Quantum representation of finite groups

Ruge Lin\textsuperscript{1,2}

\textsuperscript{1}Quantum Research Centre, Technology Innovation Institute, UAE.
\textsuperscript{2}Departament de Física Quàntica i Astrofísica and Institut de Ciències del Cosmos, Universitat de Barcelona, Spain.

The concept of quantum representation of finite groups has been a fundamental aspect of quantum computing for quite some time, playing a role in every corner, from elementary quantum logic gates to the famous Shor’s and Grover’s algorithms. In this article, we provide a formal definition of this concept using both group theory and differential geometry. Our work proves the existence of a quantum representation for any finite group and outlines two methods for translating each generator of the group into a quantum circuit, utilizing gate decomposition of unitary matrices and variational quantum algorithms. Additionally, we provide numerical simulations of an explicit example on an open-access platform. Finally, we demonstrate the usefulness and potential of the quantum representation of finite groups by showing its role in the gate-level implementation of the algorithm that solves the hidden subgroup problem.

I. INTRODUCTION

The unitarity theorem, as stated by Zee \cite{Zee1}, asserts that all finite groups possess unitary representations. This concept holds significant importance in the realm of quantum mechanics, as the theory relies on unitary representations of symmetries within physical systems \cite{Goldberg1}. Consequently, it becomes natural to explore the quantum representation of any finite group, where each element is redefined as an effective quantum operator. By encoding the mathematical rules governing the group into a series of physical motions, the quantum representation elucidates the connection between abstract mathematical concepts and applicable quantum circuits. This framework finds particular relevance within the context of quantum computation, where the quantum representation serves as the mapping from a given finite group to gates set, enabling their utilization in quantum algorithms.

II. PRELIMINARY

In this section, we lay the foundation by introducing key definitions that establish a connection between group actions on sets and quantum operations on states. To ensure clarity and avoid confusion, we adopt a notation where the symbol "," represents group action, while the symbol "\times" denotes the multiplication of numbers. This distinction in notation facilitates a clear delineation between the two concepts, enabling a seamless transition from group theory to quantum mechanics.

Definition 1. Unitary action

The unitary action \( \alpha : U (d) \cdot H_d \rightarrow H_d \) is the group action of the unitary group \( U (d) \) to the Hilbert space \( H_d \).

Definition 2. Ineffective quantum group

For \( x \) and \( y \) elements of \( H_d \), if they are indistinguishable by any measurement after any unitary action, we say that they are equivalent under the context of quantum mechanics and note \( x \sim y \). In particular, the quotient space \( H_d / \sim \) is what we call projective Hilbert space \( \mathbb{P}(H_d) \). A unitary operator is ineffective if it produces no observable difference while acting on any element of \( H_d \). All ineffective quantum operators form the ineffective quantum group \( U (1) = \exp (i \theta) I_d \), the center of \( U (d) \), where \( I_d \) is the \( d \times d \) identity matrix.

Definition 3. Effective quantum group

The effective quantum group is the quotient \( U (d) / U (1) \), the projective unitary group \( \mathbb{P}U (d) \).

A pure quantum state can be described by a normalized \( d \)-dimensional complex vector \( \mathbf{v} \). Then \( H_d \) is the hypersphere \( S^{2d-1} \), where each point of this hypersphere describes a quantum state, which is not unique since multiple points can describe the same state. And the unitary action \( \alpha \) is the differentiable action of the compact Lie group \( U (d) \) on the smooth manifold \( S^{2d-1} \). For an element \( M_d \in U (d) \) and a vector \( \mathbf{v} \), where the component of \( \mathbf{v} \) describes a point located on \( S^{2d-1} \), \( \alpha \) is the matrix multiplication \( M_d \cdot \mathbf{v} \mapsto \mathbf{v} \). This action is transitive because we can always find a unitary matrix that transfers one quantum state to another. But the action is not free since if a unitary transfers a quantum state to itself, it does not imply this unitary is the identity.

Theorem 1. Quantum state manifold

The projective Hilbert space \( \mathbb{P}(H_d) \) can be described with the quantum state manifold, defined as \( S^{2d-1}/U (1) \), which is a submanifold of \( S^{2d-2} \). Every quantum state corresponds uniquely to one point of this manifold.

