Mathematics

https://www.aimspress.com/journal/Math

AIMS Mathematics, 11(9): 27921–27946.
DOI: 10.3934/math.20261115
Received: 21 June 2026
Revised: 20 August 2026
Accepted: 21 August 2026
Published: 02 September 2026

Research article

Equivariant quantum Boolean functions and quantum locality tests

Hao Zheng, Jiajun Yuan and Xingya Fan*

College of Mathematics and System Sciences, Xinjiang University, Urumqi 830017, China

* **Correspondence:** Email: fanxingya@xju.edu.cn.

Abstract: We study quantum Boolean functions on $\mathbb{C}[\mathbb{F}_2^{2n}]$ that are equivariant under the natural action of $S_3 \times S_n$, where S_3 permutes the three nonzero elements of $\mathbb{F}_2^2$, and S_n permutes the coordinate positions n. Using character theory, we decompose the underlying representation into irreducible $S_3 \times S_n$ sectors and show that equivariant operators reduce to blocks acting on finite-dimensional multiplicity spaces. Based on this reduction, we construct a promise based quantum verification protocol combining a group symmetry test, a local purity test, and an energy expectation test. The protocol has completeness and promise gap soundness at least $1 - \delta$, where $\delta \in (0, 1)$. If the three bounded statistics are estimated to additive accuracies proportional to the corresponding promise gaps, its total query complexity is $O\left((\alpha_{\text{sym}}^{-2} + \alpha_{\text{loc}}^{-2} + \alpha_{\text{eng}}^{-2}) \log \delta^{-1}\right)$, up to explicit group sampling, locality, subsystem operation, and copy counting factors, where $\alpha_{\text{sym}}, \alpha_{\text{loc}}, \alpha_{\text{eng}} \in (0, 1)$. Conditional distance soundness follows when the stated error bound property relating the trace distance to the three promise gaps holds. The resulting framework provides a symmetry reduced approach to quantum locality verification without requiring informationally complete state tomography.

Keywords: quantum Boolean functions; quantum locality test; unitary representations
Mathematics Subject Classification: 81P15

1. Introduction

A fundamental challenge in quantum information science is to efficiently verify whether a quantum state or an observable exhibits desired properties without reconstructing the full quantum state. For multipartite quantum systems, two closely related verification tasks are:

(i) State verification: Determine whether a quantum state is separable (local) or contains multipartite entanglement.

(ii) Operator verification: Determine whether a Hermitian operator in an n-qubit system decomposes as a tensor product of single-qubit operators.

These two tasks are intimately connected: Verifying locality of states often reduces to testing properties of associated observables.

A Hermitian operator f in an n-qubit system satisfying $f^2 = I$ is called a *quantum Boolean function*. The Bravyi–Vyalyi quantum locality test [1], introduced in their analysis of local Hamiltonians, is an efficient protocol that uses such Boolean functions to verify whether a quantum state is close to a local (separable) state. Specifically, the test checks whether f is close to a tensor product of single-qubit operators; states that satisfy this condition with high probability under the test are certified as approximately local. A related test, known as the stabilizer test, asks the following question ([2, Conjecture 6.7]): *If it passes with high probability, does it guarantee that f is close to a tensor product?* This remains an open problem in quantum entanglement theory and is one of the motivations for the present work. The key difficulty with generic locality tests is that they provide only limited structural information about the quantum state or the associated Boolean function f (see the works [2–5] and the references given there). This limitation suggests the imposition of additional structural assumptions under which the admissible operator space can be characterized more explicitly. Group symmetry provides one such assumption: Invariance under a prescribed group action restricts the unknown state or observable to an invariant operator algebra that can be decomposed using representation theory. Such symmetry assumptions also arise naturally in several physical and information-theoretic settings. For example, atomic arrays often have permutation symmetry across identical atoms (see [6]), lattice systems respect spatial symmetries (see [7]), and quantum error-correcting codes are designed with stabilizer group symmetries (see [8]). These symmetries place constraints on the relevant space of quantum states and observables. In this paper, we explore how such constraints can be used to reduce the number of measurements required for a specific verification task.

The main contribution of this paper is the following generalization of the Bravyi–Vyalyi-type quantum locality test.

Theorem 1.1. *Let $G = S_3 \times S_n$ be the direct product of the symmetric group S_3 and the symmetric group S_n. For any $g \in G$, let $\theta^{(g)} = U(g)\theta U(g)^\dagger$, where $U(g)$ denotes the unitary representation of G and θ is a positive semidefinite Hermitian operator with trace 1. Fix $\eta \in (0,1)$, a Hermitian operator f, positive parameters $\alpha_{\rm sym}$, $\alpha_{\rm loc}$, $\alpha_{\rm eng}$, and $\delta \in (0,1)$. Assume that the G-invariance test controls a non-negative symmetry defect*

$$\mathsf{SD}_2(\theta) := \frac{1}{2|G|}\sum_{g\in G}\mathrm{Tr}[(\theta-\theta^{(g)})^2]$$

with $\mathsf{SD}_2(\theta) = 0$ if $\theta = \theta^{(g)}$ for any $g \in G$, and rejects with the stated confidence whenever $\mathsf{SD}_2(\theta) \geq \alpha_{\rm sym}$. Then, there exists a quantum verification protocol

$$\textbf{Test}(\theta; \eta, \alpha_{\rm sym}, \alpha_{\rm loc}, \alpha_{\rm eng}, \delta)$$

such that the following statements hold.

(i) (Completeness) *If $\theta \in \mathcal{S}_{\rm loc}(\eta)$, then the protocol accepts θ with probability at least $1-\delta$, where*

$$\mathcal{S}_{loc}(\eta) := \left\{\theta \in \mathcal{L}(\mathbb{C}[\mathbb{F}_2^{2n}]) :\ \theta \textit{ is G-invariant},\ \mathrm{Tr}(\theta f) = 1,\ P_{\rm loc}(\theta) \geq 1-\frac{\eta}{2}\right\}.$$

Here, $\mathcal{L}(\mathbb{C}[\mathbb{F}_2^{2n}])$ *is the set of all linear maps from* $\mathbb{C}[\mathbb{F}_2^{2n}]$ *to itself, and* $\mathrm{Tr}(\theta f)$ *denotes the trace of operator* θf*.*

(ii) (Promise gap soundness) *If at least one of*

$$\mathsf{SD}_2(\theta) \geq \alpha_{\mathrm{sym}}, \quad P_{\mathrm{loc}}(\theta) \leq 1 - \frac{\eta}{2} - \alpha_{\mathrm{loc}}, \quad \text{or} \quad 1 - \mathrm{Tr}(\theta f) \geq \alpha_{\mathrm{eng}} \tag{1.1}$$

holds, then the protocol rejects θ *with probability at least* $1 - \delta$*.*

(iii) (Conditional distance soundness) *Suppose, in addition, that the following error bound property holds: For every* θ*,*

$$\min_{\omega \in \mathcal{S}_{\mathrm{loc}}(\eta)} D_{\mathrm{tr}}(\theta, \omega) > \varepsilon$$

implies that at least one of the promise gap conditions in (1.1) *holds, where*

$$D_{\mathrm{tr}}(\theta, \omega) := \mathrm{Tr}\sqrt{(\theta - \omega)^{\dagger}(\theta - \omega)}.$$

Then, every state that is ε*-far from* $\mathcal{S}_{\mathrm{loc}}(\eta)$ *is rejected with probability at least* $1 - \delta$*.*

The total query complexity is the sum of the three component complexities. In particular, if each component estimates a bounded quantity to additive accuracy proportional to its promise gap, then

$$Q = O\left[\left(\alpha_{\mathrm{sym}}^{-2} + \alpha_{\mathrm{loc}}^{-2} + \alpha_{\mathrm{eng}}^{-2}\right)\log \delta^{-1}\right],$$

up to the explicit group-sampling, locality, and copy-counting factors in the component tests.

The stabilizer testing question motivating this work asks whether high acceptance probability alone guarantees proximity to a tensor product structure. This implication remains open in general. Existing Bravyi–Vyalyi-type locality tests provide efficient local consistency or purity statistics, but such statistics need not uniquely determine the global structure of an arbitrary state. Our approach does not resolve the general stabilizer test conjecture. Instead, it studies a symmetry restricted setting in which the $S_3 \times S_n$ action decomposes the admissible operator space into explicit multiplicity blocks. The verification protocol combines this symmetry information with local purity and energy statistics. Its soundness is therefore a promise gap statement, although trace distance soundness additionally requires the error bound property stated explicitly in Theorem 1.1 (iii).

The verification protocol developed here should be distinguished from quantum state tomography. Quantum state tomography aims to reconstruct the density matrix θ (it is a positive semidefinite Hermitian operator with trace 1) of a quantum system from measurement statistics. A general state of a d-dimensional quantum system, where $d = 2^n$ for an n-qubit system, is specified by $d^2 - 1$ independent real parameters. Consequently, standard quantum state tomography requires sufficient measurement data to determine these parameters [9]. Several variants have been developed to improve tomographic efficiency or accommodate specific experimental settings; see, for example, see [10–12]. In contrast, our protocol estimates only the group averaged symmetry defect, the mean local purity, and the energy defect associated with a prescribed Hermitian operator. Relevant measurements include random-site symmetry tests, and measurements of the quantum Boolean function. These measurements are not generally informationally complete and do not reconstruct the state, its spectrum, or all of its reduced density matrices. The representation theoretic decomposition may nevertheless be useful for symmetry reduced tomography because it identifies multiplicity space blocks on which equivariant operators act nontrivially. In the present paper, however, this decomposition is used for property verification rather than state reconstruction.

Finally, we clarify the role of the prime factorization in multiplicity spaces. This follows from a fundamental fact of arithmetic: Any integer $m_{\rho,\mu} > 1$ is either prime or admits a unique factorization into primes, up to permutation of the factors. That is, for $m_{\rho,\mu} > 1$ and $m_{\rho,\mu} \in \mathbb{N}$, there exist primes $p_1 \leq p_2 \leq \ldots \leq p_k$ such that $m_{\rho,\mu} = p_1 p_2 \ldots p_k$, and this representation is unique (see [13] for more details). Moreover, in group representation theory, $m_{\rho,\mu}$ is the dimension of the multiplicity space $\mathbb{C}^{m_{\rho,\mu}}$ of a certain irreducible subspace of $S_3 \times S_n$ (see Theorem 2.5 below). Then, $\mathbb{C}^{m_{\rho,\mu}}$ can be isomorphically decomposed as $\mathbb{C}^{p_1} \otimes \mathbb{C}^{p_2} \otimes \cdots \otimes \mathbb{C}^{p_k}$, where each factor $\mathbb{C}^{p_j}$ corresponds to a subsystem of dimensional p_j. In particular, the above decomposition is not arbitrary. If $S_3 \times S_n$ acts on $\mathbb{C}^{m_{\rho,\mu}}$, and $m_{\rho,\mu}$ admits a prime factorization, then the group action may decompose as a tensor product of representations on the corresponding prime dimensional factors. For example, if $m_{\rho,\mu} = 12 = 2 \times 2 \times 3$, it decomposes into the tensor product of two qubits and one qutrit, and if $m_{\rho,\mu} = 30 = 2 \times 3 \times 5$, it decomposes into the tensor product of a qubit, a qutrit and a ququint. The prime factorization of the multiplicity space dimension is used only as a formal coordinate expansion. Although one may choose an algebraic identification

$$\mathbb{C}^{m_{\rho,\mu}} \cong \bigotimes_{j=1}^{k} \mathbb{C}^{p_j},$$

this identification is noncanonical and does not define physically accessible subsystems. In particular, it does not by itself produce a quantum error correcting code, an encoding map, or a recovery procedure. Any connection with quantum coding would require additional physical structure, including a specified tensor product decomposition, an error model, a code subspace, and a recovery channel (see, e.g., the works [4, 14, 15]). Such questions are beyond the scope of the present work. Therefore, Theorems 3.1 and 4.4 as below are of independent interest but are not central to the main results of this paper; they are merely applications of prime factorization in multiplicity spaces.

