Invariant subspaces of two-qubit quantum gates and their application in the verification of quantum computers

Jacob Chevalier Drori,[1,*] Yordan S. Yordanov,[2,*,†] Thierry Ferrus,[3] Matthew Applegate,[2] and Crispin H. W. Barnes[2]
[1]*DAMTP, Department of Applied Mathematics and Theoretical Physics, University of Cambridge, Cambridge CB3 0WA, United Kingdom*
[2]*Cavendish Laboratory, Department of Physics, University of Cambridge, Cambridge CB3 0HE, United Kingdom*
[3]*Hitachi Cambridge Laboratory, Cambridge CB3 0HE, United Kingdom*

(Received 26 November 2020; revised 15 October 2021; accepted 8 November 2021; published 24 November 2021)

We present a set of techniques, based on the repeated arbitrary application of CP, CNOT, and SWAP$^\alpha$ (power-of-SWAP) quantum gate operations to an n-qubit quantum computer that can be used in its verification. We find isomorphisms between the groups generated by these gate operations and known groups and use techniques from representation theory to determine their invariant subspaces. For the CP operation, we find an isomorphism to the direct product of $n(n-1)/2$ cyclic groups of order 2, and determine 2^n one-dimensional invariant subspaces corresponding to the computational-basis vectors. For the CNOT operation, we find an isomorphism to $GL(n, 2)$, and determine two one-dimensional invariant subspaces and one $(2^n - 2)$-dimensional invariant subspace. For the SWAP$^\alpha$ operation we find a complex structure of invariant subspaces with varying dimensions and occurrences and present a recursive procedure to construct them. Using knowledge of these invariant subspaces, we propose a hardware verification scheme which tests the correct functioning of a quantum computer.

DOI: 10.1103/PhysRevA.104.052619

I. INTRODUCTION

As quantum computers are now on the cusp of practical use [1–3], there is a growing requirement for methods to verify that they are working as intended. This requirement is complicated by the fact that there are no quantum computers available that could be used as a reference system, so classical computers must be relied upon [3–5]. However, the use of classical computers to fully simulate a quantum circuit quickly becomes infeasible as the size of the quantum computer increases. For example, for even a relatively small quantum computer with 50 qubits, the wave function would require 16 petabytes of data storage. Manipulating such a large amount of data is cumbersome and expensive, and few have tried it in this context [3,6,7].

Therefore, algorithms must be run on quantum hardware whose outputs can easily be verified as correct or incorrect by a classical computer. However, running a single algorithm and getting a satisfactory outcome is not a particularly rigorous test of the full functionality of a quantum computer. What is required are classes of verification tests with effectively infinite variability where the correctness of the output can be easily checked using a classical computer.

We suggest a class of verification tests that utilize the invariance of certain Hilbert subspaces under the action of sets $\mathcal{S}$ of quantum gates. For some natural choices of $\mathcal{S}$, these invariant subspaces can be determined explicitly, and so it is possible to prepare the quantum computer in an initial state which is known to be fully contained within a chosen invariant subspace. Then, an arbitrary string of gates in $\mathcal{S}$ is applied. In the absence of hardware errors, the final state would also lie fully in the same invariant subspace. Hence, by measuring the "leakage" of the state out of the invariant subspace, the fidelity of the gates in $\mathcal{S}$ can be assessed.

Our proposal may be viewed as a hybrid *prepare-and-send* and *receive-and-measure* scheme, under the classification given in [8]. That is, the *verifier*, whose task is to verify the correct functioning of the quantum computer, prepares a state and sends it to the quantum computer, which performs a computation and returns the final state to the verifier to be measured. The result of this measurement determines whether the quantum computer passes or fails the test. In our proposal, the role of the verifier is simple: It prepares a state in a given invariant subspace, and measures whether the state has remained in that subspace during computation.

Whereas most proposed verification schemes (see [8] for an overview) demand that the hardware output agrees with the theoretical output of an error-free quantum computer, our test only demands that the output lie in the correct invariant subspace. Therefore our test is easier to pass than many others: It is not sensitive to errors which preserve the invariant subspaces. However, the benefit of our proposal is the essentially infinite variability in choice of quantum circuits to run. Rather than only running specific circuits where a classical computer can easily verify that the output is precisely correct, our proposal grants far more freedom to choose the sequence of gates to be applied. Our test can therefore be used to gain a broad overview of the performance of a given set of gates when applied to different states and in different sequences.

Here, we consider three sets of quantum gate operations: those generated by all possible CP (controlled-phase), CNOT (controlled-NOT), and the SWAP$^\alpha$ (power-of-SWAP) quantum

*These authors contributed equally to this work.
†yy387@cam.ac.uk

gate operations on an n-qubit system, respectively. These two-qubit quantum gates are commonly used in basic-gate sets [9–11] for universal, gate-based [9,12–14] quantum computing. Measuring their performance is critical for verifying the operation of NISQ devices [1–3] and early fault-tolerant quantum computers [11,15,16].

We begin by identifying the groups formed by each of the three two-qubit quantum gate operations mentioned above. We then determine the invariant Hilbert subspaces corresponding to each of the three groups. For the CP operation, we determine 2^n one-dimensional invariant subspaces corresponding to the computational state vectors. For the CNOT operation, we determine two one-dimensional invariant subspaces and one $(2^n - 2)$-dimensional invariant subspace. For the SWAP$^\alpha$ operation we find a number of $O(n^2)$ distinct invariant subspaces, and present a recursive algorithm to explicitly construct these subspaces. Then, we discuss the use of these invariant subspaces in a verification procedure for quantum hardware.

The paper is organized as follows: In Sec. II, we outline our theoretical framework and notation. In Sec. III we present our analysis of the group theoretic properties of the CP (Sec. III A), the CNOT (Sec. III B), and the SWAP$^\alpha$ (Sec. III C) gate operations, and outline our verification procedure (Sec. III D). We conclude in Sec. IV.

