The algorithm can certainly be optimized further. We leave this as implementation work for colleagues more familiar with suitable programming environments.

The presented decomposition algorithm provides a solid basis for decomposing any arbitrary unitary in $\text{SU}(2^n)$. For the construction, we assume an ideal quantum computer with any-to-any connections and no noise. This assumption is common to circuit construction algorithms and can be remedied by post-creation optimization of the circuit. The first assumption can be approached either by exchanging CNOTs on nonexisting connections with CNOT ladder chains that implement an equivalent operation. In the worst case of a linear chain, a CNOT connecting qubits k apart, $4(k - 1)$ nearest-neighbor CNOTs are required [17]. It may be possible to optimize this through our approach, since there is a direct correspondence between

the subalgebra generators and the CNOT gates between qubits. Restricting the subalgebra to exclude certain connections may provide a more optimal solution. We suggest this approach for future work.

The robustness of a circuit with respect to noise is much more difficult to measure and achieve. The current methods for achieving fault-tolerance, such as stabilizer codes [26] and logical qubits [27], are not easily implementable in our approach. However, it is possible to create a near-optimal circuit with the presented method and adjust it to be noise-tolerant afterwards.

Our approach is not limited to CNOT gates. While we use it throughout our construction, it can be readily transformed to another gate set, as long as it forms a universal family of quantum gates [14]. Thus, if the particular hardware can only (or efficiently) implement a different set of control gates, it is possible to translate the circuit into a different family of universal gates. That is, the methods described here generalize to different families of universal quantum gates, which might be more easily implemented on the particular quantum hardware.

What sets apart the Khaneja-Glaser Cartan decomposition of a unitary described here from the other decomposition methods is that it gives an explicit construction of the quantum circuit decomposing a unitary and thus can be directly implemented on a quantum computer. Moreover, this decomposition method can also be used to optimize existing computational circuits to improve their scaling.

The method presented in this paper demonstrates how to efficiently build quantum circuits implementing an n -qubit unitary operation through the Cartan decomposition of Lie algebras. Our work generalizes the previous unstructured Cartan decomposition of a three-qubit unitary to a structured recursive algorithm capable of synthesizing any desired unitary operation. Our construction allows the expansion of any quantum circuit in terms of rotation matrices and generators. Moreover, we show how these generators can be recursively decomposed through CNOT and fermionic SWAP gates into circuits that can be directly implemented on a quantum computer. This Cartan decomposition method also scales well, with a near-optimal scaling of $\frac{21}{16}4^n - 3(n2^{n-2} + 2^n)$ CNOT gates required to synthesize an n qubit unitary operation. The algorithmic structure of the method and constructions described in this paper allows for a simple yet flexible implementation, both in terms of applications of the algorithm and software and hardware architectures.

ACKNOWLEDGMENTS

The authors acknowledge funding from the German Federal Ministry of Education and Research (BMBF) under the funding program ‘‘Förderprogramm Quantentechnologien–von den Grundlagen zum Markt’’ (funding program quantum technologies—from basic research to market), project BAIQO, 13N16089.

-
- [1] M. A. Nielsen and I. Chuang, Quantum computation and quantum information, *Am. J. Phys.* **70**, 558 (2002).
 [2] T. Gabor, M. Zorn, and C. Linnhoff-Popien, The applicability of reinforcement learning for the automatic generation of

state preparation circuits, in *Proceedings of the Genetic and Evolutionary Computation Conference Companion*, GECCO ’22 (Association for Computing Machinery, New York, 2022), pp. 2196–2204.