This paper is organized as follows: In Section 2, we recall the structure of the direct product group $S_3 \times S_n$ and derive the irreducible decomposition of its unitary representations acting in space $\mathbb{C}[\mathbb{F}_2^{2n}]$. In Section 3, based on the decomposition of the irreducible unitary representations of $S_3 \times S_n$, we construct a quantum Boolean function. In Section 4, we introduce density matrices, develop a quantum testing protocol, and prove the quantum locality test.

2. Preliminaries

The objective of this section is to isolate the multiplicity spaces on which $S_3 \times S_n$-equivariant operators may act nontrivially. We first compute the character of the natural action on $\mathbb{C}[\mathbb{F}_2^{2n}]$. We then project this character onto the trivial, sign, and standard representations of S_3. Each resulting S_n-module is subsequently decomposed into Specht modules. This gives the block decomposition used in Section 3 to construct equivariant quantum Boolean functions and in Section 4 to formulate the verification protocol.

Throughout the paper, we always let $\mathbb{F}_2$ be the field with two elements. Let $\mathbb{F}_2^2 = \{e_0, e_1, e_2, e_3\}$, where $e_0 := (0,0)$, $e_1 := (0,1)$, $e_2 := (1,0)$, and $e_3 := (1,1)$. The space $\mathbb{C}[\mathbb{F}_2^2]$ is defined by

$$\mathbb{C}[\mathbb{F}_2^2] = \{\sum_{i=0}^{3} \alpha_i e_i : \alpha_i \in \mathbb{C}\}.$$

For any

$$\psi = \sum_{i=0}^{3} \alpha_i e_i \quad \text{and} \quad \phi = \sum_{i=0}^{3} \beta_i e_i$$

in $\mathbb{C}[\mathbb{F}_2^2]$, we define the inner product by

$$\langle \psi \mid \phi \rangle := \sum_{i=0}^{3} \overline{\alpha_i} \beta_i,$$

where $\bar{\alpha}_i$ denotes the complex conjugate of α_i. Thus, $\mathbb{C}[\mathbb{F}_2^2]$ is a 4-dimensional Hilbert space, and $\{e_i\}$ forms an orthonormal basis. Because $\mathbb{F}_2^{2n} \cong (\mathbb{F}_2^2)^{\otimes n}$, the corresponding Hilbert space admits a tensor product decomposition

$$\mathbb{C}[\mathbb{F}_2^{2n}] \cong \bigotimes_{j=1}^{n} \mathbb{C}[\mathbb{F}_2^2].$$

The inner product on $\mathbb{C}[\mathbb{F}_2^{2n}]$ is defined by

$$\langle \psi | \phi \rangle = \prod_{j=1}^{n} \langle \psi_j | \phi_j \rangle,$$

where $\psi = \psi_1 \otimes \cdots \otimes \psi_n$, and $\phi = \phi_1 \otimes \cdots \otimes \phi_n \in \mathbb{C}[\mathbb{F}_2^{2n}]$. Let S_n be the permutation group of order n. Then, the action of S_n on $\mathbb{F}_2^{2n}$ is given by

$$\pi \cdot A = \pi \cdot (A_1, \ldots, A_n) = (A_{\pi^{-1}(1)}, \ldots, A_{\pi^{-1}(n)}), \tag{2.1}$$

where $\pi \in S_n$, $A \in \mathbb{F}_2^{2n}$, and $A_i \in \mathbb{F}_2^2$. The action of S_3 on $\mathbb{F}_2^{2n}$ is less straightforward and requires the isomorphism $S_3 \cong GL(2, \mathbb{F}_2)$, where $GL(2, \mathbb{F}_2)$ is the set of all 2×2-invertible matrices on $\mathbb{F}_2$. For each $L_\sigma \in GL(2, \mathbb{F}_2)$, we define an invertible linear transformation L_σ: $\mathbb{F}_2^2 \to \mathbb{F}_2^2$ by $L_\sigma(v) = v'$. Moreover, restricting this action to the set of nonzero vectors $\mathbb{F}_2^2 \setminus \{e_0\}$ yields a permutation of these three elements $\{e_1, e_2, e_3\}$. For $\sigma \in S_3$, we define a representation in $\mathbb{F}_2^{2n}$ by

$$\sigma \cdot (A_1, \ldots, A_n) := (L_\sigma(A_1), \ldots, L_\sigma(A_n)). \tag{2.2}$$

Combining (2.1) and (2.2), the action of the group $S_3 \times S_n$ on $\mathbb{F}_2^{2n}$ is given by

$$(\sigma, \pi) \cdot (A_1, \ldots, A_n) := (L_\sigma(A_{\pi^{-1}(1)}), \ldots, L_\sigma(A_{\pi^{-1}(n)})).$$

By this and the group multiplication in $S_3 \times S_n$, we have

$$(\sigma_1, \pi_1) \cdot ((\sigma_2, \pi_2) \cdot A) = (\sigma_1 \sigma_2, \pi_1 \pi_2) \cdot A.$$

Indeed, for the ith coordinate, one finds

$$L_{\sigma_1}(L_{\sigma_2}(A_{\pi_2^{-1}(\pi_1^{-1}(i))})) = L_{\sigma_1 \sigma_2}(A_{(\pi_1 \pi_2)^{-1}(i)}).$$

The representation of $S_3 \times S_n$ on $\mathbb{C}[\mathbb{F}_2^{2n}]$ is given by

$$U(\sigma, \pi)(\phi_1 \otimes \cdots \otimes \phi_n) = L_\sigma(\phi_{\pi^{-1}(1)}) \otimes \cdots \otimes L_\sigma(\phi_{\pi^{-1}(n)}).$$

Definition 2.1. For any $\psi, \phi \in \mathbb{C}[\mathbb{F}_2^{2n}]$ and all $(\sigma, \pi) \in S_3 \times S_n$, if

$$\langle U(\sigma,\pi)\psi \mid U(\sigma,\pi)\phi\rangle = \langle \psi \mid \phi\rangle,$$

then $U(\sigma, \pi)$ is called a unitary representation.

In S_3, we define the character of the representation ρ by χ: $g \mapsto \mathrm{Tr}(\rho(g))$ (see [16] or [17, p57, Definition 5.2]). Let e, t, and c be the identity element, a transposition, and a 3-cycle in S_3, respectively (see [16, 17] for the complete bibliography). The irreducible representations ρ of S_3 are the trivial representation **1**, the sign representation sgn, and the 2-dimensional standard representation Std; see Table 1 as follows:

Table 1. Character table of S_3.

ρ	$\dim \rho$	e	t	c
1	1	1	1	1
sgn	1	1	−1	1
Std	2	2	0	−1

For any $\sigma \in S_3$, we define the number of fixed points of σ acting on $\mathbb{F}_2^2$ by $F(\sigma) := |\mathrm{Fix}_{\mathbb{F}_2^2}(\sigma)|$. Then, one easily obtains $F(e) = 4$, $F(t) = 2$, and $F(c) = 1$.

The following lemma is just [17, Corollary 2].

Lemma 2.2. *As an S_3-module, it admits the following decomposition into irreducible representations,*

$$\mathbb{C}[\mathbb{F}_2^2] \;\cong\; \mathbf{1}^{\oplus 2} \;\oplus\; \mathrm{Std}.$$

The decomposition of $\mathbb{C}[\mathbb{F}_2^2]$ into S_3-irreducibles established in Lemma 2.2 is the base case $n = 1$. To extend this to arbitrarily n, we must track how permutations in S_n interact with the S_3-action on each factor. The key tool is the character formula for the product action, which requires the bookkeeping of cycle types.

Definition 2.3. For $\pi \in S_n$, let m_d be the number of cycles of length d in its cycle decomposition. The cycle type of π is then given by

$$\mathrm{type}(\pi) = 1^{m_1} 2^{m_2} \dots,$$

where $\sum_d dm_d = n$.

Moreover, we define the total number of cycles by $c(\pi) := \sum_d m_d$.

For example, we consider the type of cycle $\pi = (1\ 3\ 5)(2\ 4)(6) \in S_6$. It consists of one 1 cycle (6), one 2 cycle (2 4), and one 3 cycle (1 3 5). Hence, $m_1 = 1$, $m_2 = 1$, $m_3 = 1$, $m_d = 0$ $(d \geq 4)$, and its cycle type is $1^1 2^1 3^1$.

We now consider the character of $S_3 \times S_n$ acting on $\mathbb{C}[\mathbb{F}_2^{2n}]$, where S_3 acts diagonally, and S_n permutes the tensor factors. The space $\mathbb{C}[\mathbb{F}_2^{2n}]$ has a basis $\mathcal{B} = \{A^{(1)}, \dots, A^{(4^n)}\}$, where $A^{(i)} = (A_1^{(i)}, \dots, A_n^{(i)})$ with $A_j^{(i)} \in \mathbb{F}_2^2$ for $i \in \{1, \dots, 4^n\}$ and $j \in \{1, \dots, n\}$. Note that the action of $S_3 \times S_n$ leaves $\mathcal{B}$ invariant. Indeed, for any $(\sigma, \pi) \in S_3 \times S_n$, we need to show that $(\sigma, \pi) \cdot \mathcal{B} = \mathcal{B}$ and that the action is bijective. Because $\mathcal{B}$ is finite, it suffices to prove $(\sigma, \pi) \cdot \mathcal{B} \subset \mathcal{B}$ and that the action is injective, the latter being obvious. For a basis element $A^{(i)} = (A^{(i)}_1, \dots, A^{(i)}_n)$, the group element (σ, π) acts as

$$(\sigma, \pi) \cdot A^{(i)} = \left(L_\sigma A^{(i)}_{\pi^{-1}(1)}, \dots, L_\sigma A^{(i)}_{\pi^{-1}(n)}\right). \tag{2.3}$$

Because $A^{(i)}_j \in \mathbb{F}_2^2$, and $A^{(i)}_{\pi^{-1}(j)} \in \mathbb{F}_2^2$, the invariance of $\mathbb{F}_2^2$ under σ implies $L_\sigma A^{(i)}_{\pi^{-1}(j)} \in \mathbb{F}_2^2$, and hence, $(\sigma, \pi) \cdot \mathcal{B} \subset \mathcal{B}$. We can then write

$$(\sigma, \pi) \cdot (A^{(1)}, \dots, A^{(4^n)}) = (A^{(1)}, \dots, A^{(4^n)}) T_{(\sigma,\pi)},$$

where $T_{(\sigma,\pi)}$ is a $4^n \times 4^n$ permutation matrix corresponding to the action. If we assume $L_\sigma A^{(i)}_{\pi^{-1}(j)} = A^{(i)}_j$, then $\chi_n(\sigma, \pi) = \mathrm{tr}(T_{(\sigma,\pi)})$ equals the number of diagonal entries equal to 1 in $T_{(\sigma,\pi)}$, which is precisely the number of fixed points of (σ, π) acting on $\mathcal{B}$.

With cycle type notation in place, we can now compute the character of the $S_3 \times S_n$-representation on $\mathbb{C}[\mathbb{F}_2^{2n}]$ by counting fixed points. The following lemma is trivial, and we omit the details.

Lemma 2.4. *Let χ_n be the character of $S_3 \times S_n$ on $\mathbb{C}[\mathbb{F}_2^{2n}]$. Then, for $(\sigma, \pi) \in S_3 \times S_n$,*

$$\chi_n(\sigma, \pi) = |\mathrm{Fix}_{\mathbb{F}_2^{2n}}(\sigma, \pi)| = \prod_{d \geq 1} |\mathrm{Fix}_{\mathbb{F}_2^2}(\sigma^d)|^{m_d},$$

where m_d is as in Definition 2.3.