II. THEORETICAL APPROACH AND NOTATION

A quantum gate operation is a unitary map on the Hilbert space of a qubit system. Given a set $\mathcal{S}$ of quantum gate operations, there is an associated group of unitary maps generated by the elements of $\mathcal{S}$: the group of all the maps that can be formed by sequentially performing a finite number of operations in $\mathcal{S}$ as well as their inverses. For an n-qubit system, we will denote the groups associated with the sets of CP, CNOT, and SWAP$^\alpha$ gate operations by CP$^{(n)}$, CNOT$^{(n)}$, and SWAP$^{\alpha(n)}$, respectively. We will denote gate operations over an ordered pair of qubits i and j by CP$_{ij}^{(n)}$, CNOT$_{ij}^{(n)}$, and SWAP$_{ij}^{\alpha(n)}$. To determine the elements and orders of these groups we must find all distinct operations that can be performed with the corresponding quantum gate operations.

As an example, for a two-qubit system one can easily verify by hand that the CNOT$^{(2)}$ group consists of the identity map, the two CNOT operations CNOT$_{0,1}^{(2)}$ and CNOT$_{1,0}^{(2)}$, and their unique distinct combinations, CNOT$_{0,1}^{(2)}$ CNOT$_{1,0}^{(2)}$, CNOT$_{1,0}^{(2)}$ CNOT$_{0,1}^{(2)}$ and CNOT$_{0,1}^{(2)}$ CNOT$_{1,0}^{(2)}$ CNOT$_{0,1}^{(2)}$. Hence $|\text{CNOT}^{(2)}| = 6$.

Throughout this work we use the "natural" matrix representations of the CP$^{(n)}$, CNOT$^{(n)}$, and SWAP$^{\alpha(n)}$ groups: the $2^n \times 2^n$ matrix representations which are obtained when the corresponding maps are written in the computational basis for the n-qubit Hilbert space.

III. RESULTS

A. The CP$^{(n)}$ group and invariant subspaces

The controlled-phase CP gate is a two-qubit quantum gate that performs a controlled z rotation by π on a target qubit if a control qubit is in the state $|1\rangle$. The CP gate is maximally entangling. Therefore it is extensively used as an entangling gate in basic-gate sets for universal gate-based quantum computation, and in measurement-based quantum computation [16–18] to construct cluster states [17].

The CP operations are invariant under the exchange of control and target qubits, and are their own inverses. This means that the CP$^{(2)}$ group has only one generator of order 2. Hence the CP$^{(2)}$ group is isomorphic to the cyclic group of order 2, which is denoted by C_2. The CP$^{(n)}$ group is generated by the $n(n-1)/2$ distinct CP operations on n qubits, which are all group elements of order 2. Since these operations commute, CP$^{(n)}$ is an abelian group. Moreover, these operations form a minimal generating set: None of the operations can be written as a product of the others and their inverses. As each CP operation has order 2, it follows that the CP$^{(n)}$ group is isomorphic to the direct product of $n(n-1)/2$ cyclic groups of order 2: CP$^{(n)} \cong C_2^{n(n-1)/2}$. The order of the CP$^{(n)}$ group is given by

$$|\text{CP}^{(n)}| = 2^{n(n-1)/2}. \tag{1}$$

The matrices in the matrix representation of the CP$^{(2)}$ group are

$$\text{CP}_{0,1}^{(2)} \rightarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix},$$

$$\text{and } \text{CP}_{0,1}^{(2)\,2} \rightarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \tag{2}$$

Similarly, the matrix representation of the CP$^{(n)}$ group for $n > 2$ is diagonal with $\{-1, +1\}$ entries. Therefore each computational basis state vector spans a one-dimensional invariant Hilbert subspace by itself.

B. The CNOT$^{(n)}$ group and invariant subspaces

The CNOT operation is a two-qubit quantum gate which flips the state of a target qubit if a control qubit is in the state $|1\rangle$. In the computational basis, the two generating elements of CNOT$^{(2)}$ are represented by the following matrices:

$$\text{CNOT}_{1,0}^{(2)} \rightarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

$$\text{and } \text{CNOT}_{0,1}^{(2)} \rightarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}. \tag{3}$$

Like the CP gate, the CNOT gate is maximally entangling, capable of transforming separable states to maximally entangled states. It is another commonly implemented two-qubit gate in gate-based quantum computers [9–11].

In order to investigate the CNOT$^{(n)}$ group, it is useful to associate each computational basis state vector with an element of $\mathbb{F}_2^n$, the n-dimensional vector space over the field with two elements. We do this in the natural way: For example, we associate the state vector $|010\rangle$ with the vector (0,1,0). Since each CNOT operation sends the computational basis to itself (each basis state vector is transformed to a basis state vector), we can further associate each element $g \in \text{CNOT}_n$ with a corresponding function, call it $\theta(g)$, on $\mathbb{F}_2^n$. It can be shown (see Appendix A) that $\theta(g) \in GL(n, 2)$, the group of invertible linear maps from $\mathbb{F}_2^n$ to itself, and moreover that the map $\theta : \text{CNOT}^{(n)} \to GL(n, 2)$ is a group isomorphism. Hence $\text{CNOT}^{(n)} \cong GL(n, 2)$.

By inspection we find that $\text{CNOT}^{(n)}$ has two one-dimensional invariant subspaces: $V_0 = \text{span}\{|0\rangle\}$ and $V_1 = \text{span}\{\frac{1}{\sqrt{2^n-1}} \sum_{i=1}^{2^n-1} |i\rangle\}$. The invariance of V_0 is evident, while for V_1 one should note that each CNOT operation is a bijection when restricted to the set formed of all computational basis states except $|0...0\rangle$. Furthermore, it can be shown (see Appendix B) that the Hilbert subspace orthogonal to V_0 can be decomposed into two irreducible invariant subspaces, one of which is V_1. Therefore, we deduce that the $(2^n - 2)$-dimensional subspace V_2, that is orthogonal to V_0, and V_1, is itself an irreducible invariant subspace. Hence, the action of $\text{CNOT}^{(n)}$ on the Hilbert space of n qubits has three irreducible invariant subspaces that can be defined in terms of basis vectors as

$$V_0 = \text{span}\{|0\rangle\}, \tag{4}$$

$$V_1 = \text{span}\{|v_1\rangle\}, \text{ where } |v_1\rangle = \frac{1}{\sqrt{2^n - 1}} \sum_{i=1}^{2^n-1} |i\rangle, \text{ and} \tag{5}$$

$$V_2 = \text{span}\left\{ \frac{\sqrt{2^n - 1}|i\rangle - |v_1\rangle}{2^{n/2}} : i = 1, ..., 2^n - 1 \right\} \tag{6}$$

