Tight bounds for antidistinguishability and circulant sets of pure quantum states

Nathaniel Johnston,[*] Vincent Russo,[†] and Jamie Sikora[‡]

November 28, 2023

Abstract

A set of pure quantum states is said to be antidistinguishable if upon sampling one at random, there exists a measurement to perfectly determine some state that was not sampled. We show that antidistinguishability of a set of n pure states is equivalent to a property of its Gram matrix called $(n-1)$-incoherence, thus establishing a connection with quantum resource theories that lets us apply a wide variety of new tools to antidistinguishability. As a particular application of our result, we present an explicit formula (not involving any semidefinite programming) that determines whether or not a set with a circulant Gram matrix is antidistinguishable. We also show that if all inner products are smaller than $\sqrt{(n-2)/(2n-2)}$ then the set must be antidistinguishable, and we show that this bound is tight when $n \leq 4$. We also give a simpler proof that if all the inner products are strictly larger than $(n-2)/(n-1)$, then the set cannot be antidistinguishable, and we show that this bound is tight for all n.

1 Introduction

A collection of pure quantum states $\{|\psi_0\rangle, |\psi_1\rangle, \ldots, |\psi_{n-1}\rangle\}$ is called *antidistinguishable* [CFS02, Lei14, HK18] if there exists a positive operator-valued measure $\{M_0, M_1, \ldots, M_{n-1}\}$ such that

$$\langle\psi_i|M_i|\psi_i\rangle = 0, \text{ for all } i \in \{0, 1, \ldots, n-1\}. \tag{1}$$

The outcome of the measurement can be interpreted as ruling out one of the $|\psi_i\rangle$ states. For example, if outcome M_i occurs then we know for certain that $|\psi_i\rangle$ was not measured. The notion of antidistinguishability was introduced in [CFS02] where it was referred to as *post-Peierls incompatibility*. Antidistinguishability was later used as a key part in the proof of the PBR theorem [PBR12]; a result that has significance to the foundations of quantum mechanics, and more specifically, significance to how one may interpret the reality of the quantum state.

Antidistinguishability is also referred to as *unambiguous quantum state exclusion* [BJOP14]. This setting of quantum state exclusion (sometimes referred to as error-free quantum state elimination) has also found utility in the context of quantum communication [PJO15, HK19, HB20] as well as quantum cryptography where it has been used to reduce the need for long-term quantum memory for digital signature schemes [DWA14] and to develop oblivious transfer protocols [ASR+21].

[*]Department of Mathematics & Computer Science, Mount Allison University, Sackville, NB, Canada E4L 1E4. njohnston@mta.ca

[†]Unitary Fund. vincent@unitary.fund

[‡]Department of Computer Science, Virginia Polytechnic Institute and State University, Blacksburg, VA, USA 24061. sikora@vt.edu

In contrast to quantum state exclusion is the more well-established field of quantum state distinguishability that enjoys a rich history of study and has served to be foundational to the field of quantum information. In the setting of quantum state distinguishability, the goal is to determine what state one is given from a collection of quantum states. Whereas the setting of quantum state exclusion has the goal of determining which state one is *not* given. Quantum state exclusion, and by proxy, the notion of antidistinguishability, has not been as thoroughly explored as quantum state distinguishability [BDF+99, Che00, WSHV00, GKR+01, VSPM01, WH02, HSSH03, Wat05, BC09, Ber10, QL10, BK15].

One way in which to further our understanding of the notion of antidistinguishability is to determine under which conditions a collection of states is antidistinguishable. In [BJOP14], a necessary condition for antidistinguishability was provided as a function of the fidelity of the states in the collection. Similarly, in [HK18], the authors provided a sufficient condition for antidistinguishability based on algebraic properties of the states. In a recent work [MNW23], optimal error exponents for antidistinguishability are given for the classical version of the problem and they also provide bounds for the quantum case, leaving an exact expression as an open problem.