For example, we fix $\pi = (1\ 3\ 5)(2\ 4)(6) \in S_6$. Let $A = (A_1, A_2, A_3, A_4, A_5, A_6) \in \mathbb{F}_2^{12}$. By (2.3), we have $(\sigma, \pi) \cdot A = (L_\sigma A_5, L_\sigma A_4, L_\sigma A_1, L_\sigma A_2, L_\sigma A_3, L_\sigma A_6)$. If $(\sigma, \pi) \cdot A = A$, then $L_\sigma A_5 = A_1$, $L_\sigma A_4 = A_2$, $L_\sigma A_1 = A_3$, $L_\sigma A_2 = A_4$, $L_\sigma A_3 = A_5$, and $L_\sigma A_6 = A_6$. Hence, $A_3 = L_\sigma L_\sigma L_\sigma A_3$, $A_1 = L_\sigma L_\sigma L_\sigma A_1$, $A_5 = L_\sigma L_\sigma L_\sigma A_5$, $A_2 = L_\sigma L_\sigma A_2$, $A_4 = L_\sigma L_\sigma A_4$, and $A_6 = L_\sigma A_6$. Note that A_1, A_3, A_5 are fixed points of σ^3; A_2, A_4 are fixed points of σ^2; and A_6 is a fixed point of σ. Thus, the total number of fixed points for A is $|\,\mathrm{Fix}_{\mathbb{F}_2^2}(\sigma^3)|^1\ |\,\mathrm{Fix}_{\mathbb{F}_2^2}(\sigma^2)|^1\ |\,\mathrm{Fix}_{\mathbb{F}_2^2}(\sigma^1)|^1$.

Let $\pi \in S_n$ have cycle type $1^{m_1} 2^{m_2} \cdots$, with $c(\pi)$ and m_d as in Definition 2.3. Because $t^2 = e$, and $c^3 = e$, from Lemma 2.4, it follows that

$$\begin{cases} \chi_n(e, \pi) = 4^{c(\pi)}, \\ \chi_n(t, \pi) \ = \prod_{d \text{ odd}} 2^{m_d} \prod_{d \text{ even}} 4^{m_d} \ = 2^{\#\{\text{odd-length cycles}\}} 4^{\#\{\text{even-length cycles}\}}, \\ \chi_n(c, \pi) = \prod_{3|d} 4^{m_d} \ = 4^{\#\{\text{cycles whose length is divisible by 3}\}}. \end{cases} \tag{2.4}$$

The irreducible complex representations of S_n are in one-to-one correspondence with the Young diagrams $\mu \vdash n$ (see [18] or [19] for more details). These representations are realized as Specht modules, denoted Sp_μ, and their characters are denoted by χ_μ.

The preceding character formulas (see (2.4)) determine how much of each irreducible S_3-type occurs for a fixed permutation $\pi \in S_n$. It remains to decompose the corresponding coefficient functions as characters of S_n. This second projection produces the Specht module multiplicities $m_{\rho,\mu}$ and completes the decomposition of the direct product representation.

Theorem 2.5. *For every integer $n \geq 1$, $\mathbb{C}[\mathbb{F}_2^{2n}]$ has the following decomposition as an $S_3 \times S_n$-module,*

$$\mathbb{C}[\mathbb{F}_2^{2n}] \ \cong \ \bigoplus_{\rho \in \mathrm{Irr}(S_3)} \ \bigoplus_{\mu \vdash n} (\rho \boxtimes \mathrm{Sp}_\mu)^{\oplus m_{\rho,\mu}} \ \cong \ \bigoplus_{\rho,\mu} (\rho \boxtimes \mathrm{Sp}_\mu) \otimes \mathbb{C}^{m_{\rho,\mu}}, \tag{2.5}$$

where $m_{\rho,\mu}$ denotes the multiplicity of $\rho \boxtimes \mathrm{Sp}_\mu$ in $\mathbb{C}[\mathbb{F}_2^{2n}]$.

Proof. First, we find the decomposition of the $S_3 \times S_n$-module; that is, there exist S_n-modules $M_{\mathbf{1}}(n), M_{\mathrm{sgn}}(n), M_{\mathrm{Std}}(n)$ such that

$$\mathbb{C}[\mathbb{F}_2^{2n}] \;\cong\; (\mathbf{1} \boxtimes M_{\mathbf{1}}(n)) \;\oplus\; (\mathrm{sgn} \boxtimes M_{\mathrm{sgn}}(n)) \;\oplus\; (\mathrm{Std} \boxtimes M_{\mathrm{Std}}(n)). \tag{2.6}$$

Indeed, by constructing the characters

$$\begin{cases} \chi_{M_{\mathbf{1}}(n)}(\pi) \;= \dfrac{1}{6}\Big(\chi_n(e,\pi) + 3\chi_n(t,\pi) + 2\chi_n(c,\pi)\Big), \\ \chi_{M_{\mathrm{sgn}}(n)}(\pi) = \dfrac{1}{6}\Big(\chi_n(e,\pi) - 3\chi_n(t,\pi) + 2\chi_n(c,\pi)\Big), \\ \chi_{M_{\mathrm{Std}}(n)}(\pi) = \dfrac{1}{3}\Big(\chi_n(e,\pi) - \chi_n(c,\pi)\Big), \end{cases} \tag{2.7}$$

and then by the orthogonality relations for the characters, we obtain (2.6). For a given element $\pi \in S_n$, $\sigma \mapsto \chi_n(\sigma,\pi)$ is a class function on S_3, and it admits an expansion

$$\chi_n(\sigma,\pi) = \sum_{\rho\in \mathrm{Irr}(S_3)} \chi_\rho(\sigma)\chi_{M_\rho(n)}(\pi).$$

By the orthogonality of the characters, the coefficient $\chi_{M_\rho(n)}(\pi)$ is obtained by projection

$$\chi_{M_\rho(n)}(\pi) = \frac{1}{|S_3|}\sum_{\sigma\in S_3} \chi_n(\sigma,\pi)\chi_\rho(\sigma).$$

The sum of the conjugacy classes of S_3 and by (2.4) together with the values of $\chi_{\mathbf{1}}, \chi_{\mathrm{sgn}}, \chi_{\mathrm{Std}}$ yields Eq (2.7). Hence, we arrive at the decomposition

$$\mathbb{C}[\mathbb{F}_2^{2n}] \cong \bigoplus_{\rho\in \mathrm{Irr}(S_3)} \rho \boxtimes M_\rho(n).$$

Furthermore, $M_\rho(n)$ arises as a direct summand of $\mathbb{C}[\mathbb{F}_2^2]^{\otimes n}$. Because $\mathbb{C}[\mathbb{F}_2^2]^{\otimes n}$ is finite-dimensional, $M_\rho(n)$ is a finite dimensional S_n-module. By Maschke's theorem (see [20] for more details), every finite dimensional representation of a finite group over $\mathbb{C}$ is completely reducible, so $M_\rho(n)$ decomposes as a direct sum of irreducible S_n-modules:

$$M_\rho(n) \cong \bigoplus_{\mu\vdash n} \mathrm{Sp}_\mu^{\oplus m_{\rho,\mu}},$$

where the multiplicities $m_{\rho,\mu} \geq 0$ are given by the inner product of the characters $m_{\rho,\mu} = \langle \chi_{M_\rho(n)}, \chi_\mu\rangle_{S_n}$. Expanding this inner product yields

$$\langle \chi_{M_\rho(n)}, \chi_\mu\rangle_{S_n} = \frac{1}{|S_n|}\sum_{\pi\in S_n} \chi_{M_\rho(n)}(\pi)\chi_\mu(\pi).$$

Hence,

$$m_{\rho,\mu} = \frac{1}{n!}\sum_{\pi\in S_n} \chi_{M_\rho(n)}(\pi)\chi_\mu(\pi).$$

Finally, in this finite dimensional setting, the multiplicity space can be expressed as

$$\Big(\rho \boxtimes \mathrm{Sp}_\mu\Big)^{\oplus m_{\rho,\mu}} \cong \Big(\rho \boxtimes \mathrm{Sp}_\mu\Big) \otimes \mathbb{C}^{m_{\rho,\mu}}.$$

This completes the proof of Theorem 2.5. □

The significance of the decomposition is that an operator commuting with the $S_3 \times S_n$ action is block diagonal with respect to the irreducible sectors and acts freely only on the multiplicity spaces $\mathbb{C}^{m_{\rho,\mu}}$. Hence, the symmetry assumption reduces the analysis from the full operator algebra to a collection of smaller matrix blocks. As an illustration, we work out the $n = 3$ case explicitly, as this case will serve as the running example for Section 3.

Corollary 2.6. *For $n = 3$, we have*

$$\begin{aligned}\mathbb{C}[\mathbb{F}_2^6] \cong (\mathbf{1} \boxtimes \mathrm{Sp}_{(3)})^{\oplus 7} \ \oplus \ (\mathbf{1} \boxtimes \mathrm{Sp}_{(2,1)})^{\oplus 4} \oplus (\mathrm{sgn} \boxtimes \mathrm{Sp}_{(3)})^{\oplus 1} \ \oplus \ (\mathrm{sgn} \boxtimes \mathrm{Sp}_{(2,1)})^{\oplus 2} \\ \oplus \ (\mathrm{sgn} \boxtimes \mathrm{Sp}_{(1,1,1)})^{\oplus 2} \oplus (\mathrm{Std} \boxtimes \mathrm{Sp}_{(3)})^{\oplus 6} \ \oplus \ (\mathrm{Std} \boxtimes \mathrm{Sp}_{(2,1)})^{\oplus 7} \ \oplus \ (\mathrm{Std} \boxtimes \mathrm{Sp}_{(1,1,1)})^{\oplus 1}.\end{aligned}$$

3. Quantum Boolean functions

By Theorem 2.5, we now explicitly construct quantum Boolean functions on the irreducible subspaces. Suppose that the quantum Boolean function f is $S_3 \times S_n$-equivariant; that is, $U(g)f = fU(g)$ for all $g \in S_3 \times S_n$, where $U(g)$ is as in Definition 2.1. By Schur's lemma, f acts as a scalar multiple of the identity on each irreducible subrepresentation $\rho \boxtimes \mathrm{Sp}_\mu$, which, together with Theorem 2.5, implies that

$$f = \bigoplus_{\rho \in \mathrm{Irr}(S_3)} \bigoplus_{\mu \vdash n} \left[\mathbf{I}_{\rho \boxtimes \mathrm{Sp}_\mu} \otimes M_{m_{\rho,\mu}}\right], \quad M_{m_{\rho,\mu}}^\dagger = M_{m_{\rho,\mu}}, \ M_{m_{\rho,\mu}}^2 = I_{m_{\rho,\mu}}. \tag{3.1}$$

Moreover, from $M_{m_{\rho,\mu}}^2 = I_{m_{\rho,\mu}}$, it follows that any eigenvalue λ of $M_{m_{\rho,\mu}}$, $\lambda = \pm 1$. In particular, for $n = 3$, by Corollary 2.6 and (3.1), we obtain

$$\begin{aligned}f = (\mathbf{I}_{\mathbf{1}\boxtimes \mathrm{Sp}_{(3)}} \otimes M_7) \oplus (\mathbf{I}_{\mathbf{1}\boxtimes \mathrm{Sp}_{(2,1)}} \otimes M_4) \oplus (\mathbf{I}_{\mathrm{sgn}\boxtimes \mathrm{Sp}_{(3)}} \otimes \mathbb{R}) \oplus (\mathbf{I}_{\mathrm{sgn}\boxtimes \mathrm{Sp}_{(2,1)}} \otimes M_2) \\ \oplus (\mathbf{I}_{\mathrm{sgn}\boxtimes \mathrm{Sp}_{(1,1,1)}} \otimes M_2) \ \oplus (\mathbf{I}_{\mathrm{Std}\boxtimes \mathrm{Sp}_{(3)}} \otimes M_6) \oplus (\mathbf{I}_{\mathrm{Std}\boxtimes \mathrm{Sp}_{(2,1)}} \otimes M_7) \oplus (\mathbf{I}_{\mathrm{Std}\boxtimes \mathrm{Sp}_{(1,1,1)}} \otimes \mathbb{R}),\end{aligned}$$

where M_2, M_4, M_6, and M_7 denote Hermitian matrices of order $2, 4, 6$, and 7, respectively.

By the fundamental theorem of arithmetic, any integer $m_{\rho,\mu} > 1$ admits a unique prime factorization $m_{\rho,\mu} = d_1 d_2 \dots d_k$ (see [13] for more details). Moreover, there exists a natural isomorphism

$$\mathbb{C}^{m_{\rho,\mu}} \cong \bigotimes_{j=1}^{k} \mathbb{C}^{d_j}$$

from linear algebra.