We can also use the isomorphism $\text{CNOT}^{(n)} \cong GL(n, 2)$ to find the order of the CNOT group. For large numbers of qubits n, it can approximated as

$$|\text{CNOT}^{(n)}| = |GL(n, 2)| = \prod_{i=0}^{n-1} (2^n - 2^i) \approx 0.29 \times 2^{n^2}. \tag{7}$$

C. The $\text{SWAP}^{\alpha(n)}$ group and invariant subspaces

The SWAP^α is a two-qubit quantum-gate operation that continuously exchanges the values of two qubits as α is varied. The action of the SWAP^α on a two-qubit system can be illustrated by its matrix representation:

$$\text{SWAP}_{01}^{\alpha(2)} \to \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \frac{1}{2}(1 + e^{i\pi\alpha}) & \frac{1}{2}(1 - e^{i\pi\alpha}) & 0 \\ 0 & \frac{1}{2}(1 - e^{i\pi\alpha}) & \frac{1}{2}(1 + e^{i\pi\alpha}) & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \tag{8}$$

The SWAP^α gate can entangle for noninteger values of α. It is often implemented in spin-qubit quantum computing architectures [19–22], since it arises naturally from the spin exchange interaction [23–26]. Finding a group isomorphism and the invariant subspaces for the $\text{SWAP}^{\alpha(n)}$ group is challenging for a general value of α. Therefore, we first consider the simpler case of $\alpha = 1$, and then we generalize.

1. The $\text{SWAP}^{(n)}$ group and invariant subspaces

The SWAP gate is a two-qubit quantum gate operation that exchanges two qubits, and is not entangling. The $\text{SWAP}^{(n)}$ group on a n-qubit system is isomorphic to S_n, the group of permutations over n distinguishable objects (this can be seen by regarding each qubit as a distinguishable object). To determine the invariant subspace structure of $\text{SWAP}^{(n)}$, we first note that the SWAP operation conserves the Hamming weight (the number of qubits in state $|1\rangle$) of a state. Therefore, all states with Hamming weight i span an invariant subspace V_i of order

$$|V_i| = \frac{n!}{(n-i)!i!} = \binom{n}{i}. \tag{9}$$

However V_i can be further decomposed to smaller, irreducible, invariant subspaces. Using the fact that $\text{SWAP}^{(n)} \cong S_n$, we show in Appendix C that for $i \leqslant \lfloor \frac{n}{2} \rfloor$, each V_i can be decomposed as

$$V_i = V_{i,0} \oplus V_{i,1} \oplus ..V_{i,i}, \tag{10}$$

where $V_{i,j}$ are irreducible invariant subspaces. The second subscript j denotes correspondence to the same irreducible representation (irrep) of $\text{SWAP}^{(n)}$. This implies that

$$|V_{i,j}| = |V_{i',j}| \text{ for any } j \leqslant i < i'. \tag{11}$$

For $i \geqslant \lceil \frac{n}{2} \rceil$, the irreducible invariant subspaces $V_{i,j}$ are identical upon flipping the values of all qubits. Therefore, we consider only the case $i \leqslant \lfloor \frac{n}{2} \rfloor$. From Eq. (10), it follows that the total number of irreducible invariant subspaces is

$$N = \begin{cases} \sum_{i=0}^{\frac{n}{2}-1} (i+1) + \frac{n+2}{2} = \frac{(n+2)^2}{4}, & n \text{ even} \\ 2\sum_{i=0}^{\frac{n-1}{2}} (i+1) = \frac{(n+1)(n+3)}{4}, & n \text{ odd}, \end{cases} \tag{12}$$

and that the number of irreducible invariant subspaces V_{ij} for a given value of j is

$$N_j = |n - 2j| + 1. \tag{13}$$

From Eq. (11) it follows that the dimensions of the V_{ij}s are given by

$$|V_{i,j}| = \begin{cases} \binom{n}{j}, & \text{for } j = 0 \\ \binom{n}{j} - \binom{n}{j-1}, & \text{for } 1 \leqslant j \leqslant n/2. \end{cases} \tag{14}$$

Based on Eqs. (10) and (11), and using the fact that the subspaces $V_{i,j}$ and $V_{i',j}$ correspond to the same irreducible representation of $\text{SWAP}^{(n)}$, we designed and implemented a recursive computational procedure, outlined in Appendix D, to find explicit sets of basis vectors for each of the $V_{i,j}$.

We demonstrate our procedure with the example of the $\text{SWAP}^{(8)}$ group. We find bases for its subspaces V_{ij}s, and use these bases to construct a transformation matrix, which we use to block diagonalize the matrix representation of the $\text{SWAP}^{(8)}$ group. The transformed block-diagonal form of the matrix representation of $\text{SWAP}^{(8)}$ is given in the form of a matrix plot in Fig. 1.

Each diagonal block in the transformed matrix in Fig. 1 corresponds to an irreducible invariant subspace V_{ij} (ordered, from left to right, in terms of increasing i and decreasing j). Therefore the number of occurrences and the dimensions of the blocks should match those of the V_{ij}s, given by Eqs. (13) and (14), respectively. It can be verified by inspection that this is indeed true.