In [HB20], the authors conjectured that if a collection of d states each of dimension d satisfied an inequality based on d, then the states are antidistinguishable (see Conjecture 5.1 for the precise statement). The validity of this conjecture would imply the existence of an improved separation between a classical and quantum communication task [HB20] as well as a strengthening of the PBR theorem [MW14a, MW14b]. This conjecture is known to be true for $d = 2$ and for $d = 3$ [CFS02] and also had some amount of numerical evidence to suggest that it might be true for higher dimensions as well [HB20]. However, a counterexample to the conjecture for $d = 4$ was presented in [RS23]. While this disproved the conjecture, the counterexample was not optimal and it was not clear whether the conjecture could be reframed or salvaged. We provide an optimal disproof of the conjecture for $d = 4$ in Example 6.1 as well as a correction to the conjecture in Corollary 5.5. In particular, our correction is a trivial-to-compute sufficient condition for antidistinguishability of a family of states based on their inner products.

In order to establish our results, we explore how antidistinguishability of a collection of pure quantum states can be determined by their Gram matrix. In some sense, considering the Gram matrix in this context is a natural thing to do and is inspired by the following references on the quantum change point problem [SBC+16, SCMT17]. In particular, we establish a novel connection between antidistinguishability and quantum resource theories: we show in Theorem 3.2 that a collection of pure states is antidistinguishable if and only if their Gram matrix is "$(n-1)$-incoherent" [RBC+18]. Since numerous properties of $(n-1)$-incoherent states are known [LBT19, LSLL21, LM14a, ZGY21], this provides a wide array of new tools that can be used to investigate antidistinguishability, and we use a result from [JMPP22] to establish our correction to the conjecture. We also establish numerous other necessary and sufficient conditions for antidistinguishability along the way that are of independent interest. Finally, we note that if the Gram matrix is circulant, then we derive an exact characterization of its antidistinguishability.

1.1 Structure of the paper

We start in Section 2 by presenting some mathematical background material that is required to present our results. In particular, we introduce our notation and basics of quantum information theory in Section 2.1, the mathematical basics of antidistinguishability in Section 2.2, Gram matrices in Section 2.3, circulant matrices in Section 2.4, and the concept of $(n-1)$-incoherence in Section 2.5.

We then proceed in Section 3 to establish some of our more technical results. In Section 3.1, we develop a new (somewhat simpler than previously known) semidefinite program for checking antidistinguishability of a set of quantum states that uses the set's Gram matrix as input. We then proceed in Section 3.2 to show that antidistinguishability of a set is equivalent to $(n-1)$-incoherence of its Gram

matrix.

The remaining sections of the paper are devoted to establishing bounds that can be used to determine (non-)antidistinguishability of a set in ways that are simpler to evaluate than semidefinite programs. In Section 4 we re-derive a trivial-to-compute necessary condition for antidistinguishability via our framework. In Section 5 we develop several new trivial-to-compute sufficient conditions for antidistinguishability, including a condition that is both necessary and sufficient for sets of pure states that have a circulant Gram matrix. Finally, we explore the question of how tight the conditions from Sections 4 and 5 are in Section 6.

2 Mathematical preliminaries

We now introduce our notation and the various mathematical tools that we make use of throughout the paper.

2.1 Notation and basics of quantum information theory

Throughout this paper, n and d are positive integers, and $\mathbb{C}^d$ is a finite-dimensional complex Euclidean space with standard basis $\{|0\rangle, |1\rangle, \ldots, |d-1\rangle\}$. We use the notation $\mathrm{Pos}(\mathbb{C}^d)$, $\mathrm{Herm}(\mathbb{C}^d)$, and $\mathrm{U}(\mathbb{C}^d)$ to represent the sets of positive semidefinite (PSD) operators, Hermitian operators, and unitary operators acting on $\mathbb{C}^d$, respectively. If $A, B \in \mathrm{Herm}(\mathbb{C}^d)$ then the notation $A \preceq B$ means that $B - A \in \mathrm{Pos}(\mathbb{C}^d)$. We use $I \in \mathrm{Pos}(\mathbb{C}^d)$ and $O \in \mathrm{Pos}(\mathbb{C}^d)$ for the identity and zero operators acting on $\mathbb{C}^d$ (or I_n and O_n if we want to emphasize their size), respectively. We often represent linear operators as matrices in the usual way via the standard basis but we index their entries starting at 0 (so, for example, we use $A_{0,0} = \langle 0|A|0\rangle$ to denote the $(0,0)$-entry of a matrix A, which is the entry at A's top-left corner).