Theorem 3.1. *Suppose that $m_{\rho,\mu} = d_1 d_2 \dots d_k$, where each $d_j \geq 2$ is a prime. Then, any $m_{\rho,\mu} \times m_{\rho,\mu}$ Hermitian matrix $M_{m_{\rho,\mu}}$ can be expanded as*

$$M_{m_{\rho,\mu}} = \sum_{m_1=0}^{d_1^2-1} \cdots \sum_{m_k=0}^{d_k^2-1} c_{m_1 \dots m_k} \bigotimes_{j=1}^{k} \Lambda_{m_j}^{(j)},$$

where $\{\Lambda_{m_j}^{(j)} : m_j = 0, 1, \dots, d_j^2 - 1\}$ is an orthonormal basis of Hermitian matrices on the jth subsystem, and the expansion coefficients are

$$c_{m_1 \dots m_k} = \mathrm{Tr}\left(M_{m_{\rho,\mu}} \cdot \bigotimes_{j=1}^{k} \Lambda_{m_j}^{(j)}\right) \in \mathbb{R}.$$

Here, $\mathrm{Tr}(\cdot)$ *denotes the trace of a matrix. If we choose the* $\Lambda^{(j)}_{m_j}$ *to have zero trace (except for* $m_j = 0$*, which gives the normalized identity matrix), then*

$$c_{0,0,\dots,0} = \frac{1}{\sqrt{m_{\rho,\mu}}}\,\mathrm{Tr}(M_{m_{\rho,\mu}}).$$

Proof. This follows directly from the orthonormality of the tensor product basis. □

Remark 3.2. Although the Hermitian basis expansion in Theorem 3.1 holds for any factorization $m_{\rho,\mu} = d_1 d_2 \dots d_k$ with $d_j \geq 2$, we restrict ourselves to the prime factors for the following reasons:

(i) The prime factorization is unique up to ordering, providing a canonical choice among all possible tensor decompositions.
(ii) Each factor $\mathbb{C}^{d_j}$ with the prime d_j is irreducible: It cannot be further decomposed as a nontrivial tensor product $\mathbb{C}^p \otimes \mathbb{C}^q$ with $p, q \geq 2$.
(iii) This aligns with the interpretation of each subsystem as a fundamental d_j-level quantum system (qudit), which cannot be realized as a composite of smaller subsystems.

The prime factorization thus reveals the intrinsic tensor structure of the multiplicity space, whereas an arbitrary factorization may obscure further decomposability.

In particular, if $d_1 = 2$, then the subsystem is a qubit. Thus, we choose the normalized Pauli matrices as follows:

$$\Lambda^{(1)}_0 = \frac{1}{\sqrt{2}} I_2, \quad \Lambda^{(1)}_1 = \frac{1}{\sqrt{2}}\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}, \quad \Lambda^{(1)}_2 = \frac{1}{\sqrt{2}}\begin{pmatrix}0 & -i\\ i & 0\end{pmatrix}, \quad \Lambda^{(1)}_3 = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}.$$

Note that $\mathrm{Tr}(\Lambda^{(1)}_a \Lambda^{(1)}_b) = \delta_{ab}$, and $\mathrm{Tr}(\Lambda^{(1)}_0 \Lambda^{(1)}_0) = 1$. Then, for $m_{\rho,\mu} = 2$ and any 2×2 Hermitian matrix, M_2 can be expanded as

$$M_2 = \sum_{a=0}^{3} c_a \Lambda^{(1)}_a, \quad c_a = \mathrm{Tr}(M \Lambda^{(1)}_a).$$

If $d_2 = 3$, then the subsystem is a qutrit. Thus, we take the generalized Gell-Mann matrices (see, for instance, [21]) as follows:

$$\Lambda^{(2)}_0 = \frac{1}{\sqrt{3}}\begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix}, \qquad \Lambda^{(2)}_1 = \frac{1}{\sqrt{2}}\begin{pmatrix}0 & 1 & 0\\ 1 & 0 & 0\\ 0 & 0 & 0\end{pmatrix}, \qquad \Lambda^{(2)}_2 = \frac{1}{\sqrt{2}}\begin{pmatrix}0 & -i & 0\\ i & 0 & 0\\ 0 & 0 & 0\end{pmatrix},$$

$$\Lambda^{(2)}_3 = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 0 & 0\\ 0 & -1 & 0\\ 0 & 0 & 0\end{pmatrix}, \qquad \Lambda^{(2)}_4 = \frac{1}{\sqrt{2}}\begin{pmatrix}0 & 0 & 1\\ 0 & 0 & 0\\ 1 & 0 & 0\end{pmatrix}, \qquad \Lambda^{(2)}_5 = \frac{1}{\sqrt{2}}\begin{pmatrix}0 & 0 & -i\\ 0 & 0 & 0\\ i & 0 & 0\end{pmatrix},$$

$$\Lambda^{(2)}_6 = \frac{1}{\sqrt{2}}\begin{pmatrix}0 & 0 & 0\\ 0 & 0 & 1\\ 0 & 1 & 0\end{pmatrix}, \qquad \Lambda^{(2)}_7 = \frac{1}{\sqrt{2}}\begin{pmatrix}0 & 0 & 0\\ 0 & 0 & -i\\ 0 & i & 0\end{pmatrix}, \qquad \Lambda^{(2)}_8 = \frac{1}{\sqrt{6}}\begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & -2\end{pmatrix}.$$

These matrices satisfy $\mathrm{Tr}(\Lambda^{(2)}_a) = 0$, $\mathrm{Tr}(\Lambda^{(2)}_a \Lambda^{(2)}_b) = \delta_{ab}$, $a, b = 1, \dots, 8$.

For $\Lambda_0^{(2)}$, we have $\mathrm{Tr}(\Lambda_0^{(2)}) = \sqrt{3}$, $\mathrm{Tr}(\Lambda_0^{(2)}\Lambda_0^{(2)}) = 1$. Then, any 3×3 Hermitian matrix can be expanded as

$$M_3 = \sum_{b=0}^{8} c_b \Lambda_b^{(2)}, \tag{3.2}$$

where $c_b = \mathrm{Tr}(M_3\Lambda_b^{(2)})$ for $b \neq 0$, and $c_0 = \mathrm{Tr}(M_3\Lambda_0^{(2)})$.

Let $m_{\rho,\mu} = 6 = 2 \times 3$. By Theorem 3.1 to the factorization $6 = 2 \times 3$, any 6×6 Hermitian matrix M_6 admits the expansion

$$M_6 = \sum_{a=0}^{3} \sum_{b=0}^{8} c_{ab}\, \Lambda_a^{(1)} \otimes \Lambda_b^{(2)}, \tag{3.3}$$

where

$$c_{ab} = \mathrm{Tr}\left[M_6\left(\Lambda_a^{(1)} \otimes \Lambda_b^{(2)}\right)\right] \in \mathbb{R}. \tag{3.4}$$

The coefficients c_{ab} are, in general, independent jointly indexed coefficients. In particular, they should not generally be written as products of coefficients associated with the two subsystems. If, in addition, the matrix has the product form $M_6 = M_2 \otimes M_3$, where $M_2 = \sum_{a=0}^{3} u_a \Lambda_a^{(1)}$, $M_3 = \sum_{b=0}^{8} v_b \Lambda_b^{(2)}$, then $M_6 = \sum_{a=0}^{3} \sum_{b=0}^{8} u_a v_b\, \Lambda_a^{(1)} \otimes \Lambda_b^{(2)}$. Thus, in this special factorized case, the coefficients in (3.3) satisfy $c_{ab} = u_a v_b$. This product structure is an additional assumption and is not required for the general expansion in Theorem 3.1.

We now present the following Table 2 concerning multiplicities and prime factorization for $n = 3$.

Table 2. Multiplicities and prime factorization for $n = 3$.

(ρ, μ)	$\dim(\rho)$	$\dim(\mathrm{Sp}_\mu)$	$m_{\rho,\mu}$	Prime factorization	Decomposition
$(\mathbf{1}, (3))$	1	1	7	7	$\mathbb{C}^7$
$(\mathbf{1}, (2,1))$	1	2	4	2×2	$\mathbb{C}^2 \otimes \mathbb{C}^2$
$(\mathbf{1}, (1,1,1))$	1	1	0	—	—
$(\mathrm{sgn}, (3))$	1	1	1	—	—
$(\mathrm{sgn}, (2,1))$	1	2	2	2	$\mathbb{C}^2$
$(\mathrm{sgn}, (1,1,1))$	1	1	2	2	$\mathbb{C}^2$
$(\mathrm{Std}, (3))$	2	1	6	2×3	$\mathbb{C}^2 \otimes \mathbb{C}^3$
$(\mathrm{Std}, (2,1))$	2	2	7	7	$\mathbb{C}^7$
$(\mathrm{Std}, (1,1,1))$	2	1	1	—	—

4. Quantum locality tests

4.1. Density matrices

Definition 4.1. Let $\mathcal{L}(\mathbb{C}[\mathbb{F}_2^{2n}])$ be the set of all linear maps from $\mathbb{C}[\mathbb{F}_2^{2n}]$ to itself. A matrix $\theta \in \mathcal{L}(\mathbb{C}[\mathbb{F}_2^{2n}])$ is a density matrix if it is semidefinite and Hermitian positive and satisfies $\mathrm{Tr}(\theta) = 1$.

If a quantum system can be completely described by a state vector $|\psi\rangle$ satisfying the normalization condition $\langle\psi|\psi\rangle = 1$, then the state is a pure state. In this case, the density matrix is $\theta = |\psi\rangle\langle\psi|$.

Consequently,

$$\mathrm{Tr}(\theta) = \mathrm{Tr}(|\psi\rangle\langle\psi|) = \langle\psi|\psi\rangle = 1.$$

If the system is a mixed state, that is, a collection of pure states $|\psi_i\rangle$ occur with probabilities p_i, then $\theta = \sum_i p_i|\psi_i\rangle\langle\psi_i|$, where $p_i \geq 0$, and $\sum_i p_i = 1$. In this case,

$$\mathrm{Tr}(\theta) = \sum_i p_i \mathrm{Tr}(|\psi_i\rangle\langle\psi_i|) = \sum_i p_i \cdot 1 = 1.$$

Suppose that the density matrix θ is $S_3 \times S_n$-invariant; that is, $U(g)\theta U(g)^\dagger = \theta$ for all $g \in S_3 \times S_n$, where $U(g)$ is as in Definition 2.1. By (2.5) and Schur's lemma, we have

$$\theta = \bigoplus_{\rho\in\mathrm{Irr}(S_3)} \bigoplus_{\mu\vdash n} \theta_{\rho,\mu} =: \bigoplus_{\rho,\mu} \theta_{\rho,\mu}, \tag{4.1}$$

where $\theta_{\rho,\mu}$ acts on the subspace $(\rho \boxtimes \mathrm{Sp}_\mu) \otimes \mathbb{C}^{m_{\rho,\mu}}$. We define an orthonormal basis for $\rho \boxtimes \mathrm{Sp}_\mu$ by $\{|u_a\rangle\}$, with $a = 1, \ldots, d_\rho d_\mu$. Let the basis for the multiplicity space $\mathbb{C}^{m_{\rho,\mu}}$ be $\{|v_i\rangle\}$, where $i = 1, \ldots, m_{\rho,\mu}$. Then, a basis for $(\rho \boxtimes \mathrm{Sp}_\mu) \otimes \mathbb{C}^{m_{\rho,\mu}}$ is given by

$$|u_a, v_i\rangle := |u_a\rangle \otimes |v_i\rangle. \tag{4.2}$$

The block density matrix $\theta_{\rho,\mu}$ can be written on this basis as

$$\theta_{\rho,\mu} = \sum_{a,b,i,j} (\theta_{\rho,\mu})_{ai,bj}\, |u_a, v_i\rangle\langle u_b, v_j|,$$

where

$$(\theta_{\rho,\mu})_{ai,bj} := \langle u_a, v_i|\theta_{\rho,\mu}|u_b, v_j\rangle. \tag{4.3}$$

The partial trace $\mathrm{Tr}_{\rho\boxtimes\mathrm{Sp}_\mu}$ is defined by

$$(\mathrm{Tr}_{\rho\boxtimes\mathrm{Sp}_\mu}[\theta_{\rho,\mu}])_{ij} := \sum_{a=1}^{d_\rho d_\mu} (\theta_{\rho,\mu})_{ai,aj}.$$

Let us denote

$$A_{m_{\rho,\mu}} := \mathrm{Tr}_{\rho\boxtimes\mathrm{Sp}_\mu}[\theta_{\rho,\mu}] \in \mathrm{End}(\mathbb{C}^{m_{\rho,\mu}}). \tag{4.4}$$

Then, $A_{m_{\rho,\mu}}$ is obtained by taking the partial trace over the representation space, which leaves an operator acting on the multiplicity space.