Proof. The action of \( U (1) \) on \( S^{2d-1} \) is a continuous compact Lie group action on a smooth manifold. Therefore, the action is smooth and proper. For all points on \( S^{2d-1} \), if one element of \( U (1) \) keeps the point fixed after the action, that means \( \theta = 0 \), and the element is the identity. So the action is also free. We have \( U (1) \) a Lie group acting smoothly, freely, and properly on a smooth manifold \( S^{2d-1} \), which allows us to apply the Quotient Manifold Theorem \cite{Goldberg1}. Therefore \( S^{2d-1}/U (1) \) is a manifold of dimension \( 2d - 2 = \dim \mathbb{P}(H_d) \). The result can be obtained when \( \mathbb{P}(H_d) \) is described as a complex projective space and quantum states are its rays \cite{Goldberg1}.
When \( d = 2 \), if we force the coefficient of \(|0\rangle\) to be real and non-negative, \( S^3/U(1) = S^2 \) and we recover the representation of the Bloch sphere. For \( d > 2 \), if we force the coefficient of \(|0\cdots0\rangle\) to be real and non-negative, we can obtain \( S^{2d-1}/U(1) \subset S^{2d-2} \), which means \( \mathbb{P}(H_d) \) form a submanifold of hypersphere \( S^{2d-2} \) of the same dimension. But they will never be equal since multiple points of \( S^{2d-2} \) can still define the same quantum state.

### III. QUANTUM REPRESENTATION

Once we have translated the concepts of "probability of all possibilities sum up to one" and "global phase is undetectable" into the language of group theory and differential geometry, though in a non-unique and non-original manner, we can proceed to provide a formal definition of the quantum representation of a group.

**Definition 4. Quantum representation**

Given a group \( G \), its quantum representation is a subset of \( \mathbb{P}U(d) \) that maintains the group structure of \( G \). We add a constraint that quantum representation should be faithful: each element in \( G \) corresponds to a distinct element in \( \mathbb{P}U(d) \). In particular, the identity element \( e \) is always represented as the identity operator \( I_d \).

Not all group has their quantum representation. But we can prove that when \( G \) is finite, it always does.

**Theorem 2. Quantum representation of finite groups**

For a given finite group \( G \), there is always a certain dimension \( d \) that \( G \) has its quantum representation. Additionally, there exists \( x \in \mathbb{P}(H_d) \) such that \( G \cdot x \) the orbit of \( x \) has exactly \(|G|\) element. This orbit forms a principal homogeneous space of \( G \), denoted as the \( G \)-torsor.

**Proof.** Cayley’s theorem states that every finite group \( G \) is isomorphic to a subgroup of a symmetric group \( S_n \), which is a subgroup of \( S_d \) for \( d \geq n \). We have \( S_d \) subgroup of \( \mathbb{P}U(d) \) since they can be represented as permutation matrices, which are orthogonal; also, none of them has a global phase difference from another. Then the quantum representation of \( G \) is a set of \(|G|\) permutation matrices of size \( d \times d \) that preserves the structure of \( G \). In particular, when we pick \( x = \sum_{i=0}^{d-1} c_i |i\rangle \) with distinct \( c_i \), the orbit \( G \cdot x \) forms a \( G \)-torsor. Furthermore, given a set of unitary \( \{U_1, U_2, \ldots, U_{|G|}\} \) that forms a quantum representation of \( G \), there is always \( x \in \mathbb{P}(H_d) \) such that \(|G \cdot x| = |G|\). The orbit-stabilizer theorem for finite groups gives \(|G \cdot x| \cdot |G| = |G|\), where \(|G|\) is the stabilizer of \( x \). For \( G \cdot x \) to be the \( G \)-torsor, we need \( G_x = I_d \), which means \( x \) should locate outside the union of all \( F_i \), space of fixed point of \( U_i \), defined as \( F_i = \{ \forall |\psi\rangle \in \mathbb{P}(H_d) : U_i |\psi\rangle = |\psi\rangle \} \). For \( U_i \neq I_d \), we have \( \dim F_i < \dim \mathbb{P}(H_d) = 2d-2 \) and it is impossible to cover a space with a finite number of subspaces of lower dimension, a point \( x \) always exists outside this union.