We provide only the briefest introduction to the mathematics of quantum information theory; the interested reader should pursue any of a number of standard books [NC00, Wat18] for a more thorough treatment of the subject. A *pure quantum state* is a column vector $|\psi\rangle \in \mathbb{C}^d$ with Euclidean norm equal to 1. A *positive operator-valued measure (POVM)* is a set $\{M_i : 0 \leq i \leq n-1\} \subset \mathrm{Pos}(\mathbb{C}^d)$ satisfying

$$\sum_{i=0}^{n-1} M_i = I,$$

and we refer to an individual M_i as a *measurement*.

2.2 Antidistinguishability

For a POVM $\{M_0, M_1, \ldots, M_{n-1}\} \subset \mathrm{Pos}(\mathbb{C}^d)$ and set of pure states $\{|\psi_0\rangle, |\psi_1\rangle, \ldots, |\psi_{n-1}\rangle\} \subset \mathbb{C}^d$, the probability of obtaining outcome $0 \leq i \leq n-1$, given the state $|\psi_i\rangle$, can be calculated by

$$p(i) = \langle \psi_i | M_i | \psi_i \rangle,$$

where $\langle \psi_i|$ is the conjugate transpose of $|\psi_i\rangle$. The set of states is *antidistinguishable* if there exists a POVM such that $\langle \psi_i | M_i | \psi_i \rangle = 0$ for all $0 \leq i \leq n-1$.

Whether a set is antidistinguishable or not can be determined by a semidefinite program (SDP) [BJOP14, RS23]; for a general introduction to semidefinite programming in the context of quantum information theory, see [Wat18], for example. We note here that both the primal and dual problems below share the same optimal objective function values thanks to strong duality and, moreover, both problems attain an optimal solution. In particular, a set is antidistinguishable if and only if the optimal value of the following primal-dual pair of SDPs is equal to 0:

$$
\begin{array}{lll}
\underline{\text{Primal problem}} & & \\
\text{minimize:} & \displaystyle\sum_{i=0}^{n-1} \langle\psi_i|M_i|\psi_i\rangle & \\
\text{subject to:} & \displaystyle\sum_{i=0}^{n-1} M_i = I, & \\
& M_i \in \mathrm{Pos}(\mathbb{C}^d), \quad \forall\, 0 \le i \le n-1 &
\end{array}
\qquad
\begin{array}{ll}
\underline{\text{Dual problem}} & \\
\text{maximize:} & \mathrm{Tr}(Y) \\
\text{subject to:} & Y \succeq |\psi_i\rangle\langle\psi_i| \quad \forall\, 0 \le i \le n-1, \\
& Y \in \mathrm{Herm}(\mathbb{C}^d).
\end{array}
\tag{2}
$$

Slightly more generally, if we divide the optimal value of this SDP by n then we get exactly the minimum probability of incorrectly performing state exclusion on the set (i.e., determining a state from the set that we were *not* given), when the states from the set are provided as input with uniform probability. The set is antidistinguishabile if and only if this optimal probability of being incorrect is 0.

Example 2.1. *Consider the collection* $\{|\psi_0\rangle, |\psi_1\rangle, |\psi_2\rangle\} \subset \mathbb{C}^2$ *of the "trine" states:*

$$|\psi_0\rangle = |0\rangle, \quad |\psi_1\rangle = -\frac{1}{2}\big(|0\rangle + \sqrt{3}|1\rangle\big), \quad |\psi_2\rangle = -\frac{1}{2}\big(|0\rangle - \sqrt{3}|1\rangle\big).$$

