Transforming an arbitrary finite group into quantum circuits

Ruge Lin\textsuperscript{1,2}

\textsuperscript{1}Technology Innovation Institute, Abu Dhabi, United Arab Emirates.
\textsuperscript{2}Departament de Física Quàntica i Astrofísica and Institut de Ciències del Cosmos (ICCUB), Universitat de Barcelona, Martí i Franquès 1, 08028 Barcelona, Spain.

We provide two methods to map each element of a given finite group into a different quantum circuit. In the first one, we directly sum its unitary representation with an identity matrix to obtain a new unitary matrix suitable for decomposing into a quantum circuit. In the second one, we use a Variational Quantum Algorithm trained after the absolute presentation of the group to construct the quantum circuits. This article provides explicit examples and numerical simulation.

I. INTRODUCTION

The unitarity theorem states that all finite groups have unitary representations \[1\]. Additionally, mathematical core of quantum mechanics is the theory of unitary representations of symmetries of physical systems \[2,3\]. Furthermore, \(2^n \times 2^n\) unitary matrices can be decomposed into quantum circuits \[3,4\]. It is natural to raise the question, can any finite group be converted into a series of quantum circuits?

There are three main obstacles to this problem. Firstly, how do we obtain a unitary representation for a finite group? Secondly, how to keep this representation have a dimension of \(2^n\)? Finally, because the global phase of a quantum state is not detectable, two unitary matrices with a global phase difference are identical when turned into quantum circuit \[5\]. How can we map two unitary representations into different quantum circuits with only a global phase difference?

In the following, we present two approaches. The first way that can be considered "classic to quantum" is to construct quantum circuits from a classically computed complex representation. The second one is more "quantum to classic" that we compose a Variational Quantum Algorithm (VQA) \[9\] from the group presentation, which even allows us to deduce the full unitary matrices that form a representation of the group.

II. MAPPING GROUP TO CIRCUITS WITH COMPLEX REPRESENTATIONS

For an arbitrary finite group \(G\), suppose we have a faithful non unitary group \(\tilde{\rho} : G \rightarrow M_d\), that for each \(g \in G\), \(\tilde{\rho}(g)\) is a \(d \times d\) matrix with complex entries. A faithful representation means that it is one-to-one. Therefore, no two distinct elements of \(G\) are mapped into the same matrix. It is a non-trivial work to obtain such a representation of a given finite group \[10\]. Fortunately, this work is usually already done by mathematicians.

To transform \(\tilde{\rho}\) into unitary, we first define

\[
H = \sum_{g \in G} \tilde{\rho}(g) \dagger \tilde{\rho}(g),
\]

which can be proven hermitian. Details are provided in \[11\]. Then there exists a real diagonal matrix \(P\) and a unitary matrix \(W\) such that \(P^2 = W^\dagger HW\). Finally, for all \(g \in G\), we define

\[
\rho(g) = PW^\dagger \tilde{\rho}(g) WP^{-1},
\]

which can be proven unitary.

Once we have a faithful and unitary representation, we can use it to construct another unitary and faithful representation \(U : G \rightarrow M_{2^n}\) with a higher dimension by directly summing it with other unitary representation \(\sigma_i\) (not necessarily faithful)

\[
U(g) = \begin{pmatrix} \sigma_1(g) & 0 & 0 \\ 0 & \rho(g) & 0 \\ 0 & 0 & \sigma_2(g) \end{pmatrix}.
\]

In particular, the trivial representation can be chosen for simplicity, where every element \(g \in G\) is mapped into the \(k \times k\) identity matrix \(I_k\). Here the dimension \(k\) can be any number adapting to our needs, such as \(k = 2^n - d\) to make the matrix suitable for transforming into a quantum circuit

\[
U(g) = \begin{pmatrix} \rho(g) & 0 \\ 0 & I_k \end{pmatrix}.
\]

The extra advantage of using the identity matrix to enlarge the representation is that it eliminates the effect of the global phase. In the faithful representation \(\rho(g)\), every element of \(G\) is mapped into a different matrix. On the other hand, in the trivial representation, all elements are mapped into \(I_k\). Therefore, in the representation \(U\), the identity element is the only element mapped into \(I_{2^n}\). It doesn’t exist an element \(g\) in \(G\) that verifies \(U(g) = e^{i\theta}I_{2^n}\) with \(\theta \neq 0\) because one block of the full matrix must be maintained as \(I_k\). When the dimension of the original unitary representation is already \(2^n\), but it has an non identity element \(g\) with \(\rho(g) = e^{i\theta}I_{2^n}\). We still need to directly sum \(\rho(g)\) with \(I_{2^n}\) to avoid this effect and the final \(U(g)\) will have dimension \(2^{n+1}\).