The idea of quantum representation of finite groups is not novel. The Pauli group is a 16 elements matrix group isomorphic to \( C_4 \circ D_4 \), the central product of a cyclic group of order 4 and the dihedral group of order 8. Still, its quantum representation only has 4 elements and is isomorphic to \( C_2 \times C_2 \) (× for the direct product), which is abelian. The Pauli matrices are anti-commute, but quantum Pauli gates commute to a global phase.

In Shor’s algorithm for finding prime factors \( p \) and \( q \) of an integer \( N \), a random integer \( 1 < a < N \) is selected, and the quantum circuit is designed to find the period \( r \) such that \( a^r = 1 \mod N \). The operators of quantum modular exponentiation (QME), denoted as \( Ua^{q^i} \) for \( 0 \leq i < 2n \) with \( n = \lfloor \log_2 N \rfloor \), transform any \(|x\rangle\) into \(|x \times a^{q^i} \mod N \rangle\). For any \( i \), if we apply \( r \) operators \( Ua^{q^i} \) one after the other, we will always transform \(|x\rangle\) back to itself. Additionally, though it is useless for application, any \( Ua^{q^i} \) can be generated with \( 2^i \) operators \( Ua^{q^i} \). Combining these two pieces of information, we can see that \( Ua^{q^i} \) are elements of the quantum representation of \( C_r \) with one generator \( Ua^{q^0} \). Here, we re-interpret Shor’s algorithm with our definition of quantum representation, which is unsurprising because Shor’s inspiration came from Simon’s algorithm to solve the hidden subgroup problem (defined in the following) when \( G \) is abelian. When the input state of QME is \(|1\rangle\) as demanded by the algorithm, after applying all the \( Ua^{q^i} \) operators controlled by the uniform superposition, the output of the QME register becomes the superposition (usually not uniform) of \(|a^i \mod N\rangle\) for \( 0 \leq i < r \), which is the superposition of \( C_r \)-torsor. In particular, \( C_r \)-torsor is a subset of \( C_\varphi(N) \)-torsor, where \( \varphi \) is the Euler’s totient function and \( \varphi(N) = (p-1) \times (q-1) \).

In Grover’s algorithm for searching in an unstructured database, a uniform superposition over all states \( \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle \) is first created. During each iteration step, the state vector is rotated with an angle of \( \theta = \frac{2 \arcsin \frac{1}{\sqrt{N}}}{2} \) on the 2-dimensional subspace spanned by the initial superposition and the final target state that encodes the answer. Since the operator of each Grover’s step is identical, Grover’s algorithm forms a quantum representation of cyclic groups. When \( N = 2 \), Grover’s steps are isomorphic to \( C_4 \); when \( N = 4 \), they are isomorphic to \( C_6 \). Otherwise, Grover’s steps never return the quantum state to the initial superposition, and they are all isomorphic to the same infinite cyclic group \( C_\infty \).

### IV. GROUP TO QUANTUM CIRCUITS

This section presents two approaches to transforming an arbitrary finite group \( G \) into a set of quantum circuits. The first approach, which can be described as "classic to quantum," involves constructing quantum circuits based on a classically computed complex representation of the group. The second approach, which can
be characterized as "quantum to classic," combines the group presentation with a variational quantum algorithm (VQA) [1]. By presenting these two approaches, we provide valuable insights into transforming arbitrary finite groups into sets of quantum circuits. These methods bridge the gap between classical and quantum computing paradigms, opening new avenues for utilizing quantum resources to study and analyze the properties of finite groups. A toy example of the group $C_2 \times D_4$ is provided in the appendix, with numerical simulation using the Qibo library [3], the code is available on GitHub [4].

A. Unitary Decomposition

For the first method, for a finite group $G$, suppose we are given a faithful complex representation. We can use the method in Ref. [1] to transform it into unitary representation $\tilde{\rho}$, that for each $g \in G$, $\tilde{\rho}(g)$ is an $m \times m$ matrix with complex entries. Then we can construct another unitary and faithful representation $\rho : G \rightarrow U(d)$ with a higher dimension by directly summing it with other unitary representation $\sigma_i$ (not necessarily faithful)

$$\rho(g) = \begin{pmatrix} \sigma_1(g) & 0 & 0 \\ 0 & \rho(g) & 0 \\ 0 & 0 & \sigma_2(g) \end{pmatrix}. \tag{1}$$

In the proof of Theorem [2] $\rho$ is the mapping from $G$ to permutation matrices of dimension $d$, where no extra $\sigma_i$ is needed. When translated into quantum circuits, this type of operator will provide an advantage by physically implementing $n$-control-qubit Toffoli gates [10].