This set is well-known to be antidistinguishable [Wei18] but not distinguishable (since the states are not orthogonal). Indeed, a measurement $\{M_0, M_1, M_2\}$ *that antidistinguishes this set comes from simply choosing each* M_i *to be (up to scaling) a rank-*1 *projection onto the orthogonal complement* $|\psi_i^{\perp}\rangle$ *of* $|\psi_i\rangle$*. In particular,*

$$
\begin{aligned}
M_0 &= \frac{2}{3}|\psi_0^{\perp}\rangle\langle\psi_0^{\perp}| = \frac{2}{3}(I - |\psi_0\rangle\langle\psi_0|), \\
M_1 &= \frac{2}{3}|\psi_1^{\perp}\rangle\langle\psi_1^{\perp}| = \frac{2}{3}(I - |\psi_1\rangle\langle\psi_1|), \\
M_2 &= \frac{2}{3}|\psi_2^{\perp}\rangle\langle\psi_2^{\perp}| = \frac{2}{3}(I - |\psi_2\rangle\langle\psi_2|),
\end{aligned}
$$

as illustrated in Figure 1.

Indeed, it is straightforward to check that $M_0 + M_1 + M_2 = I$*, so this measurement is feasible in the primal SDP (2), with orthogonality resulting in an objective value of* 0*. More generally, any collection of* n *pure states in* $\mathbb{C}^2$ *that have* $\frac{1}{n}\sum_{i=0}^{n-1} |\psi_i\rangle\langle\psi_i| = \frac{1}{2}I$ *(i.e., pure states that are "evenly distributed" on the surface of the Bloch sphere) is antidistinguishable, since we can choose measurement operators that are orthogonal to each of them.*

2.3 Gram matrices

The *Gram matrix* of a set $S = \{|\psi_0\rangle, |\psi_1\rangle, \ldots, |\psi_{n-1}\rangle\} \subset \mathbb{C}^d$ is the matrix

$$
G := \begin{bmatrix}
1 & \langle\psi_0|\psi_1\rangle & \langle\psi_0|\psi_2\rangle & \cdots & \langle\psi_0|\psi_{n-1}\rangle \\
\langle\psi_1|\psi_0\rangle & 1 & \langle\psi_1|\psi_2\rangle & \cdots & \langle\psi_1|\psi_{n-1}\rangle \\
\langle\psi_2|\psi_0\rangle & \langle\psi_2|\psi_1\rangle & 1 & \cdots & \langle\psi_2|\psi_{n-1}\rangle \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
\langle\psi_{n-1}|\psi_0\rangle & \langle\psi_{n-1}|\psi_1\rangle & \langle\psi_{n-1}|\psi_2\rangle & \cdots & 1
\end{bmatrix} \in \mathrm{Pos}(\mathbb{C}^n). \tag{3}
$$

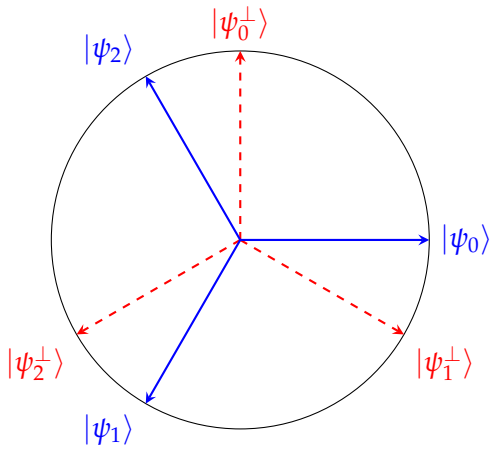

Figure 1: The trine states $\{|\psi_0\rangle, |\psi_1\rangle, |\psi_2\rangle\}$ on the unit circle in $\mathbb{R}^2$, indicated in solid blue above, are antidistinguishable as witnessed by the POVM $M_0 = \frac{2}{3}|\psi_0^\perp\rangle\langle\psi_0^\perp|$, $M_1 = \frac{2}{3}|\psi_1^\perp\rangle\langle\psi_1^\perp|$, $M_2 = \frac{2}{3}|\psi_2^\perp\rangle\langle\psi_2^\perp|$, where $\{|\psi_0^\perp\rangle, |\psi_1^\perp\rangle, |\psi_2^\perp\rangle\}$ are indicated in dashed red.

