Distinguishability of locally diagonal orthogonally invariant quantum states

Nathaniel Johnston* and Vincent Russo†

April 14, 2026

Abstract

We study the distinguishability of quantum states under local operations with classical communication (LOCC), separable, and positive-partial-transpose (PPT) measurements, focusing on *locally diagonal orthogonally invariant* (LDOI) states—those invariant under local diagonal orthogonal twirling. This class includes many important families such as Werner states, isotropic states, X-states, and Dicke states. We show that optimal PPT and separable measurements for distinguishing LDOI states can always be taken to be LDOI, and the LOCC supremum can be approached by LDOI LOCC POVMs, enabling a dimensional reduction from n^4 to $O(n^2)$ in the associated optimization problems. We establish efficiently computable bounds on the distinguishability of orthonormal LDOI bases and prove that for a broad class of such bases—including all two-qubit cases—the LOCC supremum equals the PPT and separable optima. More generally, we show the gap between PPT and LOCC distinguishability is at most $(n-2)/(2n^2)$ for local dimension n.

1 Introduction

Quantum state distinguishability is a fundamental problem in quantum information theory [Ban11, BDF+99, GKR+02, HSSH03, VSPM01, WH02, WSHV00]: given an ensemble of quantum states $\{(p_i, \rho_i)\}$, what is the maximum probability of correctly identifying which state was selected? The answer depends critically on what class of measurements is allowed. Global measurements can always achieve the optimal success probability given by the Holevo-Helstrom bound [Hol73, Hel69], but in many scenarios—particularly in distributed quantum information processing—the parties performing the measurement may be restricted to *local operations with classical communication* (LOCC) [CLM+14], *separable measurements* [DFXY09, BCJ+15], or *positive-partial-transpose* (PPT) measurements [Cos13, YDY14]. These measurement classes form a hierarchy LOCC $\subseteq$ SEP $\subseteq$ PPT $\subseteq$ Global, where each inclusion can be strict.

Determining the optimal distinguishability under these restricted measurement classes is generally a difficult problem. While semidefinite programming provides exact characterizations for both global and PPT distinguishability [Cos13, BCJ+15], and hierarchies of SDPs can approximate separable distinguishability [BCJ+15], the resulting optimization problems can be computationally intensive, and exact formulas are known only for specific families of states [BCJ+15, YDY12].

*Department of Mathematics & Computer Science, Mount Allison University. njohnston@mta.ca

†Unitary Foundation. vincentrusso1@gmail.com

Understanding when these different measurement classes achieve the same optimal value, and quantifying the gaps between them, remains an active area of research.

In this work, we focus on the class of *locally diagonal orthogonally invariant* (LDOI) states—those that are invariant under the local diagonal orthogonal twirl map [CK06, JM19, NS21, SN21]. This class encompasses many important families of quantum states including Werner states [Wer89], isotropic states [HH99], X-states [QAQJ12], mixtures of Dicke states [Yu16, TAQ+18], and various entanglement witnesses such as the Choi witness [HK11]. Our first main result shows that for any ensemble of LDOI states, optimal PPT and separable measurements can always be taken to be LDOI, and the LOCC supremum can be approached by LDOI measurements (Theorem 9), enabling a significant dimensional reduction in the associated optimization problems.

The technique of twirling to project onto an invariant subspace is well-established in quantum information theory—it is used, for example, in the study of Werner and isotropic state entanglement [Wer89, HH99]. Our contribution is in identifying that the LDOI class is simultaneously broad enough to capture many important families of states and structured enough for the resulting optimization problems to remain tractable.

We establish efficiently computable upper and lower bounds on the success probability of distinguishing orthonormal LDOI bases. We focus on uniform ensembles over orthonormal bases because basis discrimination with a uniform prior is a fundamental primitive in quantum information: it arises naturally in superdense coding [BW92], random access codes [ANTSV99], and entanglement-assisted communication [BDF+99], and every orthonormal basis composed of LDOI states—Bell bases, generalized Bell bases, and Dicke-type bases—falls within this framework. These bases can be parameterized by a pair of matrices (U, A) where U is unitary and A satisfies certain orthogonality constraints (Definition 6). Our lower bound for LOCC measurements can be computed in polynomial time via the Hungarian algorithm for the Assignment Problem [Kuh55], while our upper bound for PPT measurements requires solving a semidefinite program that is significantly smaller than the general PPT distinguishability SDP—exploiting the block structure of LDOI states to reduce the search space from dimension n^4 to $3n^2$.

For a broad class of LDOI bases—including all two-qubit LDOI bases—our upper and lower bounds coincide, yielding an exact closed-form formula showing that $\text{opt}_{\text{LOCC}} = \text{opt}_{\text{SEP}} = \text{opt}_{\text{PPT}}$ (Corollaries 11 and 12). This generalizes previous results on parametrized Bell states [BN13, BCJ+15] to the entire class of orthonormal LDOI bases in dimension two. More generally, we prove that the gap between PPT and LOCC distinguishability for any LDOI basis is at most $(n-2)/(2n^2)$, which vanishes as the dimension grows and achieves its maximum value of $1/16$ when $n = 4$ (Corollary 16). The LOCC lower bound evaluates to exactly $1/2 - (n-2)/(2n^2)$ for the Fourier basis.

The remainder of this paper is organized as follows. After establishing notation and preliminaries, Section 2 introduces LDOI states and bases and establishes their block structure. Section 3 proves our main distinguishability bounds. Section 4 concludes with a discussion of open problems and future directions.

Preliminaries

We assume the reader is familiar with the notions of quantum information as contained in [NC02] and [Wil13]. We will make use of the notation and terminology found in [Wat18]. Let $\mathcal{X} = \mathbb{C}^n$ denote a finite-dimensional complex Euclidean space with a fixed standard basis $\{|1\rangle, \ldots, |n\rangle\}$ for some positive integer n. We use sets $\text{L}(\mathcal{X})$, $\text{Pos}(\mathcal{X})$, $\text{Herm}(\mathcal{X})$, $\text{D}(\mathcal{X})$, and $\text{U}(\mathcal{X})$ to represent the set of linear operators, positive semidefinite operators, Hermitian operators, density operators, and unitary operators acting on the space $\mathcal{X}$. For a vector $|\phi\rangle$ we adopt the convention of representing the corresponding density operator as $\phi = |\phi\rangle\langle\phi|$. We denote the transpose mapping $T : \text{L}(\mathcal{X}) \rightarrow$

$\mathrm{L}(\mathcal{X})$ as the positive mapping defined as $T(X) = X^{\mathsf{T}}$ for all $X \in \mathrm{L}(\mathcal{X})$. The partial transpose is a mapping on $\mathcal{X} \otimes \mathcal{Y}$ defined as

$$\mathrm{T}_{\mathcal{X}} = T \otimes \mathbb{1}_{\mathcal{Y}}. \tag{1}$$

We write $\mathbb{1}_n$ for the $n \times n$ identity matrix and $\mathbf{1}_n$ for the $n \times n$ all-ones matrix (whose entries are all equal to 1). We denote by S_n the symmetric group on $\{1, \ldots, n\}$, i.e., the set of all permutations of n elements.

Quantum state distinguishability

We now formalize the state discrimination problem introduced above. We consider bipartite quantum states shared between two parties, Alice and Bob, each holding a subsystem. An *ensemble* is a collection of pairs

$$\mathcal{E} = \{(p_1, \rho_1), \ldots, (p_N, \rho_N)\}, \tag{2}$$

where each $\rho_i \in \mathrm{D}(\mathcal{X} \otimes \mathcal{Y})$ is a density operator representing a quantum state shared between Alice and Bob, and $p_i > 0$ is the prior probability with which ρ_i is selected, satisfying $\sum_{i=1}^{N} p_i = 1$. In the state discrimination task, a random index $k \in \{1, \ldots, N\}$ is selected according to the distribution $\{p_i\}$, Alice and Bob are provided with the state ρ_k, and their goal is to determine k by performing a measurement on their respective portions of the shared state. In most of this paper, the ensemble states are pure states $\rho_k = |\phi_k\rangle\langle\phi_k|$ for unit vectors $|\phi_k\rangle \in \mathcal{X} \otimes \mathcal{Y}$, though the definitions and Theorem 9 apply to mixed-state ensembles as well.

The optimal success probability depends critically on what class of measurements is permitted. If Alice and Bob can perform arbitrary joint (global) measurements, the maximum success probability is given by the Holevo-Helstrom theorem. However, in many practical scenarios—particularly in distributed quantum information processing—Alice and Bob are spatially separated and can only perform *local operations with classical communication* (LOCC) [CLM+14]. This restriction can strictly reduce the distinguishability of certain ensembles. Two natural relaxations of LOCC measurements are *separable measurements* (SEP) [DFXY09, BN13, BCJ+15], whose POVM elements lie in the cone of separable operators (finite sums of positive product operators), and *positive-partial-transpose measurements* (PPT) [Cos13, CR14, YDY14, BCJ+15], which require that the measurement operators remain positive under partial transpose. These classes form a strict hierarchy

$$\text{LOCC} \subseteq \text{SEP} \subseteq \text{PPT} \subseteq \text{Global}. \tag{3}$$

Computing the LOCC supremum is generally intractable, as LOCC protocols can involve arbitrary rounds of classical communication. Separable measurements are characterized by a difficult convex optimization problem. However, PPT measurements admit a tractable semidefinite programming characterization, which we now describe.

For an ensemble $\mathcal{E} = \{(p_i, \rho_i)\}_{i=1}^{N}$, the optimal success probability under PPT measurements can be characterized via semidefinite programming [Cos13, BCJ+15]. A measurement is described by a positive operator-valued measure (POVM) $\{P_k\}$, where P_k represents the measurement operator associated with outcome k. The success probability is $\sum_{k=1}^{N} p_k \langle P_k, \rho_k\rangle$. For PPT measurements, we require each P_k and its partial transpose $\mathrm{T}_{\mathcal{X}}(P_k)$ to be positive semidefinite. The primal and dual semidefinite programs characterizing $\mathrm{opt}_{\mathrm{PPT}}(\mathcal{E})$ are

$$\underline{\text{Primal problem}}$$

$$\begin{aligned}
\text{maximize:} \quad & \sum_{k=1}^{N} p_k \langle P_k, \rho_k \rangle \\
\text{subject to:} \quad & \sum_{k=1}^{N} P_k = \mathbb{1}_{\mathcal{X}\otimes\mathcal{Y}}, \\
& P_1, \ldots, P_N \in \operatorname{Pos}(\mathcal{X}\otimes\mathcal{Y}), \\
& \mathrm{T}_{\mathcal{X}}(P_1), \ldots, \mathrm{T}_{\mathcal{X}}(P_N) \in \operatorname{Pos}(\mathcal{X}\otimes\mathcal{Y}).
\end{aligned} \tag{4}$$

$$\underline{\text{Dual problem}}$$

$$\begin{aligned}
\text{minimize:} \quad & \operatorname{Tr}(H) \\
\text{subject to:} \quad & H - p_k\rho_k - \mathrm{T}_{\mathcal{X}}(Q_k) \in \operatorname{Pos}(\mathcal{X}\otimes\mathcal{Y}), \quad k = 1, \ldots, N, \\
& H \in \operatorname{Herm}(\mathcal{X}\otimes\mathcal{Y}), \\
& Q_1, \ldots, Q_N \in \operatorname{Pos}(\mathcal{X}\otimes\mathcal{Y}).
\end{aligned} \tag{5}$$

Setting $Q_k = 0$ in Equation (5) and taking the partial transpose (which preserves feasibility because $\mathrm{T}_{\mathcal{X}}$ is self-adjoint) yields the simplified dual

$$\underline{\text{Dual problem (upper bound)}}$$

$$\begin{aligned}
\text{minimize:} \quad & \operatorname{Tr}(H) \\
\text{subject to:} \quad & H - p_k\,\mathrm{T}_{\mathcal{X}}(\rho_k) \in \operatorname{Pos}(\mathcal{X}\otimes\mathcal{Y}), \quad k = 1, \ldots, N, \\
& H \in \operatorname{Herm}(\mathcal{X}\otimes\mathcal{Y}).
\end{aligned} \tag{6}$$

The primal problem directly optimizes over PPT measurements, while the dual provides a certificate for upper bounds on the optimal value. The constrained dual in Equation (6) therefore follows from fixing $Q_k = 0$ and using the self-adjointness of the partial transpose, yielding a simpler optimization problem at the cost of producing only an upper bound. If we define α, β, and β' to represent the optimal values of the primal (Equation (4)), the dual (Equation (5)), and the constrained dual (Equation (6)), respectively, then by weak duality we have $\alpha \leq \beta \leq \beta'$. When the primal and dual achieve the same optimal value ($\alpha = \beta$), strong duality holds and the optimal PPT distinguishability is exactly determined.