The following lemma is reversely, the details being omitted.

Lemma 4.2. *Suppose that θ is a density matrix as in Definition 4.1. Then, $A_{m_{\rho,\mu}}$ also is a density matrix.*

Definition 4.3. The expectation of a discrete random variable Y is defined as

$$\mathbb{E}[Y] = \sum_x x\, P(Y = x),$$

where the summation is over all possible values x of Y.

The eigenvalues of f as in (3.1) are ± 1, and therefore, $\{\pm 1\}$ can be viewed as a random variable. The probabilities for the outcomes ± 1 are $P_\pm = \mathrm{Tr}(\theta\Pi_\pm)$, where

$$\Pi_+ = \frac{I+f}{2} \quad \text{and} \quad \Pi_- = \frac{I-f}{2}$$

denote the projectors in the ± 1 eigenspaces of f. Note that $\Pi_+ - \Pi_- = f$, and $\Pi_+ + \Pi_- = I$. Then, by Definition 4.3, we obtain

$$\mathbb{E} = (+1)\mathrm{Tr}(\theta\Pi_+) + (-1)\mathrm{Tr}(\theta\Pi_-) = \mathrm{Tr}(\theta f).$$

The following result is an application of Theorem 3.1 and is of independent interest, separate from the main line of this paper.

Theorem 4.4. *Suppose that the density matrix θ is $S_3 \times S_n$-invariant. Then, the expectation of the quantum Boolean function f as in* (3.1) *on the density matrix θ is*

$$\mathbb{E} = \mathrm{Tr}[\theta f] = \sum_{\rho,\mu} \mathrm{Tr}[M_{m_{\rho,\mu}} A_{m_{\rho,\mu}}] =: \sum_{\rho\in\mathrm{Irr}(S_3)} \sum_{\mu\vdash n} \mathrm{Tr}[M_{m_{\rho,\mu}} A_{m_{\rho,\mu}}],$$

where $A_{m_{\rho,\mu}}$ is as in (4.4).

Proof. By (4.1) and (3.1), we see that

$$\mathrm{Tr}[\theta f] = \sum_{\rho,\mu} \mathrm{Tr}[\theta_{\rho,\mu}(\mathbf{I}_{\rho\boxtimes\mathrm{Sp}_\mu} \otimes M_{m_{\rho,\mu}})],$$

where $\mathbf{I}_{\rho\boxtimes\mathrm{Sp}_\mu}$ is the identity on $\rho \boxtimes \mathrm{Sp}_\mu$, and $M_{m_{\rho,\mu}}$ acts on $\mathbb{C}^{m_{\rho,\mu}}$. A complete orthonormal basis for $(\rho \boxtimes \mathrm{Sp}_\mu) \otimes \mathbb{C}^{m_{\rho,\mu}}$ is given by $|u_a, v_i\rangle$ as in (4.2). This basis satisfies

$$\sum_{b,j} |u_b, v_j\rangle\langle u_b, v_j| = I_{d_\rho d_\mu} \otimes I_{m_{\rho,\mu}} = I_{d_\rho d_\mu m_{\rho,\mu}}.$$

The action of $\mathbf{I}_{\rho\boxtimes\mathrm{Sp}_\mu} \otimes M_{m_{\rho,\mu}}$ on $|u_a, v_i\rangle$ is

$$(\mathbf{I}_{\rho\boxtimes\mathrm{Sp}_\mu} \otimes M_{m_{\rho,\mu}})|u_a, v_i\rangle = \sum_j (M_{m_{\rho,\mu}})_{ji} |u_a, v_j\rangle, \tag{4.5}$$

where $(M_{m_{\rho,\mu}})_{ji} = \langle v_j | M_{m_{\rho,\mu}} | v_i\rangle$. Define

$$\mathrm{Tr}[\theta_{\rho,\mu}(\mathbf{I}_{\rho\boxtimes\mathrm{Sp}_\mu} \otimes M_{m_{\rho,\mu}})] = \sum_{a,i} \langle u_a, v_i | \theta_{\rho,\mu}(\mathbf{I}_{\rho\boxtimes\mathrm{Sp}_\mu} \otimes M_{m_{\rho,\mu}}) | u_a, v_i\rangle.$$

Now, we compute the matrix element $\langle u_a, v_i | \theta_{\rho,\mu}(\mathbf{I}_{\rho\boxtimes\mathrm{Sp}_\mu} \otimes M_{m_{\rho,\mu}}) | u_a, v_i\rangle$. Inserting a complete set of basis states between $\theta_{\rho,\mu}$ and $\mathbf{I}_{\rho\boxtimes\mathrm{Sp}_\mu} \otimes M_{m_{\rho,\mu}}$, we obtain

$$\begin{aligned}
\theta_{\rho,\mu}(\mathbf{I}_{\rho\boxtimes\mathrm{Sp}_\mu} \otimes M_{m_{\rho,\mu}}) &= \theta_{\rho,\mu} \cdot I_{d_\rho d_\mu m_{\rho,\mu}} \cdot (\mathbf{I}_{\rho\boxtimes\mathrm{Sp}_\mu} \otimes M_{m_{\rho,\mu}}) \\
&= \theta_{\rho,\mu} \left(\sum_{b,j} |u_b, v_j\rangle\langle u_b, v_j| \right) (\mathbf{I}_{\rho\boxtimes\mathrm{Sp}_\mu} \otimes M_{m_{\rho,\mu}}).
\end{aligned}$$

From this and from (4.3), it follows that

$$\begin{aligned}\langle u_a, v_i|\theta_{\rho,\mu}(\mathbf{I}_{\rho\boxtimes\mathrm{Sp}_\mu}\otimes M_{m_{\rho,\mu}})|u_a, v_i\rangle &= \left\langle u_a, v_i|\theta_{\rho,\mu}\left(\sum_{b,j}|u_b, v_j\rangle\langle u_b, v_j|\right)(\mathbf{I}_{\rho\boxtimes\mathrm{Sp}_\mu}\otimes M_{m_{\rho,\mu}})|u_a, v_i\right\rangle\\ &= \sum_{b,j}\langle u_a, v_i|\theta_{\rho,\mu}|u_b, v_j\rangle\cdot\langle u_b, v_j|(\mathbf{I}_{\rho\boxtimes\mathrm{Sp}_\mu}\otimes M_{m_{\rho,\mu}})|u_a, v_i\rangle\\ &= \sum_{b,j}(\theta_{\rho,\mu})_{ai,bj}\cdot\langle u_b, v_j|(\mathbf{I}_{\rho\boxtimes\mathrm{Sp}_\mu}\otimes M_{m_{\rho,\mu}})|u_a, v_i\rangle,\end{aligned}$$

which, together with (4.5), implies that

$$\langle u_b, v_j|(\mathbf{I}_{\rho\boxtimes\mathrm{Sp}_\mu}\otimes M_{m_{\rho,\mu}})|u_a, v_i\rangle = \delta_{ba}(M_{m_{\rho,\mu}})_{ji}.$$

Hence,

$$\langle u_a, v_i|\theta_{\rho,\mu}(\mathbf{I}_{\rho\boxtimes\mathrm{Sp}_\mu}\otimes M_{m_{\rho,\mu}})|u_a, v_i\rangle = \sum_j(\theta_{\rho,\mu})_{ai,aj}(M_{m_{\rho,\mu}})_{ji}.$$

Furthermore, by (4.4), we have

$$\mathrm{Tr}[\theta_{\rho,\mu}(\mathbf{I}_{\rho\boxtimes\mathrm{Sp}_\mu}\otimes M_{m_{\rho,\mu}})] = \sum_{a,i,j}(\theta_{\rho,\mu})_{ai,aj}(M_{m_{\rho,\mu}})_{ji} = \sum_{i,j}(A_{m_{\rho,\mu}})_{ij}(M_{m_{\rho,\mu}})_{ji}.$$

The sum then becomes

$$\mathrm{Tr}[\theta f] = \sum_{\rho,\mu}\sum_{i,j}(A_{m_{\rho,\mu}})_{ij}(M_{m_{\rho,\mu}})_{ji} = \sum_{\rho,\mu}\sum_{i,j}(M_{m_{\rho,\mu}})_{ji}(A_{m_{\rho,\mu}})_{ij} = \sum_{\rho,\mu}\mathrm{Tr}\,[M_{m_{\rho,\mu}}A_{m_{\rho,\mu}}].$$

This completes the proof of Theorem 4.4. □

4.2. Symmetry, local purity, and energy tests

The global SWAP measurement used in this paper is defined as follows:

Definition 4.5. Let ρ and σ be the density matrices of two identical copies of the complete system. The SWAP operator SWAP exchanges the two copies and is defined by

$$\mathrm{SWAP} = \sum_{i,j}|i\rangle\langle j|\otimes|j\rangle\langle i|,$$

where $\{|i\rangle\}$ is an arbitrary orthonormal basis of the Hilbert space of the complete system. The global SWAP measurement is the measurement of SWAP, with expectation value

$$\mathbb{E}[\mathrm{SWAP}] = \mathrm{Tr}(\rho\sigma).$$

To obtain the symmetry, local purity, and energy tests, we need the classical Hoeffding inequality (see [22] for more details).

Lemma 4.6. *Let $X_1, X_2, \dots, X_t$ be independent random variables that satisfy $a \le X_i \le b$ for $i = 1, \dots, t$. Let*

$$\bar{X} = \frac{1}{t}\sum_{i=1}^{t} X_i$$

be the sample mean and $\mu = \mathbb{E}[\bar{X}]$ be the expectation. Then, for any $\eta > 0$,

$$P\left(|\bar{X} - \mu| \ge \eta\right) \le 2\exp\left(-\frac{2t\eta^2}{(b-a)^2}\right).$$

For a density matrix θ, the symmetry test estimates a non-negative group-averaged symmetry defect and determines whether this defect is zero, up to a prescribed promise gap $\alpha_{\mathrm{sym}} > 0$. Let $G = S_3 \times S_n$. For $g \in G$, define $\theta^{(g)} = U(g)\theta U(g)^\dagger$. We use the global Hilbert–Schmidt symmetry defect

$$\mathsf{SD}_2(\theta) := \frac{1}{2|G|}\sum_{g\in G} \|\theta - \theta^{(g)}\|_2^2,$$

where

$$\|\theta - \theta^{(g)}\|_2^2 = \mathrm{Tr}[(\theta - \theta^{(g)})^2].$$

This quantity satisfies $\mathsf{SD}_2(\theta) \ge 0$ and

$$\mathsf{SD}_2(\theta) = 0 \quad \Longleftrightarrow \quad U(g)\theta U(g)^\dagger = \theta \quad \text{for every } g \in G.$$

The symmetry test proceeds as follows:

(i) Choose an accuracy parameter $s_{\mathrm{sym}} = \alpha_{\mathrm{sym}}/4$ and a component failure probability $\delta_{\mathrm{sym}} \in (0, 1)$.