It is straightforward to see that if $U \in \mathrm{U}(\mathbb{C}^d)$ then $US := \{U|\psi_0\rangle, U|\psi_1\rangle, \ldots, U|\psi_{n-1}\rangle\}$ has the same Gram matrix as S (the converse of this statement is also true, but somewhat less obvious: if two sets of pure states $S, S' \subset \mathbb{C}^d$ have the same Gram matrix then there exists $U \in \mathrm{U}(\mathbb{C}^d)$ such that $S' = US$ [Joh21, Section 2.2.3]).

We can write the Gram matrix succinctly as $G = \sum_{i,j=0}^{n-1} \langle\psi_i|\psi_j\rangle |i\rangle\langle j| = W^*W$, where

$$W := \sum_{k=0}^{n-1} |\psi_k\rangle\langle k| \tag{4}$$

is the $d \times n$ matrix with $|\psi_k\rangle$ as its k-th column. A few properties of this W matrix are convenient for our analysis. Firstly, we have $W|k\rangle = |\psi_k\rangle$ for all $0 \leq k \leq n-1$. Secondly, if the set S is linearly independent, then W has full column rank, in which case there exists an $n \times d$ matrix V such that $VW = I_n$. In particular, this implies $V|\psi_k\rangle = |k\rangle$.

2.4 Circulant matrices

An $n \times n$ matrix G is called *circulant* if there exist scalars $g_0, g_1, \ldots, g_{n-1} \in \mathbb{C}$ so that

$$G = \begin{bmatrix} g_0 & g_1 & g_2 & \cdots & g_{n-2} & g_{n-1} \\ g_{n-1} & g_0 & g_1 & \cdots & g_{n-3} & g_{n-2} \\ g_{n-2} & g_{n-1} & g_0 & \cdots & g_{n-4} & g_{n-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ g_2 & g_3 & g_4 & \cdots & g_0 & g_1 \\ g_1 & g_2 & g_3 & \cdots & g_{n-1} & g_0 \end{bmatrix}.$$

If such a G is positive semidefinite (and thus Hermitian, so $g_j = \overline{g_{n-j}}$ for all $1 \leq j \leq n-1$) with $g_0 = 1$ then it is the Gram matrix of some set of pure states $S = \{|\psi_0\rangle, |\psi_1\rangle, \ldots, |\psi_{n-1}\rangle\}$. In this case, G being circulant corresponds to the inner products of the members of S being invariant under cyclic permutations of the indices: $\langle\psi_i|\psi_j\rangle = \langle\psi_{i+1 \pmod n}|\psi_{j+1 \pmod n}\rangle$ for all i, j. This motivates the following definition:

Definition 2.2. *We say that a set of pure quantum states* $S = \{|\psi_0\rangle, |\psi_1\rangle, \ldots, |\psi_{n-1}\rangle\}$ *is* circulant *if it has either of the following equivalent properties:*

a) The Gram matrix of S *is circulant.*

b) There exists a pure state $|\psi\rangle$ *and a unitary matrix* U *such that* $S = \{|\psi\rangle, U|\psi\rangle, U^2|\psi\rangle, \ldots, U^{n-1}|\psi\rangle\}$.

c) $\langle\psi_i|\psi_j\rangle = \langle\psi_{i+1 \pmod n}|\psi_{j+1 \pmod n}\rangle$ *for all* $0 \leq i, j \leq n-1$.

We note that sets of quantum states with property (b) above are sometimes called *symmetric* [DA12]. The fact that that property is equivalent to property (a) is proved in [DM16, Proposition 3.12], where it was furthermore shown that $|\psi\rangle$ can be chosen to belong to $\mathbb{R}^n$ and have non-negative entries, and U can be chosen to be $U = \operatorname{diag}(1, \omega, \omega^2, \ldots, \omega^{n-1})$, where $\omega = \exp(2\pi i/n)$ is a primitive n-th root of unity.

