Symmetry is a unifying concept in physics. In quantum information and beyond, it is known that quantum states possessing symmetry are not useful for certain information-processing tasks. For example, states that commute with a Hamiltonian realizing a time evolution are not useful for timekeeping during that evolution, and bipartite states that are highly extendible are not strongly entangled and thus not useful for basic tasks like teleportation. Motivated by this perspective, this paper details several quantum algorithms that test the symmetry of quantum states and channels. For the case of testing Bose symmetry of a state, we show that there is a simple and efficient quantum algorithm, while the tests for other kinds of symmetry rely on the aid of a quantum prover. We prove that the acceptance probability of each algorithm is equal to the maximum symmetric fidelity of the state being tested, thus giving a firm operational meaning to these latter resource quantifiers. Special cases of the algorithms test for incoherence or separability of quantum states. We evaluate the performance of these algorithms by using the variational approach to quantum algorithms, replacing the quantum prover with a variational circuit. We also show that the maximum symmetric fidelities can be calculated by semi-definite programs, which is useful for benchmarking the performance of the quantum algorithms for sufficiently small examples. Finally, we establish various generalizations of the resource theory of asymmetry, with the upshot being that the acceptance probabilities of the algorithms are resource monotones and thus well motivated from the resource-theoretic perspective.
In this paper, we show how a quantum computer can test for symmetries of quantum states and channels generated by quantum circuits. In fact, our quantum-computational tests actually quantify how symmetric a state or channel is. Given that asymmetry (i.e., breaking of symmetry) is a resource that is useful in a wide variety of contexts while being potentially difficult for a classical computer to verify, our tests are helpful in determining how useful a state will be for certain quantum information processing tasks. Related to this, our tests are in the spirit of the larger research program of using quantum computers to understand fundamental quantum-mechanical properties of high-dimensional quantum states, such as symmetry and entanglement, that are out of reach for classical computers.

We begin our development in Section II by introducing a general form of symmetry of quantum states that captures both the extendibility of bipartite states [Wer89, DPS02, DPS04], as well as symmetries of a single quantum system with respect to a group of unitary transformations [MS13, MS14]. This generalization allows for incorporating several kinds of symmetry tests into a single framework. We call this notion $G$-symmetric extendibility, and we discuss two different forms of it.

In Section III we move on to an important contribution of our paper—namely, how a quantum computer can test for and estimate quantifiers of $G$-symmetric extendibility. These quantifiers are collectively called maximum symmetric fidelities, with more particular names given in what follows. We prove that our quantum computational tests of symmetry have acceptance probabilities precisely equal to the various quantifiers, thus endowing these resource-theoretic measures with operational meanings and allowing us to estimate them to arbitrary precision. Using complexity theoretic language, we demonstrate that these quantum-computational tests of symmetry can be conducted in the form of a quantum interactive proof (QIP) system consisting of two quantum messages exchanged between a verifier and a prover [Wat09, VW16]. Our results thus generalize previous results in the context of unextendibility and entanglement of bipartite quantum states [HMW13, HMW14]; additionally, we go on to clarify the relation between our results and the previous ones (Section IV). Simpler forms of the test can be conducted without the aid of the prover and are thus efficiently computable on a quantum computer.

In Section IV, we show how the various symmetry tests specialize for testing the $k$-extendibility or $k$-Bose extendibility [Wer89, DPS02, DPS04] of both bipartite and multipartite states. These serve as tests of separability. We also show there how to test for the covariance symmetry of a quantum channel, which includes testing the symmetries of Hamiltonian evolution as a special case.

The maximum symmetric fidelities can be calculated by means of semi-definite programs (Section V), which is helpful for benchmarking the outputs of the quantum algorithms for sufficiently small circuits. This follows from combining the known semi-definite program for fidelity [Wat13] with the semi-definite constraints corresponding to the symmetry tests.

We propose variational quantum algorithms for estimating the maximum symmetric fidelities in Section VI. (See [CAB+20, BCLK+21] for reviews of variational quantum algorithms and [GRS83] for a review of the variational principle). In general, this approach is not guaranteed to estimate the maximum symmetric fidelities precisely, as the variational circuit used is not able to realize an arbitrarily powerful quantum computation. This approach thus leads only to lower bounds on the maximum symmetric fidelities. However, we find for some examples that this heuristic approach performs well. We note that a recent work adopted a similar variational approach for estimating the fidelity of quantum states generated by quantum circuits [CSZW20], though it is well known that this particular problem is QSZK-complete [Wat02], and thus likely difficult for quantum computers to solve in general. It remains an open question to determine how well this variational approach performs generally, beyond the examples considered in this paper.

Finally, we review the resource theory of asymmetry [MS13, MS14]. After doing so, we define several generalized resource theories of asymmetry (Section VII), including both the resource theory of asymmetry and the resource theory of $k$-unextendibility [KDWW19] as special cases. As part of this contribution, we also define resource theories of Bose asymmetry, which to our knowledge have not been considered yet. This development shows that the acceptance probabilities of the aforementioned algorithms, i.e., maximum symmetric fidelities, are resource monotones and thus well motivated from the resource-theoretic perspective.

In what follows, we proceed in the aforementioned order, and we finally conclude in Section VIII with a brief summary and a discussion of future questions.

II. NOTIONS OF SYMMETRY

We introduce the notions of $G$-symmetric extendibility and $G$-Bose symmetric extendibility, as generaliza-
tions of the notions of $G$-symmetry [MS13, Section 2] and extendibility [Wer98, DPS02, DPS04]. Later on in Section III, we devise quantum algorithms to test for these symmetries.

Let $\rho_S$ be a quantum state of system $S$ with corresponding Hilbert space $\mathcal{H}_S$. Let $G$ be a finite group, and let $U_{RS}(g)$ be a projective unitary representation [MS13, Section 2] of the group element $g \in G$, where $R$ indicates another Hilbert space, so that $U_{RS}(g)$ acts on the tensor-product Hilbert space $\mathcal{H}_R \otimes \mathcal{H}_S$. Let $\Pi^G_{RS}$ denote the following projection operator:

$$\Pi^G_{RS} := \frac{1}{|G|} \sum_{g \in G} U_{RS}(g).$$  (1)

Observe that

$$\Pi^G_{RS} = U_{RS}(g)\Pi^G_{RS} = \Pi^G_{RS} U_{RS}(g),$$  (2)

for all $g \in G$.

We now define $G$-symmetric-extendible and $G$-Bose-symmetric-extendible states.

**Definition II.1 ($G$-symmetric-extendible)** A state $\rho_S$ is $G$-symmetric-extendible if there exists a state $\omega_{RS}$ such that

1. the state $\omega_{RS}$ is an extension of $\rho_S$, i.e.,

$$\text{Tr}_R[\omega_{RS}] = \rho_S,$$  (3)

2. the state $\omega_{RS}$ is $G$-invariant, in the sense that

$$\omega_{RS} = U_{RS}(g)\omega_{RS}U_{RS}(g)^\dagger \quad \forall g \in G.$$  (4)

**Definition II.2 ($G$-Bose-symmetric-extendible)** A state $\rho_S$ is $G$-Bose-symmetric-extendible ($G$-BSE) if there exists a state $\omega_{RS}$ such that

1. the state $\omega_{RS}$ is an extension of $\rho_S$, i.e.,

$$\text{Tr}_R[\omega_{RS}] = \rho_R,$$  (5)

2. the state $\omega_{RS}$ satisfies

$$\omega_{RS} = \Pi^G_{RS}\omega_{RS}\Pi^G_{RS}.$$  (6)

Note that the condition in (6) is equivalent to $\omega_{RS} = \Pi^G_{RS} \omega_{RS}$ or $\omega_{RS} = U_{RS}(g)\omega_{RS}$ for all $g \in G$.

Observe that $\rho_S$ is $G$-symmetric-extendible if it is $G$-Bose-symmetric-extendible, but the opposite implication does not necessarily hold.

The above notions of symmetry generalize both $k$-extendibility of bipartite states and $G$-symmetry of multipartite states, as we discuss below.

**Example II.1 ($k$-extendible)** Recall that a bipartite state $\rho_{AB}$ is $k$-extendible [Wer98, DPS02, DPS04] if there exists an extension state $\omega_{AB_1\cdots B_k}$ such that

$$\text{Tr}_{B_2\cdots B_k}[\omega_{AB_1\cdots B_k}] = \rho_{AB}$$  (7)

and

$$\omega_{AB_1\cdots B_k} = W_{B_1\cdots B_k}(\pi)\omega_{AB_1\cdots B_k}W_{B_1\cdots B_k}(\pi)^\dagger,$$  (8)

for all $\pi \in S_k$, where each system $B_1, \ldots, B_k$ is isomorphic to the system $B$ and $W_{B_1\cdots B_k}(\pi)$ is a unitary representation of the permutation $\pi \in S_k$, with $S_k$ the symmetric group. Then the established notion of $k$-extendibility is a special case of $G$-symmetric extendibility, in which we set

$$S = AB_1,$$  (9)

$$R = B_2\cdots B_k,$$  (10)

$$G = S_k,$$  (11)

$$U_{RS}(g) = I_A \otimes W_{B_1\cdots B_k}(\pi).$$  (12)

**Example II.2 ($k$-Bose-extendible)** A bipartite state $\rho_{AB}$ is $k$-Bose-extendible if there exists an extension state $\omega_{AB_1\cdots B_k}$ such that

$$\text{Tr}_{B_2\cdots B_k}[\omega_{AB_1\cdots B_k}] = \rho_{AB}$$  (13)

and

$$\omega_{AB_1\cdots B_k} = \Pi^\text{Sym}_{B_1\cdots B_k}\omega_{AB_1\cdots B_k}\Pi^\text{Sym}_{B_1\cdots B_k},$$  (14)

where

$$\Pi^\text{Sym}_{B_1\cdots B_k} := \frac{1}{k!} \sum_{\pi \in S_k} W_{B_1\cdots B_k}(\pi).$$  (15)

is the projection onto the symmetric subspace. Thus, $k$-Bose-extendibility is a special case of $G$-Bose-symmetric extendibility under the identifications in (9)–(12).

**Example II.3 ($G$-symmetric)** Let $G$ be a group with projective unitary representation $\{U_{RS}(g)\}_{g \in G}$, and let $\rho_S$ be a quantum state of system $S$. A state $\rho_S$ is symmetric with respect to $G$ [MS13, MS14] if

$$\rho_S = U_S(g)\rho_S U_S(g)^\dagger \quad \forall g \in G.$$  (16)

Thus, the established notion of symmetry of a state $\rho_S$ with respect to a group $G$ is a special case of $G$-symmetric extendibility in which the system $R$ is trivial.

**Example II.4 ($G$-Bose-symmetric)** A state $\rho_S$ is Bose-symmetric with respect to $G$ if

$$\rho_S = U_S(g)\rho_S U_S(g)^\dagger \quad \forall g \in G,$$  (17)

which is equivalent to the condition

$$\rho_S = \Pi^G_S \rho_S \Pi^G_S,$$  (18)

where the projector $\Pi^G_S$ is defined as

$$\Pi^G_S := \frac{1}{|G|} \sum_{g \in G} U_S(g).$$  (19)

Thus, the established notion of Bose symmetry of a state $\rho_S$ with respect to a group $G$ is a special case of $G$-Bose symmetric extendibility in which the system $R$ is trivial.
Although the concepts of $G$-symmetric extendibility and $G$-Bose-symmetric extendibility, in Definitions II.1 and II.2 respectively, are generally different, we can relate them by purifying a $G$-symmetric-extendible state to a larger Hilbert space. The ability to do so plays a critical role in the algorithms proposed in Section III.

**Theorem II.1** A state $\rho_S$ is $G$-symmetric-extendible if and only if there exists a purification $\psi^g_{RS}$ of $\rho_S$ satisfying the following:

$$|\psi^g\rangle_{RS} \equiv (U_{RS}(g) \otimes \overline{U}_{RS}(g))|\psi^g\rangle_{RS} \quad \forall g \in G,$$

where the overbar denotes the complex conjugate. The condition in (20) is equivalent to

$$|\psi^g\rangle_{RS} = \Pi^G_{RS} |\psi^g\rangle_{RS},$$

where

$$\Pi^G_{RS} := \frac{1}{|G|} \sum_{g \in G} U_{RS}(g) \otimes \overline{U}_{RS}(g).$$

**Proof.** We give the proof for completeness, and we note here that it is very close to the proof of [CKMR07, Lemma II.5] (see also [KW20, Lemma 3.6]).

We begin with the forward implication. Suppose that $\rho_S$ is $G$-symmetric extendible. By definition, this means that there exists a state $\omega_{RS}$ satisfying (3) and (4). Suppose that $\omega_{RS}$ has the following spectral decomposition:

$$\omega_{RS} = \sum_k \lambda_k \Pi^k_{RS},$$

where $\lambda_k$ is an eigenvalue and $\Pi^k_{RS}$ is a spectral projection. We can write $\Pi^k_{RS}$ as

$$\Pi^k_{RS} = \sum_{\ell} |\phi^k_{\ell}\rangle_{RS} \langle \phi^k_{\ell}|,$$

where $\{|\phi^k_{\ell}\rangle_{RS}\}_{\ell}$ is an orthonormal basis. Now define

$$|\Gamma^k\rangle_{RS} := \sum_{\ell} |\phi^k_{\ell}\rangle_{RS} \otimes |\bar{\phi}^k_{\ell}\rangle_{RS},$$

$$|\psi^g\rangle_{RS} := \sum_k \sqrt{\lambda_k} |\Gamma^k\rangle_{RS},$$

where $|\bar{\phi}^k_{\ell}\rangle_{RS}$ is the complex conjugate of $|\phi^k_{\ell}\rangle_{RS}$ with respect to the standard basis. Observe that $|\psi^g\rangle_{RS}$ is a purification of $\omega_{RS}$. Now let us establish (20). Given that $\omega_{RS}$ satisfies (4), it follows that

$$U_{RS}(g)^\dagger \omega_{RS} U_{RS}(g) |\phi^k_{\ell}\rangle_{RS} = \omega_{RS} |\phi^k_{\ell}\rangle_{RS} = \lambda_k |\phi^k_{\ell}\rangle_{RS},$$

for all $k$, $\ell$, and $g$. Left multiplying by $U_{RS}(g)$ implies that

$$\omega_{RS} U_{RS}(g) |\phi^k_{\ell}\rangle_{RS} = \lambda_k U_{RS}(g) |\phi^k_{\ell}\rangle_{RS},$$

so that $U_{RS}(g) |\phi^k_{\ell}\rangle_{RS}$ is an eigenvector of $\omega_{RS}$ with eigenvalue $\lambda_k$. We conclude that the $k$th eigenspace corresponding to eigenvalue $\lambda_k$ is invariant under the action of $U_{RS}(g)$ because $|\phi^k_{\ell}\rangle_{RS}$ and $U_{RS}(g) |\phi^k_{\ell}\rangle_{RS}$ are eigenvectors of $\omega_{RS}$ with eigenvalue $\lambda_k$. This implies that the restriction of $U_{RS}(g)$ to the $k$th eigenspace is equivalent to a unitary $U^k_{RS}(g)$. Then it follows that

$$U_{RS}(g) \otimes \overline{U}_{RS}(g) |\Gamma^k\rangle_{RS} = U^k_{RS}(g) |\Gamma^k\rangle_{RS} = |\Gamma^k\rangle_{RS},$$

for all $g \in G$. The first equality follows from the fact stated just above. The second equality follows from the invariance of the maximally entangled vector $|\Gamma^k\rangle_{RS}$ under unitaries of the form $V \otimes \overline{V}$. Thus, it follows by linearity that

$$|\psi^g\rangle_{RS} = (U_{RS}(g) \otimes \overline{U}_{RS}(g))|\psi^g\rangle_{RS},$$

for all $g \in G$, which is the statement of (20).