(ii) Estimate the purity $p(\theta) := \mathrm{Tr}(\theta^2)$. For each $\ell = 1, \dots, N_p$, take two fresh copies of θ, perform a global SWAP measurement, and let $A_\ell \in \{-1, 1\}$ denote its outcome. Then, $\mathbb{E}[A_\ell] = \mathrm{Tr}(\theta^2) = p(\theta)$. Define

$$\widehat{p} = \frac{1}{N_p}\sum_{\ell=1}^{N_p} A_\ell.$$

(iii) Estimate the group-averaged transformed overlap

$$a(\theta) := \frac{1}{|G|}\sum_{g\in G} \mathrm{Tr}(\theta\theta^{(g)}).$$

For each $\ell = 1, \dots, N_a$, we take two fresh copies of θ, apply $U(g_\ell)$ to the second copy, and perform a global SWAP measurement between the first copy and the transformed second copy. Let $B_\ell \in \{-1, 1\}$ be the SWAP outcome. Then,

$$\mathbb{E}[B_\ell \mid g_\ell] = \mathrm{Tr}\left[\theta U(g_\ell)\theta U(g_\ell)^\dagger\right],$$

and hence, $\mathbb{E}[B_\ell] = a(\theta)$. Define

$$\widehat{a} = \frac{1}{N_a}\sum_{\ell=1}^{N_a} B_\ell.$$

(iv) Define the empirical symmetry defect by $\widehat{\mathsf{SD}}_2(\theta) = \widehat{p} - \widehat{a}$. The estimator is unbiased:

$$\mathbb{E}\left[\widehat{\mathsf{SD}}_2(\theta)\right] = \mathsf{SD}_2(\theta).$$

Choose N_p and N_a sufficiently large that

$$P\left(|\widehat{p} - p(\theta)| \geq \frac{s_{\mathrm{sym}}}{2}\right) \leq \frac{\delta_{\mathrm{sym}}}{2}, \quad P\left(|\widehat{a} - a(\theta)| \geq \frac{s_{\mathrm{sym}}}{2}\right) \leq \frac{\delta_{\mathrm{sym}}}{2}.$$

Because the SWAP outcomes belong to $\{-1, 1\}$, Lemma 4.6 shows that it is sufficient to take

$$N_p, N_a \geq \frac{8}{s_{\mathrm{sym}}^2} \log \frac{4}{\delta_{\mathrm{sym}}}.$$

Because $s_{\mathrm{sym}} = \alpha_{\mathrm{sym}}/4$, one may take

$$N_p, N_a \geq \frac{128}{\alpha_{\mathrm{sym}}^2} \log \frac{4}{\delta_{\mathrm{sym}}}.$$

By the union bound, we have

$$P\left(\left|\widehat{\mathsf{SD}}_2(\theta) - \mathsf{SD}_2(\theta)\right| \geq s_{\mathrm{sym}}\right) \leq \delta_{\mathrm{sym}}.$$

(v) Use the midpoint threshold $\tau_{\mathrm{sym}} = \alpha_{\mathrm{sym}}/2$. Accept the symmetry component if

$$\widehat{\mathsf{SD}}_2(\theta) \leq \tau_{\mathrm{sym}},$$

and reject otherwise.

If θ is G-invariant, then $\mathsf{SD}_2(\theta) = 0$. In the concentration event,

$$\widehat{\mathsf{SD}}_2(\theta) \leq \frac{\alpha_{\mathrm{sym}}}{4} < \frac{\alpha_{\mathrm{sym}}}{2},$$

so the symmetry component is accepted. Therefore, every invariant state is accepted by this component with probability at least $1 - \delta_{\mathrm{sym}}$. Conversely, if $\mathsf{SD}_2(\theta) \geq \alpha_{\mathrm{sym}}$, then, on the same concentration event,

$$\widehat{\mathsf{SD}}_2(\theta) \geq \alpha_{\mathrm{sym}} - \frac{\alpha_{\mathrm{sym}}}{4} = \frac{3\alpha_{\mathrm{sym}}}{4} > \frac{\alpha_{\mathrm{sym}}}{2}.$$

Hence, the symmetry component is rejected with probability at least $1 - \delta_{\mathrm{sym}}$. The test uses $2N_p + 2N_a$ copies of the global state. Its sample complexity is

$$O\left(\alpha_{\mathrm{sym}}^{-2} \log \frac{1}{\delta_{\mathrm{sym}}}\right),$$

up to the explicit cost of sampling $g \in G$, implementing $U(g)$, and performing a global SWAP measurement.

For each site $j \in \{1,\dots,n\}$, define the reduced state of one site $\theta_j = \mathrm{Tr}_{\neq j}(\theta)$. The average local purity is

$$P_{\mathrm{loc}}(\theta) = \frac{1}{n}\sum_{j=1}^{n} \mathrm{Tr}(\theta_j^2),$$

where θ_j denotes the reduced density matrix of the jth qubit. In fact,

$$\theta_j = \mathrm{Tr}_{\neq j}(\theta) = \sum_{\rho,\mu} \mathrm{Tr}_{\neq j}\left(I_{\rho\boxtimes \mathrm{Sp}_\mu} \otimes A_{m_{\rho,\mu}}\right), \tag{4.6}$$

where $\mathrm{Tr}_{\neq j}$ is the partial trace over all qubits except the jth.

Fix $\eta \in (0,1)$ and the probability of failure of the component $\delta_{\mathrm{loc}} \in (0,1)$. The local purity test proceeds as follows:

(i) For each trial $\ell = 1,\dots,N_{\mathrm{loc}}$, independently choose a site $J_\ell \sim \mathrm{Unif}\{1,\dots,n\}$.

(ii) Take two fresh copies of the global state θ, and perform a SWAP measurement on site J_ℓ only. Let $B_\ell \in \{0,1\}$ denote the outcome, where $B_\ell = 1$ corresponds to the symmetric subspace. Conditional on $J_\ell = j$, the passing probability is

$$P(B_\ell = 1 \mid J_\ell = j) = \frac{1+\mathrm{Tr}(\theta_j^2)}{2}.$$

Averaging over the uniformly sampled site gives

$$\mathbb{E}[B_\ell] = \frac{1}{n}\sum_{j=1}^{n}\frac{1+\mathrm{Tr}(\theta_j^2)}{2} = \frac{1+P_{\mathrm{loc}}(\theta)}{2}.$$

(iii) Define

$$\widehat{q}_{\mathrm{loc}} = \frac{1}{N_{\mathrm{loc}}}\sum_{\ell=1}^{N_{\mathrm{loc}}} B_\ell$$

and the estimator $\widehat{P}_{\mathrm{loc}} = 2\widehat{q}_{\mathrm{loc}} - 1$. Then, $\mathbb{E}[\widehat{P}_{\mathrm{loc}}] = P_{\mathrm{loc}}(\theta)$.

(iv) Set $s_{\mathrm{loc}} = \alpha_{\mathrm{loc}}/4$, and choose

$$N_{\mathrm{loc}} \geq \frac{32}{\alpha_{\mathrm{loc}}^2}\log\frac{2}{\delta_{\mathrm{loc}}}.$$

Because $B_\ell \in [0,1]$, it follows that from Lemma 4.8,

$$P\left(\left|\widehat{P}_{\mathrm{loc}} - P_{\mathrm{loc}}(\theta)\right| \geq s_{\mathrm{loc}}\right) \leq 2\exp\left(-\frac{N_{\mathrm{loc}}s_{\mathrm{loc}}^2}{2}\right) \leq \delta_{\mathrm{loc}}.$$

(v) Use the midpoint threshold $\tau_{\mathrm{loc}} = 1 - \eta/2 - \alpha_{\mathrm{loc}}/2$. The local purity test is accepted if $\widehat{P}_{\mathrm{loc}} \geq \tau_{\mathrm{loc}}$, and is rejected otherwise.

Let f be a Hermitian quantum Boolean function as in (3.1), so that $f^2 = I$. Define the Hamiltonian

$$\Pi_- = \frac{I-f}{2}.$$

Because the spectrum of f is contained in $\{-1, +1\}$, Π_- is the orthogonal projector onto the -1 eigenspace of f. Its eigenvalues are 0 and 1. The zero-energy subspace of Π_- is precisely the $+1$ eigenspace of f. For a density matrix θ, define its energy defect by $E_f(\theta) := 1 - \mathrm{Tr}(\theta f)$. The mean energy of Π_- is

$$h_f(\theta) := \mathrm{Tr}(\theta\Pi_-) = \frac{1 - \mathrm{Tr}(\theta f)}{2} = \frac{E_f(\theta)}{2}.$$

The energy test distinguishes the zero-energy condition $\mathrm{Tr}(\theta f) = 1$ from the promise gap condition $1 - \mathrm{Tr}(\theta f) \geq \alpha_{\text{eng}}$. Fix an energy component failure probability $\delta_{\text{eng}} \in (0, 1)$. The test proceeds as follows:

(i) On each of N_{eng} fresh copies of θ, perform the projective measurement $\{\Pi_-, I - \Pi_-\}$. Let $Z_\ell \in \{0, 1\}$, for $\ell = 1, \ldots, N_{\text{eng}}$, denote the outcome, where $Z_\ell = 1$ corresponds to the -1 eigenspace of f. Then, $\mathbb{E}[Z_\ell] = \mathrm{Tr}(\theta\Pi_-) = h_f(\theta)$.

(ii) Compute the empirical mean energy

$$\widehat{h}_f = \frac{1}{N_{\text{eng}}} \sum_{\ell=1}^{N_{\text{eng}}} Z_\ell.$$

(iii) Set the estimation accuracy to $s_{\text{eng}} = \alpha_{\text{eng}}/8$, and choose

$$N_{\text{eng}} \geq \frac{32}{\alpha_{\text{eng}}^2} \log \frac{2}{\delta_{\text{eng}}}.$$

Because the random variables Z_ℓ are independent and take values in $[0, 1]$, it follows that from Lemma 4.6,

$$P\left(\left|\widehat{h}_f - h_f(\theta)\right| \geq \frac{\alpha_{\text{eng}}}{8}\right) \leq 2\exp\left(-\frac{N_{\text{eng}}\alpha_{\text{eng}}^2}{32}\right) \leq \delta_{\text{eng}}.$$

(iv) Use the midpoint threshold $\tau_{\text{eng}} = \alpha_{\text{eng}}/4$. The energy test is aceepted if $\widehat{h}_f \leq \alpha_{\text{eng}}/4$, and is rejected otherwise.

If $\mathrm{Tr}(\theta f) = 1$, then $h_f(\theta) = 0$. On the concentration event,

$$\widehat{h}_f \leq \frac{\alpha_{\text{eng}}}{8} < \frac{\alpha_{\text{eng}}}{4},$$

so the energy test is accepted. Therefore, the completeness probability of this component is at least $1 - \delta_{\text{eng}}$. Conversely, if $1 - \mathrm{Tr}(\theta f) \geq \alpha_{\text{eng}}$, then $h_f(\theta) \geq \alpha_{\text{eng}}/2$. On the same concentration event,

$$\widehat{h}_f \geq \frac{\alpha_{\text{eng}}}{2} - \frac{\alpha_{\text{eng}}}{8} = \frac{3\alpha_{\text{eng}}}{8} > \frac{\alpha_{\text{eng}}}{4}.$$

Thus, the energy test is rejected with probability at least $1 - \delta_{\text{eng}}$.

Each measurement consumes one fresh copy of θ and one query to the measurement of f. Hence, the query complexity of the energy test is

$$Q_{\text{eng}} = N_{\text{eng}} = O\left(\alpha_{\text{eng}}^{-2} \log \delta_{\text{eng}}^{-1}\right).$$

4.3. Quantum locality test

For two density matrices $\sigma, \omega \in \mathcal{L}(\mathbb{C}[\mathbb{F}_2^{2n}])$, the trace distance is defined by

$$D_{\mathrm{tr}}(\sigma, \omega) := \|\sigma - \omega\|_{\mathcal{F}} = \operatorname{Tr}\sqrt{(\sigma - \omega)^{\dagger}(\sigma - \omega)},$$

where $\|\cdot\|_{\mathcal{F}}$ denotes the Frobenius norm. Let

$$\mathcal{S}_{loc}(\eta) := \left\{ \theta \in \mathcal{L}(\mathbb{C}[\mathbb{F}_2^{2n}]) : \begin{array}{l} \theta \text{ is } S_3 \times S_n\text{-invariant}, \\ \operatorname{Tr}(\theta f) = 1, \\ \dfrac{1}{n}\displaystyle\sum_{j=1}^{n} \operatorname{Tr}(\theta_j^2) \geq 1 - \dfrac{\eta}{2},\ \theta_j = \operatorname{Tr}_{[n]\setminus\{j\}}(\theta) \end{array} \right\}. \tag{4.7}$$

The following is a generalization of the Bravyi–Vyalyi-type quantum locality test.