There are two special matrices that are of particular importance when working with circulant matrices. In particular, we define

$$P := \begin{bmatrix} 0 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & 0 & \cdots & 0 \end{bmatrix} \quad \text{and} \quad F := \frac{1}{\sqrt{n}} \begin{bmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \cdots & \omega^{n-1} \\ 1 & \omega^2 & \omega^4 & \omega^6 & \cdots & \omega^{2(n-1)} \\ 1 & \omega^3 & \omega^6 & \omega^9 & \cdots & \omega^{3(n-1)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{n-1} & \omega^{2(n-1)} & \omega^{3(n-1)} & \cdots & \omega^{(n-1)^2} \end{bmatrix} \tag{5}$$

(P is a cyclic permutation matrix and F is the Fourier matrix). The following characterization of circulant matrices is well-known (see [Dav79], for example):

Proposition 2.3. *Let* G *be an* $n \times n$ *matrix, and let* P *and* F *be as in Equation* (5)*. The following are equivalent:*

a) G *is circulant.*

b) $G = PGP^*$.

c) G *is diagonalized by the Fourier matrix:* $G = FDF^*$ *for some diagonal matrix* D.

Condition (c) of the above proposition is particularly useful for us, as it tells us that we can construct a circulant Gram matrix with any (necessarily non-negative, adding up to n) eigenvalues that we like: just place those eigenvalues along the diagonal of a diagonal matrix D and then $G = FDF^*$ will be a circulant Gram matrix with those eigenvalues.

2.5 $(\mathbf{n-1})$-incoherence

One of our main results is the fact that antidistinguishability of a set of pure states is equivalent to a certain notion from the theory of quantum resources:

Definition 2.4 ([LM14b, SV15])**.** *Let* k *be a positive integer. Then* $X \in \operatorname{Pos}(\mathbb{C}^n)$ *is called* k-incoherent *if there exists a positive integer* m*, a set* $S = \{|\psi_0\rangle, |\psi_1\rangle, \ldots, |\psi_{m-1}\rangle\} \in \mathbb{C}^n$ *with the property that each* $|\psi_i\rangle$ *has at most* k *non-zero entries, and real scalars* $c_0, c_1, \ldots, c_{m-1} \geq 0$ *for which*

$$X = \sum_{i=0}^{m-1} c_i |\psi_i\rangle\langle\psi_i|.$$

Strictly speaking, the term "k-incoherent" is typically only applied to positive semidefinite operators with trace 1. However, the trace does not substantially affect any properties of k-incoherence, and it is more convenient for us to omit the trace restriction. In pure mathematics, a k-incoherent operator is sometimes said to have *factor width at most k* [BCPT05]. Informally, X is k-incoherent exactly when it can be written as a convex combination of positive semidefinite matrices, each of which is identically zero outside of a single $k \times k$ principal submatrix. For example, a positive semidefinite matrix is 1-incoherent if and only if it is diagonal, and every $n \times n$ PSD matrix is n-incoherent.

We are particularly interested in the case when $k = n-1$, so we restrict our attention to $(n-1)$-incoherence for the rest of the paper. When $n = 2$ the $(n-1)$-incoherent operators are (as mentioned earlier) exactly those that are PSD and diagonal. When $n \geq 3$ this set of matrices is somewhat more complicated, but membership in it can be determined efficiently by semidefinite programming [RBC+18]. For example, decompositions like the one below can be found quickly by computer software, thus certifying $(n-1)$-incoherence:

$$\begin{bmatrix} 2 & 1 & 2 \\ 1 & 2 & -1 \\ 2 & -1 & 5 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix} + \begin{bmatrix} 1 & 0 & 2 \\ 0 & 0 & 0 \\ 2 & 0 & 4 \end{bmatrix} + \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & -1 & 1 \end{bmatrix}.$$