Throughout this paper, we denote ensembles of quantum states explicitly as $\mathcal{E} = \{(p_i, \rho_i)\}_{i=1}^{N}$ where p_i are the prior probabilities and ρ_i are the density matrices. For an orthonormal basis $\eta = \{|\phi_1\rangle, \ldots, |\phi_N\rangle\}$, we write $\mathcal{E} = \{(1/N, |\phi_i\rangle\langle\phi_i|)\}_{i=1}^{N}$ to denote the ensemble with uniform prior distribution. We use the notation $\operatorname{opt}_{\mathrm{PPT}}(\mathcal{E})$ and $\operatorname{opt}_{\mathrm{SEP}}(\mathcal{E})$ for the optimal success probabilities under PPT and separable measurements, and $\operatorname{opt}_{\mathrm{LOCC}}(\mathcal{E})$ for the supremum over LOCC measurements (since LOCC is not topologically closed, the supremum may not be attained).

2 Locally diagonal orthogonally invariant states and bases

Let $n \geq 2$ be an integer (the case $n = 1$ is trivial) and let $\mathcal{X} = \mathcal{Y} = \mathbb{C}^n$ be complex Euclidean spaces. Let $\mathrm{DO}(\mathcal{X})$ denote the set of diagonal matrices with diagonal entries equal to ± 1 acting on $\mathcal{X}$. (These are sometimes called diagonal sign matrices or diagonal orthogonal matrices, as each element $O \in \mathrm{DO}(\mathcal{X})$ satisfies $O^2 = \mathbb{1}$ and $O = O^*$.) Consider the *local diagonal orthogonal twirl* map $\Phi_{\mathrm{O}} : \mathrm{L}(\mathcal{X}\otimes\mathcal{Y}) \to \mathrm{L}(\mathcal{X}\otimes\mathcal{Y})$ defined by

$$\Phi_{\mathrm{O}}(A) \triangleq \frac{1}{2^n} \sum_{O \in \mathrm{DO}(\mathcal{X})} (O \otimes O) A (O \otimes O). \tag{7}$$

Since $|\mathrm{DO}(\mathcal{X})| = 2^n$, this map can be thought of as an average of A over symmetric local diagonal orthogonal conjugations. We begin with a few notes about Φ_{O}, all of which are straightforward to verify. Here $\mathrm{PPT}(\mathcal{X} : \mathcal{Y})$ denotes the cone of operators whose partial transpose on $\mathcal{X}$ is positive semidefinite, and $\mathrm{SEP}(\mathcal{X} : \mathcal{Y})$ denotes the cone of separable (convex combinations of product) operators on $\mathcal{X} \otimes \mathcal{Y}$.

- Φ_{O} is a quantum channel (i.e., completely positive and trace-preserving).
- Φ_{O} is self-dual (with respect to the usual trace inner product): $\Phi_{\mathrm{O}}^* = \Phi_{\mathrm{O}}$.
- If $A \in \mathrm{PPT}(\mathcal{X} : \mathcal{Y})$ then $\Phi_{\mathrm{O}}(A) \in \mathrm{PPT}(\mathcal{X} : \mathcal{Y})$.
- If $A \in \mathrm{SEP}(\mathcal{X} : \mathcal{Y})$ then $\Phi_{\mathrm{O}}(A) \in \mathrm{SEP}(\mathcal{X} : \mathcal{Y})$.

The twirl map Φ_{O} has a simple form in terms of the computational basis (see [JM19, SN21], for example): if the entry of $A \in \mathrm{L}(\mathcal{X} \otimes \mathcal{Y})$ corresponding to the basis matrix $|i\rangle\langle j| \otimes |k\rangle\langle \ell|$ is denoted by $a_{i,j;k,\ell}$ then

$$\Phi_{\mathrm{O}}(A) = \sum_{i,j=1}^{n} a_{i,i;j,j} |i\rangle\langle i| \otimes |j\rangle\langle j| + \sum_{\substack{i,j=1 \\ i\neq j}}^{n} a_{i,j;i,j} |i\rangle\langle j| \otimes |i\rangle\langle j| + \sum_{\substack{i,j=1 \\ i\neq j}}^{n} a_{i,j;j,i} |i\rangle\langle j| \otimes |j\rangle\langle i|. \tag{8}$$

We refer to Φ_{O} as the *local diagonal orthogonal twirl* (LDOT) map; it is the orthogonal projection onto the set of matrices whose only non-zero entries are located in the $|i\rangle\langle i| \otimes |j\rangle\langle j|$, $|i\rangle\langle j| \otimes |i\rangle\langle j|$, or $|i\rangle\langle j| \otimes |j\rangle\langle i|$ positions for some $1 \leq i, j \leq n$.

A matrix $A \in \mathrm{L}(\mathcal{X} \otimes \mathcal{Y})$ is called *locally diagonal orthogonally invariant (LDOI)* if $\Phi_{\mathrm{O}}(A) = A$. Many important families of quantum states and operators studied in quantum information theory are LDOI, including Werner states, isotropic states, X-states, mixtures of Dicke states, and various entanglement witnesses [Wer89, HH99, QAQJ12, Yu16, TAQ+18, HK11]. Detailed examples of these families are provided in Section 2.3.

To illustrate the block structure of LDOI matrices, consider first the case $n = 2$. The two-qubit LDOI states, known as X-states [QAQJ12], have matrix representation of the form

$$\rho = \begin{bmatrix} * & \cdot & \cdot & * \\ \cdot & * & * & \cdot \\ \cdot & * & * & \cdot \\ * & \cdot & \cdot & * \end{bmatrix} \in \mathrm{D}(\mathcal{X} \otimes \mathcal{Y}), \tag{9}$$

where dots denote entries equal to 0 and asterisks ($*$) denote potentially non-zero entries.

In all dimensions, LDOI states have a very simple block matrix structure much like that of the X-states: we can write them as a direct sum of a $n \times n$ matrix and $n(n-1)/2$ different 2×2 matrices as follows:

$$\begin{aligned} \rho = &\left(\sum_{i,j=1}^{n} \rho_{i,j;i,j} |i\rangle\langle j| \otimes |i\rangle\langle j| \right) \\ &+ \sum_{\substack{i,j=1 \\ i>j}}^{n} \big(\rho_{i,i;j,j} |i\rangle\langle i| \otimes |j\rangle\langle j| + \rho_{i,j;j,i} |i\rangle\langle j| \otimes |j\rangle\langle i| + \rho_{j,i;i,j} |j\rangle\langle i| \otimes |i\rangle\langle j| + \rho_{j,j;i,i} |j\rangle\langle j| \otimes |i\rangle\langle i| \big). \end{aligned} \tag{10}$$

For example, if $n = 3$ then the LDOI states $\rho \in \mathrm{D}(\mathcal{X} \otimes \mathcal{Y})$ are the ones with a matrix representation of the form

$$\rho = \left[\begin{array}{ccc|ccc|ccc}
* & \cdot & \cdot & \cdot & * & \cdot & \cdot & \cdot & * \\
\cdot & * & \cdot & * & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & * & \cdot & \cdot & \cdot & * & \cdot & \cdot \\
\hline
\cdot & * & \cdot & * & \cdot & \cdot & \cdot & \cdot & \cdot \\
* & \cdot & \cdot & \cdot & * & \cdot & \cdot & \cdot & * \\
\cdot & \cdot & \cdot & \cdot & \cdot & * & \cdot & * & \cdot \\
\hline
\cdot & \cdot & * & \cdot & \cdot & \cdot & * & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & * & \cdot & * & \cdot \\
* & \cdot & \cdot & \cdot & * & \cdot & \cdot & \cdot & *
\end{array}\right], \tag{11}$$

where we can see that such a ρ is a direct sum of the 3×3 submatrix defined by rows 1, 5, and 9, as well as the 2×2 submatrices defined by rows 2 and 4, 3 and 7, and 6 and 8.

2.1 Structure and parameterization of LDOI matrices

The block structure exhibited above has a remarkably simple algebraic characterization: every LDOI matrix can be uniquely parameterized by a triple of $n \times n$ matrices sharing a common diagonal. This result, established in [SN21], significantly reduces the complexity of working with LDOI matrices and provides both theoretical and computational advantages.

Proposition 1 ([SN21])**.** *The space of LDOI matrices is in bijection with triples (A, B, C) of $n \times n$ complex matrices satisfying $diag(A) = diag(B) = diag(C)$, where $diag(M)$ denotes the vector of diagonal entries of M. Specifically, an LDOI matrix $X \in \mathrm{L}(\mathcal{X} \otimes \mathcal{Y})$ corresponds to the triple (A, B, C) via*

$$X = \sum_{i,j=1}^{n} a_{ij} |i\rangle\langle i| \otimes |j\rangle\langle j| + \sum_{\substack{i,j=1 \\ i \neq j}}^{n} b_{ij} |i\rangle\langle j| \otimes |i\rangle\langle j| + \sum_{\substack{i,j=1 \\ i \neq j}}^{n} c_{ij} |i\rangle\langle j| \otimes |j\rangle\langle i|. \tag{12}$$

This parameterization reveals that the LDOI subspace has dimension $3n^2 - 2n$ over the reals (for Hermitian matrices), compared to dimension n^4 for general $n \times n$ bipartite matrices. The shared diagonal constraint $\mathrm{diag}(A) = \mathrm{diag}(B) = \mathrm{diag}(C)$ ensures that the coefficients of each $|i\rangle\langle i| \otimes |j\rangle\langle j|$ basis element are consistent across the triple.

The connection between the triple parameterization and the block structure described earlier is now transparent: the matrix A encodes the $n \times n$ "diagonal block" (entries of the form $|i\rangle\langle i| \otimes |j\rangle\langle j|$), while B and C encode the $n(n-1)/2$ distinct off-diagonal blocks. For each pair $i < j$, the 4×4 block on the subspace spanned by $\{|ii\rangle, |ij\rangle, |ji\rangle, |jj\rangle\}$ decomposes as the direct sum

$$\begin{bmatrix} a_{ii} & b_{ij} \\ b_{ji} & a_{jj} \end{bmatrix} \oplus \begin{bmatrix} a_{ij} & c_{ij} \\ c_{ji} & a_{ji} \end{bmatrix}. \tag{13}$$

This structure has important implications for quantum information-theoretic properties. The positivity of an LDOI density matrix ρ corresponding to (A, B, C) can be characterized through its block-diagonal structure [SN21]: (i) the $n \times n$ matrix B restricted to the diagonal subspace $\{|ii\rangle\}$ must be positive semidefinite, i.e., $B \succeq 0$; and (ii) for each $i < j$, the 2×2 block $\left(\begin{smallmatrix} a_{ij} & c_{ij} \\ c_{ji} & a_{ji} \end{smallmatrix}\right)$ must be positive semidefinite, which requires $a_{ij}, a_{ji} \geq 0$ and $a_{ij}a_{ji} \geq |c_{ij}|^2$. The condition $a_{ii}a_{jj} \geq |b_{ij}|^2$ for $i \neq j$ follows from $B \succeq 0$. These block-wise constraints are far simpler to verify than checking positive semidefiniteness of the full $n^2 \times n^2$ matrix.