Let us now consider the opposite implication; suppose that $\Pi^G_{RS}$ is a purification of $\rho_S$ and $\psi^g_{RS}$ satisfies (20). Set

$$\omega_{RS} = \text{Tr}_{RS}[\psi^g_{RS}],$$

Then $\omega_{RS}$ is an extension of $\rho_S$. Furthermore, employing the shorthand $U_{RS} = U_{RS}(g)$ and $\overline{U}_{RS} = \overline{U}_{RS}(g)$, we find that $\omega_{RS} = U_{RS}(g) \omega_{RS} U_{RS}(g)^\dagger$ for all $g \in G$ because

$$\omega_{RS} = \text{Tr}_{RS} |\psi^g_{RS}\rangle \langle \psi^g_{RS}|$$

$$= \text{Tr}_{RS} [U_{RS} \otimes \overline{U}_{RS}] |\psi^g_{RS}\rangle \langle \psi^g_{RS}| U_{RS} \otimes \overline{U}_{RS}]^\dagger$$

$$= U_{RS}(g) \text{Tr}_{RS} |\psi^g_{RS}\rangle \langle \psi^g_{RS}| U_{RS}(g)^\dagger U_{RS}(g)$$

$$= U_{RS}(g) \text{Tr}_{RS} |\psi^g_{RS}\rangle \langle \psi^g_{RS}| U_{RS}(g)^\dagger$$

$$= U_{RS}(g) \omega_{RS} U_{RS}(g)^\dagger.$$

Thus, it follows that $\rho_S$ is $G$-symmetric extendible.

We now justify the equivalence of (20) and (21). Using the result in (32), observe that

$$|\psi^g\rangle_{RS} = \frac{1}{|G|} \sum_{g \in G} (U_{RS}(g) \otimes \overline{U}_{RS}(g))|\psi^g\rangle_{RS},$$

which simplifies to (21) by substituting in (22). Now starting with (22), let us apply the property in (2), and we have that

$$|\psi^g\rangle_{RS} = (U_{RS}(g) \otimes \overline{U}_{RS}(g)) \Pi^G_{RS} |\psi^g\rangle_{RS},$$

for all $g \in G$. This reduces to (20) by applying (21).
III. TESTING SYMMETRY AND EXTENDIBILITY ON QUANTUM COMPUTERS

We can use a quantum computer to test for $G$-symmetric extendibility of a quantum state, as well as for other forms of symmetry discussed in the previous section. We assume the following in doing so:

1. there is a quantum circuit available that prepares a purification $\psi_{s'}^\rho$ of the state $\rho_S$,
2. there is an efficient implementation of each of the unitary operators in the set $\{U_{RS}(g)\}_{g \in G}$,
3. and there is an efficient implementation of each of the unitary operators in the set $\{U_{RS}^*(g)\}_{g \in G}$.

The first assumption can be made less restrictive by employing the variational, purification-learning procedure from [CSZW20]. That is, given a circuit that prepares the state $\rho_S$, the variational algorithm from [CSZW20] outputs a circuit that approximately prepares a purification of $\rho_S$. We should note that the convergence of the algorithm from [CSZW20] has not been established, and so the first assumption might be necessary for some applications.

The last assumption can be relaxed by the following reasoning: a standard gate set for approximating arbitrary unitaries in quantum computing consists of the controlled NOT gate, the Hadamard gate, and the $t$-controlled unitary:

$U = \sum_{g \in G} g \otimes g \otimes 1 \otimes 1 \otimes g^{-1}$

Thus, the complex conjugate of this gate is $U^* = \sum_{g \in G} g^{-1} \otimes g^{-1} \otimes 1 \otimes 1 \otimes g$. Thus, if a circuit for $U_{RS}(g)$ is constructed from this standard gate set, then we can generate a circuit for $U_{RS}^*(g)$ by replacing every $T$ gate in the original circuit with $T^\dagger$.

We now consider various quantum computational tests of symmetry that have increasing complexity.

A. Testing $G$-Bose symmetry

Let us begin by discussing the simplest version of the problem. Suppose that the state $\rho_S$ is pure, so that we can write it as $\rho_S = \psi_S \equiv |\psi_S\rangle \langle \psi_S|$, and that the $R$ system is trivial. We recover the traditional case of $G$-Bose symmetry mentioned in Example II.4. Thus, our goal is to decide if

$$|\psi_S\rangle \langle \psi_S| = U_S(g)|\psi_S\rangle \langle \psi_S| U_S(g)^\dagger \quad \forall g \in G,$$

(42)

or equivalently, if

$$|\psi_S\rangle = U_S(g)|\psi_S\rangle \quad \forall g \in G.$$  

(43)

This latter condition is equivalent to

$$|\psi_S\rangle = \Pi_S^G|\psi_S\rangle,\quad (44)$$

FIG. 1. Quantum circuit to implement Algorithm 1. The unitary $U^*$ prepares a purification $\psi_{s'}^\rho$ of the state $\rho_S$. Algorithm 1 tests whether the state $\rho_S$ is $G$-Bose symmetric, as defined in Example II.4. Its acceptance probability is equal to $\text{Tr}[\Pi^G_S \rho_S]$, where $\Pi^G_S$ is defined in (45).

where

$$\Pi^G_S := \frac{1}{|G|} \sum_{g \in G} U_S(g),$$

(45)

which is in turn equivalent to

$$\|\Pi^G_S |\psi_S\rangle\|_2 = 1.$$  

(46)

The equivalence

$$|\psi_S\rangle = \Pi^G_S |\psi_S\rangle \iff \|\Pi^G_S |\psi_S\rangle\|_2 = 1$$

(47)

holds by expanding the norm in terms of the inner product and using the adjoint property of the projector. Thus, if we have a method to perform the projection onto $\Pi^G_S$, then we can decide whether (46) holds.

There is a simple quantum algorithm that decides if (46) holds. It proceeds as follows and can be summarized as “performing the quantum phase estimation algorithm with respect to the unitary representation $\{U_S(g)\}_{g \in G}$”:

Algorithm 1 ($G$-Bose symmetry test) The algorithm consists of the following steps:

1. Prepare an ancillary register $C$ in the state $|0\rangle_C$.

2. Act on register $C$ with a quantum Fourier transform.

3. Append the state $|\psi_S\rangle$ and perform the following controlled unitary:

$$\sum_{g \in G} |g\rangle \langle g|_C \otimes U_S(g),$$

(48)

4. Perform an inverse quantum Fourier transform on register $C$, measure in the basis $\{ |g\rangle \langle g|_C \}_{g \in G}$, and accept if the zero outcome $|0\rangle |0\rangle_C$ occurs.
Note that the register $C$ has dimension $|G|$. Also, we can write the state $|0\rangle_C$ as $|e\rangle_C$, where $e$ is the identity element of the group. The result of Step 2 of Algorithm 1 is to prepare the following uniform superposition state:

$$|+\rangle_C := \frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle_C. \quad (49)$$

The overall state after Step 3 is as follows:

$$\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle_C U_S(g) |\psi\rangle_s. \quad (50)$$

The final step of Algorithm 1 projects the register $C$ onto the state $|+\rangle_C$. According to the aforementioned convention, Algorithm 1 accepts if the identity element outcome $|e\rangle e_C$ occurs. The probability that Algorithm 1 accepts is equal to

$$\left\| (|+\rangle \otimes I_S) \left( \frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle_C U_S(g) |\psi\rangle_s \right) \right\|_2^2 = \left\| \frac{1}{|G|} \sum_{g \in G} U_S(g) |\psi\rangle_s \right\|_2^2 \quad (51)$$

$$= \left\| \Pi_S^G |\psi\rangle_s \right\|_2^2. \quad (52)$$

Figure 1 depicts this quantum algorithm. Not only does it decide whether the state $|\psi\rangle_s$ is symmetric, but it also quantifies how symmetric it is. Since the acceptance probability is equal to $\left\| \Pi_S^G |\psi\rangle_s \right\|_2^2$ and this quantity is a measure of symmetry (see Theorem VII.2), we can repeat the algorithm a large number of times to estimate the acceptance probability to arbitrary precision.

The same quantum algorithm can decide whether a given mixed state $\rho_S$ is $G$-Bose symmetric (see Example II.4). Similar to the above, it also can estimate how $G$-Bose symmetric the state $\rho_S$ is. To see this, consider that the acceptance probability for a pure state can be rewritten as follows:

$$\left\| \Pi_S^G |\psi\rangle_s \right\|_2^2 = \text{Tr}[\Pi_S^G |\psi\rangle_s |\psi\rangle_s]. \quad (53)$$

Then since every mixed state can be written as a probabilistic mixture of pure states, it follows that the acceptance probability of Algorithm 1, when acting on the mixed state $\rho_S$, is equal to

$$\text{Tr}[\Pi_S^G \rho_S]. \quad (54)$$

This acceptance probability is equal to one if and only if $\rho_S = \Pi_S^G \rho_S \Pi_S^G$, and so this test is a faithful test of $G$-Bose symmetry. The equivalence

$$\text{Tr}[\Pi_S^G \rho_S] = 1 \iff \rho_S = \Pi_S^G \rho_S \Pi_S^G \quad (55)$$

dollows as a limiting case of the gentle measurement lemma [Win99, ON07];

$$\frac{1}{2} \left\| \rho_S - \Pi_S^G \rho_S \Pi_S^G \right\|_1 \leq \sqrt{1 - \text{Tr}[\Pi_S^G \rho_S]} \quad (56)$$

and the positive definiteness of the trace norm. Again, through repetition, we can estimate the acceptance probability $\text{Tr}[\Pi_S^G \rho_S]$ and then employ it as a measure of $G$-Bose symmetry (see Theorem VII.2).

### B. Testing G-symmetry

We now discuss how to upgrade Algorithm 1 to one that decides whether a state $\rho_S$ is $G$-symmetric (see Example II.3), i.e., if

$$\rho_S = U_S(g) \rho_S U_S(g)^\dagger \quad \forall g \in G. \quad (57)$$

We also prove that the acceptance probability of the upgraded algorithm is equal to the maximum $G$-symmetric fidelity, defined as

$$\max_{\sigma \in \text{Sym}_G} F(\rho_S, \sigma_S), \quad (58)$$

where

$$\text{Sym}_G := \{ \sigma_S \in \mathcal{D}(\mathcal{H}_S) : \sigma_S = U_S(g) \sigma_S U_S(g)^\dagger \quad \forall g \in G \}, \quad (59)$$

$\mathcal{D}(\mathcal{H}_S)$ denotes the set of density operators acting on the Hilbert space $\mathcal{H}_S$, and the fidelity of quantum states $\omega$ and $\tau$ is defined as [Uhl76]

$$F(\omega, \tau) := \left\| \sqrt{\omega} \sqrt{\tau} \right\|_1. \quad (60)$$

Thus, this quantum algorithm gives an operational meaning to the maximum $G$-symmetric fidelity in terms of its acceptance probability, and it can be used to estimate this fundamental measure of symmetry.

In the upgraded approach, we suppose that the quantum computer (now called the verifier) is equipped with access to a “quantum prover”—an agent having access to arbitrarily powerful quantum computations. We suppose that the quantum computer is allowed to exchange two quantum messages with the prover. The resulting class of problems that can be solved using this approach is abbreviated QIP(2), for quantum interactive proofs with two quantum messages exchanged, and we note that computational problems related to entanglement of bipartite states [HMW13, HMW14] and recoverability of tripartite states [CHM16] were previously shown to be decidable in QIP(2). These latter problems were proven to be QSZK-hard, and it remains an open question to determine their precise computational complexity.

Let $|\psi\rangle_{S,S}$ be a purification of the state $\rho_S$, and suppose that the verifier has access to a circuit $U^p$ that prepares this purification of $\rho_S$.

**Algorithm 2 (G-symmetry test)** The algorithm consists of the following steps:

1. The verifier uses the circuit $U^p$ to prepare the state $|\psi\rangle_{S,S}$.
2. The verifier transmits the purifying system $S'$ to the prover.
3. The prover appends an ancillary register $E$ in the state $|0\rangle_E$ and performs a unitary $V_{S'E \rightarrow SE'}$.
4. The prover sends the system $\hat{S}$ back to the verifier.
5. The verifier prepares a register $C$ in the state $|0\rangle_C$.
6. The verifier acts on register $C$ with a quantum Fourier transform.
7. The verifier performs the following controlled unitary:
\[
\sum_{g \in G} |g\rangle_C \otimes U_S(g) \otimes \overline{U}_S(g).
\]
8. The verifier performs an inverse quantum Fourier transform on register $C$, in the basis $\{|g\rangle_C\}_{g \in G}$, and accepts if and only if the zero outcome $|0\rangle_C$ occurs.