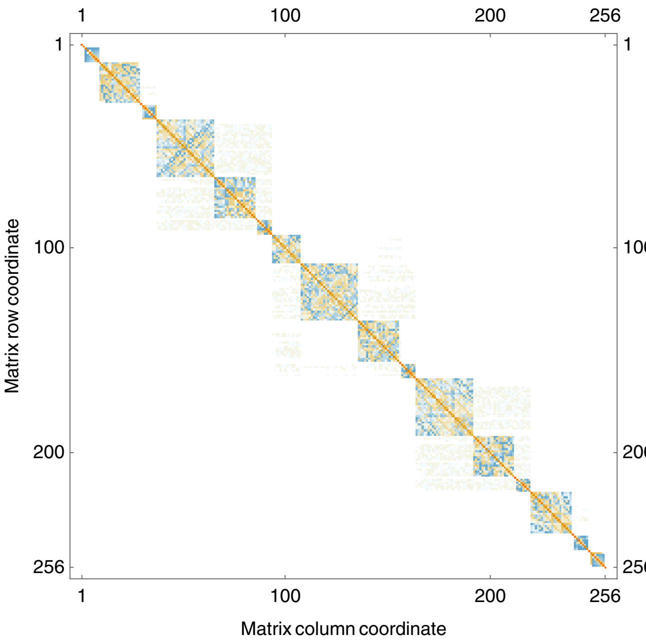

FIG. 1. Matrix color plot of the $2^8 \times 2^8$ block diagonalized matrix representation of the SWAP$^{(8)}$ group. The matrix plot is obtained by summing and block diagonalizing a large number of matrices from the matrix representation of the SWAP$^{(8)}$. Blue-green elements correspond to negative values. Yellow-red elements correspond to positive values. Pale colored matrix elements outside the diagonal blocks correspond to small rounding errors.

2. *Invariant subspaces of* SWAP$^{\alpha}$

We show that the SWAP$^{\alpha(n)}$ has the same irreducible invariant subspaces for any real $\alpha \neq 0$, including the case of $\alpha = 1$. To see why this is true, we decompose the matrix representation of $\text{SWAP}_{01}^{\alpha(2)}$, given in Eq. (8), as

$$\text{SWAP}_{01}^{\alpha(2)} = c\, \text{SWAP}_{01}^{(2)} + b\, I^{(2)}, \tag{15}$$

where $c = \frac{1}{2}(1 - e^{i\pi\alpha})$, $b = \frac{1}{2}(1 + e^{i\pi\alpha})$, and I is the identity. This decomposition is true for any number of qubits n, so we can write

$$\text{SWAP}_{pq}^{\alpha(n)} = c\, \text{SWAP}_{pq}^{(n)} + b\, I^{(n)}. \tag{16}$$

Suppose $|\psi\rangle \in V_{i,j}$, where $V_{i,j}$ is the invariant subspace of SWAP$^{(n)}$ as described above. Then

$$\text{SWAP}_{pq}^{\alpha(n)}|\psi\rangle = c\, \text{SWAP}_{pq}^{(n)}|\psi\rangle + b|\psi\rangle, \tag{17}$$

since the invariance of $V_{i,j}$ under SWAP$^{(n)}$ implies that $\text{SWAP}_{pq}^{(n)}\, |\psi\rangle \in V_{i,j}$. Hence the invariant subspaces of SWAP$^{\alpha(n)}$ are contained within those of SWAP$^{(n)}$. Conversely, provided $\alpha \neq 0$, so that $c \neq 0$, we may invert (16) to get

$$\text{SWAP}_{pq}^{(n)} = \frac{\text{SWAP}_{pq}^{\alpha(n)} - b\, I^{(n)}}{c}, \tag{18}$$

and the previous argument shows that the invariant subspaces of SWAP$^{(n)}$ are contained in those of SWAP$^{\alpha(n)}$. Therefore SWAP$^{(n)}$ and SWAP$^{\alpha(n)}$ share the same irreducible invariant subspaces $V_{i,j}$.

D. Invariant subspace verification test

In this section we outline a procedure that uses our knowledge of the invariant subspaces of a group $G^{(n)}$ generated by a set $\mathcal{S}$ of gates on an n-qubit system (e.g., $G^{(n)} = \text{CNOT}^{(n)}$) to test the performance of a quantum computer. Let the invariant irreducible subspaces of $G^{(n)}$ be $\{U_i\}$, and let P_i be the orthogonal projector onto U_i.

The procedure consists of the following three steps.

(1) Choose an i, and initialize the quantum computer in a state $|\psi_{\text{in}}\rangle \in U_i$.

(2) Apply a sequence of gates from $\mathcal{S}$. This sequence could be randomly generated. The more gates applied, the more difficult the test is to pass.

(3) Perform a projective measurement with projection operators P_i and $\mathbb{1} - P_i$. If the state is found to lie in U_i (i.e., the measurement result corresponding to the projector P_i), then the test is passed; otherwise the test is failed.

If the gate operations are implemented perfectly, then the final state $|\psi_{\text{out}}\rangle$ of the quantum computer remains confined within the initial invariant subspace U_i. However, in practice, the gate operations are implemented with fidelity less than one. Hence, the state of the quantum computer will "leak" out of the initial invariant subspace: the failure probability of the test $p_{\text{fail}} = 1 - \langle\psi_{\text{out}}|P_i|\psi_{\text{out}}\rangle$ will become nonzero.

Let $p_{\text{fail}}(k)$ be the test failure probability when a sequence of k gates is applied during step 2. The speed at which $p_{\text{fail}}(k)$ grows with k depends on the form and severity of errors that occur when applying gates. To gain a basic intuition for this growth, consider the following simple error model: Whenever a gate is applied during step 2, move a small distance in a random direction orthogonal to the current state, and then rescale the result to ensure correct normalization. More precisely, fix a small $\epsilon > 0$. After applying each gate, choose $|\phi\rangle$ uniformly randomly from the set of states orthogonal to the current state $|\psi\rangle$, and update the state via $|\psi\rangle \to \frac{|\psi\rangle + \epsilon|\phi\rangle}{\sqrt{1+\epsilon^2}}$.