Because of this block structure, the only pure states $\rho = |\phi\rangle\langle\phi|$ that are LDOI are those of the form

$$\begin{aligned} |\phi\rangle &= \sum_{k=1}^{n} \gamma_k |k\rangle \otimes |k\rangle \quad \text{or} \\ |\phi\rangle &= \alpha|i\rangle \otimes |j\rangle + \beta|j\rangle \otimes |i\rangle \quad \text{for some} \quad 1 \le i \ne j \le n. \end{aligned} \tag{14}$$

2.2 Properties of the LDOI subspace

The set of LDOI matrices enjoys several important structural properties that make it amenable to both theoretical analysis and numerical computation. We summarize the key facts:

- **Vector subspace:** The set of LDOI matrices forms a linear subspace of $\mathrm{L}(\mathcal{X} \otimes \mathcal{Y})$. This follows immediately from the linearity of the LDOT map: if $\Phi_{\mathrm{O}}(A) = A$ and $\Phi_{\mathrm{O}}(B) = B$, then $\Phi_{\mathrm{O}}(\alpha A + \beta B) = \alpha A + \beta B$ for any scalars $\alpha, \beta \in \mathbb{C}$.

- **Orthogonal projection:** The LDOT map Φ_{O} is the orthogonal projection onto the LDOI subspace with respect to the Hilbert-Schmidt inner product $\langle A, B\rangle = \mathrm{Tr}(A^* B)$. This follows from the fact that Φ_{O} is self-adjoint ($\Phi_{\mathrm{O}}^* = \Phi_{\mathrm{O}}$) and idempotent ($\Phi_{\mathrm{O}}^2 = \Phi_{\mathrm{O}}$).

- **Preservation under quantum channels:** If ρ is an LDOI state and Λ is a quantum channel that commutes with the LDOT map (i.e., $\Lambda \circ \Phi_{\mathrm{O}} = \Phi_{\mathrm{O}} \circ \Lambda$), then $\Lambda(\rho)$ is also LDOI. Important examples include local depolarizing channels and certain entanglement-breaking channels.

- **Dimension reduction:** As established in Proposition 1, the LDOI subspace has dimension $3n^2 - 2n$ over $\mathbb{R}$ (for Hermitian matrices), compared to dimension n^4 for the full space $\mathrm{Herm}(\mathcal{X} \otimes \mathcal{Y})$. This dramatic reduction—from quartic to quadratic in n—is the key to computational tractability.

These properties have important consequences for quantum state distinguishability. The preservation of LDOI structure under PPT, separable, and LOCC measurements (as we will show in Section 3) means that when distinguishing LDOI states, we can restrict our search for optimal measurements to the LDOI subspace. Combined with the dimension reduction, this leads to semidefinite programs with $O(n^2)$ variables rather than $O(n^4)$, making exact computation feasible even for moderately large dimensions.

2.3 Examples of LDOI states

We now present several important families of LDOI states, showing their explicit structure via the triple parameterization. These examples illustrate the diversity of LDOI states and their relevance to quantum information theory. Additional examples of LDOI states can also be found in [SN21].

Example 2 (Werner states)**.** The Werner states [Wer89] are a one-parameter family of states on $\mathbb{C}^n \otimes \mathbb{C}^n$ defined by

$$\rho_{\mathrm{W}}(p) = p\frac{\mathbb{1}_{n^2} + F}{n(n+1)} + (1-p)\frac{\mathbb{1}_{n^2} - F}{n(n-1)}, \tag{15}$$

where $F = \sum_{i,j=1}^{n} |ij\rangle\langle ji|$ is the swap operator and $p \in [0, 1]$. These states are invariant under all symmetric local unitaries $U \otimes U$, which implies they are LDOI. In the triple parameterization, the

Werner state $\rho_W(p)$ corresponds to

$$a_{ij} = \alpha + \beta\delta_{i,j}, \qquad b_{ij} = \begin{cases} \alpha+\beta & \text{if } i = j, \\ 0 & \text{if } i \neq j, \end{cases} \qquad c_{ij} = \begin{cases} \alpha+\beta & \text{if } i = j, \\ \beta & \text{if } i \neq j, \end{cases} \tag{16}$$

where $\alpha = \frac{p}{n(n+1)} + \frac{1-p}{n(n-1)}$ and $\beta = \frac{p}{n(n+1)} - \frac{1-p}{n(n-1)}$. Equivalently, $A = \alpha\mathbf{1}_n + \beta\mathbb{1}_n$, $B = (\alpha+\beta)\mathbb{1}_n$, and $C = \beta\mathbf{1}_n + \alpha\mathbb{1}_n$. Werner states are PPT if and only if $p \geq 1/2$, since the partially transposed state has eigenvalues α (multiplicity n^2-1) and $(2p-1)/n$. Due to their symmetry, Werner states are separable if and only if they are PPT, so Werner states with $p \geq 1/2$ are separable. This makes them a convenient test family for our bounds. The matrices A, B, and C are real symmetric, and $\rho_W(p)$ is a normalized Hermitian density operator for every real $p \in [0,1]$.

We note that Werner states possess the full $U \otimes U$ symmetry, which is strictly finer than the local diagonal orthogonal symmetry exploited here. The $U \otimes U$-invariant subspace is only 2-dimensional (spanned by the identity and the swap), whereas the LDOI subspace has dimension $3n^2 - 2n$. When our LDOI framework is applied to Werner states, the resulting bounds from the upcoming Theorem 10 are consistent with known optimal discrimination results, but may not be as tight as those obtainable from the full $U \otimes U$ reduction. This is the natural trade-off: the LDOI framework applies uniformly to a much broader class of states, at the cost of not fully exploiting the additional symmetry present in specific subfamilies.

Example 3 (X-states)**.** As noted earlier, X-states [QAQJ12] are precisely the LDOI states when $n = 2$. With entries labeled as

$$\rho = \begin{bmatrix} \rho_{11} & 0 & 0 & \rho_{14} \\ 0 & \rho_{22} & \rho_{23} & 0 \\ 0 & \rho_{32} & \rho_{33} & 0 \\ \rho_{41} & 0 & 0 & \rho_{44} \end{bmatrix} \in \mathrm{D}(\mathbb{C}^4), \tag{17}$$

the triple parameterization obtained from Equation (12) is

$$A = \begin{bmatrix} \rho_{11} & \rho_{22} \\ \rho_{33} & \rho_{44} \end{bmatrix}, \quad B = \begin{bmatrix} \rho_{11} & \rho_{14} \\ \rho_{41} & \rho_{44} \end{bmatrix}, \quad C = \begin{bmatrix} \rho_{11} & \rho_{23} \\ \rho_{32} & \rho_{44} \end{bmatrix}. \tag{18}$$

Many important two-qubit states are X-states, including Bell-diagonal states (when $\rho_{22} = \rho_{33}$ and $\rho_{23} = \rho_{32}$) and various mixed states arising in quantum communication protocols. The entries ρ_{ij} may be complex, although density-operator normalization enforces $\sum_i \rho_{ii} = 1$ and positivity requires the matrix to be Hermitian.

Example 4 (Maximally entangled state)**.** The standard maximally entangled state $|\phi^+\rangle = \frac{1}{\sqrt{n}}\sum_{i=1}^{n}|ii\rangle$ has density matrix $\phi^+ = |\phi^+\rangle\langle\phi^+| = \frac{1}{n}\sum_{i,j=1}^{n}|i\rangle\langle j| \otimes |i\rangle\langle j|$, which is LDOI. Its triple parameterization is

$$A = \frac{1}{n}\mathbb{1}_n, \quad B = \frac{1}{n}\mathbf{1}_n, \quad C = \frac{1}{n}\mathbb{1}_n, \tag{19}$$

where $\mathbb{1}_n$ is the $n \times n$ identity matrix and $\mathbf{1}_n$ is the all-ones matrix. To verify: the A matrix encodes coefficients of $|i\rangle\langle i| \otimes |j\rangle\langle j|$, which only appear when $i = j$ in ϕ^+ (giving $a_{ii} = 1/n$, $a_{ij} = 0$ for $i \neq j$). The B matrix encodes coefficients of $|i\rangle\langle j| \otimes |i\rangle\langle j|$ for $i \neq j$, all of which equal $1/n$. The C matrix encodes coefficients of $|i\rangle\langle j| \otimes |j\rangle\langle i|$ for $i \neq j$, none of which appear in ϕ^+ (giving $c_{ij} = 0$ for $i \neq j$). This state is maximally entangled and hence not separable, but it can be perfectly distinguished from any orthogonal state by a global measurement.

Example 5 (Product states)**.** Any product state $\rho = \rho_A \otimes \rho_B$ where both ρ_A and ρ_B are diagonal in the computational basis is LDOI. For instance, the product basis states $|ij\rangle$ for $1 \le i, j \le n$ are LDOI. The state $|ij\rangle\langle ij|$ has triple parameterization

$$A_{k\ell} = \begin{cases} 1 & \text{if } k = i, \ell = j, \\ 0 & \text{otherwise,} \end{cases} \qquad B_{k\ell} = C_{k\ell} = \begin{cases} a_{kk} & \text{if } k = \ell, \\ 0 & \text{otherwise,} \end{cases} \tag{20}$$

so that B and C are diagonal matrices satisfying the constraint $\operatorname{diag}(A) = \operatorname{diag}(B) = \operatorname{diag}(C)$. Product bases are perfectly distinguishable by local measurements, demonstrating that not all LDOI bases exhibit nonlocal distinguishability phenomena. The matrices appearing in this example are real, and the basis vectors $|ij\rangle$ are normalized product states.

These examples demonstrate the breadth of LDOI states: from maximally entangled (Example 4) to separable (Example 5), and from well-studied families with known separability criteria (Example 2) to general parametric classes (Example 3). In the context of state distinguishability, LDOI states are particularly amenable to analysis due to their reduced parameter space and tractable SDP characterizations.

2.4 Orthonormal LDOI bases

We now characterize which orthonormal bases of $\mathcal{X} \otimes \mathcal{Y}$ consist entirely of LDOI pure states. As the preceding discussion shows, such bases must contain exactly n states supported on the diagonal subspace (of the form $\sum_k \gamma_k |kk\rangle$) and $n(n-1)$ Schmidt-rank-2 states (of the form $\alpha|ij\rangle + \beta|ji\rangle$). The diagonal states are maximally entangled only when all $|\gamma_k| = 1/\sqrt{n}$; in general they have Schmidt rank at most n. The following definition makes this structure precise.