Theorem 4.7. *Fix $\eta \in (0,1)$, a Hermitian operator f, and positive parameters α_{sym}, α_{loc}, α_{eng}, and $\delta \in (0,1)$. Assume that the group invariance test controls a non-negative symmetry defect $\mathsf{SD}_2(\theta)$ with $\mathsf{SD}_2(\theta) = 0$ for every $S_3 \times S_n$-invariant state, and is rejected with the stated confidence whenever $\mathsf{SD}_2(\theta) \geq \alpha_{\mathrm{sym}}$. Then, there exists a quantum verification protocol* **Test**$(\theta; \eta, \alpha_{\mathrm{sym}}, \alpha_{\mathrm{loc}}, \alpha_{\mathrm{eng}}, \delta)$ *such that the following statements hold.*

(i) (Completeness) *If $\theta \in \mathcal{S}_{\mathrm{loc}}(\eta)$, then the protocol accepts θ with probability at least $1 - \delta$.*

(ii) (Promise gap soundness) *If at least one of*

$$\mathsf{SD}_2(\theta) \geq \alpha_{\mathrm{sym}}, \quad P_{\mathrm{loc}}(\theta) \leq 1 - \frac{\eta}{2} - \alpha_{\mathrm{loc}}, \quad \text{or} \quad 1 - \operatorname{Tr}(\theta f) \geq \alpha_{\mathrm{eng}} \tag{4.8}$$

holds, then the protocol rejects θ with probability at least $1 - \delta$.

(iii) (Conditional distance soundness) *Suppose, in addition, that the following error bound property holds: For every density operator θ,*

$$\min_{\omega \in \mathcal{S}_{\mathrm{loc}}(\eta)} D_{\mathrm{tr}}(\theta, \omega) > \varepsilon$$

implies that at least one of the promise gap conditions in (4.8) holds. Then, every state that is ε-far from $\mathcal{S}_{\mathrm{loc}}(\eta)$ is rejected with probability at least $1 - \delta$.

The total query complexity is the sum of the three component complexities. In particular, if each component estimates a bounded quantity to additive accuracy proportional to its promise gap, then

$$Q = O\left[\left(\alpha_{\mathrm{sym}}^{-2} + \alpha_{\mathrm{loc}}^{-2} + \alpha_{\mathrm{eng}}^{-2}\right) \log \frac{1}{\delta}\right],$$

up to the explicit group-sampling, locality, and copy counting factors in the component tests.

To prove the theorem, we need the following technical lemma.

Lemma 4.8. *Let $\eta \in (0,1)$, and let f a Hermitian operator. Suppose that $\mathcal{S}_{\mathrm{loc}}(\eta)$ is the nonempty target set as in (4.7). For $\theta \in \mathcal{L}(\mathbb{C}[\mathbb{F}_2^{2n}])$, define*

$$V(\theta) := \max\left\{ \mathrm{SD}_2(\theta), \left(1 - \frac{\eta}{2} - P_{\mathrm{loc}}(\theta)\right)_+, 1 - \operatorname{Tr}(\theta f) \right\}.$$

Then, for every $\varepsilon > 0$ for which

$$K_\varepsilon := \left\{\theta \in \mathcal{L}(\mathbb{C}[\mathbb{F}_2^{2n}]) : D_{\mathrm{tr}}(\theta, \mathcal{S}_{\mathrm{loc}}(\eta)) \geq \varepsilon\right\}$$

is nonempty, the constant $\alpha(\varepsilon) := \min_{\theta\in K_\varepsilon} V(\theta)$ is well-defined and strictly positive. Consequently, if $D_{\mathrm{tr}}(\theta, \mathcal{S}_{\mathrm{loc}}(\eta)) \geq \varepsilon$, then $V(\theta) \geq \alpha(\varepsilon)$.

Proof. Because $\mathbb{C}[\mathbb{F}_2^{2n}]$ is finite-dimensional, then $\mathcal{L}(\mathbb{C}[\mathbb{F}_2^{2n}])$ is compact. The functions $\mathrm{SD}_2(\theta)$, $P_{\mathrm{loc}}(\theta)$, and $\mathrm{Tr}(\theta f)$ are continuous, and hence, $V(\theta)$ is continuous. Each term in the definition of $V(\theta)$ is non-negative. In particular, because f is a Hermitian operator, and $\|f\|_\infty = 1$, $\mathrm{Tr}(\theta f) \leq 1$ for every $\theta \in \mathcal{L}(\mathbb{C}[\mathbb{F}_2^{2n}])$. Moreover, $\mathrm{SD}_2(\theta) = 0$ if and only if $U(g)\theta U(g)^\dagger = \theta$ for every $g \in S_3 \times S_n$. It follows that $V(\theta) = 0$ if and only if $\theta \in \mathcal{S}_{\mathrm{loc}}(\eta)$. Thus, $\mathcal{S}_{\mathrm{loc}}(\eta) = V^{-1}(\{0\})$ is closed. Because $\mathcal{S}_{\mathrm{loc}}(\eta)$ is nonempty and closed, the function $\theta \mapsto D_{\mathrm{tr}}(\theta, \mathcal{S}_{\mathrm{loc}}(\eta))$ is continuous. Therefore, K_ε is a closed subset of the compact space $\mathcal{L}(\mathbb{C}[\mathbb{F}_2^{2n}])$ and is therefore compact. Because K_ε is assumed to be nonempty, and V is continuous, the minimum $\alpha(\varepsilon) = \min_{\theta\in K_\varepsilon} V(\theta)$ exists. Suppose that $\alpha(\varepsilon) = 0$. Then, there exists $\theta_* \in K_\varepsilon$ such that $V(\theta_*) = 0$. Hence, $\theta_* \in \mathcal{S}_{\mathrm{loc}}(\eta)$, so $D_{\mathrm{tr}}(\theta_*, \mathcal{S}_{\mathrm{loc}}(\eta)) = 0$. On the other hand, $\theta_* \in K_\varepsilon$ implies

$$D_{\mathrm{tr}}(\theta_*, \mathcal{S}_{\mathrm{loc}}(\eta)) \geq \varepsilon > 0,$$

a contradiction. Therefore, $\alpha(\varepsilon) > 0$. The claimed implication follows immediately from the definition of $\alpha(\varepsilon)$. □

Proof of Theorem 4.7. Let $\delta_{\mathrm{sym}} = \delta_{\mathrm{loc}} = \delta_{\mathrm{eng}} = \delta/3$. The protocol applies the symmetry defect test, the local purity test, and the energy test to disjoint copies of the input state. It is accepted if and only if all three component tests are accepted. We assume that f is a Hermitian contraction, namely, $\|f\|_\infty \leq 1$. In particular, this condition holds when f is a Hermitian involution satisfying $f^2 = I$.

Suppose that $\theta \in \mathcal{S}_{\mathrm{loc}}(\eta)$. By the definition of the target set, we see that

$$\mathsf{SD}_2(\theta) = 0, \qquad P_{\mathrm{loc}}(\theta) \geq 1 - \frac{\eta}{2}, \qquad \mathrm{Tr}(\theta f) = 1.$$

Thus, the symmetry, local purity, and energy components accept except with probabilities at most δ_{sym}, δ_{loc}, and δ_{eng}, respectively. The three tests use disjoint copies; probabilistic independence is not required. By the union bound, we know that

$$P(\text{the protocol rejects } \theta) \leq \delta_{\mathrm{sym}} + \delta_{\mathrm{loc}} + \delta_{\mathrm{eng}} = \delta.$$

Therefore, $P(\text{the protocol accepts } \theta) \geq 1 - \delta$. This proves part (i).

Suppose that at least one of

$$\mathsf{SD}_2(\theta) \geq \alpha_{\mathrm{sym}}, \quad P_{\mathrm{loc}}(\theta) \leq 1 - \frac{\eta}{2} - \alpha_{\mathrm{loc}}, \quad 1 - \mathrm{Tr}(\theta f) \geq \alpha_{\mathrm{eng}}$$

holds. If the first condition holds, the symmetry component is rejected with probability at least

$$1 - \delta_{\mathrm{sym}} \geq 1 - \delta.$$

If the second condition holds, the local purity component is rejected with probability at least

$$1 - \delta_{\mathrm{loc}} \geq 1 - \delta.$$

If the third condition holds, the energy component is rejected with probability at least

$$1 - \delta_{\text{eng}} \geq 1 - \delta.$$

is rejected. Because the full protocol is rejected whenever any component is rejected, it rejects θ with probability at least $1 - \delta$. This proves part (ii). The three conditions need not be mutually exclusive.

Assume the additional error bound property in part (iii). If

$$\min_{\omega \in \mathcal{S}_{\text{loc}}(\eta)} D_{\text{tr}}(\theta, \omega) > \varepsilon,$$

then, by Lemma 4.8, we know that, every such θ, satisfies at least one of

$$\mathrm{SD}_2(\theta) \geq \alpha(\varepsilon), \quad P_{\text{loc}}(\theta) \leq 1 - \frac{\eta}{2} - \alpha(\varepsilon), \quad \text{or} \quad 1 - \mathrm{Tr}(\theta f) \geq \alpha(\varepsilon).$$

Part (ii) therefore shows that the protocol rejects θ with probability at least $1 - \delta$. This proves part (iii).

The component tests are performed on disjoint collections of copies, so their query complexities add the following: $Q = Q_{\text{sym}} + Q_{\text{loc}} + Q_{\text{eng}}$. If each component estimates a bounded quantity to additive accuracy proportional to its corresponding promise gap, then

$$Q_{\text{sym}} = O\left(\alpha_{\text{sym}}^{-2} \log \delta_{\text{sym}}^{-1}\right), \quad Q_{\text{loc}} = O\left(\alpha_{\text{loc}}^{-2} \log \delta_{\text{loc}}^{-1}\right), \quad Q_{\text{eng}} = O\left(\alpha_{\text{eng}}^{-2} \log \delta_{\text{eng}}^{-1}\right).$$

Because $\delta_{\text{sym}} = \delta_{\text{loc}} = \delta_{\text{eng}} = \delta/3$, it follows that

$$Q = O\left[\left(\alpha_{\text{sym}}^{-2} + \alpha_{\text{loc}}^{-2} + \alpha_{\text{eng}}^{-2}\right) \log \delta^{-1}\right],$$

up to the explicit group sampling, locality, subsystem operation, and copy counting factors in the three component tests. This completes the proof. □

5. Examples

In this section, we present an application of Theorem 4.7, restricting our attention to the energy and local purity components.

Example 5.1. (Local purity promise gap soundness) Consider the two-ququart Hilbert space

$$(\mathbb{C}^4)^{\otimes 2} \cong \mathbb{C}[\mathbb{F}_2^4],$$

and let

$$|\Phi_4\rangle = \frac{1}{2} \sum_{a=0}^{3} |a\rangle \otimes |a\rangle, \qquad \theta_\Phi = |\Phi_4\rangle\langle\Phi_4|.$$

Set $f = I_{16}$, $\eta = 0.2$, $\alpha_{\text{loc}} = 0.1$, and $\delta = 0.05$. The symmetry promise gap $\alpha_{\text{sym}} > 0$ is left as a parameter determined by the symmetry component. By (4.6), the reduced density operator in the first subsystem is

$$\theta_1 := \mathrm{Tr}_2(\theta_\Phi) = \frac{1}{4} \sum_{a,b=0}^{3} |a\rangle\langle b| \; \mathrm{Tr}\left(|a\rangle\langle b|\right) = \frac{1}{4} \sum_{a,b=0}^{3} |a\rangle\langle b| \, \delta_{ab} = \frac{1}{4} \sum_{a=0}^{3} |a\rangle\langle a| = \frac{I_4}{4}.$$

Similarly, the reduced density operator on the second subsystem is $\theta_2 := \mathrm{Tr}_1(\theta_\Phi) = I_4/4$. Therefore,

$$\theta_1 = \theta_2 = \frac{I_4}{4} = \frac{1}{4}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Hence,

$$P_{\mathrm{loc}}(\theta_\Phi) = \frac{1}{2}\left[\mathrm{Tr}(\theta_1^2) + \mathrm{Tr}(\theta_2^2)\right] = \frac{1}{4}.$$

By the definition of the target set $\mathcal{S}_{\mathrm{loc}}(0.2)$, we see that $P_{\mathrm{loc}}(\theta_\Phi) < 0.9$, namely, $\theta_\Phi \notin \mathcal{S}_{\mathrm{loc}}(0.2)$. Thus, the state θ_Φ is not a completeness example. Notice that

$$P_{\mathrm{loc}}(\theta_\Phi) = \frac{1}{4} < 1 - \frac{\eta}{2} - \alpha_{\mathrm{loc}} = 0.8.$$

By Theorem 4.7 (ii), the protocol is rejected θ_Φ. Therefore, the local purity component is rejected. From Theorem 4.7 (ii), it follows that

$$P(\text{local purity rejection}) \geq 1 - \delta_{\mathrm{loc}} = 1 - \frac{\delta}{3} \geq 1 - \delta = 0.95.$$

Because the full protocol is rejected whenever any component rejects,

$$P(\text{full protocol rejection}) \geq 1 - \delta = 0.95.$$

This rejection is due to the local purity component.