Figure 2 depicts this quantum algorithm. The overall state after Step 3 of Algorithm 2 is
\[
V_{S'E \rightarrow SE'}|\psi^+\rangle_S |0\rangle_E.
\]
The result of Step 6 is to prepare the uniform superposition state $|+\rangle_C$. After Step 7, the overall state is
\[
\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle_C \left(U_S(g) \otimes \overline{U}_S(g)\right) V_{S'E \rightarrow SE'}|\psi^+\rangle_S |0\rangle_E.
\]
For a fixed unitary $V_{S'E \rightarrow SE'}$, the probability of accepting, by following the same reasoning in (51)–(52), is equal to
\[
\|\Pi_{SS}^G V_{S'E \rightarrow SE'}|\psi^+\rangle_S |0\rangle_E\|_2^2,
\]
where
\[
\Pi_{SS}^G := \frac{1}{|G|} \sum_{g \in G} U_S(g) \otimes \overline{U}_S(g).
\]

Since the goal of the prover in a quantum interactive proof is to convince the verifier to accept [Wat09, VW16], the prover should be able to apply a unitary taking the purification $|\psi\rangle_{S'S} \rightarrow \|\phi\|_{S'S}$ in Example II.3. Its acceptance probability is equal to the maximum $G$-symmetric fidelity, as defined in (58).

**Theorem III.1** The acceptance probability of Algorithm 2 is equal to the maximum $G$-symmetric fidelity in (58), i.e.,
\[
\max_{V_{S'E \rightarrow SE'}} \|\Pi_{SS}^G V_{S'E \rightarrow SE'}|\psi^+\rangle_S |0\rangle_E\|_2^2 = \max_{\sigma_S \in \text{Sym}_G} F(\rho_S, \sigma_S).
\]

**Proof.** Recall the following property of the norm of an arbitrary vector $|\varphi\rangle$:
\[
||\varphi||_2^2 = \max_{|\psi\rangle : \|\psi\|_2 = 1} \langle \phi | \varphi \rangle.
\]
This follows from the Cauchy–Schwarz inequality and the conditions for saturating it. The formula in (69) implies that
\[
\max_{V_{S'E \rightarrow SE'}} \|\Pi_{SS}^G V_{S'E \rightarrow SE'}|\psi^+\rangle_S |0\rangle_E\|_2^2 = \max_{V_{S'E \rightarrow SE'}|\psi\rangle_{S'S}} \langle \phi | S_{S'E} \Pi_{SS}^G V_{S'E \rightarrow SE'} |\psi\rangle_{S'S} |0\rangle_E \|_2^2.
\]

For positive semi-definite operators $\omega_A$ and $\tau_A$ and corresponding rank-one operators $\psi_{RA}$ and $\psi'_{RA}$ satisfying
\[
\text{Tr}_R[\omega_A] = \omega_A, \quad \text{Tr}_R[\psi''_{RA}] = \tau_A,
\]

![Quantum circuit](image-url)
Uhlmann’s theorem [Uhl76] states that
\[ \| \sqrt{\omega \mathcal{A} \mathcal{F}_\mathcal{A}} \|_1^2 = \max_{V_R} | \langle \psi_\omega | R_A (V_R \otimes I_A) | \psi_\tau \rangle |^2, \] (73)
where the optimization is over every unitary \( V_R \) acting on the reference system \( R \). Applying this theorem to (70) with the identifications \( R \leftrightarrow S'E' \approx S'E \) and \( S \leftrightarrow A \) and noting that
\[ \text{Tr}_{S'E}[\langle \psi | S \otimes \mathcal{0} | \mathcal{0} \rangle E \langle \psi | S \rangle] = \rho_S, \] (74)
\[ \text{Tr}_{S'E}[\Pi_{SS'} \phi \langle \psi | S \otimes \mathcal{0} | \mathcal{0} \rangle E \langle \psi | S \rangle] = \text{Tr}_{S} \Pi_{SS'} \sigma_{SS'}, \] (75)
we conclude that
\[ \max_{\phi_{SS'}} | \langle \phi | S \Pi_{SS'} \Pi_{SS'} V_{S'E} E \langle \psi | S' \Pi_{SS'} \Pi_{SS'} \rangle |^2 \] (76)
with the optimization in the last line over every quantum state \( \sigma_{SS'} \).

We finally prove that
\[ \max_{\sigma_{SS'}} F(\rho_S, \text{Tr}_{S}[\Pi_{SS'} \sigma_{SS'} \Pi_{SS'}]) = \max_{\sigma \in \text{Sym}_G} F(\rho_S, \sigma_S). \] (77)
To justify the inequality \( \geq \) in (77), let \( \sigma_S \in \text{Sym}_G \). Pick \( \sigma_{SS} \) to be the purification \( \phi_{SS} \) of \( \rho_S \) from Theorem II.1 (with trivial reference systems \( RR' \)) that satisfies
\[ \Pi_{SS'} \sigma_{SS} \Pi_{SS'} = \phi_{SS}. \] (78)
Then we find that
\[ \text{Tr}_{S}[\Pi_{SS'} \phi_{SS} \Pi_{SS'}] = \text{Tr}_{S}[\phi_{SS}] = \sigma_S, \] (79)
and so, given that \( \sigma_S \in \text{Sym}_G \) is arbitrary, it follows that
\[ \max_{\sigma_{SS'}} F(\rho_S, \text{Tr}_{S}[\Pi_{SS'} \sigma_{SS'} \Pi_{SS'}]) \geq \max_{\sigma \in \text{Sym}_G} F(\rho_S, \sigma_S). \] (80)
To justify the inequality \( \leq \) in (77), let \( \sigma_{SS} \) be an arbitrary state. If \( \sigma_{SS} \) is outside of the subspace onto which \( \Pi_{SS'} \) projects, then \( \Pi_{SS'} \sigma_{SS} \Pi_{SS'} = 0 \) and the fidelity in (76) is equal to zero. Let us then suppose that this is not the case, and let us define
\[ \sigma'_{SS} := \frac{1}{p} \Pi_{SS} \sigma_{SS} \Pi_{SS'}, \] (81)
\[ p := \text{Tr}[\Pi_{SS'} \sigma_{SS'}. \] (82)
Then we find that
\[ F(\rho_S, \text{Tr}_{S}[\Pi_{SS'} \sigma_{SS' \Pi_{SS'}}]) = p F(\rho_S, \tau_S) \leq F(\rho_S, \tau_S), \] (83)
(84)
where
\[ \tau_S := \text{Tr}[\sigma'_{SS}]. \] (85)
and we used the fact that \( p \leq 1 \). It remains to be proven that \( \tau_S \in \text{Sym}_G \). To see this, consider that
\[ \tau_S = \text{Tr}_{S}[\sigma'_{SS}] = \text{Tr}_{S}[\Pi_{SS'} \sigma_{SS'} \Pi_{SS'}], \] (86)
\[ = \text{Tr}_{S}[\{U_S \otimes \mathcal{U}_S \} \Pi_{SS'} \sigma_{SS'} \Pi_{SS'} (U_S \otimes \mathcal{U}_S)^\dagger] \] (87)
\[ = U_S \text{Tr}_{S}[\{U_S \otimes \mathcal{U}_S \} \sigma_{SS'} \Pi_{SS'} \Pi_{SS'} U_S^\dagger] \] (88)
\[ = U_S \text{Tr}_{S}[\{U_S \otimes \mathcal{U}_S \} \Pi_{SS'} \Pi_{SS'} U_S^\dagger] \] (89)
\[ = U_S \text{Tr}_{S}[\{U_S \otimes \mathcal{U}_S \} \Pi_{SS'} \Pi_{SS'} U_S^\dagger] \] (90)
where we have used the shorthand \( U_S \equiv U_S(g) \) and \( \mathcal{U}_S \equiv \mathcal{U}_S(g) \). Since the equality \( \tau_S = U_S(g) \tau_S U_S^\dagger(g) \) holds for all \( g \in G \), it follows that
\[ \max_{\sigma_{SS'}} F(\rho_S, \text{Tr}_{S}[\Pi_{SS'} \sigma_{SS'} \Pi_{SS'}]) \leq \max_{\tau_S \in \text{Sym}_G} F(\rho_S, \sigma_S), \] (91)
(92)
(93)
(94)

**Remark 1 (Testing incoherence)** We note here that testing the incoherence of a quantum state, in the sense of [BCP14, SAP17], is a special case of testing G-symmetry. To see this, we can pick \( G \) to be the cyclic group over \( d \) elements with unitary representation \( \{ Z(z) \}_z \), where \( Z(z) \) is the generalized Pauli phase-shift unitary, defined as
\[ Z(z) := \sum_{j=0}^{d-1} e^{2\pi ijz/d} \hat{j} \hat{j}. \] (95)
A state is symmetric with respect to this group if the condition in (57) holds. This condition is equivalent to the following one:
\[ \rho_S = \frac{1}{|G|} \sum_{g \in G} U_S(g) \rho_S U_S(g)^\dagger. \] (96)
For the choice mentioned above, this condition holds if and only if the state \( \rho_S \) is diagonal in the incoherent basis, i.e., it can be written as \( \rho_S = \sum_j p(j) |j \rangle \langle j| \), where \( p(j) \) is a probability distribution. Thus, Algorithm 2 can be used to test the incoherence of quantum states.

C. Testing G-Bose symmetric extendibility

We now describe an algorithm for testing G-Bose symmetric extendibility of a quantum state \( \rho_S \), as defined in Definition II.2. The algorithm bears some similarities with Algorithms 1 and 2. Like Algorithm 2, it involves an interaction between a verifier and a prover. We prove
that its acceptance probability is equal to the maximum G-BSE fidelity:

$$\max_{\sigma_S \in \text{BSE}_G} F(\rho_S, \sigma_S),$$

(97)

where BSE$_G$ is the set of G-Bose symmetric extendible states:

\[
\text{BSE}_G := \{ \sigma_S : \exists \omega_{RS} \in D(\mathcal{H}_{RS}), \text{Tr}_R[\omega_{RS}] = \sigma_S, \omega_{RS} = U_{RS}(g)\omega_{RS} \forall g \in G \}. \tag{98}
\]

Thus, the algorithm endows the maximum G-BSE fidelity with an operational meaning. Note that the condition $\omega_{RS} = U_{RS}(g)\omega_{RS}$ for all $g \in G$ is equivalent to $\omega_{RS} = \Pi^G_{RS} \omega_{RS} \Pi^G_{RS}$, where

$$\Pi^G_{RS} := \frac{1}{|G|} \sum_{g \in G} U_{RS}(g). \tag{100}$$

The algorithm is similar to Algorithm 2, but we list it here for completeness. Let $|\psi\rangle_{SS'}$ be a purification of the state $\rho_S$, and suppose that the circuit $U^p$ prepares this purification of $\rho_S$.

**Algorithm 3 (G-BSE test)** The algorithm proceeds as follows:

1. The verifier uses the circuit provided to prepare the state $|\psi\rangle_{SS'}$.
2. The verifier transmits the purifying system $S'$ to the prover.
3. The prover appends an ancillary register $E$ in the state $|0\rangle_E$ and performs a unitary $V_{S'E \rightarrow RE'}$.
4. The prover sends the system $R$ back to the verifier.
5. The verifier prepares a register $C$ in the state $|0\rangle_C$.
6. The verifier acts on register $C$ with a quantum Fourier transform.
7. The verifier performs the following controlled unitary:

$$\sum_{g \in G} |g\rangle_C \langle g| \otimes U_{RS}(g), \tag{101}$$

8. The verifier performs an inverse quantum Fourier transform on register $C$, measures in the basis $\{|g\rangle_C\}_{g \in G}$, and accepts if and only if the zero outcome $|0\rangle_C$ occurs.

Figure 3 depicts this quantum algorithm. The overall state after Step 3 is

$$V_{S'E \rightarrow RE'} |\psi\rangle_{SS'} |0\rangle_E. \tag{102}$$

Step 6 prepares the uniform superposition state $|+\rangle_C$, which is defined in (49). After Step 7, the overall state is

$$\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle_C (U_{RS}(g)) V_{S'E \rightarrow RE'} |\psi\rangle_{SS'} |0\rangle_E. \tag{103}$$

The last step can be understood as the verifier projecting the register $C$ onto the state $|+\rangle_C$.

The probability of accepting, following the same reasoning as before, is equal to

$$\|\Pi^G_{RS} V_{S'E \rightarrow RE'} |\psi\rangle_{SS'} |0\rangle_E \|^2_2, \tag{104}$$

where $\Pi^G_{RS}$ is defined in (100). As before, the goal of the prover in a quantum interactive proof is to convince the verifier to accept [Wat09, VW16], and so the prover optimizes over every unitary $V_{S'E \rightarrow SS'}$. The acceptance probability of Algorithm 3 is then given by

$$\max_{V_{S'E \rightarrow SS'}} \|\Pi^G_{RS} V_{S'E \rightarrow SS'} |\psi\rangle_{SS'} |0\rangle_E \|^2_2. \tag{105}$$

Our proof of the following theorem is similar to the proof given for Theorem III.1; for completeness, we provide our proof in Appendix A.

**Theorem III.2** The maximum acceptance probability of Algorithm 3 is equal to the maximum G-BSE fidelity in (97), i.e.,

$$\max_{V_{S'E \rightarrow SS'}} \|\Pi^G_{RS} V_{S'E \rightarrow SS'} |\psi\rangle_{SS'} |0\rangle_E \|^2_2 = \max_{\sigma_S \in \text{BSE}_G} F(\rho_S, \sigma_S), \tag{106}$$

where the set BSE$_G$ is defined in (98).
D. Testing G-symmetric extendibility

The final algorithm that we introduce tests whether a state $\rho_S$ is G-symmetric extendible (recall Definition II.1). Similar to the algorithms in the previous sections, not only does it decide whether $\rho_S$ is G-symmetric extendible, but it also quantifies how similar it is to a state in the set of G-symmetric extendible states. The acceptance probability is equal to the maximum G-symmetric extendible fidelity:

$$\max_{\sigma_S \in \text{SymExt}_G} F(\rho_S, \sigma_S),$$

where

$$\text{SymExt}_G := \{ \sigma_S : \exists \omega_{RS} \in \mathcal{D}(\mathcal{H}_{RS}), \text{Tr}_R[\omega_{RS}] = \sigma_S \} \omega_{RS} = U_{RS}(g)\omega_{RS}U_{RS}(g)\rangle \text{ for all } g \in G \}.$$  \hfill (108)

We again operate in the model of quantum interactive proofs, in which a verifier interacts with a prover.