Definition 6. Let $n \ge 2$ be an integer, let $\mathcal{X} = \mathcal{Y} = \mathbb{C}^n$ be complex Euclidean spaces. We say that a set $\eta \subset \mathcal{X} \otimes \mathcal{Y}$ is an *orthonormal LDOI basis* of $\mathcal{X} \otimes \mathcal{Y}$ if there exist $U \in \mathrm{U}(\mathcal{X})$ and $A \in \mathrm{L}(\mathcal{X})$ with $|a_{i,j}|^2 + |a_{j,i}|^2 = 1$ for all $1 \le i \ne j \le n$, such that $\eta = \{|\phi_{i,j}\rangle : 1 \le i, j \le n\}$, where

$$\begin{aligned} |\phi_{i,i}\rangle &= \sum_{k=1}^{n} u_{i,k} |k\rangle \otimes |k\rangle \quad \text{for all} \quad 1 \le i \le n, \\ |\phi_{i,j}\rangle &= a_{i,j} |i\rangle \otimes |j\rangle + \overline{a_{j,i}} |j\rangle \otimes |i\rangle \quad \text{for all} \quad 1 \le i < j \le n, \quad \text{and} \\ |\phi_{j,i}\rangle &= a_{j,i} |i\rangle \otimes |j\rangle - \overline{a_{i,j}} |j\rangle \otimes |i\rangle \quad \text{for all} \quad 1 \le i < j \le n. \end{aligned} \tag{21}$$

Indeed, in the above definition each $|\phi_{k,k}\rangle$ is immediately orthogonal to each $|\phi_{i,j}\rangle$ when $i \ne j$ since they have disjoint supports, unitarity of U is equivalent to the fact that the $|\phi_{k,k}\rangle$'s have unit length and are orthogonal to each other, and the constraint $|a_{i,j}|^2 + |a_{j,i}|^2 = 1$ is equivalent to the fact that each $|\phi_{i,j}\rangle$ has unit length when $i \ne j$. Note that the diagonal entries of the matrix A are unconstrained and do not appear in the parameterization of η, as they play no role in defining the basis states. An orthonormal LDOI basis of $\mathcal{X} \otimes \mathcal{Y}$ contains exactly n^2 vectors, so in the terminology of the preliminaries we have $N = n^2$ measurement operators when distinguishing such bases.

Remark 7 (Orthonormal CLDUI bases)**.** Numerous variants of Definition 6 are possible, since numerous variants of LDOI states are possible. For example, if we instead considered matrices that are *conjugate locally diagonal unitarily invariant (CLDUI)* throughout this work (as in [JM19]), then we could analogously define *orthonormal CLDUI bases* of $\mathcal{X} \otimes \mathcal{Y}$ to be just as in Definition 6, but with A upper triangular (so that each $|\phi_{i,j}\rangle$ is a pure product state).

Our reason for working with LDOI states (and the LDOI twirl, and orthonormal LDOI bases) in this work is that it is the largest family of states we are aware of that arises in a natural way from a local twirl, so we get more general results this way. All of our results concerning distinguishability of orthonormal LDOI bases apply automatically to orthonormal CLDUI bases, for example, since CLDUI states are LDOI.

Example 8. When $\mathcal{X} = \mathcal{Y} = \mathbb{C}^2$, the Bell basis consists of the states

$$\begin{aligned} |\phi_{1,1}\rangle &= \frac{1}{\sqrt{2}}(|11\rangle + |22\rangle), \quad |\phi_{1,2}\rangle = \frac{1}{\sqrt{2}}(|12\rangle + |21\rangle), \\ |\phi_{2,1}\rangle &= \frac{1}{\sqrt{2}}(|12\rangle - |21\rangle), \quad |\phi_{2,2}\rangle = \frac{1}{\sqrt{2}}(|11\rangle - |22\rangle). \end{aligned} \tag{22}$$

The Bell basis is an orthonormal LDOI basis in the sense of Definition 6 with

$$A = U = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}. \tag{23}$$

At the other extreme, the product basis $\{|11\rangle, |12\rangle, |21\rangle, |22\rangle\}$ is also an orthonormal LDOI basis, with

$$A = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \quad \text{and} \quad U = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}. \tag{24}$$

In both of these examples, A is non-unique since its diagonal entries are irrelevant.

3 Distinguishability of LDOI states

We begin by establishing a simple but important result: when distinguishing LDOI states, we may restrict to LDOI measurement operators without loss of generality.

Theorem 9. *Suppose $\{\rho_1, \ldots, \rho_N\}$ is a set of LDOI quantum states. Then the optimal value of the semidefinite program* (4) *for PPT measurements and the analogous convex optimization problem for separable measurements are attained by LDOI measurement operators. Furthermore, the supremum over LOCC measurements is unchanged and can be approached arbitrarily closely by LDOI LOCC POVMs.*

Proof. For PPT and separable measurements, the result follows from the self-adjointness of the LDOT map Φ_{O}. If each ρ_k is LDOI then

$$\langle P_k, \rho_k \rangle = \langle P_k, \Phi_{\mathrm{O}}(\rho_k) \rangle = \langle \Phi_{\mathrm{O}}(P_k), \rho_k \rangle, \tag{25}$$

where the second equality uses $\Phi_{\mathrm{O}}^* = \Phi_{\mathrm{O}}$. Furthermore, the operators $\Phi_{\mathrm{O}}(P_1)$, ..., $\Phi_{\mathrm{O}}(P_N)$ satisfy all of the same constraints that P_1, ..., P_N do (since $P_k \in \mathrm{PPT}(\mathcal{X} : \mathcal{Y})$ implies $\Phi_{\mathrm{O}}(P_k) \in \mathrm{PPT}(\mathcal{X} : \mathcal{Y})$, and similarly for separability).

For LOCC measurements, we use a shared-randomness argument. Given any LOCC POVM $\{P_k\}$, consider the following protocol: using shared randomness, Alice and Bob sample a diagonal sign matrix O uniformly at random, apply the local unitaries $O \otimes O$, then execute the original LOCC protocol for $\{P_k\}$. The effective POVM elements are $\Phi_{\mathrm{O}}(P_k) = \frac{1}{2^n}\sum_O (O \otimes O) P_k (O \otimes O)$, which remain LOCC since LOCC is closed under local unitaries and shared randomness. For LDOI states ρ_k, the success probability is unchanged by (25), so the LOCC supremum can be approached by LDOI LOCC POVMs. □

Theorem 9 shows that when distinguishing LDOI states, we can restrict our search for optimal measurements to LDOI measurements without loss of generality. This has significant computational implications: for an ensemble of LDOI states on $\mathbb{C}^n \otimes \mathbb{C}^n$, the standard PPT semidefinite program requires optimizing over n^4 variables, but by exploiting the block structure of LDOI matrices (Subsection 2.1), the optimization can be restricted to the $3n^2 - 2n$ dimensional LDOI subspace. For even moderately large dimensions (e.g., $n = 10$), this represents a reduction from 10,000 variables to 280 variables—more than a 30-fold decrease in problem size. This dimensional reduction makes previously intractable problems computationally feasible.

Since LDOI states are invariant under local diagonal orthogonal symmetries, any optimization (like computing the optimal success probabilities) can be restricted to the LDOI subspace, drastically reducing the problem size. Our main result of this section establishes bounds on the probability of successfully distinguishing LDOI bases via LOCC, separable, and PPT measurements.

The following theorem applies the (U, A) parameterization of Definition 6 to uniform ensembles over orthonormal LDOI bases, yielding computable lower and upper bounds on the optimal success probabilities.

Theorem 10. *Let $n \geq 2$ be an integer, let $\mathcal{X} = \mathcal{Y} = \mathbb{C}^n$, and let $A \in \mathrm{L}(\mathcal{X})$ and $U \in \mathrm{U}(\mathcal{X})$ parameterize an orthonormal LDOI basis of $\mathcal{X} \otimes \mathcal{Y}$ as in Definition 6. Define the ensemble $\mathcal{E} = \{(1/n^2, |\phi_{i,j}\rangle\langle\phi_{i,j}|) : 1 \leq i, j \leq n\}$ with uniform prior distribution, where $|\phi_{i,j}\rangle$ are the basis vectors from Definition 6. The success probability of correctly distinguishing the states in $\mathcal{E}$ via LOCC satisfies*

$$\mathrm{opt}_{\mathrm{LOCC}}(\mathcal{E}) \geq \frac{1}{n^2} \left(\sum_{\substack{i,j=1 \\ i \neq j}}^{n} \max\left\{|a_{i,j}|^2, |a_{j,i}|^2\right\} + \max_{\sigma \in S_n} \left\{ \sum_{i=1}^{n} |u_{i,\sigma(i)}|^2 \right\} \right). \tag{26}$$

Furthermore, if $c_1, \ldots, c_n$ are any real numbers for which

$$c_i \geq \max_{1 \leq k \leq n} \left\{|u_{k,i}|^2\right\} \quad \text{and} \quad c_i c_j \geq |a_{i,j}|^2 |a_{j,i}|^2 \tag{27}$$

for all $1 \leq i \leq n$ (first inequality) and all $1 \leq i < j \leq n$ (second inequality), then

$$\mathrm{opt}_{\mathrm{PPT}}(\mathcal{E}) \leq \frac{1}{n^2} \left(\sum_{\substack{i,j=1 \\ i \neq j}}^{n} \max\left\{|a_{i,j}|^2, |a_{j,i}|^2\right\} + \sum_{i=1}^{n} c_i \right). \tag{28}$$

Before we prove the above theorem, we make numerous remarks about the bounds that it provides:

- The lower bound (26) and the upper bound (28) are very close to each other (see Corollary 16), and often even equal to each other (see Corollary 11). In particular, the initial term $\sum_{\substack{i,j=1 \\ i \neq j}}^{n} \max\left\{|a_{i,j}|^2, |a_{j,i}|^2\right\}$ is the same in both bounds, and it is just the second summation in each bound that might differ.
- The term $\max_{\sigma \in S_n} \left\{ \sum_{i=1}^{n} |u_{i,\sigma(i)}|^2 \right\}$ in the bound (26) perhaps looks difficult to compute. However, it is actually an instance of the Assignment Problem, which can be solved in $O(n^3)$ time by the Hungarian algorithm [Kuh55].

- Similarly, the optimal c_i's for the bound (28) can be found via semidefinite programming, since the constraint $c_i c_j \geq |a_{i,j}|^2 |a_{j,i}|^2$ is equivalent to the matrix

$$\begin{bmatrix} c_i & a_{i,j}\overline{a_{j,i}} \\ \overline{a_{i,j}}a_{j,i} & c_j \end{bmatrix} \tag{29}$$

  being positive semidefinite. This gives a much smaller (and thus much faster to evaluate numerically) semidefinite program than the general semidefinite program (5) that is used to find upper bounds on $\mathrm{opt}_{\mathrm{PPT}}(\mathcal{E})$. However, it is not always the case that there exist c_i's for which equality is attained in bound (28) (see Example 18).

- One feasible choice for the c_i's is $c_i = \max\left\{\frac{1}{2}, \max_{1\leq k\leq n}\left\{|u_{k,i}|^2\right\}\right\}$, since $c_i, c_j \geq 1/2$ ensures $c_i c_j \geq 1/4 \geq |a_{i,j}|^2 |a_{j,i}|^2$, with the final inequality following from the fact that $|a_{i,j}|^2 + |a_{j,i}|^2 = 1$. This gives the following explicit (but slightly weaker than (28)) upper bound for $\mathrm{opt}_{\mathrm{PPT}}(\mathcal{E})$

$$\mathrm{opt}_{\mathrm{PPT}}(\mathcal{E}) \leq \frac{1}{n^2}\left(\sum_{\substack{i,j=1 \\ i\neq j}}^{n} \max\left\{|a_{i,j}|^2, |a_{j,i}|^2\right\} + \sum_{i=1}^{n} \max\left\{\frac{1}{2}, \max_{1\leq k\leq n}\left\{|u_{k,i}|^2\right\}\right\}\right). \tag{30}$$

- The bound (30) shows that an orthonormal LDOI basis is perfectly distinguishable by PPT measurements if and only if it consists entirely of product states. To see this, notice that $\mathrm{opt}_{\mathrm{PPT}}(\mathcal{E}) = 1$ implies $\max\left\{|a_{i,j}|^2, |a_{j,i}|^2\right\} = 1$ and $\max_{1\leq k\leq n}\left\{|u_{k,i}|^2\right\} = 1$ for all $1 \leq i \neq j \leq n$. This implies that every entry in the matrices A and U from Definition 6 has magnitude equal to 0 or 1, giving the result.

- The bound (26) immediately implies a universal lower bound on LOCC distinguishability for all LDOI bases (see Corollary 15 below).