The trivial representation can be chosen as $\sigma_i$ for simplicity, like in Eq. (2), where every element $g \in G$ is mapped into $I_k$. The dimension $k$ can be a number adapting to the quantum system, such as $k = d - m$.

$$\rho(g) = \begin{pmatrix} \tilde{\rho}(g) & 0 \\ 0 & I_k \end{pmatrix}. \tag{2}$$

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 $\tilde{\rho}$, 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 $\rho$, the identity element $e$ is the only element mapped into $I_d$. It does not exist an element $g$ in $G$ that verifies $\rho(g) = \exp(i\theta) I_d$ with $\theta \neq 0$ because one block of the full matrix must be maintained as $I_k$.

When $d = 2^n$, after each $g \in G$ is mapped into a different $2^n \times 2^n$ unitary matrix, we can use the method provided in Ref. [11, 12] to map it into a quantum circuit with a number of $CNOT$ gates $O(4^n)$. In particular, any cyclic group can be mapped into single qubit gates.

Monster group [13], the largest sporadic simple group $\mathbb{M}$, which contains $\sim 8 \times 10^{53}$ elements, has 12 generators and a faithful representation of dimension $196884 < 2^{18}$. Therefore, $\mathbb{M}$ can be represented by 18-qubit gates, where the $\mathbb{M}$-torsor is made of 18-qubit states. This gives us a new perspective; besides a concept that appears during the study of quantum computing, quantum representation might exist as a natural phenomenon, which is experimentally observable and non-artificial, that grants mythical finite groups a physical meaning. Otherwise, why do these structures emerge from axioms?

B. Variational Quantum Algorithm

For the second method, we directly construct the quantum representation from the presentation of the group. Finite groups can be defined by their absolute presentations, which list the essential relations and irrelations that the generators satisfy

$$G = \langle S \mid R, I \rangle. \tag{3}$$

Every relation can be written into a formula of a word equal to the identity. A word in the group is defined as the product of group elements. If $G$ is generated by elements $g_1$ and $g_2$ which satisfy the relation $g_1g_2 = g_2g_1$, we can transform it into $g_2^{-1}g_1g_2^{-1} = e$, where $g_2^{-1}g_1g_2^{-1}$ is a word. The presentation of the cyclic group $C_8$ is $\langle g \mid g^8 = e \rangle$. However, $g = e$ will also satisfy the condition $g^8 = e$. To eliminate the confusion, we specify that certain words should not equal the identity. These are called irrelations. For $C_8$, the irrelation is $g^4 \neq e$, the absolute presentation is $\langle g \mid g^8 = e, g^4 \neq e \rangle$.

The second method revolves around a central principle of formulating a quantum operator for each generator of the group. The key aspect is that applying these operators in the order dictated by the relations of the group preserves the quantum state of the system. In other words, there are no observable changes to the quantum state when the operators are applied according to the group’s relations. However, when these operators are applied in the order of relations, noticeable changes occur in certain quantum states.

Then, a Variational Quantum Algorithm (VQA) can be devised to construct a quantum circuit for each generator, with the circuits depending on a set of classical parameters. These parameters can be adjusted iteratively within a quantum-classical optimization loop, aiming to minimize a predefined 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 group. Each word is the concatenation of such ansatzes. Multiple circuits, as illustrated in FIG. 1, are simultaneously trained to maximize the amplitude of the state $|00...0\rangle$ while minimizing the amplitudes of other states. Notably, only one quantum system of dimension $d$ is required, as the classical optimization of
A variational circuit to train a relation into identity. $U_H$ is a random unitary. The circuit is well-trained when it transform $|0\ldots0\rangle$ into $|0\ldots0\rangle$ with any $U_H$. 

A circuit to verify that an irrelation is not the identity. $U_H$ is a random unitary. The circuit is validated if there is some $U_H$ that transformed $|0\ldots0\rangle$ into non $|0\ldots0\rangle$.