We again list the algorithm for completeness, noting its similarity to the previous algorithms. Let $|\psi\rangle_{S'G}$ be a purification of the state $\rho_S$, and suppose that the circuit $U^P$ prepares this purification of $\rho_S$.

**Algorithm 4** The algorithm proceeds as follows:

1. The verifier uses the circuit $U^P$ to prepare the state $|\psi\rangle_{S'G}$, which is a purification of the state $\rho_S$.
2. The verifier transmits the purifying system $S'$ to the prover.
3. The prover appends an ancillary register $E$ in the state $|0\rangle_E$ and performs a unitary $V_{S'E' \rightarrow \text{RS}E'}$.
4. The prover sends the systems $\text{RS}E'$ back to the verifier.
5. The verifier prepares a register $C$ in the state $|0\rangle_C$.
6. The verifier acts on register $C$ with a quantum Fourier transform.
7. The verifier performs the following controlled unitary:

$$\sum_{g \in G} |g\rangle\langle g|_C \otimes U_{RS}(g) \otimes \overline{U}_{\text{RS}}(g),$$

where $U_{RS}(g)$ is defined in (22). As before, the prover optimizes over every unitary $V_{S'E' \rightarrow \text{RS}E'}$. The acceptance probability of Algorithm 4 is then given by

$$\max_{\sigma_S \in \text{SymExt}_G} |\langle 0|_{E'} \Pi^G_{\text{RS}S'E'} V_{S'E' \rightarrow \text{RS}E'} |\psi\rangle_{S'S} |0\rangle_E|^2,$$

where $\Pi^G_{\text{RS}S'E'}$ is defined in (22).

Our proof of the following theorem is similar to the proof given for Theorem III.1. For completeness, we provide our proof in Appendix B.

**Theorem III.3** The maximum acceptance probability of Algorithm 4 is equal to the maximum G-symmetric extendible fidelity in (107), i.e.,

$$\max_{\sigma_S \in \text{SymExt}_G} |\langle 0|_{E'} \Pi^G_{\text{RS}S'E'} V_{S'E' \rightarrow \text{RS}E'} |\psi\rangle_{S'S} |0\rangle_E|^2 \leq \max_{\sigma_S \in \text{SymExt}_G} F(\rho_S, \sigma_S).$$

where the set $\text{SymExt}_G$ is defined in (108).
IV. TESTS OF $k$-EXTENDIBILITY OF STATES AND COVARIANCE SYMMETRY OF CHANNELS

The theory developed in Section III is rather general. In the forthcoming subsections, we apply it to test for extendibility of bipartite and multipartite quantum states and to test for covariance symmetry of a quantum channel.

A. Separability test for pure bipartite states

We illustrate the $G$-Bose symmetry test from Section III A on a case of interest: deciding whether a pure bipartite state is entangled. This problem is known to be BQP-complete [GHMW15], and one can decide it by means of the SWAP test as considered in [HM10]. The SWAP test as a quantum computational method of quantifying entanglement has been further studied in recent work [FKS21, BGCC21].

Let $\psi_{AB}$ be a pure bipartite state, and let $\psi_{AB}^{\otimes k}$ denote $k$ copies of it. Then we can consider the permutation unitaries $W_{B_1 \cdots B_k}(\pi)$ from Example II.1. This example is a special case of Bose $G$-symmetry with the identifications

\[ S \leftrightarrow A_1 B_1 \cdots A_k B_k, \]
\[ U_S(g) \leftrightarrow I_{A_1 \cdots A_k} \otimes W_{B_1 \cdots B_k}(\pi). \]

The acceptance probability of Algorithm 1 is equal to

\[ \text{Tr}\left[ \Pi_{B_1 \cdots B_k} \rho_B^{\otimes k} \right], \]

where the projection $\Pi^{\text{Sym}}_{B_1 \cdots B_k}$ onto the symmetric subspace is defined in (15) and $\rho_B := \text{Tr}_A[\psi_{AB}]$. For $k = 2$, this reduces to the well known SWAP test with acceptance probability

\[ p^{(2)}_{\text{acc}} := \frac{1}{2} \left( 1 + \text{Tr}[\rho_B^2] \right). \]

For $k = 3$, the acceptance probability is

\[ p^{(3)}_{\text{acc}} := \frac{1}{6} \left( 1 + 3 \text{Tr}[\rho_B^2] + 2 \text{Tr}[\rho_B^3] \right). \]

For $k = 4$, the acceptance probability is

\[ p^{(4)}_{\text{acc}} := \frac{1}{24} \left( 1 + 6 \text{Tr}[\rho_B^2] + 3 (\text{Tr}[\rho_B^2])^2 + 8 \text{Tr}[\rho_B^3] + 6 \text{Tr}[\rho_B^4] \right). \]

We conclude that

\[ p^{(2)}_{\text{acc}} \geq p^{(3)}_{\text{acc}} \geq p^{(4)}_{\text{acc}}, \]

because $\text{Tr}[\rho^k] = \sum_j \lambda_j^k$, where the eigenvalues of $\rho$ are $\{\lambda_j\}_j$, and for all $x, y \in [0, 1]$,

\[ \frac{1}{2} (x + x^2) \geq \frac{1}{6} (x + 3x^2 + 2x^3) \geq \frac{1}{24} (x + 6x^2 + 3x^2 y + 8x^3 + 6x^4). \]

The inequalities in (121) imply that the tests become more stringent as $k$ increases. We expect, but have not proven, that this trend of decreasing acceptance probability continues as $k$ increases.

We can interpret these findings in two different ways. For each $k$, the rejection probability $1 - p^{(k)}_{\text{acc}}$ can be understood as an entanglement measure for pure states, similar to how the linear entropy $1 - \text{Tr}[\rho_B^2]$ is interpreted as an entanglement measure. Indeed, these quantities are non-increasing under local operations and classical communication that take pure states to pure states, as every Rényi entropy (defined as $\frac{1}{1-\alpha} \log \text{Tr}[^{\otimes k} \rho_B^\alpha]$ for $\alpha \in (0, 1) \cup (1, \infty)$) is an entanglement measure for pure states [HHHH09]. Another interpretation is that, if using these tests to decide if a given pure state is product or entangled, a decision can be determined with fewer repetitions of the basic test by using tests with higher values of $k$.

B. Separability test for pure multipartite states

We can generalize the test from the previous section to one for pure multipartite entanglement. Let $\psi_{A_1 \cdots A_m}$ be a multipartite pure state, and let $\psi_{A_1 \cdots A_m}^{\otimes k}$ denote $k$ copies of it. For $i \in \{1, \ldots, m\}$ and $\pi_i \in S_k$, let $W_{A_1 \cdots A_k}(\pi_i)$ denote a permutation unitary, where $i$ is an index for the $i$th party, and the notation $A_{i,j}$ for $j \in \{1, \ldots, k\}$ indicates the $j$th system of the $i$th party. This example is a special case of Bose $G$-symmetry with the identifications:

\[ S \leftrightarrow A_{1,1} \cdots A_{1,k} \cdots A_{m,1} \cdots A_{m,k}, \]
\[ U_S(g) \leftrightarrow \bigotimes_{i=1}^m W_{A_{i,1} \cdots A_{i,k}}(\pi_i) \]
\[ \text{G} \leftrightarrow S_k \times \cdots \times S_k, \]
\[ g \leftrightarrow (\pi_1, \ldots, \pi_m), \]

where $\times$ denotes the direct product of groups. The $G$-Bose symmetry test from Section III A has the following acceptance probability in this case:

\[ \text{Tr}\left[ \bigotimes_{i=1}^m \Pi^{\text{Sym}}_{A_{1,i} \cdots A_{m,i}} \psi_{A_1 \cdots A_m}^{\otimes k} \right]. \]

For $k = 2$, this test is known to be a test of multipartite pure-state entanglement [HM10], which has been considered in more recent works [FKS21, BGCC21]. As far as we aware, the test proposed above, for larger values of $k$, has not been considered previously. Presumably, as was the case for the bipartite entanglement test mentioned above, the multipartite test is such that it becomes easier to detect an entangled state as $k$ increases. We leave its detailed analysis for future work.
C. \( k \)-Bose extendibility test for bipartite states

We now demonstrate how the test for \( G \)-Bose symmetric extendibility from Section III C can realize a test for \( k \)-Bose extendibility of a bipartite state. Since every separable state is \( k \)-Bose extendible, this test is then indirectly a test for separability. To see this in detail, recall that a bipartite state \( \sigma_{AB} \) is separable if it can be written as a convex combination of pure product states [HHHH09, KW20]:

\[
\sigma_{AB} = \sum_x p_X(x) \phi_A^x \otimes \phi_B^x,
\]

(129)

where \( p_X \) is a probability distribution and \( \{ \phi_A^x \}_x \) and \( \{ \phi_B^x \}_x \) are sets of pure states. A \( k \)-Bose extension for this state is as follows:

\[
\omega_{AB_1...B_k} = \sum_x p_X(x) \phi_A^x \otimes \phi_{B_1}^x \otimes \cdots \otimes \phi_{B_k}^x.
\]

(130)

By making the identifications discussed in Example II.2, it follows from Theorem III.2 that the test from Section III C is a test for \( k \)-Bose extendibility. For an input state \( \rho_{AB} \), the acceptance probability of Algorithm 3 is equal to the maximum \( k \)-Bose extendible fidelity

\[
\max_{\omega_{AB} \in k-\text{BE}} F(\rho_{AB}, \omega_{AB}),
\]

(131)

where \( k \)-BE denotes the set of \( k \)-Bose extendible states, as defined in Example II.2.

This test for \( k \)-Bose extendibility was proposed in [HMW13, HMW14] for understanding the computational complexity of the circuit separability problem. In that work, it was not mentioned that the test employed is a test for \( k \)-Bose extendibility; instead, it was suggested to be a test for \( k \)-extendibility. Thus, our observation here (also made earlier by [Mar13]) is that the test proposed in [HMW13, HMW14] is actually a test for \( k \)-Bose extendibility, and we consider in the next section a true test for \( k \)-extendibility. The main results of [HMW13, HMW14] were the computational complexity of the circuit version of the separability problem, and so the precise kind of test used was not particularly important there.

D. \( k \)-Extendibility test for bipartite states

In this section, we discuss how the test for \( G \)-symmetric extendibility from Section III D can realize a test for \( k \)-extendibility of a bipartite state. Due to the known connections between \( k \)-extendibility and separability [CKMR07, BCY11a, BCY11b, BH13], this test is an indirect test for separability of a bipartite state. Since every separable state is \( k \)-Bose extendible, as discussed in Section IV C, and every \( k \)-Bose extendible state is \( k \)-extendible, it follows that every separable state is \( k \)-extendible.

By making the identifications discussed in Example II.1, it follows from Theorem III.3 that the test from Section III D is a test for \( k \)-extendibility. For an input state \( \rho_{AB} \), the acceptance probability of Algorithm 4 is equal to the maximum \( k \)-extendible fidelity

\[
\max_{\omega_{AB} \in k-E} F(\rho_{AB}, \omega_{AB}),
\]

(132)

where \( k \)-E denotes the set of \( k \)-extendible states, as defined in Example II.1.

As far as we are aware, this quantum computational test for \( k \)-extendibility is original to this paper, however inspired by the approach from [HMW13, HMW14]. It was argued in [HMW13, HMW14] that the acceptance probability of the test there is bounded from above by the maximum \( k \)-extendible fidelity, which is consistent with the fact that the set of \( k \)-Bose extendible states is contained in the set of \( k \)-extendible states and our observation here that the acceptance probability of the test in [HMW13, HMW14] is equal to the maximum \( k \)-Bose extendible fidelity.

E. Extendibility tests for multipartite states

We discuss briefly how the tests from Sections III C and III D apply to the multipartite case, using identifications similar to those in (124)–(127).

First, let us recall the definition of multipartite extendibility [DPS05]. Let \( \sigma_{A_1...A_m} \) be a multipartite state. Such a state is \((k_1, \ldots, k_m)\)-extendible if there exists a state \( \omega_{A_1,1:A_k,1:A_{m,1}...A_{m,k_m}} \) such that

\[
\sigma_{A_1...A_m} = \text{Tr}_{A_1,2:A_k,1:A_{m,2}...A_{m,k_m}} [\omega_{A_1,1:A_k,1:A_{m,1}...A_{m,k_m}}],
\]

(133)

and

\[
\omega_{A_1,1:A_k,1:A_{m,1}...A_{m,k_m}} = W_{A_1,1:A_k,1:A_{m,1}...A_{m,k_m}}^{\pi} \omega_{A_1,1:A_k,1:A_{m,1}...A_{m,k_m}} \times \prod_{i=1}^{m} W_{A_1,1:A_{k_i}}^{\pi} \omega_{A_1,k_i%A_{m,k_i}},
\]

(134)

for all \( \pi \), where \( \pi = (\pi_1, \ldots, \pi_m) \in S_{k_1} \times \cdots \times S_{k_m} \) and

\[
W_{A_1,1:A_k,1:A_{m,1}...A_{m,k_m}}^{\pi} := \bigotimes_{i=1}^{m} W_{A_1,1:A_k}^{\pi_i}.
\]

(135)

A multipartite state is \((k_1, \ldots, k_m)\)-Bose extendible if there exists a state \( \omega_{A_1,1:A_k,1:A_{m,1}...A_{m,k_m}} \) such that (133) holds and

\[
\omega_{A_1,1:A_k,1:A_{m,1}...A_{m,k_m}} = \Pi_{A_1,1:A_k,1:A_{m,1}...A_{m,k_m}} \omega_{A_1,1:A_k,1:A_{m,1}...A_{m,k_m}} \times \Pi_{A_1,1:A_k,1:A_{m,1}...A_{m,k_m}},
\]

(136)
where
\[ \Pi_{A_{1}, \ldots, A_{k_1} \cdots A_{m}, k_m} := \bigotimes_{i=1}^{m} \Pi^{\text{Sym}}_{A_{i}, A_{i}}, \] (137)
and
\[ \Pi^{\text{Sym}}_{A_{1}, A_{i}, k_i} := \frac{1}{k_i!} \sum_{\pi_i \in S_{k_i}} W_{\pi_i}, \] (138)

By making the identifications
\[ S \leftrightarrow A_{1, \ldots, A_{m}, 1}, \]
\[ R \leftrightarrow A_{1, 2, \ldots, A_{1}, k_1, \ldots, A_{m}, 2, \ldots, A_{m}, k_m}, \]
\[ U_S(g) \leftrightarrow \bigotimes_{i=1}^{m} W_{A_{i}, 1, \cdots, A_{i}, k_i}(\pi_i), \]
\[ G \leftrightarrow S_{k_1} \times \cdots \times S_{k_m}, \]
\[ g \leftrightarrow (\pi_1, \ldots, \pi_m), \] (143)
it follows that Algorithm 3 is a test for multipartite \((k_1, \ldots, k_m)\)-Bose extendibility of a state \(\rho_{A_{1} \cdots A_{m}}\), with acceptance probability equal to
\[ \max_{\omega_{A_{1} \cdots A_{m}} \in (k_1, \ldots, k_m)\text{-BE}} F(\rho_{A_{1} \cdots A_{m}}, \omega_{A_{1} \cdots A_{m}}), \] (144)

and Algorithm 4 is a test for multipartite \((k_1, \ldots, k_m)\)-extendibility of a state \(\rho_{A_{1} \cdots A_{m}}\), with acceptance probability equal to
\[ \max_{\omega_{A_{1} \cdots A_{m}} \in (k_1, \ldots, k_m)\text{-E}} F(\rho_{A_{1} \cdots A_{m}}, \omega_{A_{1} \cdots A_{m}}), \] (145)
where \((k_1, \ldots, k_m)\text{-BE}\) and \((k_1, \ldots, k_m)\text{-E}\) denote the sets of \((k_1, \ldots, k_m)\)-Bose extendible and \((k_1, \ldots, k_m)\)-extendible states, respectively.