Example 5.2. (Energy promise gap soundness) We consider a protocol instance with $\alpha_{\mathrm{sym}} = \alpha_{\mathrm{loc}} = \alpha_{\mathrm{eng}} = 0.1$, $\delta = 0.05$ and allocate $\delta_{\mathrm{sym}} = \delta_{\mathrm{loc}} = \delta_{\mathrm{eng}} = \delta/3 = 1/60$. To illustrate the energy component, consider a separate instance with

$$f_{\mathrm{eng}} = I_{16} - 2|00\rangle\langle 00|, \quad \theta_{\mathrm{bad}} = |00\rangle\langle 00|.$$

Then, we have $f_{\mathrm{eng}}^\dagger = f_{\mathrm{eng}}$ and

$$f_{\mathrm{eng}}^2 = (I_{16} - 2\theta_{\mathrm{bad}})^2 = I_{16} - 4\theta_{\mathrm{bad}} + 4\theta_{\mathrm{bad}}^2 = I_{16}.$$

Thus, f_{eng} is a Hermitian operator. Moreover, $f_{\mathrm{eng}}|00\rangle = -|00\rangle$, and hence,

$$\mathrm{Tr}\left(\theta_{\mathrm{bad}} f_{\mathrm{eng}}\right) = -1.$$

Therefore,

$$1 - \mathrm{Tr}\left(\theta_{\mathrm{bad}} f_{\mathrm{eng}}\right) = 2 \geq \alpha_{\mathrm{eng}} = 0.1.$$

Thus, the energy component rejects this state deterministically. From Theorem 4.7 (ii), it follows that

$$P(\text{energy rejection}) \geq 1 - \delta_{\mathrm{eng}} = 1 - \frac{\delta}{3} \geq 1 - \delta = 0.95.$$

Because the full protocol is rejected whenever any component is rejected,

$$P(\text{full protocol rejection}) \geq 1 - \delta = 0.95.$$

This rejection is due to the energy component.

6. Conclusions

In this work, we studied quantum Boolean functions on $\mathbb{C}[\mathbb{F}_2^{2n}]$ that are equivariant under the natural action of $S_3 \times S_n$. By combining the representation theories of S_3 and S_n, we decomposed the underlying module into irreducible symmetry sectors and identified the corresponding multiplicity spaces. This decomposition reduces equivariant operators to a collection of smaller matrix blocks. Using these blocks, we constructed a promise-based quantum verification protocol with three components: a symmetry defect test, a local purity test, and an energy test associated with a prescribed Hermitian quantum Boolean function. We established completeness and promise gap soundness using finite-sample concentration estimates. Conditional distance soundness follows when an additional error bound property relates trace distance from the target set to the three tested quantities.

The present framework has several limitations. It is restricted to the $S_3 \times S_n$ action and to the class of target sets considered in the manuscript. Moreover, the conditional distance soundness statement requires the error bound hypothesis in Theorem 4.7 (iii). The prime factorization of multiplicity space dimensions is used only as a formal coordinate expansion and does not, by itself-define physical subsystems or a quantum error correcting code.

Several directions for future research remain open. One natural direction is to extend the representation theoretic analysis to other local alphabets, larger local symmetry groups, and more general permutation group actions. Such extensions may reveal additional families of equivariant quantum Boolean functions and verification problems beyond the action of $S_3 \times S_n$ considered here. Another important problem is to identify concrete target operators and group representations for which an explicit distance-to-promise property, as required in Theorem 4.7 (iii), can be established. The finite dimensional compactness argument yields only an implicit positive modulus and does not provide an unconditional quadratic error bound or an explicit relation between the trace distance and the three promise gaps. The second direction is to develop noise aware and experimentally robust versions of the symmetry, local purity, and energy components. The present concentration bounds quantify finite sample fluctuations under the assumed measurement model, but practical implementations may also be affected by state preparation errors, measurement bias, imperfect SWAP operations, inaccurate implementations of $U(g)$, and calibration drift. Future work could incorporate confidence intervals and bias aware acceptance thresholds for the estimated group averaged symmetry defect, local purity, and energy defect. For example, if certified upper bounds on systematic estimation errors are available, the corresponding promise gaps and decision thresholds can be adjusted to preserve completeness and soundness whenever the remaining effective gaps are positive.

Calibration procedures and robust estimators for imperfect group actions and SWAP measurements would therefore be particularly valuable. It would also be useful to perform a systematic analysis of sensitivity and uncertainty propagation. Such an analysis should quantify how small perturbations of the input density operator affect the three measured quantities and the resulting accept or reject decision. It should also distinguish statistical uncertainty, which can be reduced by increasing the number of samples, from systematic uncertainty, which generally requires calibration, error mitigation, or an explicit noise model. More broadly, expert judgment and uncertainty-aware decision frameworks may provide useful perspectives for selecting conservative thresholds and interpreting verification outcomes under incomplete experimental information; see, for example, [23, 24]. These connections are conceptual rather than a substitute for quantum-specific noise analysis, but they may help organize future approaches to robustness and decision making under uncertainty. Finally, additional physical assumptions may identify operationally meaningful tensor product structures within multiplicity spaces. Such assumptions could connect the present representation theoretic framework to quantum coding, many body symmetry, and nonlocality applications. The factorization of multiplicity space dimensions alone does not define a physical subsystem decomposition or a quantum error correcting code; establishing such interpretations requires further structural and experimental input. Combining these physical structures with calibrated, uncertainty aware verification procedures is therefore a promising direction for future work.

Author contributions

Xingya Fan: writing-original draft; Jiajun Yuan: reporting and verifing the results of the paper; Hao Zheng: reported and verified the results of the paper. All authors have read and agreed to the published version of the manuscript.

Use of Generative-AI tools declaration

The authors declare they have not used Artificial Intelligence (AI) tools in the creation of this article.

Acknowledgments

This project is partially supported by the Undergraduate Innovation Training Program of Xinjiang University (Grant No. XD10755042). The authors express their deep thanks to the referees for their very careful reading and useful comments which do improve the presentation of this article.

Conflict of interest

The authors declare no conflicts of interest.

References

1 S. Bravyi, M. Vyalyi, Commutative version of the local Hamiltonian problem and common eigenspace problem, *Quantum Inf. Comput.*, **5** (2005), 187–215. https://doi.org/10.26421/QIC5.3-2

2 A. Montanaro, T. Osborne, Quantum Boolean functions, *Chicago J. Theor. Comput. Sci.*, **2009** (2010), 3. https://doi.org/10.4086/cjtcs.2010.001

3 K. Bu, W. Gu, A. Jaffe, Stabilizer testing and magic entropy via quantum Fourier analysis, *Commun. Math. Phys.*, **406** (2025), 236. https://doi.org/10.1007/s00220-025-05421-3

4 T. Cusick, P. Stănică, *Cryptographic Boolean functions and applications*, Academic Press, 2017. https://doi.org/10.1016/B978-0-12-374890-4.X0001-8

5 A. Montanaro, R. de Wolf, A survey of quantum property testing, *Theory Comput.*, **7** (2016), 7. https://doi.org/10.4086/toc.gs.2016.007

6 A. Browaeys, T. Lahaye, Many-body physics with individually controlled Rydberg atoms, *Nat. Phys.*, **16** (2020), 132–142. https://doi.org/10.1038/s41567-019-0733-z

7 S. Sachdev, *Quantum phase transitions*, 2 Eds., Cambridge University Press, 2011. https://doi.org/10.1017/CBO9780511622540

8 D. Gottesman, Stabilizer codes and quantum error correction, *ArXiv*, 1997. https://doi.org/10.48550/arXiv.quant-ph/9705052

9 M. Grassl, Tomography of quantum states in small dimensions, *Electron. Notes Discrete Math.*, **20** (2005), 151–164. https://doi.org/10.1016/j.endm.2005.05.060

10 M. Cao, T. Deng, Y. Wang, Dynamical quantum state tomography with time-dependent channels, *J. Phys.*, **A57** (2024), 215301. https://doi.org/10.1088/1751-8121/ad45ce

11 A. Czerwiński, Quantum state tomography with informationally complete POVMs generated in the time domain, *Quantum Inf. Process.*, **20** (2021), 105. https://doi.org/10.1007/s11128-021-03045-9

12 H. Y. Huang, H. Kueng, J. Preskill, Predicting many properties of a quantum system from very few measurements, *Nat. Phys.*, **16** (2020), 1050–1057. https://doi.org/10.1038/s41567-020-0932-7

13 G. Hardy, E. Wright, *An introduction to the theory of numbers*, Oxford University Press, 2008. https://doi.org/10.1093/oso/9780199219858.001.0001

14 J. Bell, On the Einstein Podolsky Rosen paradox, *Phys. Phys. Fiz.*, **1** (1964), 195–200. https://doi.org/10.1103/PhysicsPhysiqueFizika.1.195

15 T. Vértesi, N. Brunner, Disproving the Peres conjecture by showing Bell nonlocality from bound entanglement, *Nat. Commun.*, **5** (2014) 5297. https://doi.org/10.1038/ncomms6297

16 B. Sagan, *The symmetric group, representations, combinatorial algorithms, and symmetric functions*, Springer-Verlag, 2001. https://doi.org/10.1007/978-1-4757-6804-6

17 E. Vinberg, *Linear representations of groups*, Springer, 2010. https://doi.org/10.1007/978-3-0348-9274-2

18 G. James, *The representation theory of the symmetric groups*, Springer, 1978. https://doi.org/10.1007/BFb0067708

19 M. Alshammari, F. Ali, Specht modules and representations of symmetric group, In: S. Ali, M. Ashraf, V. de Filippis, N. ur Rehman, *Advances in ring theory and applications*, Springer, 2024, 29–60. https://doi.org/10.1007/978-3-031-50795-3_4

20 S. Lang, *Algebra*, Springer-Verlag, 2002. https://doi.org/10.1007/978-1-4613-0041-0

21 A. Macfarlane, A. Sudbery, P. Weisz, On Gell-Mann's λ-matrices, d- and f-tensors, octets, and parametrizations of $SU(3)$, *Commun. Math. Phys.*, **11** (1968), 77–90. https://doi.org/10.1007/BF01654302

22 W. Hoeffding, Probability inequalities for sums of bounded random variables, *J. Amer. Stat. Assoc.*, **58** (1963), 13–30. https://doi.org/10.1080/01621459.1963.10500830

23 H. Li, M. Yazdi, Stochastic game theory approach to solve system safety and reliability decision-making problem under uncertainty, In: H. Li, M. Yazdi, *Advanced decision-making methods and applications in system safety and reliability problems*, Springer, 2022, 127–151. https://doi.org/10.1007/978-3-031-07430-1_8

24 E. Zarei, M. Yazdi , R. Moradi, A. Bahootoroody, Expert judgment and uncertainty in sociotechnical systems analysis, In: E. Zarei, *Safety causation analysis in sociotechnical systems: advanced models and techniques*, Springer, 2024. https://doi.org/10.1007/978-3-031-62470-4