Each loop is performed after the quantum state measurement. Besides the ground state of a qubit, $|0\rangle$ can also be the ground state of qudit or qudit. This VQA works on a mixed-radix quantum architecture. A maximization (minimization) always exists if the ansatzes are designed properly. In the worst-case scenario, the trivial representation is obtained, where every generator is mapped into the identity circuit. Similar parameters can be considered the same for the next training, and the circuits can be trained iteratively. After training, a quantum circuit for each generator can be reconstructed from the numerical output. Finally, trained parameters are inserted in the verification circuits, as shown in FIG. 2 to check that the word in the irrelation does not equal the identity, such that the quantum representation is faithful. With a large enough $d$ and universal ansätze, the existence of a trained result validated by the verification circuits is justified by the Theorem 2. Furthermore, suppose the ansätze are chosen specifically to avoid the effect of the global phase, we can obtain a classical and analytical representation of $G$ from the trained parameters.

V. APPLICATION

The transformation of a finite group $G$ into quantum circuits holds practical significance, particularly for the gate-level implementation of quantum algorithms aimed at solving the hidden subgroup problem [14], which is a foundational topic within theoretical computer science.

Definition 5. Hidden subgroup problem (HSP)

Let $G$ be a group, $X$ a finite set, and a function $f: G \rightarrow X$ that hides a subgroup $H \leq G$, which means for $g_1, g_2 \in G$, $f(g_1) = f(g_2)$ if and only if $g_1$ and $g_2$ are on the same coset of $H$. The function $f$ is given as an oracle. The task is to output the generating set of $H$.

Shor’s algorithm is a simple case of HSP, where $G = C_{\infty}$ and $H = C_r$, and $f$ transform any integer $x$ to $a^x \mod N$. We highlight that $G$ is not $C_{2^{2n}}$ as the initial superposition on the register that controls QME. Because $r$ does not always devise $2^{2n}$, and by Lagrange’s theorem, $C_r$ can not be a subgroup of $C_{2^n}$. But only a finite number of elements can be encoded in the superposition and the algorithm still works because it is a simple case.

The general quantum algorithm solves HSP for finite $G$ with polynomial (in $\log |G|$) query complexity, which is exponentially better than the best classical algorithm. But it requires exponential time, as in the classical case.

In this article, we do not discuss the principle of the algorithm and focus on the preparation of the initial state

$$\frac{1}{|G|} \sum_{g \in G} |g\rangle |f(g)\rangle.$$  (4)

Multiple initial states are requested as the input. On a quantum computer, the oracle of the problem is a unitary $O_f$ that transforms $|g\rangle |0\ldots0\rangle$ to $|g\rangle |f(g)\rangle$ for all $g \in G$. Therefore, before applying $O_f$, we need to prepare $\frac{1}{|G|} \sum_{g \in G} |g\rangle$, which is not indicated in the article. Preparing group elements as states actually means preparing the orbit of the quantum representation. The oracle operator $O_f$ should be implemented with the quantum representation of $G$ and $H$ because it controls on $\frac{1}{|G|} \sum_{g \in G} |g\rangle$ and targets on $\frac{1}{|C_r|} \sum_{g \in G} |f(g)\rangle$, the superposition of $G$-torsor and $H$-torsor.

The quantum representation of finite groups, which guarantees a finite number of accessible states with limited operators, can serve as the necessary building blocks for constructing quantum finite automata, which, as discussed by Moore and Crutchfield [15], harness the power of quantum mechanics to perform computation on finite languages.

VI. CONCLUSION

By revisiting the group axioms, we can gain insight into why the quantum representation is defined in terms of operators rather than states. Even in the absence of quantum properties such as unitarity, reversible operators still satisfy the group axioms. Applying two operators in succession results in a new operator, and this combination of operators adheres to the associative property. There exists a unique identity element, representing the concept of doing nothing or having no effect. Applying an operator after its inverse leaves the system unchanged.

In contrast, combining two quantum states to form a new state lacks a natural binary operation. Without the introduction of an operator, it is not possible to combine states in a meaningful way within the framework of group theory. It is through the quantum representation, which acts on these states, that the group structure can be defined and studied. Therefore, the choice to define the
quantum representation as operators rather than states is motivated by the fundamental properties of groups. While states are important in quantum mechanics, it is the operators that enable the mathematical formulation and exploration of group theory within the context of quantum systems.