### F. Testing covariance symmetry of a quantum channel

We can also use the test from Algorithm 4 to test for covariance symmetry of a quantum channel. Before stating it, let us recall the notion of a covariant channel \([Hol02]\). Let \(G\) be a group and let \(\{U_{A}(g)\}_{g \in G}\) and \(\{V_{B}(g)\}_{g \in G}\) denote projective unitary representations of \(G\). A channel \(\mathcal{N}_{A \rightarrow B}\) is covariant if the following G-covariance symmetry condition holds
\[ \mathcal{N}_{A \rightarrow B} \circ U_{A}(g) = V_{B}(g) \circ \mathcal{N}_{A \rightarrow B} \quad \forall g \in G, \] (146)
where the unitary channels \(U_{A}(g)\) and \(V_{B}(g)\) are respectively defined from \(U_{A}(g)\) and \(V_{B}(g)\) as
\[ U_{A}(g)(\omega_{A}) := U_{A}(g)\omega_{A}U_{A}^{-1}(g), \]
\[ V_{B}(g)(\tau_{B}) := V_{B}(g)\tau_{B}V_{B}^{-1}(g). \] (147)

It is well known that a channel is covariant in the sense above if and only if its Choi state is invariant in the following sense \([CDP09, \text{Eq. (59)}]\):
\[ \Phi_{RB}^{\mathcal{N}} = (\overline{U}_{R}(g) \otimes V_{B}(g))(\Phi_{RB}^{\mathcal{N}}) \quad \forall g \in G, \] (149)
where
\[ \overline{U}_{R}(g)(\omega_{R}) := \overline{U}_{R}(g)\omega_{R}U_{R}(g)^{T}, \] (150)
and the superscript \(T\) indicates the transpose. Also, the Choi state \(\Phi_{RB}^{\mathcal{N}}\) is defined as
\[ \Phi_{RB}^{\mathcal{N}} := \mathcal{N}_{A \rightarrow B}(\Phi_{RA}), \]
\[ \Phi_{RA} := \frac{1}{|A|} \sum_{i,j} |i\rangle \langle j|_{R} \otimes |i\rangle \langle j|_{A}. \] (152)

Suppose then that a circuit is available that generates the channel \(\mathcal{N}_{A \rightarrow B}\). Similar to the first assumption in Section III, we suppose that the circuit realizes a unitary channel \(W_{AE' \rightarrow BE}\) that extends the original channel, in the sense that
\[ \mathcal{N}_{A \rightarrow B}(\omega_{A}) = (\text{Tr}_{E} \circ W_{AE' \rightarrow BE})(\omega_{A} \otimes |0\rangle \langle 0|_{E'}). \] (153)

Then to decide whether the channel is covariant, we send in one share of a maximally entangled state to the unitary extension channel, such that the overall state is
\[ W_{AE' \rightarrow BE}(\Phi_{RA} \otimes |0\rangle \langle 0|_{E'}). \] (154)

Now making the identifications
\[ E \leftrightarrow S', \]
\[ RB \leftrightarrow S, \]
\[ \overline{U}_{R}(g) \otimes V_{B}(g) \leftrightarrow U_{S}(g), \] (157)
we apply Algorithm 2, and as a consequence of Theorem III.1, the acceptance probability is equal to
\[ \max_{\sigma_{RB} \in \text{Sym}_{G}} F(\Phi_{RB}^{\mathcal{N}}, \sigma_{RB}). \] (158)

where
\[ \text{Sym}_{G} := \left\{ \sigma_{RB} \in \mathcal{D}(\mathcal{H}_{RB}) : \sigma_{RB} = (\overline{U}_{R}(g) \otimes V_{B}(g))(\sigma_{RB}) \quad \forall g \in G \right\}. \] (159)

Thus, the test accepts with probability equal to one if and only if the channel is covariant in the sense of (146).

### V. SEMI-DEFINITE PROGRAMS FOR MAXIMUM SYMMETRIC FIDELITIES

In this section, we note that the acceptance probabilities of Algorithms 1–4 can be computed by means of semi-definite programming (see \([BV04, Wat18, KW20]\) for reviews). This can be useful for comparing the true values of the acceptance probabilities of Algorithms 1–4 to estimates formed from executing them on near-term quantum computers; however, the latter approach only works well in practice if the circuit \(U^{p}\) acts on a small number of qubits and does not have too large of a depth. This limitation holds because the semi-definite programs (SDPs) run in a time polynomial in the dimension of the
states involved, but the dimension of a state grows exponentially with the number of qubits involved.

We note that the fact that the acceptance probabilities of Algorithms 1–4 can be computed by semi-definite programming follows from a more general fact that the acceptance probability of a QIP(2) algorithm can be computed in this manner [Wat09, VW16]; however, it is helpful to have the explicit form of the SDPs available.

We now list the SDPs for the acceptance probabilities of Algorithms 1–4. To begin with, let us note that the acceptance probability of Algorithm 1 is equal to $\text{Tr}[^\Pi G \rho_S]$, and so there is no need for an optimization. This quantity can be calculated directly if the projection matrix $^\Pi G$ and the density matrix $\rho_S$ are available. Moving on, let us note that the root fidelity of states $\omega$ and $\tau$ can be calculated by the following SDP [Wat13]:

$$\sqrt{F(\omega, \tau)} = \max_{X \in \mathcal{L}(H)} \left\{ \text{Tr}[\text{Re}[X]] : \omega X^\dagger X \tau \geq 0 \right\}.$$  \hspace{1cm} (160)

Each of the sets Sym$G$, BSE$G$, and SymExt$G$ are specified by semi-definite constraints. Thus, combining the optimization in (160) with various constraints, we find that the acceptance probabilities of Algorithms 2–4 can be calculated by using the following SDPs, respectively:

$$\max_{\sigma_S \in \text{Sym}_G} \sqrt{F(\rho_S, \sigma_S)}$$

$$= \max_{X \in \mathcal{L}(H), \sigma_S \geq 0} \left\{ \text{Tr}[\text{Re}[X]] : \rho_S X^\dagger X \sigma_S \geq 0, \text{Tr}[\sigma_S] = 1, \sigma_S = U_S(g)\sigma_S U_S(g)^\dagger \forall g \in G \right\}, \hspace{1cm} (161)$$

$$\max_{\sigma_S \in \text{BSE}_G} \sqrt{F(\rho_S, \sigma_S)}$$

$$= \max_{X \in \mathcal{L}(H), \omega_{RS} \geq 0} \left\{ \text{Tr}[\text{Re}[X]] : \rho_S X^\dagger X \omega_{RS} \geq 0, \text{Tr}[\omega_{RS}] = 1, \omega_{RS} = \Pi_{RS} \omega_{RS} \Pi_{RS}^G \right\}, \hspace{1cm} (162)$$

$$\max_{\sigma_S \in \text{SymExt}_G} \sqrt{F(\rho_S, \sigma_S)}$$

$$= \max_{X \in \mathcal{L}(H), \omega_{RS} \geq 0} \left\{ \text{Tr}[\text{Re}[X]] : \rho_S X^\dagger X \omega_{RS} \geq 0, \text{Tr}[\omega_{RS}] = 1, \omega_{RS} = U_{RS}(g)\omega_{RS} U_{RS}(g)^\dagger \forall g \in G \right\}. \hspace{1cm} (163)$$

VI. VARIATIONAL ALGORITHMS FOR TESTING SYMMETRY

Having established that the acceptance probabilities can be computed by SDPs for circuits on a sufficiently small number of qubits, we now propose quantum variational algorithms (QVAs) for use on quantum computers. These algorithms make use of variational machine learning techniques to mimic the action of the prover in Algorithms 2–4; however, these techniques are in general limited in terms of their capabilities and thus do not fully satisfy the all-powerful nature of the prover called for in quantum interactive proofs. Note also that training QVAs has been shown to be NP-Hard [BR21]; nonetheless, implementing such methods on near-term quantum devices gives a rough lower bound on the quantities of interest. We present here a series of proof-of-concept implementations of the aforementioned algorithms, and, where applicable, present the results of running these programs on currently available devices.

For the algorithms discussed in this section, all code was implemented in Python using either the Qiskit (used for quantum computing with IBM Quantum) or the Braket (used for AWS services) packages. Any algorithms portrayed were run using local simulators, unless an applicable quantum computer or specific simulator is directly specified.

A. Testing G-Bose symmetry

In order to test membership in Sym$G$, a group with an established unitary representation is needed. One somewhat trivial, albeit easily testable, example is the group generated by the identity and the Pauli Z gate. We begin with a test for Bose symmetry, which in this case is a test whether the state is equal to $|0\rangle|0\rangle$, because the group projection $(I + Z)/2 = |0\rangle|0\rangle$. Calculation by hand or classical computation can easily verify whether a state is Bose symmetric with respect to $I$ and $Z$. Additionally, this simple gate set can be easily implemented on noisy intermediate-scale quantum (NISQ) computers as in Figure 5. We show calculations of this $Z$-Bose symmetry test in Table I for the machines IBMQ_Belem and IBMQ_Rome. Rome has a quantum volume of 32 versus Belem which has 16. We observed a typical deviation of $\pm 3\%$ from both Belem and Rome.

| Input State | Fidelity: Expected | Belem | Rome |
|-------------|--------------------|-------|------|
| | | 0.97 | 0.96 |
| 1 | | 0.08 | 0.05 |
| + | | 0.52 | 0.51 |
| - | | 0.49 | 0.52 |
B. Testing $G$-Symmetry

We now consider a simple test for $G$-symmetry. Considering once more the group formed by the identity and Pauli-Z matrices, we implement the test in Figure 6. As mentioned in Remark 1, this is also a test for incoherence of the input state, i.e., to determine if it is diagonal in the computational basis. In the circuit depicted in Figure 6, a prover is introduced with control over the unitary $W$. Here, a QVA substitutes the role of an all-powerful prover. We begin with an ansatz for the prover’s unitary, which we denote by $W(\alpha, \theta)$. In this trial algorithm, we specify $W(\alpha, \theta)$ according to [BCB+95], namely,

$$W(\alpha, \theta) = \left( e^{i\alpha} \cos \frac{\theta}{2} - e^{-i\alpha} \sin \frac{\theta}{2} \right).$$

Without loss of generality, we can also consider an equivalent ansatz where we act with a Pauli X-gate before or after $W(\alpha, \theta)$. These parameters $\alpha$ and $\theta$ can be altered for machine-learning purposes. We sketch the computational code in the algorithm listed on this page (for the case of testing $k$-extendibility), which demonstrates the framework for all QVAs considered in this section.

For a pure state, we expect that states that are symmetric with regards to this group are also Bose symmetric; mixed states therefore are of particular interest in that they may be symmetric but not Bose symmetric. To achieve this, we consider a slightly altered circuit in Figure 7 where the state of interest is now $\rho$. One interesting choice of $\rho$ is given by the maximally mixed state, which can be achieved by tracing over one qubit of a Bell state. Implementing this test for 20 time steps with an initial ansatz of $W(\pi/2, \pi, 2)$ on IBMQ_Manila, an average fidelity of 0.59 was achieved. This fidelity is rather low compared to the ideal value of one and will be revisited in a future version of this paper.

C. Testing $k$-extendibility

We previously argued that tests of $k$-extendibility are a subset of the more general notion of tests for $G$-symmetric extendibility. Thus, for proof-of-concept purposes, we now demonstrate an example of a QVA capable of testing $k$-extendibility of a state. Using the circuit in Figure 4 as a guide, we developed a trial algorithm using Braket where the unitary implemented by the prover is given by a simple feedback loop as described below. We supposed the prover has an initial ansatz $W(\alpha, \theta)$ as previously described. This approach has an easy generalization, wherein each input to the prover has such a
unitary acting on it. For proof-of-concept attempts, this unitary acted solely on the reference system and the remaining subsystems consisted of a series of CNOT gates.

To test the viability of such an approach, as well as to illustrate it, we test the approach on a state \( \rho_{AB} = \frac{1}{2}(|00\rangle\langle 00| + |11\rangle\langle 11|) \). Let \( U|0\rangle^{\otimes 3} = |\psi^0\rangle_{ABC} \) be a purification of such a state. We can ascertain that the three-qubit GHZ state

\[
|\psi^0\rangle_{ABC} = \frac{1}{\sqrt{2}}(|000\rangle_{ABC} + |111\rangle_{ABC}) \tag{165}
\]

is just such a purification. Then we create an ansatz by allowing the prover to act on only one of the qubits with some initial combination of \( W(\alpha, \theta) \) and the Pauli-X gate, followed by a cascade of CNOT gates on the remaining qubits. The \( k = 2 \) implementation of this type of ansatz can be seen in Figure 8.

For \( k = 2 \), we initially set the \( W \) unitary such that it is equivalent to a Hadamard gate on the reference. This being the incorrect choice for creating an extension of \( \rho_{AB} \), the algorithm then has a chance to learn a correct choice. Running this algorithm 20 times with a time limit of 100 steps through the algorithm yielded a final probability of one every time, although the final unitary varied in its exact form. Running the simulation for just 20 time steps returned an average fidelity of 0.92 ± 0.07.