- [3] E. Knill, Approximation by quantum circuits, [arXiv:quant-ph/9508006](https://arxiv.org/abs/quant-ph/9508006) (1995).
- [4] K. Hietala, R. Rand, S.-H. Hung, X. Wu, and M. Hicks, A verified optimizer for Quantum circuits, *Proc. ACM Program. Lang.* **5**, 1 (2021).
- [5] P. W. Shor, Algorithms for quantum computation: discrete logarithms and factoring, in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science, Los Alamitos* (IEEE Computer Society, Piscataway, NJ, 1994), pp. 124–134.
- [6] L. K. Grover, A fast quantum mechanical algorithm for database search, in *Proceedings of the Twenty-eighth Annual ACM Symposium on Theory of Computing, STOC '96* (Association for Computing Machinery, New York, 1996), pp. 212–219.
- [7] P. W. Shor, Progress in Quantum Algorithms, *Quant. Inf. Proc.* **3**, 5 (2004).
- [8] C. Shao, Y. Li, and H. Li, Quantum algorithm design: Techniques and applications, *J. Syst. Sci. Complex.* **32**, 375 (2019).
- [9] M. Schuld, I. Sinayskiy, and F. Petruccione, An introduction to quantum machine learning, *Contemp. Phys.* **56**, 172 (2015).
- [10] J. Biamonte, P. Wittek, N. Pancotti, P. Rebentrost, N. Wiebe, and S. Lloyd, Quantum machine learning, *Nature (London)* **549**, 195 (2017).
- [11] M. Cerezo, G. Verdon, H.-Y. Huang, L. Cincio, and P. J. Coles, Challenges and opportunities in quantum machine learning, *Nat. Comput. Sci.* **2**, 567 (2022).
- [12] F. Vatan and C. P. Williams, Realization of a general three-qubit quantum gate, [arXiv:quant-ph/0401178](https://arxiv.org/abs/quant-ph/0401178) (2004).
- [13] N. Khaneja and S. J. Glaser, Cartan decomposition of $SU(2n)$ and control of spin systems, *Chem. Phys.* **267**, 11 (2001).
- [14] 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).
- [15] J. J. Vartiainen, M. Möttönen, and M. M. Salomaa, Efficient Decomposition of Quantum Gates, *Phys. Rev. Lett.* **92**, 177902 (2004).
- [16] M. Möttönen, J. J. Vartiainen, V. Bergholm, and M. M. Salomaa, Quantum Circuits for General Multiqubit Gates, *Phys. Rev. Lett.* **93**, 130502 (2004).
- [17] V. V. Shende, S. S. Bullock, and I. L. Markov, Synthesis of quantum logic circuits, in *Proceedings of the 2005 Asia and South Pacific Design Automation Conference, ASP-DAC '05* (Association for Computing Machinery, New York, 2005), pp. 272–275.
- [18] C. Paige and M. Wei, History and generality of the cs decomposition, *Lin. Alg. Appl.* **208-209**, 303 (1994).
- [19] E. Cartan, Sur une classe remarquable d'espaces de Riemann, *Bul. Soc. Math. France* **2**, 214 (1873).
- [20] E. Cartan, Sur une classe remarquable d'espaces de Riemann. II, *Bul. Soc. Math. France* **2**, 114 (1873).
- [21] J. E. Humphreys, *Introduction to Lie Algebras and Representation Theory* (Springer Science & Business Media, New York, 2012).
- [22] F. Vatan and C. Williams, Optimal quantum circuits for general two-qubit gates, *Phys. Rev. A* **69**, 032315 (2004).
- [23] 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).
- [24] V. V. Shende, I. L. Markov, and S. S. Bullock, Minimal universal two-qubit controlled-not-based circuits, *Phys. Rev. A* **69**, 062321 (2004).
- [25] See Supplemental Material at <http://link.aps.org/supplemental/10.1103/PhysRevA.108.052607> for a Jupyter python notebook that implements the decomposition algorithm for $SU(4)$.
- [26] P. Webster, M. Vasmer, T. R. Scruby, and S. D. Bartlett, Universal fault-tolerant quantum computing with stabilizer codes, *Phys. Rev. Res.* **4**, 013092 (2022).
- [27] J. F. Marques, B. M. Varbanov, M. S. Moreira, H. Ali, N. Muthusubramanian, C. Zachariadis, F. Battistel, M. Beekman, N. Haider, W. Vlothuizen, A. Bruno, B. M. Terhal, and L. DiCarlo, Logical-qubit operations in an error-detecting surface code, *Nat. Phys.* **18**, 80 (2022).