After each \(g \in G\) is mapped into a different \(2^n \times 2^n\) unitary matrix, we can use the method provided by \[4\]
to mapped it into quantum circuit with a number of CNOT gates $O(4^n)$. In particular, any cyclic group can be mapped into single qubit gates. For example, the element 1 in the group $C_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$ can be mapped into a $T$ gate

$$U(1) = T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi} \end{pmatrix}.$$  

A 3-qubit example circuit of an element in the symmetric group $S_8$ is provided in FIG. 1 which involves a Toffoli gate. The full unitary matrix of this element is shown in Eq. (5). This kind of circuit will provide a quantum advantage with physical implementation of $n$-control-qubit Toffoli gates [12, 13]. Furthermore, all symmetric groups can be represented as permutation matrices, which are orthogonal and thus unitary. Cayley’s theorem states that every finite group $G$ is isomorphic to a subgroup of a symmetric group [1, 14]. We can have an alternative proof that all finite groups have unitary representation.

$$U((185)\, (3674)) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}.$$ (6)

III. MAPPING GROUP TO CIRCUITS WITH ABSOLUTE PRESENTATION

Finite groups can be defined by their absolute presentations [1, 12], which list the essential relations and irreations that the generators satisfy

$$G = \langle \sum_{\text{set of generators}} | \sum_{\text{set of relations}} | \sum_{\text{set of irreations}} \rangle.$$ (7)

Every relation can be written into a formula of a word (defined as the product of group elements) equal to the identity. If $G$ is generated by elements $a$ and $b$ which satisfy the relation $ab = ba$, we can transform it into $b^{-1}aba^{-1} = 1$. For example, the presentation of the cyclic group $C_8$ is $\langle a | a^8 = 1 \rangle$, where $a^8$ is a word. However, $a = 1$ will also satisfy the condition $a^8 = 1$. To eliminate the confusion, we specify that certain words should not equal the identity. These are called irreations. In the case of $C_8$, the irrelation is $a^4 \neq 1$. Therefore, the absolute presentation of $C_8$ is $\langle a | a^8 = 1, a^4 \neq 1 \rangle$.

We can construct a VQA to obtain a quantum circuit for each generator. In the VQA, quantum circuits depend on a set of classical parameters that can be adjusted using a quantum-classical optimization loop by minimizing a cost function.

Firstly, each generator is described as a variational ansatz with the same set of parameters. Here we highlight that the ansatz for each generator can be set differently depending on the problem. Each word is the concatenation of such ansatzes. Then multiple circuits, as shown in FIG. 2 are trained simultaneously to maximize the amplitude of $|0, ..., 0\rangle$ (minimizing the amplitude of other states). A maximization (minimization) always exists if the ansatzes are designed properly. In the worst case, we will obtain the trivial representation that every generator is mapped into the identity. After training, a quantum circuit for each generator can be reconstructed from the numerical output. Finally, trained parameters are inserted in the verification circuit, as shown in FIG. 3 to check that the word in the irrelation does not equal the identity. Furthermore, if the ansatzes are chosen carefully to avoid the effect of the global phase, we can obtain a complex analytical representation of the finite group from the trained parameters. A detailed example is provided in the next section.
IV. A TOY EXAMPLE

We use a toy example to explain explicitly how to turn a finite group into quantum circuit. Let us take one of the 16 elements finite group $C_2 \times D_4$ \textsuperscript{16}, which is the direct product of the cyclic group $C_2$ and the dihedral group $D_4$, and transform it into a 2-qubits quantum circuit. The absolute presentation of $C_2 \times D_4$ is

$$\langle a, b, c | a^2 = b^2 = c^4 = (bc)^2 = 1, ab = ba, ac = ca, a \neq 1, b \neq 1, ab \neq 1, c^2 \neq 1 \rangle,$$

(8)

where $ab = ba$ can be converted into $(ab)^2 = 1$ with $a^2 = b^2 = 1$ and $ac = ca$ can be converted into $ac^3 \neq ac$ with $a^2 = c^4 = 1$.