In this model, the initial growth of p_{fail} is easily quantified. Let $d = \dim U_i$, and $D = 2^n$ be the dimension of the full Hilbert space. Then $p_{\text{fail}}(k) \approx k\epsilon^2(1 - \frac{d-1}{D-1})$, where the approximation holds when $\epsilon \ll 1$ and k is small enough that $p_{\text{fail}}(k) \ll 1$ (the proof is elementary, but only tangentially related to the bulk of this paper, so we omit it). Note that the growth is fastest when d is small compared to D, and slowest when d is of comparable size to D. Although we have only discussed a very simple error model, we expect this feature to remain true for more realistic models.

We remark that on the current NISQ computers, the initialization and the measurement steps, 1 and 3, respectively, might incur errors of comparable magnitudes to the error incurred from the multiple gate operations, which we want to measure. A possible solution to mitigate the initialization and measurement errors would be to use POVMs [27–30] followed by post-processing, to initialize and measure the state in steps 1 and 3, respectively. We will consider such error mitigation in a future work.

1. *Verification with* CP

As noted in Sec. III A, the individual n-qubit computational basis states are one-dimensional invariant subspaces under the action of the CP$^{(n)}$ group. Multiple CP operations do not change the Z-basis measurement probabilities. Therefore, the verification procedure outlined above will require simply (1) an initial measurement in the Z basis, (2) application of multiple different $\text{CP}^{(n)}$ operations, and (3) a final measurement in the Z basis. Any deviation from the measurement probabilities will indicate an error. Since the CP operation can be created in a number of different ways, for example, from a combination of CNOT operations and single-qubit operations, this simple test can be used to test multiple operations of a quantum computer.

2. Verification with \text{\sc cnot}

As shown in Sec. III B the $\text{CNOT}^{(n)}$ group has a large $(2^n - 2)$-dimensional irreducible invariant subspace. This implies that the CNOT operation alone is of limited value in our verification procedure described above. Even imperfect CNOT operations acting on a qubit state, initialized within the large subspace, would be likely to produce small projections onto the two one-dimensional invariant subspaces. Alternatively, initializing a state in either of the two one-dimensional invariant subspaces would be a useful test, but not as comprehensive as the CP operation.

3. Verification with SWAP^{α}

The SWAP^{α} gate is the most interesting and resourceful when it comes to invariant subspaces and their use in our verification procedure. The most simple procedure involving the SWAP^{α} gate would be to check if multiple applications of randomly chosen operations conserves the Hamming weight of the initial state. This would correspond to testing the invariance of the V_i subspaces. A more complicated and comprehensive test would utilize the irreducible invariant subspaces V_{ij}. Such a test would require a more elaborate procedure to initialize the state in a given irreducible invariant subspace V_{ij} and subsequently to perform a measurement projecting onto the basis of this subspace. Again, this test can be made more comprehensive by constructing the SWAP^{α} operation from combinations of the other entangling gates and single-qubit operations.

IV. CONCLUSION

In this work we analyzed the operation of the CP, the CNOT, and the SWAP^{α} quantum gate operations from a group theoretic point of view. We found that the group of CP operations on n qubits is isomorphic to the direct product of $n(n-1)/2$ cyclic groups of order 2 and determined that its irreducible invariant subspaces correspond to the individual computational basis state vectors. We found that the group of CNOT operations on n qubits is isomorphic to the general linear group of n-dimensional space over a field with two elements, $GL(n, 2)$. We used this result to demonstrate that the group generated by CNOT operations on n qubits has one $(2^n - 2)$-dimensional and two one-dimensional irreducible invariant subspaces. For the SWAP^{α} operation we showed that its irreducible invariant subspaces are the same for all values of α. We therefore investigated the simpler case of the SWAP operation and constructed a method to determine its irreducible invariant subspaces.

For each group we considered, we suggested how to construct verification tests for the operation of a quantum computer, using the invariant subspaces discovered. These tests initialize a state in a particular invariant subspace, and measure by how much the state has deviated out of subspace after multiple applications of the corresponding quantum gate operations. We believe that these tests will be important for verifying the operation of NISQ and early fault-tolerant quantum computers.

ACKNOWLEDGMENTS

Y.S.Y. acknowledges financial support from the Engineering and Physics Research Council (EPSRC) and Hitachi Cambridge Laboratory via CASE studentships RG97399 (voucher 18000078). C.H.W.B. and Y.Y. would like to thank Dr. Ross Lawther for his guidance in constructing the invariant subspaces for both the CNOT and the SWAP^{α} operations. We also would like to thank A. Lasek, D. Arvidsson-Shukur, H. Lepage, and N. Devlin for useful discussions.

APPENDIX A: PROOF THAT $\text{CNOT}^{(n)} \cong GL(n, 2)$

For each $g \in \text{CNOT}^{(n)}$, let $\theta(g)$ be the function from $\mathbb{F}_2^n \to \mathbb{F}_2^n$ obtained by associating computational basis elements with elements of $\mathbb{F}_2^n$ as previously described. First note that for all $f, g \in \text{CNOT}^{(n)}$, we have $\theta(f \circ g) = \theta(f) \circ \theta(g)$ (this follows trivially from the one-to-one association between the computational basis and $\mathbb{F}_2^n$). Hence, if we can show that $\theta(\text{CNOT}_{ij}^{(n)}) \in GL(n, 2)$ for all i, j, then since the $\text{CNOT}_{ij}^{(n)}$s generate $\text{CNOT}^{(n)}$ it will follow that $\theta(g) \in GL(n, 2)$ for all $g \in \text{CNOT}^{(n)}$.

Let $g = \text{CNOT}_{ij}^{(n)}$. Since $\theta(g)$ leaves all but the i^{th} and j^{th} entries unaffected, it suffices to consider only the two-qubit case with $g = \text{CNOT}_{01}^{(2)}$, and show that $\theta(g)$ is linear and invertible. To do so, we simply write down the effect of $\theta(g)$ on each element of $\mathbb{F}_2^2$: $(0, 0) \mapsto (0, 0)$, $(0, 1) \mapsto (0, 1)$, $(1, 0) \mapsto (1, 1)$, and $(1, 1) \mapsto (1, 0)$. One can easily see that $\theta(g)$ is invertible, and remembering that addition is modulo 2, $\theta(g)$ is also linear as required.