Transitioning this trial algorithm to Qiskit, we were able to run the same test state on IBMQ_16_Melbourne, a 16-qubit quantum computer. Using the previous ansatz, the QVA was able to learn an additional 10% higher fidelity in 20 time steps. Despite this, it was not able to achieve unity. Following this test, we used an ansatz with simulated fidelity of 0.9. Upon running on the actual machine and before performing machine learning, Melbourne returned an initial fidelity of around 0.6—indicating that machine error dominated in this regime. The algorithm was then performed on IBMQ_Casablanca—a seven-qubit machine with a quantum volume of 32—which achieved an average fidelity of 0.99 after 20 time steps, indicating that this task is achievable on a machine with sufficient quantum volume.

D. Testing \( k \)-Bose-extendibility

Similar to the non-extended cases, it is simpler to test if a state exhibits \( G \)-BSE—or, in this case, if the state is \( k \)-Bose-symmetric-extendible—than to test if it is merely symmetric. This is reflected in Figure 9, which shows a test for 2-BSE. Running this test on a reduced GHZ state with same ansatz as in the previous section on IBMQ_Casablanca, we observed a fidelity of 0.64. This fidelity is also rather low compared to the ideal value of one and will be revisited in a future version of this paper.

VII. RESOURCE THEORIES

In this section, we prove that the various maximum symmetric fidelities proposed in Section III are proper resource-theoretic monotones, in the sense reviewed in [CG19]. Thus, they are indeed measures of symmetry as claimed.

To begin with, let us recall the basics of a resource theory (see [CG19, Definition 1]). Let \( \mathcal{F} \) be a mapping that assigns a unique set of quantum channels to arbitrary input and output systems \( A \) and \( B \), respectively, which includes the identity channel and has the transitive property

\[
\mathcal{N}_{A \to B} \in \mathcal{F}(A \to B) \quad \land \quad \mathcal{M}_{B \to C} \in \mathcal{F}(B \to C) \quad \Rightarrow \quad \mathcal{M}_{B \to C} \circ \mathcal{N}_{A \to B} \in \mathcal{F}(A \to C). \tag{166}
\]

The set \( \mathcal{F}(C \to A) \) defines the set of free states (i.e., channels from the trivial space to system \( A \) are quantum states), and the set \( \mathcal{F}(A \to B) \) defines the set of free channels from system \( A \) to system \( B \). Then the mapping \( \mathcal{F} \) defines the resource theory.

A. Resource theory of asymmetry

The resource theory of asymmetry is well established by now [MS13], but to the best of our knowledge, the resource theory of Bose asymmetry has not been defined yet. Let us begin by recalling the resource theory of asymmetry. Afterwards, we establish the resource theory of Bose asymmetry as well as two other generalizations involving unextendibility, which are in turn generalizations of the resource theory of unextendibility proposed in [KDWW19].

Let \( G \) be a group, and let \( \{U_A(g)\}_{g \in G} \) and \( \{V_B(g)\}_{g \in G} \) denote projective unitary representations of \( G \). A channel \( \mathcal{N}_{A \to B} \) is a free channel in the resource theory of asymmetry if the following \( G \)-covariance symmetry condition holds

\[
\mathcal{N}_{A \to B} \circ U_A(g) = V_B(g) \circ \mathcal{N}_{A \to B} \quad \forall g \in G, \tag{167}
\]

where the unitary channels \( U_A(g) \) and \( V_B(g) \) are respectively defined from \( U_A(g) \) and \( V_B(g) \) as in (147). It then
follows that a state \( \sigma_A \) is free in this resource theory if it is \( G \)-symmetric such that
\[
\sigma_A = U_A(g)(\sigma_A) \quad \forall g \in G,
\]
with a similar definition for the \( B \) system; furthermore, the free channels take free states to free states [MS13], in the sense that \( N_{A\rightarrow B}(\sigma_A) \) is a free state if \( N_{A\rightarrow B} \) is a free channel and \( \sigma_A \) is a free state.

The maximum \( G \)-symmetric fidelity is a resource monotone in the following sense:
\[
\max_{\sigma_A \in \text{Sym}_G} F(\rho_A, \sigma_A) \geq \max_{\sigma_B \in \text{Sym}_G} F(N_{A\rightarrow B}(\rho_A), \sigma_B).
\]
(169)
This follows from the facts that the fidelity does not decrease under the action of a quantum channel and the free channels take free states to free states.

**B. Resource theory of Bose asymmetry**

Now we define the resource theory of Bose asymmetry and prove that the acceptance probability \( \text{Tr}[\Pi_A^G \rho_A] \) of Algorithm 1 is a resource monotone in this resource theory. This demonstrates that \( \text{Tr}[\Pi_A^G \rho_A] \) is a legitimate quantifier of Bose symmetry of a state.

Following the same notation as in Section VII A, recall that a state \( \sigma_A \) is Bose symmetric if the following condition holds
\[
\sigma_A = \Pi_A^G \sigma_A \Pi_A^G,
\]
(170)
where \( \Pi_A^G \) is given by (45). Similarly, a state \( \tau_B \) is Bose symmetric if it obeys the same conditions but for the projector \( \Pi_B^G \) specified by \( \{V_B(g)\}_{g \in G} \). These are the free states in the resource theory of Bose asymmetry.

To define the resource theory, we need to specify the free channels.

**Definition VII.1 (Bose symmetric channel)** We define a channel \( N_{A\rightarrow B} \) to be a Bose symmetric channel (i.e., free channel) if the following condition holds
\[
(N_{A\rightarrow B})^\dagger (\Pi_B^G) \geq \Pi_A^G,
\]
(171)
where \( (N_{A\rightarrow B})^\dagger \) is the Hilbert–Schmidt adjoint of \( N_{A\rightarrow B} \) [Wil17, KW20].

**Proposition VII.1** Bose symmetric channels include the identity channel and they obey the transitive property in (166). Additionally, Bose symmetric states are a
special case of Bose symmetric channels when the input space is trivial.

Proof. When the input and output systems are the same, as well as the unitary representations, it follows that $\Pi_B^G = \Pi_A^G$. Since the identity channel is its own adjoint, we then conclude that (171) holds for the identity channel.

Suppose that $\mathcal{N}_{A \rightarrow B}$ is a quantum channel that obeys the condition in (171). Let $\{W_C(g)\}_{g \in G}$ be a projective unitary representation of $G$, and suppose that $\mathcal{M}_{B \rightarrow C}$ is a Bose symmetric channel satisfying

\[(\mathcal{M}_{B \rightarrow C})^\dagger (\Pi_C^G) \geq \Pi_B^G,\]  

where $\Pi_C^G := \frac{1}{|G|} \sum_{g \in G} W_C(g)$. Consider that

\[ (\mathcal{M}_{B \rightarrow C} \circ \mathcal{N}_{A \rightarrow B})^\dagger (\Pi_C^G) = (\mathcal{N}_{A \rightarrow B})^\dagger [((\mathcal{M}_{B \rightarrow C})^\dagger (\Pi_C^G))] \geq (\mathcal{N}_{A \rightarrow B})^\dagger [\Pi_B^G] \geq \Pi_A^G.\]  

The first equality follows by exploiting the identity $(\mathcal{M}_{B \rightarrow C} \circ \mathcal{N}_{A \rightarrow B})^\dagger = (\mathcal{N}_{A \rightarrow B})^\dagger \circ (\mathcal{M}_{B \rightarrow C})^\dagger$ for adjoints.

The first inequality follows from the assumption that $\mathcal{M}_{B \rightarrow C}$ is a Bose symmetric channel and from the fact that $\mathcal{N}_{A \rightarrow B}$ is completely positive, so that $(\mathcal{N}_{A \rightarrow B})^\dagger$ is also. We thus conclude that $\mathcal{M}_{B \rightarrow C} \circ \mathcal{N}_{A \rightarrow B}$ is a Bose symmetric channel, so that the transitive property in (166) holds.

Finally, suppose that the input system $A$ of a Bose symmetric channel $\mathcal{N}_{A \rightarrow B}$ is trivial. Then each group element $g$ is trivially represented by the number one. It follows that $\Pi_C^G = 1$. Then the channel $\mathcal{N}_{A \rightarrow B}$ is really just a state $\omega_B$ [Will17] with some spectral decomposition $\omega_B = \sum_x p(x) |x\rangle \langle x|_B$; furthermore, the associated Kraus operators are given by $\{\sqrt{p(x)} |x\rangle \langle x|_B\}_x$. Then the condition

\[ (\mathcal{N}_{A \rightarrow B})^\dagger (\Pi_B^G) \geq \Pi_A^G\]  

reduces to

\[ \sum_x p(x) |x\rangle \langle x|_B \Pi_B^G |x\rangle \langle x|_B \geq 1,\]  

which is the same as

\[ \text{Tr}[\Pi_B^G \omega_B] \geq 1.\]  

Since $\omega_B$ is a state and $\Pi_B^G$ is a projection, it follows that $\text{Tr}[\Pi_B^G \omega_B] \leq 1$. Combining these inequalities, we conclude that $\text{Tr}[\Pi_B^G \omega_B] = 1$. Finally, we apply (55) to conclude that $\omega_B$ is a Bose symmetric state.

**Theorem VII.1** Suppose that a quantum channel $\mathcal{N}_{A \rightarrow B}$ obeys the condition in (171). Let $\sigma_A$ be a Bose symmetric state. Then $\mathcal{N}_{A \rightarrow B}(\sigma_A)$ is a Bose symmetric state.

**Proof.** Recall from (55) that a state $\sigma_A$ is Bose symmetric if and only if $\text{Tr}[\Pi_A^G \sigma_A] = 1$. Then consider that

\[ 1 \geq \text{Tr}[\Pi_B^G \mathcal{N}_{A \rightarrow B}(\sigma_A)] = \text{Tr}[(\mathcal{N}_{A \rightarrow B})^\dagger (\Pi_B^G) \sigma_A] \geq \text{Tr}[\Pi_B^G \sigma_A] = 1.\]  

It follows that $\text{Tr}[\Pi_B^G \mathcal{N}_{A \rightarrow B}(\sigma_A)] = 1$, and, by applying (55) again, that $\mathcal{N}_{A \rightarrow B}(\sigma_A)$ is Bose symmetric. 

By essentially the same proof, it follows that the measure $\text{Tr}[\Pi_B^G \rho_A]$ from (54) is non-decreasing under the action of a Bose symmetric channel $\mathcal{N}_{A \rightarrow B}$. Thus, the acceptance probability $\text{Tr}[\Pi_B^G \rho_A]$ of a Bose symmetry test is a resource monotone in the resource theory of Bose asymmetry.

**Theorem VII.2** Let $\rho_A$ be a state, and let $\mathcal{N}_{A \rightarrow B}$ be a Bose symmetric channel. Then $\text{Tr}[\Pi_B^G \rho_A]$ is a resource monotone in the following sense:

\[ \text{Tr}[\Pi_B^G \mathcal{N}_{A \rightarrow B}(\rho_A)] \geq \text{Tr}[\Pi_B^G \rho_A].\]  

**Proof.** Consider that

\[ \text{Tr}[(\mathcal{N}_{A \rightarrow B})^\dagger (\Pi_B^G) \rho_A] \geq \text{Tr}[\Pi_B^G \rho_A],\]  

which follows from (171).

Throughout this section, we have adopted the perspective that Bose symmetric channels are defined by the condition in (171). It then follows as a consequence that $\text{Tr}[\Pi_B^G \rho_A]$ is a resource monotone. We can adopt a different perspective and conclude consistency between them. Let us instead suppose that $\text{Tr}[\Pi_B^G \rho_A]$ is non-decreasing under the action of a free channel $\mathcal{N}_{A \rightarrow B}$. That is, suppose that the following inequality holds for every state $\rho_A$:

\[ \text{Tr}[\Pi_B^G \mathcal{N}_{A \rightarrow B}(\rho_A)] \geq \text{Tr}[\Pi_B^G \rho_A].\]  

Then by rewriting this inequality as

\[ \text{Tr}[(\mathcal{N}_{A \rightarrow B})^\dagger (\Pi_B^G) \rho_A] \geq 0 \quad \forall \rho_A \in \mathcal{D}(\mathcal{H}_A),\]  

we conclude that $(\mathcal{N}_{A \rightarrow B})^\dagger (\Pi_B^G) - \Pi_A^G$ is a positive semi-definite operator, which is equivalent to the condition in (171). Thus, $\mathcal{N}_{A \rightarrow B}$ is a Bose symmetric channel if and only if $\text{Tr}[\Pi_B^G \rho_A]$ is a resource monotone.

**C. Resource theory of asymmetric unextendibility**

We now propose a resource theory that generalizes that proposed in [KDW19], just as the set of $G$-symmetric extendible states generalizes the set of $k$-extendible states (recall Example II.1). One of the main ideas is to use the notion of channel extension introduced in [KDW19]:
additionally, this resource theory allows us to conclude that the acceptance probability of Algorithm 4 (i.e., the maximum $G$-symmetric extendible fidelity) is a resource monotone and thus well motivated in this sense.

Let $G$ be a group, and let $\{U_{RS}(g)\}_{g \in G}$ and $\{V_{R'S'}(g)\}_{g \in G}$ be projective unitary representations of $G$ acting on $\mathcal{H}_R \otimes \mathcal{H}_S$ and $\mathcal{H}_{R'} \otimes \mathcal{H}_{S'}$, respectively.

**Definition VII.2** ($G$-symmetric extendible channel)

A channel $\mathcal{N}_{S \rightarrow S'}$ is $G$-symmetric extendible if there exists a bipartite channel $\mathcal{M}_{RS \rightarrow R'S'}$ such that

1. $\mathcal{M}_{RS \rightarrow R'S'}$ is a channel extension of $\mathcal{N}_{S \rightarrow S'}$:
   \[
   \text{Tr}_R \circ \mathcal{M}_{RS \rightarrow R'S'} = \mathcal{N}_{S \rightarrow S'} \circ \text{Tr}_R, \tag{188}
   \]

2. $\mathcal{M}_{RS \rightarrow R'S'}$ is covariant with respect to $\{U_{RS}(g)\}_{g \in G}$ and $\{V_{R'S'}(g)\}_{g \in G}$:
   \[
   \mathcal{M}_{RS \rightarrow R'S'} \circ U_{RS}(g) = V_{R'S'}(g) \circ \mathcal{M}_{RS \rightarrow R'S'} \quad \forall g \in G, \tag{189}
   \]

where $U_{RS}(g)(\cdot)$ and $V_{R'S'}(g)(\cdot)$ are defined similarly to (147).