And its representations are

$$\rho(a) = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix},$$

(9)

$$\rho(b) = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix},$$

(10)

and

$$\rho(c) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix}.$$  

(11)

In this case, the representation is already unitary, but the dimension is 3 which is not a power of 2, and $\rho(a)$ is identical to $I_4$ with a global phase. To have a unitary matrix that can be transformed into a quantum circuit, we can directly sum an $I_4$ after each representation. They become

$$U(a) = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

(12)

$$U(b) = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

(13)

and

$$U(c) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$ 

(14)

In particular, we have

$$U(bc^2) = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

(15)

which is a $Z$ gate on the first qubit and

$$U(bc^3) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

(16)

which is a $SWAP$ gate acting on both qubits. Since $U(c) = U(bc^2)U(bc^3), U(c)$ can be obtained by applying a $Z$ gate on the first qubit then $SWAP$ gate. Other elements of $C_2 \times D_4$ can be transformed into circuit with FIG. 4.

Alternatively, we can construct a set of variational circuits as shown in FIG. 5. Generators $a$, $b$ and $c$ are trained with the same ansatz illustrated in FIG. 6 with

$$R_y(\theta) = \begin{pmatrix} \cos(\theta/2) & -\sin(\theta/2) \\ \sin(\theta/2) & \cos(\theta/2) \end{pmatrix}.$$ 

(17)

This ansatz is particularly chosen for three reasons. Firstly, it can not be trained into identity, thus the result can not be the trivial representation. In the worse case, when every parameter equals 0, we will have $U(a) = U(b) = U(c) \neq I_4$. They form a faithful representation of $C_2$, which is a subgroup of $C_2 \times D_4$. Secondly, the components of the full unitary matrix are real numbers, and the problem of the global phase will be less disturbing. Finally, similar structure has been widely used in previous QVA research \textsuperscript{17, 19}.

We perform a numerical simulation with the library Qibo \textsuperscript{20} and the final result is shown in TABLE. \textsuperscript{1} The code is provided on GitHub \textsuperscript{21}. Our readers are encouraged to test this method with a different finite group or a different ansatz. After obtaining the trained parameters, we use the circuits in FIG. 5 to verify that the representation is faithful, and the trained ansatz are suitable for quantum computation of finite group.

\begin{figure}
\centering
\includegraphics[width=0.8\textwidth]{figure4.png}
\caption{Quantum circuits of the group $C_2 \times D_4$.}
\end{figure}
Furthermore, by studying the final values, we can construct an analytical relation between the parameters as shown in TABLE I. It is not evident to deduce such an interpretation for a more complex group. However, we can fix certain parameters and train the circuits iteratively. For example, in TABLE I, $\theta_2$ for $U_a$ and $U_c$ are approximate, then they can be treated as the same parameter for the second training. Likewise, $\theta_4$ for $U_a$ and $U_c$ have a difference of $16\pi$, which can be considered the same for the next iteration. Although it is complicated to expand the full matrices, numerical simulation demonstrates that these relations satisfy circuits in FIG. 5 and FIG. 7 with one arbitrary parameter $\theta$.

By applying $\theta = 0$, we can have the full unitary matrices to represent $a$, $b$ and $c$ as shown in Eq. (18). It can be verified numerically that they form a faithful representation of $C_2 \times D_4$ [21]. In this way, analytical representations of finite group can be reconstructed from the output of the VQA.

$$U_{\theta=0} (a) = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \quad (18)$$
convert it into unitary, then directly summing an identity matrix to enlarge the representation to dimension $2^n$ and eliminate the effect of the global phase if necessary. Then we decompose the $2^n \times 2^n$ unitary matrices into one-qubit and two-qubit gates. On the other hand, we can design and train a set of variational quantum circuits according to the relations in the absolute presentation of the finite group. The final parameters are then tested on quantum circuits that encode the irrelations. With particular circuits and ansatz chosen for the VQA, full matrices of an analytical representation of the finite group can be obtained. These techniques of transformation enables quantum computers to perform the calculation of abstract algebra.

V. CONCLUSION

In this article we provide two systematic approaches to map an arbitrary finite group into a quantum circuit and use detailed examples to demonstrate them. We can take a given complex representation of the group and

\[
U_{\theta=0}(b) = \begin{pmatrix}
0 & 1 & 0 & 0 \\
1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 \\
0 & 0 & -1 & 0
\end{pmatrix}
\]

\[
U_{\theta=0}(c) = \begin{pmatrix}
0 & 0 & -1 & 0 \\
0 & 1 & 0 & 0 \\
1 & 0 & 0 & 0 \\
0 & 0 & 0 & -1
\end{pmatrix}
\]

ACKNOWLEDGMENTS

We acknowledge Stavros Efthymiou for useful support in Qibo, Sergi Ramos-Calderer and Prof. J. I. Latorre for helpful discussion.