- When $a_{i,j} = 1/\sqrt{2}$ for all $i \neq j$, numerical evidence (via the software described in Section 4.1) strongly suggests that equality holds in the bound (28). That is, there exist $c_1, \ldots, c_n$ satisfying the constraints (27) such that $\mathrm{opt}_{\mathrm{PPT}}(\mathcal{E})$ exactly equals the upper bound. This has been verified numerically for various choices of U (including identity, Hadamard, and random unitary matrices) in dimensions $n = 2, 3, 4$), and for the Fourier matrix in all dimensions (see Example 17).

We note that Theorem 10 and its corollaries are stated for the uniform prior distribution $p_i = 1/n^2$. For non-uniform priors, the structural reduction of Theorem 9 still applies: optimal PPT and separable measurements can be taken to be LDOI regardless of the prior. However, the explicit bounds change character. The LOCC lower bound (26) generalizes by weighting each term by its prior probability, but the resulting assignment problem is no longer symmetric and may not admit a closed-form solution. The PPT upper bound (28) similarly generalizes with prior-weighted diagonal entries, though the constraints on the c_i become prior-dependent. Extending these bounds to obtain tight results for non-uniform priors remains a direction for future work.

Proof of Theorem 10. To prove the lower bound on $\mathrm{opt}_{\mathrm{LOCC}}(\mathcal{E})$, let $\sigma \in S_n$ and consider the local measurement operators

$$P_{i,i} = |\sigma(i)\rangle\langle\sigma(i)| \otimes |\sigma(i)\rangle\langle\sigma(i)| \quad \text{for} \quad 1 \leq i \leq n,$$
$$P_{i,j} = \begin{cases} |i\rangle\langle i| \otimes |j\rangle\langle j| & \text{if } |a_{i,j}| \geq |a_{j,i}| \\ |j\rangle\langle j| \otimes |i\rangle\langle i| & \text{otherwise} \end{cases} \quad \text{for} \quad 1 \leq i < j \leq n, \quad \text{and} \tag{31}$$
$$P_{j,i} = \begin{cases} |j\rangle\langle j| \otimes |i\rangle\langle i| & \text{if } |a_{i,j}| \geq |a_{j,i}| \\ |i\rangle\langle i| \otimes |j\rangle\langle j| & \text{otherwise} \end{cases} \quad \text{for} \quad 1 \leq i < j \leq n.$$

A direct calculation shows that $\sum_{i,j=1}^{n} P_{i,j} = \mathbb{1}$,

$$\langle P_{i,i}, \phi_{i,i}\rangle = |u_{i,\sigma(i)}|^2 \quad \text{and} \quad \langle P_{i,j}, \phi_{i,j}\rangle = \max\left\{|a_{i,j}|^2, |a_{j,i}|^2\right\}, \tag{32}$$

for all $1 \leq i, j \leq n$. The lower bound (26) now follows by maximizing over all $\sigma \in S_n$.

To prove the upper bound on $\text{opt}_{\text{PPT}}(\mathcal{E})$, for each pair (i, j) with $1 \leq i, j \leq n$, let $\gamma_{i,j}$ be a non-negative real number. Define the Hermitian operator

$$H = \frac{1}{n^2}\left(\sum_{i,j=1}^{n} \gamma_{i,j} Q_{i,j}\right) \in \text{Herm}(\mathcal{X} \otimes \mathcal{Y}), \tag{33}$$

where $Q_{i,j} = |i\rangle\langle i| \otimes |j\rangle\langle j|$. It is clear that H is diagonal with non-negative entries, and is thus positive semidefinite. We now investigate which values of $\{\gamma_{i,j}\}$ result in H being a feasible point of the semidefinite program (6), i.e.,

$$H - \frac{1}{n^2}\,\text{T}_{\mathcal{X}}\left(\phi_{i,j}\right) \in \text{Pos}(\mathcal{X} \otimes \mathcal{Y}) \tag{34}$$

for all $1 \leq i, j \leq n$.

A calculation reveals that

$$\begin{aligned} H - \frac{1}{n^2}\,\text{T}_{\mathcal{X}}\left(\phi_{k,k}\right) &= \frac{1}{n^2}\left(\sum_{i,j=1}^{n} \gamma_{i,j} Q_{i,j} - \sum_{i,j=1}^{n} u_{k,i}\overline{u_{k,j}}|i\rangle\langle j| \otimes |j\rangle\langle i|\right) \\ &= \frac{1}{n^2}\left(\sum_{i=1}^{n}(\gamma_{i,i} - |u_{k,i}|^2)Q_{i,i} + \sum_{\substack{i,j=1 \\ i\neq j}}^{n}\left(\gamma_{i,j}Q_{i,j} - u_{k,i}\overline{u_{k,j}}|i\rangle\langle j| \otimes |j\rangle\langle i|\right)\right). \end{aligned} \tag{35}$$

The bottom line of Equation (35) is a decomposition of $H - \text{T}_{\mathcal{X}}\left(\phi_{k,k}\right)/n^2$ as a direct sum of 1×1 and 2×2 blocks, so it is positive semidefinite if and only if $\gamma_{i,i} \geq |u_{k,i}|^2$ and $\gamma_{i,j}\gamma_{j,i} \geq |u_{k,i}|^2|u_{k,j}|^2$ for all $1 \leq i, j \leq n$, where the latter condition follows from the Schur complement criterion for the 2×2 blocks.

Similarly, if $1 \leq k < \ell \leq n$ then

$$\begin{aligned} H - \frac{1}{n^2}\,\text{T}_{\mathcal{X}}\left(\phi_{k,\ell}\right) &= \frac{1}{n^2}\left(\sum_{i,j=1}^{n} \gamma_{i,j}Q_{i,j} - |a_{k,\ell}|^2 Q_{k,\ell} - |a_{\ell,k}|^2 Q_{\ell,k} - a_{k,\ell}a_{\ell,k}|kk\rangle\langle\ell\ell| - \overline{a_{k,\ell}a_{\ell,k}}|\ell\ell\rangle\langle kk|\right) \\ &= \frac{1}{n^2}\left(\sum_{\substack{i,j=1 \\ i,j\notin\{k,\ell\}}}^{n} \gamma_{i,j}Q_{i,j}\right) + \frac{1}{n^2}\Big((\gamma_{k,\ell} - |a_{k,\ell}|^2)Q_{k,\ell} + (\gamma_{\ell,k} - |a_{\ell,k}|^2)Q_{\ell,k} \\ &\qquad + \gamma_{k,k}Q_{k,k} + \gamma_{\ell,\ell}Q_{\ell,\ell} - a_{k,\ell}a_{\ell,k}|kk\rangle\langle\ell\ell| - \overline{a_{k,\ell}a_{\ell,k}}|\ell\ell\rangle\langle kk|\Big). \end{aligned} \tag{36}$$

The bottom line of Equation (36) is a decomposition of $H - \mathrm{T}_{\mathcal{X}}\left(\phi_{k,\ell}\right)/n^2$ as a direct sum of 1×1 and 2×2 blocks, so it is positive semidefinite if and only if $\gamma_{k,\ell} \geq |a_{k,\ell}|^2$, $\gamma_{\ell,k} \geq |a_{\ell,k}|^2$, and $\gamma_{k,k}\gamma_{\ell,\ell} \geq |a_{k,\ell}|^2|a_{\ell,k}|^2$. A similar computation of $H - \mathrm{T}_{\mathcal{X}}\left(\phi_{\ell,k}\right)/n^2$ when $1 \leq k < \ell \leq n$ shows that we also need $\gamma_{k,\ell} \geq |a_{\ell,k}|^2$.

Altogether, this means that H is a feasible point of the semidefinite program (6) if and only if the scalars $\{\gamma_{i,j}\}$ satisfy the following constraints for all $1 \leq i,j \leq n$:

$$\begin{aligned} \gamma_{i,i} &\geq \max_{1\leq k\leq n}\left\{|u_{k,i}|^2\right\}, & \gamma_{i,i}\gamma_{j,j} &\geq |a_{i,j}|^2|a_{j,i}|^2, \\ \gamma_{i,j} &\geq \max\left\{|a_{i,j}|^2, |a_{j,i}|^2\right\}, & \gamma_{i,j}\gamma_{j,i} &\geq \max_{1\leq k\leq n}\left\{|u_{k,i}|^2|u_{k,j}|^2\right\}. \end{aligned} \tag{37}$$

Notice that the bottom-right constraint is redundant. To see this, observe that $\gamma_{i,j} \geq \max\left\{|a_{i,j}|^2, |a_{j,i}|^2\right\} \geq 1/2$ (using $|a_{i,j}|^2 + |a_{j,i}|^2 = 1$), and similarly $\gamma_{j,i} \geq 1/2$. Therefore $\gamma_{i,j}\gamma_{j,i} \geq 1/4$. Since U is unitary, we have $|u_{k,i}|^2|u_{k,j}|^2 \leq 1/4$ for all i, j, k (when $i \neq j$), which implies the bottom-right constraint is automatically satisfied. In particular, this means that we can choose

$$\gamma_{i,j} = \max\left\{|a_{i,j}|^2, |a_{j,i}|^2\right\} \tag{38}$$

for all $1 \leq i \neq j \leq n$. Setting $c_i = \gamma_{i,i}$ then shows that the objective value in the semidefinite program (6) equals

$$\mathrm{Tr}(H) = \frac{1}{n^2}\sum_{i,j=1}^{n}\gamma_{i,j} = \frac{1}{n^2}\left(\sum_{\substack{i,j=1\\ i\neq j}}^{n}\max\left\{|a_{i,j}|^2, |a_{j,i}|^2\right\} + \sum_{i=1}^{n}c_i\right) \tag{39}$$

which is exactly the desired upper bound (28). □

While the bounds of Theorem 10 perhaps look a bit complicated, there is a wide class of LDOI bases for which the bounds simplify considerably, and we actually get equality: whenever each column of U contains a sufficiently large entry, the two expressions collapse to the same value.

Corollary 11. *Let $n \geq 2$ be an integer, let $\mathcal{X} = \mathcal{Y} = \mathbb{C}^n$, and let $A \in \mathrm{L}(\mathcal{X})$ and $U \in \mathrm{U}(\mathcal{X})$ parameterize an orthonormal LDOI basis of $\mathcal{X} \otimes \mathcal{Y}$ as in Definition 6. Define the ensemble $\mathcal{E} = \{(1/n^2, |\phi_{i,j}\rangle\langle\phi_{i,j}|) : 1 \leq i,j \leq n\}$ with uniform prior distribution, where $|\phi_{i,j}\rangle$ are the basis vectors from Definition 6. Suppose further that there exists a permutation $\sigma \in S_n$ such that $|u_{\sigma(i),i}| \geq 1/\sqrt{2}$ for every $1 \leq i \leq n$ (i.e., each row and column of U has an entry with magnitude at least $1/\sqrt{2}$). Then*

$$\mathrm{opt}_{\mathrm{LOCC}}(\mathcal{E}) = \mathrm{opt}_{\mathrm{SEP}}(\mathcal{E}) = \mathrm{opt}_{\mathrm{PPT}}(\mathcal{E}) = \frac{1}{n^2}\left(\sum_{\substack{i,j=1\\ i\neq j}}^{n}\max\left\{|a_{i,j}|^2, |a_{j,i}|^2\right\} + \sum_{i=1}^{n}\left(\max_{1\leq k\leq n}\left\{|u_{k,i}|^2\right\}\right)\right). \tag{40}$$

Proof. By assumption there is $\sigma \in S_n$ with $|u_{\sigma(i),i}|^2 \geq 1/2$ for all i. For each column define

$$c_i = \max_{1\leq k\leq n}\left\{|u_{k,i}|^2\right\} \tag{41}$$

for $1 \leq i \leq n$, then we have $c_i \geq 1/2$. It follows that $c_ic_j \geq 1/4 \geq |a_{i,j}|^2|a_{j,i}|^2$, with the latter inequality following from the fact that $|a_{i,j}|^2 + |a_{j,i}|^2 = 1$. In other words, the second inequality of (27) follows from the first.