The condition in (188) implies that the extension channel $\mathcal{M}_{RS \rightarrow R'S'}$ is non-signaling from $R$ to $S'$ [BGNP01, ESW02, PHHH06], in the sense that

\[
\text{Tr}_R \circ \mathcal{M}_{RS \rightarrow R'S'} = \text{Tr}_R \circ \mathcal{M}_{RS \rightarrow R'S'} \circ \mathcal{R}_R \tag{190}
\]

where $\mathcal{R}_R(\cdot) := \text{Tr}[\cdot]_{\pi_R}$ is a replacer channel that traces out its input and replaces with the maximally mixed state $\pi_R$. This follows because

\[
\text{Tr}_R \circ \mathcal{M}_{RS \rightarrow R'S'} \circ \mathcal{R}_R = \mathcal{N}_{S \rightarrow S'} \circ \text{Tr}_R \circ \mathcal{R}_R = \mathcal{N}_{S \rightarrow S'} \circ \text{Tr}_R \tag{191}
\]

where we have exploited the identity in (188) in the first and last lines, and in the second line used the fact that $\text{Tr}_R \circ \mathcal{R}_R = \text{Tr}_R$.

Definition VII.2 leads to a consistent resource theory of $G$-asymmetric extendibility, in the sense that the free states are $G$-symmetric extendible states and the output of a $G$-symmetric extendible channel acting on a $G$-symmetric extendible state is a $G$-symmetric extendible state.

**Proposition VII.3** Let $\mathcal{N}_{S \rightarrow S'}$ be a $G$-symmetric extendible channel, and let $\rho_S$ be a $G$-symmetric extendible state. Then $\mathcal{N}_{S \rightarrow S'}(\rho_S)$ is a $G$-symmetric extendible state.

**Proof.** Since $\rho_S$ is a $G$-symmetric extendible state, by Definition II.1, there exists an extension state $\omega_{RS}$ satisfying the conditions stated there. Since $\mathcal{N}_{S \rightarrow S'}$ is a $G$-symmetric extendible channel, by Definition VII.2, there exists an extension channel $\mathcal{M}_{RS \rightarrow R'S'}(\omega_{RS})$ satisfying the conditions stated there. It follows that $\mathcal{M}_{RS \rightarrow R'S'}(\omega_{RS})$ is an extension of $\mathcal{N}_{S \rightarrow S'}(\rho_S)$ as

\[
\text{Tr}_R(\mathcal{M}_{RS \rightarrow R'S'}(\omega_{RS})) = \mathcal{N}_{S \rightarrow S'}(\text{Tr}_R(\omega_{RS})) = \mathcal{N}_{S \rightarrow S'}(\rho_S), \tag{194}
\]

where the first equality follows from (188). Also, consider that the following holds for all $g \in G$:

\[
(\omega_{R'S'}(g) \circ \mathcal{M}_{RS \rightarrow R'S'})(\omega_{RS}) = (\mathcal{M}_{RS \rightarrow R'S'} \circ U_{RS}(g))(\omega_{RS}) = \mathcal{M}_{RS \rightarrow R'S'}(\omega_{RS}), \tag{196}
\]

where the first equality follows from (189) and the second from (4).

As a consequence of Proposition VII.3 and the data-processing inequality for fidelity, the maximum $G$-symmetric extendible fidelity is a resource monotone.

**Corollary VII.3** Let $\rho_S$ be a state, and let $\mathcal{N}_{S \rightarrow S'}$ be a $G$-symmetric extendible channel. Then the maximum $G$-symmetric extendible fidelity is a resource monotone,

\[
\max_{\sigma_S \in \text{SymExt}_G} F(\rho_S, \sigma_S) \geq \max_{\sigma_S' \in \text{SymExt}_G} F(\mathcal{N}_{S \rightarrow S'}(\rho_S), \sigma_S'). \tag{189}
\]

**Example VII.1** ($k$-unextendibility) The resource theory of $k$-unextendibility, proposed in [KDWW19], is a special case of the resource theory of $G$-asymmetric extendibility. To see this, recall that a bipartite channel $\mathcal{N}_{AB \rightarrow A'B'}$ is $k$-extendible if there exists an extension channel $\mathcal{M}_{AB_1 \cdots B_k \rightarrow A'B'_1 \cdots B'_k}$ satisfying

\[
\text{Tr}_{B'_2 \cdots B'_k} \circ \mathcal{M}_{AB_1 \cdots B_k \rightarrow A'B'_1 \cdots B'_k} = \mathcal{N}_{AB \rightarrow A'B'} \circ \text{Tr}_{B_2 \cdots B_k} \tag{199}
\]

and

\[
\mathcal{W}_{B'_1 \cdots B'_k} = \mathcal{M}_{AB_1 \cdots B_k \rightarrow A'B'_1 \cdots B'_k} \circ \mathcal{W}_{B_1 \cdots B_k}, \tag{200}
\]

for all $\pi \in S_k$, where $\mathcal{W}_{B_1 \cdots B_k}$ and $\mathcal{W}_{B'_1 \cdots B'_k}$ are unitary permutation channels. Thus, by setting

\[
S = AB, \tag{201}
\]

\[
R = B_2 \cdots B_k, \tag{202}
\]

\[
S' = A'B', \tag{203}
\]

\[
R' = B'_2 \cdots B'_k, \tag{204}
\]

\[
U_{RS}(g) = I_A \otimes W_{B_1 \cdots B_k}(\pi), \tag{205}
\]

\[
V_{R'S'}(g) = I_A' \otimes W_{B'_1 \cdots B'_k}(\pi), \tag{206}
\]
we see that a $k$-extendible channel is a special case of a G-symmetric extendible channel.

### D. Resource theory of Bose asymmetric unextendibility

We finally consider the resource theory of Bose asymmetric unextendibility, with the goal being similar to that of the previous sections; we want to justify the acceptance of metric unextendibility, with the goal being similar to that of Definition VII.3 (i.e., the maximum G-BSE fidelity) as a resource monotone. At the same time, we establish a novel resource theory that could have further applications in quantum information.

Let $G, \{U_{RS}(g)\}_{g \in G}$, and $\{V_{RS'}(g)\}_{g \in G}$ be defined the same way as in Section VII.C.

**Definition VII.3 (G-BSE channel)** A channel $N_{S \rightarrow S'}$ is G-Bose symmetric extendible (G-BSE) if there exists a bipartite channel $M_{RS \rightarrow R'S'}$ such that

1. $M_{RS \rightarrow R'S'}$ is a channel extension of $N_{S \rightarrow S'}$:
   \[
   \text{Tr}_R \circ M_{RS \rightarrow R'S'} = N_{S \rightarrow S'} \circ \text{Tr}_R, \quad (207)
   \]
2. $M_{RS \rightarrow R'S'}$ is Bose symmetric:
   \[
   (M_{RS \rightarrow R'S'})^G(R_{RS'}) \geq \Pi_{RS}^G, \quad (208)
   \]
   where $\Pi_{RS}^G$ and $\Pi_{RS'}^G$ are defined as in ((100)) as sums over $U_{RS}(g)$ and $V_{RS'}(g)$ respectively.

As discussed in (190)–(193), the condition in (207) can be understood as imposing a no-signaling constraint, from $R$ to $S'$.

With the same line of reasoning given in the proof of Proposition VII.2, we conclude the following:

**Proposition VII.4** A G-BSE channel $N_{S \rightarrow S'}$ with trivial input system is a G-BSE state.

The following proposition demonstrates that the resource theory delineated by Definition VII.3 is indeed a consistent resource theory.

**Proposition VII.5** Let $N_{S \rightarrow S'}$ be a G-BSE channel, and let $\rho_{S}$ be a G-BSE state. Then $N_{S \rightarrow S'}(\rho_{S})$ is a G-BSE state.

As this proof is similar to that of Proposition VII.3, we include it in Appendix C. As a consequence of Proposition VII.5 and the data-processing inequality for fidelity, it follows that the maximum G-BSE fidelity is a resource monotone.

**Corollary VII.4** Let $\rho_{S}$ be a state, and let $N_{S \rightarrow S'}$ be a G-BSE channel. Then the maximum G-BSE fidelity is a resource monotone in the following sense:

\[
\max_{\sigma \in \mathcal{B}_{S}} F(\rho_{S}, \sigma_{S}) \geq \max_{\sigma_{S} \in \mathcal{B}_{S}} F(N_{S \rightarrow S'}(\rho_{S}), \sigma_{S'}). \quad (209)
\]

To the best of our knowledge, the resource theory of $k$-Bose unextendibility has not been proposed in prior work. To define it, we establish the notion of a free channel (i.e., a $k$-Bose extendible bipartite channel) and discuss it in the following example.

**Example VII.2 ($k$-Bose unextendibility)** We say that a bipartite channel $\mathcal{N}_{AB \rightarrow AB'}$ is $k$-Bose-extendible if there exists an extension channel $\mathcal{M}_{AB \rightarrow AB'}$ satisfying

\[
\text{Tr}_{B'_{1} \cdots B'_{k}} \circ \mathcal{M}_{AB \rightarrow AB'} = \mathcal{N}_{AB \rightarrow AB'} \circ \text{Tr}_{B2 \cdots Bk}, \quad (210)
\]

and

\[
(\mathcal{M}_{AB \rightarrow AB'})(\Pi_{B'_{1} \cdots B'_{k}}) \geq \Pi_{B_{1} \cdots B_{k}}, \quad (211)
\]

where $\Pi_{B'_{1} \cdots B'_{k}}$ and $\Pi_{B_{1} \cdots B_{k}}$ are projections onto symmetric subspaces,

\[
\Pi_{B_{1} \cdots B_{k}}^{\text{Sym}} := \frac{1}{k!} \sum_{\pi \in S_{k}} W_{\pi}^{*} B_{1} \cdots B_{k}, \quad (212)
\]

\[
\Pi_{B'_{1} \cdots B'_{k}}^{\text{Sym}} := \frac{1}{k!} \sum_{\pi \in S_{k}} W_{\pi}^{*} B'_{1} \cdots B'_{k}, \quad (213)
\]

and $W_{B_{1} \cdots B_{k}}$ and $W_{B'_{1} \cdots B'_{k}}$ are unitary representations of the permutation $\pi \in S_{k}$. Thus, by setting

\[
S = AB, \quad R = B_{2} \cdots B_{k}, \quad (214)
\]

\[
S' = A'B', \quad (215)
\]

\[
R' = B'_{2} \cdots B'_{k}, \quad (216)
\]

\[
U_{RS}(g) = I_{A} \otimes W_{B_{1} \cdots B_{k}}(\pi), \quad (217)
\]

\[
V_{RS'}(g) = I_{A'} \otimes W_{B'_{1} \cdots B'_{k}}(\pi), \quad (218)
\]

we see that a $k$-Bose-extendible channel is a special case of a G-Bose symmetric extendible channel.

### VIII. Conclusion

In summary, we have proposed various quantum computational tests of symmetry, as well as various notions of symmetry like $G$-symmetric extendibility and $G$-Bose symmetric extendibility, which include previous notions of symmetry from [MS13, MS14, Wer89, DPS02, DPS04] as a special case. These tests have acceptance probabilities equal to various maximum symmetric fidelities, thus endowing these measures with operational meaning. We have also established resource theories of asymmetry beyond that proposed in [MS13], which put the maximum symmetric fidelities on firm ground in a resource-theoretic sense. Finally, we evaluated the quantum computational tests on existing quantum computers, by employing a variational algorithm to replace the role of the prover in a quantum interactive proof.
Going forward from here, one could generalize the approach we have taken here to any quantum interactive proof by, for instance, replacing the prover with a variational circuit. This approach will allow for estimating distinguishability measures like the diamond distance [RW05]. This method is not guaranteed to perform well in general, simply because a variational circuit cannot realize an arbitrarily powerful quantum computation like a quantum prover can. For sufficiently small examples, however, this seemingly interesting approach has the potential to go beyond what can be estimated using a classical computer alone.

We are also interested in generalizing the quantum computational tests proposed here to test for extendibility and symmetry of quantum channels. The algorithm outlined in Section IVF is an initial finding in this direction, but more generally, we would like to test for $G$-symmetric extendibility and $G$-Bose symmetric extendibility of bipartite and multipartite channels. This would involve testing for the no-signaling constraint in addition to the symmetry constraint of $k$-extendible channels.

ACKNOWLEDGMENTS

We dedicate this paper to the memory of Jonathan P. Dowling, an outstanding mentor and scientist whose brilliance and friendship will be greatly missed. May he live on through the lives and works of all those he inspired. We thank Patrick Coles and Iman Marvian for discussions. We also acknowledge helpful discussions with ambassadors from Amazon and IBM. MLL acknowledges support from the DoD SMART Scholarship program. MMW acknowledges support from NSF Grant No. 1907615.

[AS67] Yakir Aharonov and Leonard Susskind. Charge superselection rule. Physical Review, 155(5):1428–1431, March 1967.

[BBC+95] Adriano Barenco, Charles Bennett, Richard Cleve, David P. DiVincenzo, Norman Margolus, Peter Shor, Tycho Sleator, John A. Smolin, and Harald Weinfurter. Elementary gates for quantum computing. Physical Review A, 52-5, 1995.

[BCLK+21] Kishor Bharti, Alba Cervera-Lierta, Thi Ha Kyaw, Tobias Haug, Sumner Alperin-Lea, Abhinav Anand, Matthias Degroote, Hermanni Himonen, Jakob S. Kottmann, Tim Menke, Wai-Keong Mok, Sukin Sim, Leong-Chuan Kwek, and Alán Aspuru-Guzik. Noisy intermediate-scale quantum (NISQ) algorithms. 2021. arXiv:2101.08448.

[BCP14] Tillman Baumgratz, Marcus Cramer, and Martin B. Plenio. Quantifying coherence. Physical Review Letters, 113(14):140401, September 2014. arXiv:1311.0275.

[BCY11a] Fernando G. S. L. Brandão, Matthias Christandl, and Jon Yard. Faithful squashed entanglement. Communications in Mathematical Physics, 306(3):805–830, September 2011. arXiv:1010.1750.