[1] Anthony Zee. *Group theory in a nutshell for physicists*, volume 17. Princeton University Press, 2016. Pages 96-97.

[2] Vladimir V Kornyak. Computations in finite groups and quantum physics. In *International Workshop on Computer Algebra in Scientific Computing*, pages 263-279. Springer, 2011.

[3] Stan Gudder. Quantum mechanics on finite groups. *Foundations of Physics*, 38(6):1160–1192, 2006.

[4] Juha J Vartiainen, Mikko Mottonen, and Martti M Salomaa. Efficient decomposition of quantum gates. *Physical review letters*, 92(17):177902, 2004.

[5] Chi-Kwong Li, Rebecca Roberts, and Xiaoyan Yin. Decomposition of unitary matrices and quantum gates. *International Journal of Quantum Information*, 11(01):1350015, 2013.

[6] Anna M Krol, Aritra Sarkar, Imran Ashraf, Zaid Al-Ars, and Koen Bertels. Efficient decomposition of unitary matrices in quantum circuit compilers. *Applied Sciences*, 12(2):759, 2022.

[7] Mikko Mottonen and Juha J Vartiainen. Decomposition of general quantum gates. 2006.

[8] Michael A Nielsen and Isaac Chuang. Quantum computation and quantum information, 2002.

[9] Marco Cerezo, Andrew Arrasmith, Ryan Babbush, Simon C Benjamin, Suguru Endo, Keisuke Fujii, Jarrod R McClean, Kosuke Mitarai, Xiao Yuan, Lukasz Cincio, et al. Variational quantum algorithms. *Nature Reviews Physics*, 3(9):625–644, 2021.

[10] László Babai and Lajos Rónyai. Computing irreducible representations of finite groups. *Mathematics of computation*, 55(192):705–722, 1990.

[11] Weyl's Unitarity Trick. [http://mathonline.wikidot.com/weyls-unitarity-trick#toc0](http://mathonline.wikidot.com/weyls-unitarity-trick#toc0).

[12] T Monz, K Kim, W Hänsel, M Riebe, AS Villar, P Schindler, M Chwalla, M Hennrich, and R Blatt. Realization of the quantum toffoli gate with trapped ions. *Physical Review Letters*, 102(4):040501–040501, 2009.

[13] Nilesh Goel and JK Freericks. Native multiqubit toffoli gates on ion trap quantum computers. *Quantum Science and Technology*, 6(4):044010, 2021.

[14] Charles C Pinter. *A book of abstract algebra*. Courier Corporation, 2010.

[15] Bernhard H Neumann. The isomorphism problem for algebraically closed groups. In *Studies in Logic and the Foundations of Mathematics*, volume 71, pages 553–562. Elsevier, 1973.

[16] Tim Dokchitser. [https://people.maths.bris.ac.uk/~matyd/GroupNames/1/C2xD4.html](https://people.maths.bris.ac.uk/~matyd/GroupNames/1/C2xD4.html).

[17] Carlos Bravo-Prieto, Josep Lumbraeras-Zarapico, Luca Tagliacozzo, and José I Latorre. Scaling of variational quantum circuit depth for condensed matter systems. *Quantum*, 4:272, 2020.

[18] Jonathan Romero, Jonathan P Olson, and Alan Aspuru-Guzik. Quantum autoencoders for efficient compression of quantum data. *Quantum Science and Technology*, 2(4):045001, 2017.

[19] Carlos Bravo-Prieto. Quantum autoencoders with enhanced data encoding. *Machine Learning: Science and Technology*, 2(3):035028, 2021.

[20] Stavros Efthymiou, Sergi Ramos-Calderer, Carlos Bravo-Prieto, Adrián Pérez-Salinas, Diego García-Martín, Artur García-Saez, José Ignacio Latorre, and Stefano Carrazza. Qibo: a framework for quantum simulation with hardware acceleration. *Quantum Science and Technology*, 7(1):015018, 2021.

[21] Ruge Lin. [https://github.com/GoGoKo699/group-to-circuits](https://github.com/GoGoKo699/group-to-circuits).

[22] Nikolaus Hansen, yoshihiikoueno, ARF1, Kento Nozawa, Luca Rolshoven, Matthew Chan, Youhei Akimoto, brieglhostis, and Dimo Brockhoff. Cma-es/pycma: r3.2.0, February 2022.

[23] Charles C Pinter. *A book of abstract algebra*. Courier Corporation, 2010.