Under this choice of c_i, the upper bound (28) becomes

$$\mathrm{opt}_{\mathrm{PPT}}(\mathcal{E}) \leq \frac{1}{n^2}\left(\sum_{\substack{i,j=1\\ i\neq j}}^{n} \max\left\{|a_{i,j}|^2, |a_{j,i}|^2\right\} + \sum_{i=1}^{n}\left(\max_{1\leq k\leq n}\left\{|u_{k,i}|^2\right\}\right)\right). \tag{42}$$

For the lower bound (26), we evaluate the permutation σ guaranteed by the hypothesis to obtain

$$\max_{\sigma'\in S_n}\left\{\sum_{i=1}^{n}|u_{i,\sigma'(i)}|^2\right\} \geq \sum_{i=1}^{n}|u_{\sigma(i),i}|^2 = \sum_{i=1}^{n}\left(\max_{1\leq k\leq n}\left\{|u_{k,i}|^2\right\}\right), \tag{43}$$

since each $|u_{\sigma(i),i}|^2$ is one of the maximizers for column i. Thus the lower bound specializes to

$$\mathrm{opt}_{\mathrm{LOCC}}(\mathcal{E}) \geq \frac{1}{n^2}\left(\sum_{\substack{i,j=1\\ i\neq j}}^{n} \max\left\{|a_{i,j}|^2, |a_{j,i}|^2\right\} + \sum_{i=1}^{n}\left(\max_{1\leq k\leq n}\left\{|u_{k,i}|^2\right\}\right)\right). \tag{44}$$

Since the bounds (42) and (44) are the same as each other, the result follows. □

In the two-qubit case, all LDOI bases satisfy the hypotheses of Corollary 11, so we get the following simple result:

Corollary 12. *Let $\mathcal{X} = \mathcal{Y} = \mathbb{C}^2$ and let $\alpha, \beta, \gamma, \delta \in \mathbb{C}$ be such that $|\alpha|^2 + |\beta|^2 = |\gamma|^2 + |\delta|^2 = 1$. Define the ensemble $\mathcal{E} = \{(1/4, |\phi_i\rangle\langle\phi_i|) : 1 \leq i \leq 4\}$ with uniform prior distribution, where*

$$\begin{aligned} |\phi_1\rangle &= \alpha|11\rangle + \overline{\beta}|22\rangle, \quad |\phi_2\rangle = \beta|11\rangle - \overline{\alpha}|22\rangle, \\ |\phi_3\rangle &= \gamma|12\rangle + \overline{\delta}|21\rangle, \quad |\phi_4\rangle = \delta|12\rangle - \overline{\gamma}|21\rangle. \end{aligned} \tag{45}$$

Then

$$\mathrm{opt}_{\mathrm{LOCC}}(\mathcal{E}) = \mathrm{opt}_{\mathrm{SEP}}(\mathcal{E}) = \mathrm{opt}_{\mathrm{PPT}}(\mathcal{E}) = \frac{1}{2}\Big(\max\left\{|\alpha|^2, |\beta|^2\right\} + \max\left\{|\gamma|^2, |\delta|^2\right\}\Big). \tag{46}$$

Proof. The states $\{|\phi_i\rangle\}$ form an orthonormal LDOI basis, and every 2×2 unitary matrix has the property that each column has an entry with magnitude at least $1/\sqrt{2}$. Therefore Corollary 11 applies and gives the claimed formula immediately. □

Remark 13. When $|\alpha| = |\beta| = |\gamma| = |\delta| = 1/\sqrt{2}$, the ensemble $\mathcal{E}$ in Corollary 12 reduces to the uniform ensemble over the standard Bell basis, for which $\mathrm{opt}_{\mathrm{LOCC}}(\mathcal{E}) = \mathrm{opt}_{\mathrm{SEP}}(\mathcal{E}) = \mathrm{opt}_{\mathrm{PPT}}(\mathcal{E}) = 1/2$. More generally, the parametrized families of states in Corollary 12 generalize the parametrized Bell states studied in Example 3 of [BN13] and in [BCJ+15]. Corollary 12 shows that the explicit formula for optimal distinguishability holds not just for these specific parametrized families, but for *all* orthonormal LDOI bases in the two-qubit setting.

Corollary 14. *Among all two-qubit orthonormal LDOI bases, the uniform ensemble over the Bell basis achieves the minimum LOCC (and PPT and separable) distinguishability. That is, for any two-qubit LDOI basis with uniform ensemble $\mathcal{E} = \{(1/4, |\phi_i\rangle\langle\phi_i|) : 1 \leq i \leq 4\}$,*

$$\mathrm{opt}_{\mathrm{LOCC}}(\mathcal{E}) \geq \frac{1}{2}, \tag{47}$$

with equality if and only if the basis is the Bell basis (up to local unitaries).

Proof. By Corollary 12, for any two-qubit LDOI basis with uniform ensemble $\mathcal{E}$ we have

$$\mathrm{opt}_{\mathrm{LOCC}}(\mathcal{E}) = \frac{1}{2}\Big(\max\left\{|\alpha|^2, |\beta|^2\right\} + \max\left\{|\gamma|^2, |\delta|^2\right\} \Big), \tag{48}$$

where $|\alpha|^2 + |\beta|^2 = |\gamma|^2 + |\delta|^2 = 1$. Since $\max\{a, b\} \geq 1/2$ when $a + b = 1$ and $a, b \geq 0$, with equality if and only if $a = b = 1/2$, we have

$$\max\left\{|\alpha|^2, |\beta|^2\right\} \geq \frac{1}{2} \quad \text{and} \quad \max\left\{|\gamma|^2, |\delta|^2\right\} \geq \frac{1}{2}, \tag{49}$$

with equality in both inequalities if and only if $|\alpha| = |\beta| = |\gamma| = |\delta| = 1/\sqrt{2}$, which corresponds to the Bell basis. □

Corollary 15. *For any orthonormal LDOI basis of $\mathcal{X} \otimes \mathcal{Y}$ where $\mathcal{X} = \mathcal{Y} = \mathbb{C}^n$, let $\mathcal{E} = \{(1/n^2, |\phi_{i,j}\rangle\langle\phi_{i,j}|) : 1 \leq i, j \leq n\}$ denote the uniform ensemble, where $|\phi_{i,j}\rangle$ are the basis vectors. Then*

$$\mathrm{opt}_{\mathrm{LOCC}}(\mathcal{E}) \geq \frac{1}{2} - \frac{n-2}{2n^2}. \tag{50}$$

In particular, this function is minimized when $n = 4$, giving the dimension-independent bound

$$\mathrm{opt}_{\mathrm{LOCC}}(\mathcal{E}) \geq \frac{7}{16} = 0.4375 \tag{51}$$

for all uniform ensembles over orthonormal LDOI bases in any dimension.

Proof. Since $\max\left\{|a_{i,j}|^2, |a_{j,i}|^2\right\} \geq 1/2$ for all $i \neq j$ and $\max_{\sigma \in S_n} \sum_{i=1}^n |u_{i,\sigma(i)}|^2 \geq 1$ (because the matrix with entries $|u_{i,j}|^2$ is doubly stochastic), the lower bound (26) immediately gives

$$\mathrm{opt}_{\mathrm{LOCC}}(\mathcal{E}) \geq \frac{1}{n^2}\left(\frac{n(n-1)}{2} + 1\right) = \frac{1}{n^2}\frac{n^2 - n + 2}{2} = \frac{n^2 - n + 2}{2n^2} = \frac{1}{2} - \frac{n-2}{2n^2}. \tag{52}$$

To find the dimension-independent lower bound, we minimize $f(n) = 1/2 - (n-2)/(2n^2)$ for $n \geq 2$. Taking the derivative,

$$f'(n) = \frac{n-4}{2n^3}, \tag{53}$$

which is negative for $n < 4$ and positive for $n > 4$, so the minimum occurs at $n = 4$, giving $f(4) = 7/16$. □

The lower bound expression (26) of Theorem 10 evaluates to the universal bound value for specific bases. Consider an orthonormal LDOI basis where U is the $n \times n$ Fourier matrix (normalized so that all entries have magnitude $1/\sqrt{n}$) and A is defined by $a_{i,j} = 1/\sqrt{2}$ for all $i \neq j$ (with arbitrary diagonal entries). For this basis, the Fourier matrix has the property that all entries have equal magnitude, making it maximally "spread out" across rows and columns. This structure minimizes the optimal assignment value: the maximum over permutations $\sigma \in S_n$ of $\sum_{i=1}^n |u_{i,\sigma(i)}|^2$ equals exactly $n(1/n) = 1$, the minimum possible value given unitarity. Combined with $\sum_{i \neq j} \max\{|a_{i,j}|^2, |a_{j,i}|^2\} = n(n-1)(1/2)$, the lower bound (26) evaluates to precisely $\frac{1}{2} - \frac{n-2}{2n^2}$, matching the universal bound. This shows that the lower bound formula cannot be uniformly tightened.

While Corollary 15 establishes the rigorous lower bound of $7/16$ for all dimensions, it is natural to ask whether a uniform bound of $1/2$ holds for all uniform ensembles over LDOI bases. For

$n = 2$, Corollary 12 shows that $\text{opt}_{\text{LOCC}}(\mathcal{E}) \geq 1/2$ for all two-qubit LDOI uniform ensembles, with equality achieved by the uniform ensemble over the Bell basis. For $n \geq 3$, the Fourier basis example shows that the lower bound (26) evaluates to exactly $\frac{1}{2} - \frac{n-2}{2n^2}$. Whether $\text{opt}_{\text{LOCC}}(\mathcal{E})$ for the Fourier basis equals this lower bound value or is strictly larger remains an open question (see Example 17).

While equality $\text{opt}_{\text{LOCC}}(\mathcal{E}) = \text{opt}_{\text{PPT}}(\mathcal{E})$ holds for uniform ensembles over a broad class of LDOI bases—including all two-qubit cases by Corollary 12 and those satisfying the conditions of Corollary 11—it remains an open question whether this equality holds for *all* orthonormal LDOI bases. Example 17 exhibits a basis where the upper and lower bounds in Theorem 10 do not match, suggesting the possibility of a strict gap in higher dimensions. In any case, we can show that these two quantities are always close together. In particular, the following result shows that the maximal gap between $\text{opt}_{\text{PPT}}(\mathcal{E})$ and $\text{opt}_{\text{LOCC}}(\mathcal{E})$ for uniform ensembles approaches 0 as $n \to \infty$, and the largest potential gap between these quantities in any dimension is $1/16 = 0.0625$ (when $n = 4$).