The set of all $(n-1)$-incoherent $X \in \mathrm{Pos}(\mathbb{C}^n)$ is a closed convex cone inside the real vector space $\mathrm{Herm}(\mathbb{C}^n)$, so it admits separating hyperplanes. That is, for every $\widetilde{X} \in \mathrm{Pos}(\mathbb{C}^n)$ which is *not* $(n-1)$-incoherent, there exists $Y \in \mathrm{Herm}(\mathbb{C}^n)$ (a separating hyperplane) with the property that $\mathrm{Tr}(XY) \geq 0$ for all $(n-1)$-incoherent $X \in \mathrm{Pos}(\mathbb{C}^n)$ and $\mathrm{Tr}(\widetilde{X}Y) < 0$. The following theorem describes these separating hyperplanes more explicitly:

Definition 2.5 ([BDSS22, JMPP22])**.** *We say that $Y \in \mathrm{Herm}(\mathbb{C}^n)$ is $(n-1)$-*locally PSD *if it has any of the following equivalent properties:*

a) $\mathrm{Tr}(XY) \geq 0$ *for all $(n-1)$-incoherent $X \in \mathrm{Pos}(\mathbb{C}^n)$.*

b) $\langle \psi | Y | \psi \rangle \geq 0$ *for all pure states $|\psi\rangle \in \mathbb{C}^n$ with at most $n-1$ non-zero entries.*

c) Every $(n-1) \times (n-1)$ principal submatrix of Y is positive semidefinite.

In other words, the sets of $(n-1)$-incoherent operators and $(n-1)$-locally PSD operators are dual cones of each other (see [BV04] for an introduction to dual cones). Given an operator $X \in \mathrm{Pos}(\mathbb{C}^n)$ that is not $(n-1)$-incoherent, it is straightforward to use semidefinite programming to find an $(n-1)$-locally PSD operator Y for which $\mathrm{Tr}(XY) < 0$, thus certifying non-$(n-1)$-incoherence of X. For example, if

$$X = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \quad \text{and} \quad Y = \begin{bmatrix} 1 & -1 & -1 \\ -1 & 1 & -1 \\ -1 & -1 & 1 \end{bmatrix}$$

then it is straightforward to show that every $(n-1) \times (n-1) = 2 \times 2$ principal submatrix of Y is PSD, so Y is $(n-1)$-locally PSD, but $\mathrm{Tr}(XY) = -3 < 0$, so X is not $(n-1)$-incoherent (despite being PSD).

We close this section by showing that circulant matrices play particularly well with $(n-1)$-incoherence and $(n-1)$-locally positive semidefiniteness. The following result shows that when investigating $(n-1)$-incoherence of circulant matrices, it suffices to consider $(n-1)$-locally PSD matrices that are also circulant:

Lemma 2.6. *Suppose $X \in \mathrm{Herm}(\mathbb{C}^n)$ is circulant. Then we have that X is $(n-1)$-incoherent if and only if $\mathrm{Tr}(XY) \geq 0$ for all $n \times n$ circulant $(n-1)$-locally PSD matrices Y.*

Proof. The "only if" direction follows immediately from Definition 2.5: if X is $(n-1)$-incoherent then $\mathrm{Tr}(XY) \geq 0$ for *all* (not necessarily circulant) $(n-1)$-locally PSD matrices Y. We thus just need to prove the "if" direction.

To this end, consider the linear map $P_{\mathrm{C}} : \mathrm{Herm}(\mathbb{C}^n) \to \mathrm{Herm}(\mathbb{C}^n)$ defined by

$$P_{\mathrm{C}}(X) \stackrel{\text{def}}{=} \frac{1}{n} \sum_{j=0}^{n-1} P^j X (P^j)^*,$$

where P is the permutation matrix from Equation (5). It is straightforward to show that $P_{\mathrm{C}}(X)$ is circulant for all (not necessarily circulant) $X \in \mathrm{Herm}(\mathbb{C}^n)$. In fact, P_{C} is the orthogonal projection onto the n-dimensional subspace of $\mathrm{Herm}(\mathbb{C}^n)$ consisting of circulant matrices. Furthermore, if X is $(n-1)$-locally PSD then so is each $P^j X (P^j)^*$, so $P_{\mathrm{C}}(X)$ is $(n-1)$-locally PSD too.