So θ maps into $GL(n, 2)$, and since it is structure preserving [i.e., $\theta(f \circ g) = \theta(f) \circ \theta(g)$] it is a group homomorphism from $\text{CNOT}^{(n)} \to GL(n, 2)$. In order to show that θ is an isomorphism, we must further show that it is a bijection. Injectivity is immediate, since $\ker\theta = \{\text{id}\}$. In order to show surjectivity, it suffices to show that $\text{im}\theta$ contains a generating set. It can be shown [31] that $GL(n, 2)$ is generated by the linear maps m_1 and m_2 given in the standard basis by the matrices

$$M_1 := \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & \ddots & \\ 1 & & & 1 \end{pmatrix} \text{ and } M_2 := \begin{pmatrix} 0 & 1 & & & \\ & 0 & 1 & & \\ & & & \ddots & 1 \\ 1 & & & & 0 \end{pmatrix}.$$

Since $m_1 = \theta(\text{CNOT}_{n-1\,0}^{(n)})$, $m_1 \in \text{im}\theta$. The map m_2 acts on elements of $\mathbb{F}_2^n$ by applying the permutation (01...n-1) to entries. Since $\text{CNOT}_{ij}^{(n)}\text{CNOT}_{ji}^{(n)}\text{CNOT}_{ij}^{(n)} = \text{SWAP}_{ij}^{(n)}$, the group $\text{CNOT}^{(n)}$ contains all SWAPs and hence $\text{im}\theta$ contains all maps which are transpositions of tuple entries. Since transpositions generate S_n, we conclude that $m_2 \in \text{im}\theta$ and hence that θ is surjective, finishing the proof.

APPENDIX B: IRREDUCIBLE INVARIANT SUBSPACES OF CNOT$^{(n)}$

Here we consider the decomposition of the Hilbert space of n qubits to subspaces that are invariant under the action of the CNOT$^{(n)}$ group. First we note that the CNOT operations do not affect the zeroth state $|0\rangle = |00..0\rangle$, so it spans a one-dimensional invariant subspace $V_0 = \text{span}\{|0\rangle\}$, on its own. Let us denote the set of computational basis states excluding the zeroth as X, so that $X = \{|i\rangle : i = 1, ..., 2^n - 1\}$, and the Hilbert space spanned by the set as $V_0^\perp$. To find the decomposition to irreducible invariant subspaces of $V_0^\perp$, we first show that the action of the CNOT$^{(n)}$ group on X is doubly transitive.[1]

Proof. Note that it suffices to provide a single tuple of states $(|\psi_1\rangle, |\psi_2\rangle)$ such that any other tuple $(|\psi_1'\rangle, |\psi_2'\rangle)$ with $|\psi_1'\rangle \neq |\psi_2'\rangle$ may be obtained by successive application of CNOT gates: Double transitivity will then follow. Consider $(|\psi_1\rangle, |\psi_2\rangle) = (|010..0\rangle, |100..0\rangle)$. Using CNOT operations with the zeroth and first qubits as control qubits, we can change the values of the other $n-2$ qubits of each state separately, and take the initial tuple to any other tuple of states where the first two qubits are unchanged. Therefore we only need to show that CNOT$^{(2)}$ acts doubly transitively on the set $\{|01\rangle, |10\rangle, |11\rangle\}$. This can be verified easily by hand, completing the proof.

We now use proposition 4.4.4 from [32], which states that for a group G that acts doubly transitively on a set of vectors S, the space spanned by S decomposes to two irreducible invariant subspaces. Transferring this result to the context of our problem, it means that $V_0^\perp$ decomposes to two irreducible invariant subspaces under the action of CNOT$^{(n)}$.

Finally we note that the state vector $v_1 = \frac{1}{\sqrt{2^n-1}} \sum_{i=1}^{2^n-1} |i\rangle$ is invariant under CNOT$^{(n)}$ because each CNOT operation is a bijection (one-to-one and onto) between all computational basis state vectors, except the zeroth state vector. Therefore the (2^n-2)-dimensional subspace V_2, that is orthogonal to both V_0 and V_1, is an irreducible invariant subspace.

APPENDIX C: IRREDUCIBLE INVARIANT SUBSPACES OF SWAP$^{(n)}$

Since SWAP operations conserve the Hamming weight of quantum states, the subspace V_i spanned by all state vectors of Hamming weight i is invariant under SWAP$^{(n)}$. However V_i can be decomposed further to smaller invariant subspaces.

Consider the action of the group SWAP$^{(n)}$ on n qubits. For $i \leqslant \frac{n}{2}$, let x_i be the set of i-element subsets of X (so that the action of S_n on x_i is isomorphic to the action of SWAP$^{(n)}$ on V_i).

Let π_i be the permutation representation character of the action of S_n on x_i. The Hermitian product of two such characters π_k and π_l is given by

$$\langle \pi_k, \pi_l \rangle = \frac{1}{|S_n|} \sum_{s \in S_n} \pi_k(s)\pi_l(s) = \langle \pi_k \pi_l, 1_G \rangle = l + 1, \quad \text{(C1)}$$

where $0 \leqslant l \leqslant k \leqslant \frac{n}{2}$, and 1_G denotes the trivial representation.

Fix $k \leqslant \lfloor n \rfloor$ and assume for our inductive hypothesis that for $0 \leqslant i \leqslant k-1$,

$$\pi_i = \chi^{(n,0)} + \chi^{(n-1,1)} + ... + \chi^{(n-i,i)} \quad \text{(C2)}$$

where the χs are irreducible characters (characters of irreducible representation of S_n).

For $r = 0$, x_0 has one element so S_n acts trivially on it, thus $\pi_0 = 1_G$. This implies that $\chi^{(n,0)} = 1_G$.