Corollary 16. *Let $n \geq 2$ be an integer and let $\mathcal{X} = \mathcal{Y} = \mathbb{C}^n$. For any orthonormal LDOI basis of $\mathcal{X} \otimes \mathcal{Y}$, define the ensemble $\mathcal{E} = \{(1/n^2, |\phi_{i,j}\rangle\langle\phi_{i,j}|) : 1 \leq i, j \leq n\}$ with uniform prior distribution, where $|\phi_{i,j}\rangle$ are the basis vectors. Then*

$$0 \leq \text{opt}_{\text{PPT}}(\mathcal{E}) - \text{opt}_{\text{LOCC}}(\mathcal{E}) \leq \frac{n-2}{2n^2}. \tag{54}$$

Proof. The left inequality is trivial. To verify the right inequality, we subtract the bound (26) from (30) to see that

$$\text{opt}_{\text{PPT}}(\mathcal{E}) - \text{opt}_{\text{LOCC}}(\mathcal{E}) \leq \frac{1}{n^2}\left(\sum_{i=1}^{n} \max\left\{\frac{1}{2}, \max_{1\leq k\leq n}\left\{|u_{k,i}|^2\right\}\right\} - \max_{\sigma\in S_n}\left\{\sum_{i=1}^{n}|u_{i,\sigma(i)}|^2\right\}\right). \tag{55}$$

Suppose that there are M columns of U containing an entry with magnitude at least $1/\sqrt{2}$ (M may equal 0). By permuting the columns of U we can assume without loss of generality that these are its first M columns, and by permuting the rows of U we can further assume without loss of generality that $|u_{i,i}| \geq 1/\sqrt{2}$ for $1 \leq i \leq M$. Then

$$\sum_{i=1}^{n} \max\left\{\frac{1}{2}, \max_{1\leq k\leq n}\left\{|u_{k,i}|^2\right\}\right\} = \frac{n-M}{2} + \sum_{i=1}^{M}|u_{i,i}|^2. \tag{56}$$

Similarly, we claim that

$$\max_{\sigma\in S_n}\left\{\sum_{i=1}^{n}|u_{i,\sigma(i)}|^2\right\} \geq \sum_{i=1}^{M}|u_{i,i}|^2 + \begin{cases}\frac{n-3M/2}{n-M} & \text{if } M < n,\\ 0 & \text{if } M = n.\end{cases} \tag{57}$$

To verify this inequality, we apply some Frobenius norm estimates to U: if we partition U as a block matrix

$$U = \begin{bmatrix} U_1 & U_2 \\ U_3 & U_4 \end{bmatrix} \tag{58}$$

with U_1 being $M \times M$, then $\|U_1\|_{\text{F}}^2 \geq \sum_{i=1}^{M}|u_{i,i}|^2 \geq M/2$, since $|u_{i,i}|^2 \geq 1/2$ for all $1 \leq i \leq M$. Now use the fact that U is unitary to see that $\|U_1\|_{\text{F}}^2 + \|U_2\|_{\text{F}}^2 = M$, which implies $\|U_2\|_{\text{F}}^2 \leq M - M/2 = M/2$. Finally, using unitarity of U again shows that $\|U_2\|_{\text{F}}^2 + \|U_4\|_{\text{F}}^2 = n - M$, so $\|U_4\|_{\text{F}}^2 \geq n - M - M/2 = n - 3M/2$. Since U_4 is $(n-M) \times (n-M)$ with Frobenius norm squared at least $n - 3M/2$, and the optimal assignment for U_4 selects one entry per row and column, this assignment must achieve total squared magnitude at least $(n - 3M/2)/(n-M)$ on average.

Therefore, there must exist some $\sigma \in S_n$ with $\sigma(i) = i$ for $1 \le i \le M$ such that $\sum_{i=M+1}^{n} |u_{i,\sigma(i)}|^2 \ge (n - 3M/2)/(n - M)$, giving the bound (57).

Substituting Equation (56) and the bound (57) into Inequality (55) then shows that

$$\mathrm{opt}_{\mathrm{PPT}}(\mathcal{E}) - \mathrm{opt}_{\mathrm{LOCC}}(\mathcal{E}) \le \frac{n-M}{2n^2} - \begin{cases} \frac{n-3M/2}{n^2(n-M)} & \text{if } M < n, \\ 0 & \text{if } M = n. \end{cases} \tag{59}$$

The above bound is maximized when $M = 0$ or $M = n - 1$, in which cases it simplifies to

$$\mathrm{opt}_{\mathrm{PPT}}(\mathcal{E}) - \mathrm{opt}_{\mathrm{LOCC}}(\mathcal{E}) \le \frac{n-2}{2n^2}, \tag{60}$$

which completes the proof. □

Table 1 shows the gap bound $(n-2)/(2n^2)$ for small dimensions, illustrating that the maximum gap of $1/16 = 0.0625$ occurs at $n = 4$ and decreases for larger n, vanishing as $n \to \infty$.

n	$(n-2)/(2n^2)$	Decimal
2	0	0
3	1/18	≈ 0.0556
4	1/16	$= 0.0625$
5	3/50	$= 0.06$
10	1/25	$= 0.04$
20	9/400	$= 0.0225$
∞	0	0

Table 1: Upper bound on the gap $\mathrm{opt}_{\mathrm{PPT}}(\mathcal{E}) - \mathrm{opt}_{\mathrm{LOCC}}(\mathcal{E})$ for uniform LDOI ensembles as a function of dimension n. The gap is maximized at $n = 4$.

Example 17. Let $n \ge 3$ and consider an orthonormal LDOI basis arising from Definition 6 with $A = (1/\sqrt{2})\mathbf{1}_n$ (the all-ones matrix scaled by $1/\sqrt{2}$) and U equal to the n-dimensional Fourier matrix. Define the uniform ensemble $\mathcal{E} = \{(1/n^2, |\phi_{i,j}\rangle\langle\phi_{i,j}|) : 1 \le i,j \le n\}$, where $|\phi_{i,j}\rangle$ are the basis vectors. This basis consists of n maximally entangled states $|\phi_{i,i}\rangle$ and $n(n-1)$ Schmidt-rank-2 states $|\phi_{i,j}\rangle$ with $i \ne j$ that are symmetric or antisymmetric Bell-like states with Schmidt coefficients $1/\sqrt{2}, 1/\sqrt{2}$.

Since the Fourier matrix has all entries with magnitude $1/\sqrt{n}$, we have $\max_{1\le k\le n} |u_{k,i}|^2 = 1/n < 1/2$ for all i. The bounds of Theorem 10 therefore show that

$$\mathrm{opt}_{\mathrm{LOCC}}(\mathcal{E}) \ge \frac{1}{2} - \frac{n-2}{2n^2} \quad \text{and} \quad \mathrm{opt}_{\mathrm{PPT}}(\mathcal{E}) \le \frac{1}{2}. \tag{61}$$

The upper and lower bounds do not match, indicating a potential gap between LOCC and PPT distinguishability. We now show that the upper bound is tight: $\mathrm{opt}_{\mathrm{PPT}}(\mathcal{E}) = 1/2$.

For each ordered pair (i, j) with $i \ne j$, define

$$P_{i,j} = \frac{1}{2}\big(|ij\rangle\langle ij| + |ji\rangle\langle ji|\big) + \frac{s_{i,j}}{2n-2}\big(|ij\rangle\langle ji| + |ji\rangle\langle ij|\big) + \frac{1}{2n-2}\big(|ii\rangle\langle ii| + |jj\rangle\langle jj|\big), \tag{62}$$

where $s_{i,j} = 1$ when $i < j$ and $s_{i,j} = -1$ when $i > j$. In particular $s_{j,i} = -s_{i,j}$, which will ensure the cross terms cancel when the operators are summed. For the diagonal pairs we set $P_{i,i} = 0$ for all $1 \le i \le n$.

Each $P_{i,j}$ with $i \neq j$ acts only on the 4-dimensional subspace spanned by $\{|ii\rangle, |ij\rangle, |ji\rangle, |jj\rangle\}$. The block on $\{|ij\rangle, |ji\rangle\}$ has matrix representation $\left(\begin{smallmatrix} 1/2 & s_{i,j}/(2n-2) \\ s_{i,j}/(2n-2) & 1/2 \end{smallmatrix}\right)$, whose eigenvalues are $1/2 \pm 1/(2n-2) \geq 0$, so it is positive semidefinite. The block on $\{|ii\rangle, |jj\rangle\}$ is diagonal with positive entries $1/(2n-2)$. Taking the partial transpose swaps $|ij\rangle\langle ji|$ with $|jj\rangle\langle ii|$, which simply replaces the latter block with $\left(\begin{smallmatrix} 1/(2n-2) & s_{i,j}/(2n-2) \\ s_{i,j}/(2n-2) & 1/(2n-2) \end{smallmatrix}\right)$, again positive semidefinite. Hence every $P_{i,j}$ is PPT.

Summing over all ordered pairs gives

$$\sum_{i,j=1}^{n} P_{i,j} = \sum_{\substack{i,j=1 \\ i\neq j}}^{n} P_{i,j} = \sum_{\substack{i,j=1 \\ i\neq j}}^{n} \frac{1}{2}(|ij\rangle\langle ij| + |ji\rangle\langle ji|) + \sum_{\substack{i,j=1 \\ i\neq j}}^{n} \frac{1}{2n-2}(|ii\rangle\langle ii| + |jj\rangle\langle jj|), \tag{63}$$

because the off-diagonal terms $|ij\rangle\langle ji|$ cancel between $P_{i,j}$ and $P_{j,i}$ (which have opposite signs). Every basis vector $|ij\rangle$ with $i \neq j$ appears in exactly two summands, each contributing $1/2$, and every $|ii\rangle$ appears in $2(n-1)$ summands, each contributing $1/(2n-2)$. Thus $\sum_{i,j} P_{i,j} = \mathbb{1}$.

A direct calculation shows

$$\langle P_{i,j}, \phi_{i,j}\rangle = \frac{1}{2} + \frac{1}{2n-2} = \frac{n}{2n-2} \tag{64}$$

for all $i \neq j$, regardless of whether $i < j$ or $i > j$: the symmetric (resp., antisymmetric) combinations pick up the positive (resp., negative) cross term with the same magnitude. Because $\langle P_{i,i}, \phi_{i,i}\rangle = 0$ for all i, the average success probability is

$$\frac{1}{n^2}\sum_{i,j=1}^{n} \langle P_{i,j}, \phi_{i,j}\rangle = \frac{1}{n^2} \cdot n(n-1) \cdot \frac{n}{2n-2} = \frac{1}{2}, \tag{65}$$

establishing $\mathrm{opt}_{\mathrm{PPT}}(\mathcal{E}) = 1/2$.

Each $P_{i,j}$ is supported on a $(2\otimes 2)$-dimensional subsystem (the subspace spanned by $\{|ii\rangle, |ij\rangle, |ji\rangle, |jj\rangle\} \cong \mathbb{C}^2 \otimes \mathbb{C}^2$). Since PPT is equivalent to separability for $2 \otimes 2$ systems, the measurements are also separable. Thus $\mathrm{opt}_{\mathrm{SEP}}(\mathcal{E}) = 1/2$ as well.

Whether the lower bound in Equation (61) is tight—that is, whether $\mathrm{opt}_{\mathrm{LOCC}}(\mathcal{E}) = 1/2 - (n-2)/(2n^2)$—remains an open question. Whether $\mathrm{opt}_{\mathrm{LOCC}}(\mathcal{E})$ coincides with one of these bounds or takes an intermediate value remains unknown; resolving this would require new techniques for analyzing the full LOCC hierarchy beyond the product measurement strategy of Theorem 10.

Corollaries 11 and 12, as well as Example 17, might lead us to conjecture that, for every LDOI basis with uniform ensemble $\mathcal{E}$, the upper bound (28) on $\mathrm{opt}_{\mathrm{PPT}}(\mathcal{E})$ is actually equality (for some suitably chosen $c_1, \ldots, c_n$). We now present the simplest example that we have been able to find to demonstrate that this is not the case.