[BCY11b] Fernando G. S. L. Brandão, Matthias Christandl, and Jon Yard. A quasipolynomial-time algorithm for the quantum separability problem. Proceedings of ACM Symposium on Theory of Computation, pages 343–351, June 2011. arXiv:1011.2751.

[BGCC21] Jacob L. Beckey, N. Gigena, Patrick J. Coles, and M. Cerezo. Computable and operationally meaningful multipartite entanglement measures. April 2021. arXiv:2104.06923.

[BGNP01] David Beckman, Daniel Gottesman, Michael A. Nielsen, and John Preskill. Causal and localizable quantum operations. Physical Review A, 64(5):052309, October 2001. arXiv:quant-ph/0102043.

[BH13] Fernando G. S. L. Brandão and Aram W. Harrow. Quantum de Finetti theorems under local measurements with applications. In Proceedings of the 45th annual ACM Symposium on the Theory of Computing, pages 861–870, Palo Alto, California, USA, June 2013. arXiv:1210.6367.

[BK21] Lennart Bitte and Martin Kliesch. Training variational quantum algorithms is NP-hard – even for logarithmically many qubits and free fermionic systems. January 2021. arXiv:2101.07267.

[BRSS07] Stephen D. Bartlett, Terry Rudolph, and Robert W. Spekkens. Reference frames, superselection rules, and quantum information. Reviews of Modern Physics, 79(2):555–609, April 2007. arXiv:quant-ph/0610030.

[BV04] Stephen Boyd and Lieven Vandenberghe. Convex Optimization. Cambridge University Press, The Edinburgh Building, Cambridge, CB2 8RU, UK, 2004.

[CAB+20] M. Cerezo, Andrew Arrasmith, Ryan Babbush, Simon C. Benjamin, Suguru Endo, Keisuke Fujii, Jarrod R. McClean, Kosuke Mitarai, Xiao Yuan, Lukasz Cincio, and Patrick J. Coles. Variational quantum algorithms. December 2020. arXiv:2012.09265.

[CDP09] Giulio Chiribella, Giacomo Mauro D’Ariano, and Paolo Perinotti. Realization schemes for quantum instruments in finite dimensions. Journal of Mathematical Physics, 50(4):042101, April 2009.

[CG19] Eric Chitambar and Gilad Gour. Quantum resource theories. Reviews of Modern Physics, 91(2):025001, April 2019. arXiv:1806.06107.

[CHM+16] Tom Cooney, Christoph Hirche, Ciara Morgan, Jonathan P. Olson, Kaushik P. Seshadreesan, John Watrous, and Mark M. Wilde. Operational meaning of quantum measures of recovery. Physical Review A, 94(2):022310, August 2016. arXiv:1512.05324.

[CKMR07] Matthias Christandl, Robert Koenig, Graeme Mitchison, and Renato Renner. One-and-a-half quantum de Finetti theorems. Communications in Mathematical Physics, 273(2):473–498, July 2007. arXiv:quant-ph/0602130.

[CSZW20] Ranyiliu Chen, Zhixin Song, Xuanqiang Zhao, and Xin Wang. Variational quantum algorithms for trace distance and fidelity estimation. December 2020. arXiv:2012.05768.

[Die82] D. Dieks. Communication by EPR devices. Physics...
Appendix A: Proof of Theorem III.2

Following the same reasoning given in (69)–(76), by using Uhlmann’s theorem, we conclude that

\[
\max_{V_{S'E\to RE'}} \left\| \Pi_{RS}^G V_{S'E\to RE'}(\psi)' S'S'[0] E \right\|^2 = \max_{\sigma_{RS}} F(\rho_S, Tr_R[\Pi_{RS}^G \sigma_{RS} \Pi_{RS}^G]), \tag{A1}
\]

where the optimization is over every state \(\sigma_{RS}\) and \(\Pi_{RS}^G\) is defined in (100). The next part of the proof shows that

\[
\max_{\sigma_{RS}} F(\rho_S, Tr_R[\Pi_{RS}^G \sigma_{RS} \Pi_{RS}^G]) = \max_{\sigma_S \in \text{BSE}_G} F(\rho_S, \sigma_S) \tag{A2}
\]

and is similar to (77)–(94). To justify the inequality \(\geq\), let \(\sigma_S\) be an arbitrary state in \(\text{BSE}_G\). Then by Definition II.2, this means that there exists a state \(\omega_{RS}\) such that \(Tr_R[\omega_{RS}] = \sigma_S\) and \(\Pi_{RS}^G \omega_{RS} \Pi_{RS}^G = \omega_{RS}\). This means that

\[
F(\rho_S, \sigma_S) = F(\rho_S, Tr_R[\omega_{RS}]) = F(\rho_S, Tr_R[\Pi_{RS}^G \sigma_{RS} \Pi_{RS}^G]) \leq \max_{\sigma_{RS}} F(\rho_S, Tr_R[\Pi_{RS}^G \sigma_{RS} \Pi_{RS}^G]), \tag{A5}
\]

which implies that

\[
\max_{\sigma_{RS}} F(\rho_S, Tr_R[\Pi_{RS}^G \sigma_{RS} \Pi_{RS}^G]) \geq \max_{\sigma_S \in \text{BSE}_G} F(\rho_S, \sigma_S) \tag{A6}
\]

To justify the inequality \(\leq\), let \(\sigma_{RS}\) be an arbitrary state. If \(\Pi_{RS}^G \sigma_{RS} \Pi_{RS}^G = 0\), then the desired inequality trivially follows. Supposing then that this is not the case, let us define

\[
\sigma'_{RS} = \frac{1}{p} \Pi_{RS}^G \sigma_{RS} \Pi_{RS}^G, \tag{A7}
\]

\[
p := Tr[\Pi_{RS}^G \sigma_{RS}]. \tag{A8}
\]

We then find that

\[
F(\rho_S, Tr_R[\Pi_{RS}^G \sigma_{RS} \Pi_{RS}^G]) = p F(\rho_S, Tr_R[\sigma'_{RS}]) \leq F(\rho_S, Tr_R[\sigma_{RS}]). \tag{A9}
\]

Consider that \(\sigma'_{RS} := Tr_R[\sigma_{RS}]\) is \(G\)-Bose symmetric extendible because \(\sigma_{RS}\) is an extension of it that satisfies \(\Pi_{RS}^G \sigma'_{RS} \Pi_{RS}^G = \sigma_{RS}\). We conclude that

\[
F(\rho_S, Tr_R[\Pi_{RS}^G \sigma_{RS} \Pi_{RS}^G]) \leq \max_{\sigma_{RS} \in \text{BSE}_G} F(\rho_S, \sigma_S). \tag{A11}
\]

Since this inequality holds for every state \(\sigma_{RS}\), we surmise the desired result

\[
\max_{\sigma_{RS}} F(\rho_S, Tr_R[\Pi_{RS}^G \sigma_{RS} \Pi_{RS}^G]) \leq \max_{\sigma_S \in BSE_G} F(\rho_S, \sigma_S). \tag{A12}
\]

Appendix B: Proof of Theorem III.3

Following the same reasoning given in (69)–(76), by using Uhlmann’s theorem, we conclude that

\[
\max_{V_{S'E\to RE'}} \left\| \Pi_{RS}^G V_{S'E\to RE'}(\psi)' S'S'[0] E \right\|^2 = \max_{\sigma_{RS}} F(\rho_S, Tr_R[\Pi_{RS}^G \sigma_{RS} \Pi_{RS}^G]), \tag{B1}
\]

where the optimization is over every state \(\sigma_{RS}\) and \(\Pi_{RS}^G\) is defined in (22). The next part of the proof shows that

\[
\max_{\sigma_{RS}} F(\rho_S, Tr_R[\Pi_{RS}^G \sigma_{RS} \Pi_{RS}^G]) = \max_{\sigma_S \in \text{SymExt}_G} F(\rho_S, \sigma_S) \tag{B2}
\]

and is similar to (77)–(94). To justify the inequality \(\geq\), let \(\sigma_S\) be a state in \(\text{SymExt}_G\). Then by Theorem II.1, there exists a purification \(\varphi_{RSRS}\) of \(\sigma_S\) satisfying \(\varphi_{RSRS} = \Pi_{RSRS}^G \varphi_{RSRS} \Pi_{RSRS}^G\). We find that

\[
F(\rho_S, \sigma_S) = F(\rho_S, Tr_R[\varphi_{RSRS}]) = \max_{\sigma_S \in \text{SymExt}_G} F(\rho_S, \sigma_S) \tag{B3}
\]

\[
= \max_{\sigma_S \in \text{SymExt}_G} F(\rho_S, Tr_R[\Pi_{RSRS}^G \varphi_{RSRS} \Pi_{RSRS}^G]). \tag{B4}
\]

Since the inequality holds for all \(\sigma_S \in \text{SymExt}_G\), we conclude that

\[
\max_{\sigma_S \in \text{SymExt}_G} F(\rho_S, \sigma_S) \leq \max_{\sigma_{RSRS}} F(\rho_S, Tr_R[\Pi_{RSRS}^G \sigma_{RSRS} \Pi_{RSRS}^G]). \tag{B6}
\]

To justify the inequality \(\leq\), let \(\sigma_{RSRS}\) be an arbitrary state. If \(\Pi_{RSRS}^G \sigma_{RSRS} \Pi_{RSRS}^G = 0\), then the desired inequality follows trivially. Supposing then that this is not the case, then define

\[
\sigma'_{RSRS} = \frac{1}{p} \Pi_{RSRS}^G \sigma_{RSRS} \Pi_{RSRS}^G; \tag{B7}
\]

\[
p := Tr[\Pi_{RSRS}^G \sigma_{RSRS}]. \tag{B8}
\]
Then we find that

$$F(\rho_S, \Tr_{RS}[\Pi^G_{RS\hat{S}}\sigma_{RS\hat{S}}\Pi^G_{RS\hat{S}}]) = pF(\rho_S, \Tr_{RS}[\sigma_{RS\hat{S}}]) \leq F(\rho_S, \Tr_{RS}[\sigma_{RS\hat{S}}]) \leq F(\rho_S, \tau_S),$$  \hspace{1cm} (B9) (B10) (B11)

where $\tau_S := \Tr_{RS}[\sigma_{RS\hat{S}}]$. We now aim to show that $\tau_S \in \text{SymExt}_G$. To do so, it suffices to prove that $\sigma_{RS} = U_{RS}(g)\sigma'_{RS}U_{RS}(g)\dagger$ for all $g \in G$. Abbreviating $U \otimes U \equiv U_{RS}(g) \otimes U_{RS}(g)$, consider that

$$\sigma'_{RS} = \Tr_{RS}[\sigma'_{RS\hat{S}}] \quad \sigma'_{RS} = \Tr_{RS}[\Pi^{G}_{RS\hat{S}}\sigma'_{RS\hat{S}}\Pi^{G}_{RS\hat{S}}] \quad \sigma'_{RS} = \Tr_{RS}[U \otimes U]\Pi^{G}_{RS\hat{S}}\sigma'_{RS\hat{S}}\Pi^{G}_{RS\hat{S}}(U \otimes U)\dagger \quad \sigma'_{RS} = \Tr_{RS}[U \otimes U]\Pi^{G}_{RS\hat{S}}\sigma'_{RS\hat{S}}\Pi^{G}_{RS\hat{S}}U\dagger \quad \sigma'_{RS} = U_{RS}(g)\sigma'_{RS}U_{RS}(g)^\dagger.$$

It follows that $\tau_S \in \text{SymExt}_G$, and we conclude that

$$F(\rho_S, \Tr_{RS}[\Pi^G_{RS\hat{S}}\sigma_{RS\hat{S}}\Pi^G_{RS\hat{S}}]) \leq \max_{\sigma_S \in \text{SymExt}_G} F(\rho_S, \sigma_S).$$  \hspace{1cm} (B20)

Since the inequality holds for every state $\sigma_{RS\hat{S}}$, we conclude that

$$\max_{\sigma_{RS\hat{S}}} F(\rho_S, \Tr_{RS}[\Pi^G_{RS\hat{S}}\sigma_{RS\hat{S}}\Pi^G_{RS\hat{S}}]) \leq \max_{\sigma_S \in \text{SymExt}_G} F(\rho_S, \sigma_S).$$  \hspace{1cm} (B21)

**Appendix C: Proof of Proposition VII.5**

The idea of the proof is similar to that for Proposition VII.3. Since $\rho_S$ is a G-BSE state, by Definition II.2, there exists an extension state $\omega_{RS}$ satisfying the conditions stated there. Since $\mathcal{N}_{S \rightarrow S'}$ is a G-BSE channel, by Definition VII.3, there exists an extension channel $\mathcal{M}_{RS \rightarrow R'S'}$ satisfying the conditions stated there. It follows that $\mathcal{M}_{RS \rightarrow R'S'}(\omega_{RS})$ is an extension of $\mathcal{N}_{S \rightarrow S'}(\rho_S)$ because

$$\Tr_{R'}[\mathcal{M}_{RS \rightarrow R'S'}(\omega_{RS})] = \mathcal{N}_{S \rightarrow S'}(\Tr_{R}[\omega_{RS}]) \quad \mathcal{N}_{S \rightarrow S'}(\rho_S),$$  \hspace{1cm} (C1) (C2)

where the first equality follows from (207). Also, consider that the following holds

$$1 \geq \Tr[\Pi^{G}_{R'S'}\mathcal{M}_{RS \rightarrow R'S'}(\omega_{RS})] = \Tr[(\mathcal{M}_{RS \rightarrow R'S'})\Pi^{G}_{R'S'}(\omega_{RS})] \geq \Tr[\Pi^{G}_{R'S'}(\omega_{RS})] = 1.$$  \hspace{1cm} (C3) (C4) (C5)

The first inequality follows because $\mathcal{M}_{RS \rightarrow R'S'}(\omega_{RS})$ is a state and $\Pi^{G}_{R'S'}$ is projection. The first equality follows from the definition of channel adjoint. The second inequality follows from (208), where the first equality follows from (189) and the second from (4). We conclude that $\Tr[\Pi^{G}_{R'S'}\mathcal{M}_{RS \rightarrow R'S'}(\omega_{RS})] = 1$, which by (55), implies that $\mathcal{M}_{RS \rightarrow R'S'}(\omega_{RS})$ is a G-Bose symmetric state. It then follows that $\mathcal{N}_{S \rightarrow S'}(\rho_S)$ is G-Bose symmetric extendible.