In this article, we present a formal definition of the quantum representation of finite groups, employing concepts from both group theory and differential geometry. Our research establishes the existence of a quantum representation for any finite group, offering a solid theoretical insight. We propose two distinct methods for translating the generators of a group into quantum circuits, utilizing gate decomposition of unitary matrices and variational quantum algorithms. To support our findings, we provide numerical simulations of a specific example, which are accessible on an open-access platform.

Moreover, we emphasize the practical significance of the quantum representation of finite groups by demonstrating its application in the gate-level implementation of an algorithm designed to solve the hidden subgroup problem. This unveils the potential and usefulness of our approach in addressing fundamental challenges in theoretical computer science. Overall, our work contributes to the understanding and advancement of the quantum representation of finite groups, offering theoretical foundations, practical implementation methods, and supporting numerical simulations.

ACKNOWLEDGMENTS

The author extends their gratitude to Stavros Efthymiou for valuable support in Qibo, as well as Sheng Li, Sergi Ramos-Calderer, Ingo Roth, Prof. Germán Sierra and Prof. José Ignacio Latorre for their helpful discussions. Acknowledging their contributions, the author recognizes that the concept of the quantum representation of finite groups has primarily been investigated within the field of quantum computing. However, the author welcomes readers from diverse backgrounds to share their insights and perspectives on the subject. The author expresses their appreciation in advance to those who contribute their knowledge and enrich the discussion.

[1] Anthony Zee. Group theory in a nutshell for physicists. Princeton University Press, 2016. Pages 96-97.
[2] Stan Gudder. Quantum mechanics on finite groups. Foundations of Physics, 36(8):1160–1192, 2006.
[3] John M Lee. Introduction to smooth manifolds. Springer, 2012. Pages 544-547.
[4] Abhay Ashtekar and Troy A Schilling. Geometrical formulation of quantum mechanics. In Einstein’s Path: Essays in Honor of Engelbert Schucking, pages 23–65, 1999.
[5] Peter W Shor. Algorithms for quantum computation: discrete logarithms and factoring. In Proceedings 35th annual symposium on foundations of computer science, pages 124–134, Ieee, 1994.
[6] Lov K Grover. A fast quantum mechanical algorithm for database search. In Proceedings of the twenty-eighth annual ACM symposium on Theory of computing, pages 212–219, 1996.
[7] 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.
[8] Stavros Efthymiou, Sergi Ramos-Calderer, Carlos Bravo-Prieto, Adrián Pérez-Salinas, Diego García-Martín, Artur García-Saez, José Ignacio Latorre, and Stefano Carraza. Qibo: a framework for quantum simulation with hardware acceleration. Quantum Science and Technology, 7(1):015018, dec 2021.
[9] Ruge Lin. https://github.com/GoGoKo699/group-to-circuits.
[10] 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.
[11] Juha J Vartiainen, Mikko Möttönen, and Martti M Salomaa. Efficient decomposition of quantum gates. Physical review letters, 92(17):177902, 2004.
[12] Chi-Kwong Li, Rebecca Roberts, and Xiaoyan Yin. Decomposition of unitary matrices and quantum gates. International Journal of Quantum Information, 11(01):1350015, 2013.
[13] John Horton Conway. Atlas of finite groups. Oxford University Press, 1985.
[14] Mark Ettinger, Peter Høyer, and Emanuel Knill. The quantum query complexity of the hidden subgroup problem is polynomial. Information Processing Letters, 91(1):43–48, 2004.
[15] Cristopher Moore and James P Crutchfield. Quantum automata and quantum grammars. Theoretical Computer Science, 237(1-2):275–306, 2000.
[16] Tim Dokchitser. https://people.maths.bris.ac.uk/~matyd/GroupNames/index.html.
[17] Carlos Bravo-Prieto, Josep Lumbraeras-Zarapico, Luca Tagliaozzo, 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] Nikolaus Hansen, yoshihikoueno, ARF1, Kento Nozawa, Luca Rolshoven, Matthew Chan, Youhei Akimoto, brieglhostis, and Dimo Brockhoff. Cma-es/pycma: r3.2.0, February 2022.
Appendix A: Quantum representation of $C_2 \times D_4$