For $1 \leqslant i \leqslant k-1$, writing $\chi^{(n-i,i)} = \pi_i - \pi_{i-1}$, and using (C1) we get

$$\langle \pi_k, \chi^{(n-i,i)} \rangle = \langle \pi_k, \pi_i \rangle - \langle \pi_k, \pi_{i-1} \rangle = 1. \quad \text{(C3)}$$

Therefore $\chi^{(n-i,i)}$ is a component of π_k with multiplicity 1. Hence we can write

$$\pi_k = \chi^{(n,0)} + \chi^{(n-1,1)} + ... + \chi^{(n+1-k,k-1)} + \chi' \quad \text{(C4)}$$

for some χ'.

But $\langle \pi_k, \pi_k \rangle = k + 1$ from (C1), and $\langle \pi_k, \pi_k \rangle = k + \langle \chi', \chi' \rangle$ from (C4), so $\langle \chi', \chi' \rangle = 1$. Therefore χ' is an irreducible character which we denote as $\chi^{(n-k,k)}$. Hence:

$$\pi_k = \chi^{(n,0)} + \chi^{(n-1,1)} + ... + \chi^{(n-k,k)}, \quad \text{(C5)}$$

where each χ is an irreducible character (corresponding to an irreducible invariant subspace). Thus the inductive step is complete. This result implies that for an n-qubit system, V_i decomposes into irreducible invariant subspaces, under SWAP$^{(n)}$, as

$$V_i = V_{i,0} \oplus V_{i,1} \oplus ..V_{i,i}, \quad \text{(C6)}$$

where subspace $V_{i,j}$ corresponds to irrep $\chi^{(n-j,j)}$.

APPENDIX D: CONSTRUCTING BASIS STATE VECTORS FOR THE IRREDUCIBLE INVARIANT SUBSPACES OF SWAP(n)

The Hilbert subspaces V_i corresponding to n-qubit states of Hamming weight i are invariant under the action of SWAP$^{(n)}$. However, as proved in Appendix C, the subspaces V_i can be decomposed further as $V_i = V_{i,0} \bigoplus V_{i,1} \bigoplus ... \bigoplus V_{i,i}$ where $V_{i,j}$ are irreducible invariant subspaces, and the second subscript j denotes correspondence to the same irrep. of SWAP$^{(n)}$. In particular, we have $|V_{i,j}| = |V_{i',j}|$ for any $j \leqslant i < i'$. Below we outline a procedure to construct a set of basis state vectors for the subspaces $V_{i,j}$ for an n-qubit system. We consider the case of $i \leqslant \lfloor \frac{n}{2} \rfloor$ only, since the case for $i > \lfloor \frac{n}{2} \rfloor$ is identical upon global qubit flip.

Constructing basis state vectors for $V_{i,j}$.

(1.) For $i = 0$, we have the one-dimensional invariant subspace V_0 spanned by the zeroth state vector,

$$V_0 = V_{0,0} = \text{span}\{|0..0\rangle\}. \quad \text{(D1)}$$

(2.) For $i = 1$, $|V_1| = n$, and $V_1 = V_{1,0} \bigoplus V_{1,1}$. Also $|V_{0,0}| = |V_{1,0}| = 1$ and $|V_{1,1}| = |V_1| - |V_{0,0}| = n - 1$. The single state vector of $V_{1,0}$ can be written as the sum of all computational state vectors in V_1 (all state vectors with

[1] An action of a group on a set of elements is doubly transitive if for any two ordered tuples, each having a pair of distinct elements from the set, there is a group element taking one ordered tuple to the other.

Hamming weight 1):

$$V_{1,0} = \text{span}\left\{\frac{1}{\sqrt{n}}\sum_{|\phi\rangle\in V_1}|\phi\rangle\right\} = \frac{1}{\sqrt{n}}\sum_{i=0}^{n-1}|..0_{i-1}1_i0_{i+1}..\rangle\bigg\}. \tag{D2}$$

$V_{1,1}$ can be determined by taking an arbitrary set of basis state vectors for the orthogonal compliment of $V_{1,0}$ in V_1.

(3.) For $i \geqslant 2$, $V_i = V_{i,0} \bigoplus V_{i,1} \bigoplus ... \bigoplus V_{i,i}$ and $|V_i| = \binom{n}{i}$. Let $V_{i,i}^{\perp}$ denote the orthogonal complement of $V_{i,i}$ in V_i.

First we need to find sets of basis state vectors that span $V_{i,i}$ and $V_{i,i}^{\perp}$. Note that $|V_{i,i}^{\perp}| = |V_{i-1}|$, since the two spaces consist of irreducible subspaces that correspond to the same irreps of SWAP$^{(n)}$ ($V_{i,i}^{\perp} = V_{i,0} \bigoplus V_{i,1} \bigoplus ... \bigoplus V_{i,i-1}$ and $V_{i-1} = V_{i-1,0} \bigoplus V_{i-1,1} \bigoplus ... \bigoplus V_{i-1,i-1}$, respectively). Furthermore, this means that we can construct basis state vectors for $V_{i,i}^{\perp}$ such that they transform, under SWAP operations, in the same way as the computational state vectors in V_{i-1} (the state vectors with Hamming weight $i-1$). Then we will be able to decompose $V_{i,i}^{\perp}$ in the same way as we decomposed V_{i-1}. In practice this can be conveniently implemented recursively.

The basis state vectors for $V_{i,i}^{\perp}$ can be constructed in the following way.

(1) Denote the $\binom{n}{i-1}$ basis state vectors for $V_{i,i}^{\perp}$ by $v_{s_k}^{i}$, where $\{s_k\}$ are all subsets of size $i-1$ of the set $\{0, .., n-1\}$, for $k = 0, ..., \binom{n}{i-1} - 1$; e.g., for $n = 4$, $i = 2$: $s_0 = \{0\}$, $s_1 = \{1\}$, $s_2 = \{2\}$, $s_3 = \{3\}$.