Example 18. Let $n = 3$ and $\mathcal{X} = \mathcal{Y} = \mathbb{C}^n$. Consider an LDOI basis of $\mathcal{X} \otimes \mathcal{Y}$ arising from Definition 6 via the matrices

$$A = \frac{1}{5}\begin{bmatrix} 0 & 3 & 3 \\ 4 & 0 & 3 \\ 4 & 4 & 0 \end{bmatrix} \quad \text{and} \quad U = \frac{1}{3}\begin{bmatrix} 2 & -2 & 1 \\ 1 & 2 & 2 \\ 2 & 1 & -2 \end{bmatrix}. \tag{66}$$

Define the uniform ensemble $\mathcal{E} = \{(1/9, |\phi_{i,j}\rangle\langle\phi_{i,j}|) : 1 \leq i,j \leq 3\}$, where $|\phi_{i,j}\rangle$ are the basis vectors. Semidefinite programming shows that $c_1 + c_2 + c_3$ is minimized (subject to the constraints (27)) when $c_1 = c_2 = c_3 = 12/25$. Note that in this example, the constraint $c_i c_j \geq |a_{i,j}|^2 |a_{j,i}|^2$

is satisfied with equality for all $i \neq j$: we have $c_i c_j = (12/25)^2 = 144/625 = (3/5)^2(4/5)^2 = |a_{i,j}|^2|a_{j,i}|^2$ exactly. With these values, the best bound (28) is equal to

$$\frac{1}{n^2}\left(\sum_{\substack{i,j=1\\ i\neq j}}^{n} \max\left\{|a_{i,j}|^2, |a_{j,i}|^2\right\} + \sum_{i=1}^{n} c_i\right) = 44/75 \approx 0.5867. \tag{67}$$

However, solving the semidefinite program (4) directly for this ensemble $\mathcal{E}$ shows that

$$\text{opt}_{\text{PPT}}(\mathcal{E}) = 26/45 \approx 0.5778, \tag{68}$$

demonstrating that the upper bound (28) on $\text{opt}_{\text{PPT}}(\mathcal{E})$ is not always attained. The gap arises because the upper bound (28) is derived from the constrained dual (6) with H restricted to be diagonal. For this particular (U, A) pair, the columns of U have no entry with magnitude at least $1/\sqrt{2}$, so the condition of Corollary 11 fails. In the full dual (5), the auxiliary variables Q_k provide additional degrees of freedom that allow a tighter certificate; restricting to the diagonal ansatz H forfeits this flexibility. More generally, the bound (28) is tight precisely when the diagonal ansatz suffices to certify optimality, which holds whenever the column-magnitude condition of Corollary 11 is satisfied.

4 Conclusion

We have studied the local distinguishability of quantum states with local diagonal orthogonal invariance—a broad class that includes Werner states, isotropic states, X-states, and Dicke states. Our main structural result, Theorem 9, shows that for LDOI ensembles, the search for optimal measurements can be restricted to the LDOI subspace without loss of generality. For orthonormal LDOI bases, we established efficiently computable upper and lower bounds on distinguishability (Theorem 10) and proved that the LOCC supremum equals the PPT and separable optima for a broad class of bases, including all two-qubit cases (Corollary 12) and bases with sufficiently large entries in the unitary matrix U (Corollary 11). More generally, we showed that the gap between PPT and LOCC distinguishability is bounded by $(n-2)/(2n^2)$, which achieves its maximum value of $1/16$ at $n = 4$ and vanishes asymptotically. The LOCC lower bound evaluates to exactly $1/2 - (n-2)/(2n^2)$ for the Fourier basis with uniform ensemble $\mathcal{E}$. Whether $\text{opt}_{\text{LOCC}}(\mathcal{E})$ equals this lower bound value or is strictly larger remains open.

Several natural questions remain open and suggest promising directions for future investigation. First, while we have shown that $\text{opt}_{\text{LOCC}}(\mathcal{E}) = \text{opt}_{\text{PPT}}(\mathcal{E})$ for a broad class of uniform LDOI ensembles (Corollaries 11 and 12), it remains open whether this equality holds for *all* uniform ensembles of orthonormal LDOI bases. Example 17 demonstrates that the bounds in Theorem 10 do not always coincide, but this does not rule out equality between the optimal values. It would also be interesting to extend the explicit bounds of Theorem 10 to non-uniform prior distributions and to understand how the relationship between LOCC and PPT distinguishability depends on the prior.

Second, while orthonormal LDOI bases may not achieve perfect minimum-error distinguishability under PPT measurements (as demonstrated by Example 17), we conjecture the following:

Conjecture 1. *Every orthonormal LDOI basis of $\mathcal{X} \otimes \mathcal{Y}$ can be unambiguously distinguished by PPT measurements.*

This has been verified numerically for random LDOI bases in dimensions $n = 2, 3, 4$, and 5 using the software described in Section 4.1. In each case, the SDP for unambiguous PPT discrimination was feasible for every randomly generated LDOI basis tested. Note that the projective measurement onto the basis states is not PPT (the partial transpose has negative eigenvalues), so if this conjecture is true, the proof would require constructing a nontrivial PPT POVM achieving unambiguous discrimination. One heuristic reason to expect the conjecture to hold is that the LDOI block structure severely constrains the partial transposes: the PPT condition decomposes into $n + \binom{n}{2}$ small semidefinite constraints (on blocks of size at most $n \times n$ and 2×2), providing considerably more room for feasibility than the general $n^2 \times n^2$ PPT condition.

4.1 Software

Companion software for determining whether a collection of quantum states constitute an LDOI basis, implementing the LDOT map, along with the semidefinite programs for determining the PPT distinguishability of a collection of quantum states in this work are provided within the `toqito` quantum information package [Rus21] which leverages `PICOS` [SS22] and the `CVXOPT` solver [ADV20] for semidefinite program optimization.

Acknowledgments

N.J. was supported by NSERC Discovery Grant RGPIN-2022-04098.

References

[ADV20] Martin Andersen, Joachim Dahl, and Lieven Vandenberghe. CVXOPT: Convex Optimization. *Astrophysics Source Code Library*, page ascl:2008.017, 2020. ADS Bibcode: 2020ascl.soft08017A.

[ANTSV99] Andris Ambainis, Ashwin Nayak, Amnon Ta-Shma, and Umesh Vazirani. Dense quantum coding and a lower bound for 1-way quantum automata. In *Proceedings of the thirty-first annual ACM symposium on Theory of computing*, pages 376–383. ACM, 1999.

[Ban11] Somshubhro Bandyopadhyay. More nonlocality with less purity. *Physical Review Letters*, 106(21):210402, 2011.

[BCJ+15] Somshubhro Bandyopadhyay, Alessandro Cosentino, Nathaniel Johnston, Vincent Russo, John Watrous, and Nengkun Yu. Limitations on separable measurements by convex optimization. *IEEE Transactions on Information Theory*, 61(6):3593–3604, 2015.

[BDF+99] Charles H Bennett, David P DiVincenzo, Christopher A Fuchs, Tal Mor, Eric Rains, Peter W Shor, John A Smolin, and William K Wootters. Quantum nonlocality without entanglement. *Physical Review A*, 59(2):1070, 1999.

[BN13] Somshubhro Bandyopadhyay and Michael Nathanson. Tight bounds on the distinguishability of quantum states under separable measurements. *Physical Review A*, 88(5):052313, 2013.

[BW92] Charles H. Bennett and Stephen J. Wiesner. Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. *Physical Review Letters*, 69(20):2881–2884, 1992.

[CK06] Dariusz Chruściński and Andrzej Kossakowski. Class of positive partial transposition states. *Physical Review A—Atomic, Molecular, and Optical Physics*, 74(2):022308, 2006.

[CLM$^+$14] Eric Chitambar, Debbie Leung, Laura Mančinska, Maris Ozols, and Andreas Winter. Everything you always wanted to know about LOCC (but were afraid to ask). *Communications in Mathematical Physics*, 328(1):303–326, 2014.

[Cos13] Alessandro Cosentino. Positive-partial-transpose-indistinguishable states via semidefinite programming. *Physical Review A*, 87(1):012321, 2013.

[CR14] Alessandro Cosentino and Vincent Russo. Small sets of locally indistinguishable orthogonal maximally entangled states. *Quantum Information and Computation*, 14(13–14):1098–1106, 2014.

[DFXY09] Runyao Duan, Yuan Feng, Yu Xin, and Mingsheng Ying. Distinguishability of quantum states by separable operations. *IEEE Transactions on Information Theory*, 55(3):1320–1330, 2009.

[GKR$^+$02] Sibasish Ghosh, Guruprasad Kar, Anirban Roy, Debasis Sarkar, Aditi Sen, Ujjwal Sen, et al. Local indistinguishability of orthogonal pure states by using a bound on distillable entanglement. *Physical Review A*, 65(6):062307, 2002.

[Hel69] Carl W. Helstrom. Quantum detection and estimation theory. *Journal of Statistical Physics*, 1(2):231–252, 1969.

[HH99] Michał Horodecki and Pawel Horodecki. Reduction criterion of separability and limits for a class of distillation protocols. *Physical Review A*, 59:4206–4216, 1999.

[HK11] Kil-Chan Ha and Seung-Hyeok Kye. One-parameter family of indecomposable optimal entanglement witnesses arising from generalized Choi maps. *Physical Review A*, 84:024302, 2011.

[Hol73] Alexander Semenovich Holevo. Bounds for the quantity of information transmitted by a quantum communication channel. *Problemy Peredachi Informatsii*, 9(3):3–11, 1973.

[HSSH03] Michał Horodecki, Aditi Sen, Ujjwal Sen, and Karol Horodecki. Local indistinguishability: More nonlocality with less entanglement. *Physical review letters*, 90(4):047902, 2003.

[JM19] Nathaniel Johnston and Olivia MacLean. Pairwise completely positive matrices and conjugate local diagonal unitary invariant quantum states. *Electronic Journal of Linear Algebra*, 35:156–180, 2019.

[Kuh55] Harold W. Kuhn. The Hungarian method for the assignment problem. *Naval Research Logistics Quarterly*, 2:83–97, 1955.

[NC02] Michael A. Nielsen and Isaac L. Chuang. Quantum Computation and Quantum Information, 2002.

[NS21] Ion Nechita and Satvik Singh. A graphical calculus for integration over random diagonal unitary matrices. *Linear Algebra and its Applications*, 613:46–86, 2021.

[QAQJ12] Nicolás Quesada, Asma Al-Qasimi, and Daniel F. V. James. Quantum properties and dynamics of X states. *Journal of Modern Optics*, 59(15):1322–1329, 2012.

[Rus21] Vincent Russo. toqito – Theory of quantum information toolkit: A Python package for studying quantum information. *Journal of Open Source Software*, 6(61):3082, 2021.

[SN21] Satvik Singh and Ion Nechita. Diagonal unitary and orthogonal symmetries in quantum theory. *Quantum*, 5:519, 2021.

[SS22] Guillaume Sagnol and Maximilian Stahlberg. PICOS: A Python interface to conic optimization solvers. *Journal of Open Source Software*, 7(70):3915, 2022.

[TAQ+18] Jordi Tura, Albert Aloy, Ruben Quesada, Maciej Lewenstein, and Anna Sanpera. Separability of diagonal symmetric states: A quadratic conic optimization problem. *Quantum*, 2:45, 2018.

[VSPM01] Shashank Virmani, Massimiliano F Sacchi, Martin B Plenio, and Damian Markham. Optimal local discrimination of two multipartite pure states. *Physics Letters A*, 288(2):62–68, 2001.

[Wat18] John Watrous. *The Theory of Quantum Information*. Cambridge University Press, 2018.

[Wer89] Reinhard F. Werner. Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model. *Physical Review A*, 40:4277–4281, 1989.

[WH02] Jonathan Walgate and Lucien Hardy. Nonlocality, asymmetry, and distinguishing bipartite states. *Physical Review Letters*, 89(14):147901, 2002.

[Wil13] Mark M. Wilde. *Quantum Information Theory*. Cambridge University Press, 2013.

[WSHV00] Jonathan Walgate, Anthony J Short, Lucien Hardy, and Vlatko Vedral. Local distinguishability of multipartite orthogonal quantum states. *Physical Review Letters*, 85(23):4972, 2000.

[YDY12] Nengkun Yu, Runyao Duan, and Mingsheng Ying. Four locally indistinguishable ququad-ququad orthogonal maximally entangled states. *Physical review letters*, 109(2):020506, 2012.

[YDY14] Nengkun Yu, Runyao Duan, and Mingsheng Ying. Distinguishability of quantum states by positive operator-valued measures with positive partial transpose. *IEEE Transactions on Information Theory*, 60(4):2069–2079, 2014.

[Yu16] Nengkun Yu. Separability of a mixture of Dicke states. *Physical Review A*, 94:060101(R), 2016.