The absolute presentation of $C_2 \times D_4$ is

$$\langle a, b, c | a^2 = b^2 = c^4 = (bc)^2 = 1, ab = ba,\nonumber$$

$$ac = ca, a \neq e, b \neq e, ab \neq e, c^2 \neq e \rangle,$$  \hspace{1cm} (A1)

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

For the first method, we use its classical representations on Dockchitser’s site [16], which are

$$\tilde{\rho}(a) = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$  \hspace{1cm} (A2)

$$\tilde{\rho}(b) = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix},$$  \hspace{1cm} (A3)

and

$$\tilde{\rho}(c) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix}.$$  \hspace{1cm} (A4)

In this case, the representation is already unitary, but the dimension is 3, and $\tilde{\rho}(a)$ is identical to $I_3$ with a global phase. We can directly sum an $I_1$ after each representation. They become

$$\rho(a) = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$  \hspace{1cm} (A5)

$$\rho(b) = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix},$$  \hspace{1cm} (A6)

and

$$\rho(c) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix}.$$  \hspace{1cm} (A7)

In particular, we have

$$\rho(bc^2) = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$  \hspace{1cm} (A8)

which is a Z gate on the first qubit and

$$\rho(bc^3) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$  \hspace{1cm} (A9)

which is a SWAP gate acting on both qubits. Since $\rho(c) = \rho(bc^2) \rho(bc^3)$, $\rho(c)$ can be obtained by applying a Z gate on the first qubit then SWAP gate. Other elements can be turned into circuits with FIG. 3.

For the second method, we can construct a set of variational circuits, as shown in FIG. 4 where quantum generators are trained with the same ansatz illustrated in FIG. 5 with

$$R_y(\theta) = \begin{pmatrix} \cos(\frac{\theta}{2}) & -\sin(\frac{\theta}{2}) \\ \sin(\frac{\theta}{2}) & \cos(\frac{\theta}{2}) \end{pmatrix}. $$  \hspace{1cm} (A10)

This ansatz is particularly chosen for three reasons. Firstly, it can not be trained into identity. Thus the result can not be a 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 $C_2$, 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. Thirdly, similar architecture has been widely applied in previous VQA research [15–19]. We perform a numerical simulation with the library Qibo [8], and the final result is shown in TABLE I. The code is provided on GitHub [9]. After obtaining the trained parameters, we can use the circuits in FIG. 6 to verify that the quantum representation is faithful.

```
| $\theta_1$ | $\theta_2$ | $\theta_3$ | $\theta_4$ |
|------------|------------|------------|------------|
| $U_a$      | 5.84551574 | -8.06312285 | -12.12870095 | -17.06961836 |
| $U_b$      | 16.17214308 | 13.9280257 | -9.88895781 | 4.92153015 |
| $U_c$      | 13.69949734 | -8.06312285 | 2.00846589 | 33.19586423 |
```

TABLE I: One numerical outcome of the VQA. $U_H$ is also prepared with the ansatz in FIG. 3 with random parameters. The classical optimizer is the genetic algorithm CMA [20].
with one arbitrary parameter $\phi$. By applying $\phi = 0$, the full unitary matrices to represent $a, b$ and $c$ are given in Eq. \(\text{A11} - \text{A13}\).

It can be verified numerically that they form a faithful representation of $C_2 \times D_4$. In this way, classical representations of the finite group can be reconstructed from the output of the VQA.

\begin{table}[h]
\centering
\begin{tabular}{|c|c|c|c|c|}
\hline
$\th_1$ & $\th_2$ & $\th_3$ & $\th_4$ \\
\hline
$U_a$ & $3\pi - \phi$ & $3\phi$ & $\phi - \pi$ & $4\pi - 3\phi$ \\
$U_b$ & $\phi$ & $3\phi - \pi$ & $2\pi - \phi$ & $3\phi - 3\pi$ \\
$U_c$ & $\frac{5\pi}{2}$ & $3\phi$ & $\frac{3\pi}{2}$ & $4\pi - 3\phi$ \\
\hline
\end{tabular}
\caption{One possible analytical interpretation of the numerical result.}
\end{table}

\begin{align}
\rho_{\phi=0}(a) &= \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \\
\rho_{\phi=0}(b) &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \\
\rho_{\phi=0}(c) &= \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}
\end{align}