(2) Construct $v_{s_k}^{(i)}$ by summing over all computational state vectors, with Hamming weight i, whose qubits in positions given by the elements of s_k are in the $|1\rangle$ state; e.g., for $n = 4$, $i = 2$:

$$|v_0^{(2)}\rangle = \frac{|1100\rangle + |1010\rangle + |1001\rangle}{\sqrt{3}}$$

$$|v_1^{(2)}\rangle = \frac{|1100\rangle + |0110\rangle + |0101\rangle}{\sqrt{3}},$$

$$|v_2^{(2)}\rangle = \frac{|1010\rangle + |0110\rangle + |0011\rangle}{\sqrt{3}},$$

$$|v_3^{(2)}\rangle = \frac{|1001\rangle + |0101\rangle + |0011\rangle}{\sqrt{3}}.$$

The SWAP$^{(n)}$ action on the $\{|v_k^{(i)}\rangle\}$ basis is isomorphic to the SWAP$^{(n)}$ action on the computational basis of V_{i-1}, where the isomorphism is the map taking $v_{s_k}^{(i)}$ to the computational state vector with Hamming weight $i-1$ and qubits in positions given by the elements of s_k, in the $|1\rangle$ state. Therefore $V_{i,i}^{\perp}$ can be decomposed to irreducible invariant subspaces in the same way as V_{i-1}, by regarding the state vectors $\{|v_k^{(i)}\rangle\}$ as the new basis for $V_{i,i}^{\perp}$.

$V_{i,i}$ can be found by taking the orthogonal complement of $V_{i,i}^{\perp}$ in V_i.

This procedure is implemented as a recursive method on MATHEMATICA. The code is available upon request from the authors.

[1] J. Preskill, Quantum **2**, 79 (2018).

[2] S. S. Tannu and M. K. Qureshi, arXiv:1805.10224.

[3] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. G. Brandao, D. A. Buell *et al.*, Nature (London) **574**, 505 (2019).

[4] H. De Raedt, F. Jin, D. Willsch, M. Willsch, N. Yoshioka, N. Ito, S. Yuan, and K. Michielsen, Comput. Phys. Commun. **237**, 47 (2019).

[5] M. Nest, Quant. Inf. Comp. **11**, 784 (2011).

[6] Z.-Y. Chen, Q. Zhou, C. Xue, X. Yang, G.-C. Guo, and G.-P. Guo, Science Bulletin **63**, 964 (2018).

[7] R. Li, B. Wu, M. Ying, X. Sun, and G. Yang, arXiv:1804.4797.

[8] A. Gheorghiu, T. Kapourniotis, and E. Kashefi, Theory Comput. Systems **63**, 715 (2018).

[9] D. P. DiVincenzo, Phys. Rev. A **51**, 1015 (1995).

[10] M. Hsieh, J. Kempe, S. Myrgren, and K. B. Whaley, Quant. Info. Proc. **2**, 289 (2003).

[11] J. M. Chow, J. M. Gambetta, A. D. Córcoles, S. T. Merkel, J. A. Smolin, C. Rigetti, S. Poletto, G. A. Keefe, M. B. Rothwell, J. R. Rozen, M. B. Ketchen, and M. Steffen, Phys. Rev. Lett. **109**, 060501 (2012).

[12] N. B. Lovett, S. Cooper, M. Everitt, M. Trevers, and V. Kendon, Phys. Rev. A **81**, 042330 (2010).

[13] D. Deutsch, Proc. R. Soc. A: Math. Phys. Eng. Sci. **400**, 97 (1985).

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

[15] P. G. Kwiat, A. J. Berglund, J. B. altepeter, and A. G. White, Science **290**, 498 (2000).

[16] B. J. Brown and S. Roberts, Phys. Rev. Research **2**, 033305 (2020).

[17] R. Raussendorf, D. E. Browne, and H. J. Briegel, Phys. Rev. A **68**, 022312 (2003).

[18] H. J. Briegel, D. E. Browne, W. Dür, R. Raussendorf, and M. Van den Nest, Nat. Phys. **5**, 19 (2009).

[19] J. J. Pla, K. Y. Tan, J. P. Dehollain, W. H. Lim, J. J. Morton, D. N. Jamieson, A. S. Dzurak, and A. Morello, Nature (London) **489**, 541 (2012).

[20] K. D. Petersson, L. W. McFaul, M. D. Schroer, M. Jung, J. M. Taylor, A. A. Houck, and J. R. Petta, Nature (London) **490**, 380 (2012).

[21] E. Togan, Y. Chu, A. S. Trifonov, L. Jiang, J. Maze, L. Childress, M. G. Dutt, A. S. Sørensen, P. Hemmer, A. S. Zibrov *et al.*, Nature (London) **466**, 730 (2010).

[22] J. Yoneda, K. Takeda, T. Otsuka, T. Nakajima, M. R. Delbecq, G. Allison, T. Honda, T. Kodera, S. Oda, Y. Hoshi *et al.*, Nat. Nanotechnol. **13**, 102 (2018).

[23] B. E. Kane, Nature (London) **393**, 133 (1998).

[24] R. Vrijen, E. Yablonovitch, K. Wang, H. W. Jiang, A. Balandin, V. Roychowdhury, T. Mor, and D. DiVincenzo, Phys. Rev. A **62**, 012306 (2000).

[25] M. Veldhorst, H. G. J. Eenink, C. H. Yang, and A. S. Dzurak, Nat. Commun. **8**, 1766 (2017).

[26] H. V. Lepage, A. A. Lasek, D. R. M. Arvidsson-Shukur, and C. H. W. Barnes, Phys. Rev. A **101**, 022329 (2020).

[27] Y. S. Yordanov and C. H. W. Barnes, Phys. Rev. A **100**, 062317 (2019).

[28] M. Oszmaniec, F. B. Maciejewski, and Z. Puchała, Phys. Rev. A **100**, 012351 (2019).

[29] D. R. M. Arvidsson-Shukur, H. V. Lepage, E. T. Owen, T. Ferrus, and C. H. W. Barnes, Phys. Rev. A **96**, 052305 (2017).

[30] S. E. Ahnert and M. C. Payne, Phys. Rev. A **71**, 012330 (2005).

[31] W. C. Waterhouse, Linear and Multilinear Algebra **24**, 227 (1989).

[32] R. Goodman and N. R. Wallach, in *Symmetry, Representations, and Invariants* Vol. 255 (Springer, Berlin/Heidelberg, 2009), pp. 219–220.