Now suppose that X is circulant (so $P_{\mathrm{C}}(X) = X$) and $\mathrm{Tr}(XY) \geq 0$ for all circulant $(n-1)$-locally PSD matrices Y. Then for any (not necessarily circulant) $(n-1)$-locally PSD matrix Z we have

$$\mathrm{Tr}(XZ) = \mathrm{Tr}\left(P_{\mathrm{C}}(X)Z\right) = \mathrm{Tr}\left(XP_{\mathrm{C}}(Z)\right) \geq 0,$$

since $P_{\mathrm{C}}(Z)$ is circulant and $(n-1)$-locally PSD. It follows that X is $(n-1)$-incoherent. □

3 A reduced semidefinite programming formulation and technical results

We now present our technical results and mathematical framework for exploring antidistinguishability.

3.1 An SDP formulation in terms of the Gram matrix

Our first result in this section is an alternate version of the semidefinite program (2) that is typically easier to work with (e.g., for finding explicit optimal solutions). This SDP uses the Gram matrix G of the set of pure states S, rather than the states themselves:

$$\begin{array}{lll}
\underline{\text{Primal problem}} & & \\
\text{minimize:} & \displaystyle\sum_{i=0}^{n-1} \langle i|F_i|i\rangle & \\
\text{subject to:} & \displaystyle\sum_{i=0}^{n-1} F_i = G, & \\
& F_i \in \mathrm{Pos}(\mathbb{C}^n), \quad \forall\, 0 \leq i \leq n-1 &
\end{array}
\qquad
\begin{array}{ll}
\underline{\text{Dual problem}} & \\
\text{maximize:} & \mathrm{Tr}(XG) \\
\text{subject to:} & X \preceq |i\rangle\langle i|, \quad \forall\, 0 \leq i \leq n-1, \\
& X \in \mathrm{Herm}(\mathbb{C}^n).
\end{array}
\tag{6}$$

Before proving that this semidefinite program has the same optimal value as the SDP (2), we note that the primal and dual problems have a zero duality gap. This can be seen by the feasible primal solution $(F_0, F_1, \ldots, F_{n-1}) = (\frac{1}{n}G, \ldots, \frac{1}{n}G)$ and the strictly feasible dual solution $X = -I_n$. This also implies that the optimal value of this SDP is attained in the primal problem (so we do not need to consider sequences of primal feasible solutions converging onto our notion of antidistinguishability).

Theorem 3.1. *The semidefinite programs* (2) *and* (6) *have the same optimal value.*

Proof. Let G be the Gram matrix of the set $S \subset \mathbb{C}^d$, and define W as in Equation (4), so that $G = W^*W$. We prove this theorem by demonstrating a method of converting a feasible point of one SDP into a feasible point of the other SDP with the same objective function value.

If $(M_0, M_1, \ldots, M_{n-1})$ is a feasible point of the SDP (2) then define $F_i = W^* M_i W$ for all indices $0 \leq i \leq n-1$. Then $(F_0, F_1, \ldots, F_{n-1})$ is a feasible point of the SDP (6) since each F_i is positive semidefinite and

$$\sum_{i=0}^{n-1} F_i = \sum_{i=0}^{n-1} W^* M_i W = W^* \left(\sum_{i=0}^{n-1} M_i \right) W = W^* I W = W^* W = G.$$

Furthermore, these feasible points give the same objective values in their respective SDPs since we have $W|i\rangle = |\psi_i\rangle$ and so

$$\sum_{i=0}^{n-1} \langle i | F_i | i \rangle = \sum_{i=0}^{n-1} \langle i | W^* M_i W | i \rangle = \sum_{i=0}^{n-1} \langle \psi_i | M_i | \psi_i \rangle.$$

Conversely, if $(F_0, F_1, \ldots, F_{n-1})$ is a feasible point of the SDP (6) then let $W^\dagger$ be the (Moore–Penrose) pseudoinverse of W and define $M_i = (W^\dagger)^* F_i W^\dagger + \frac{1}{n}(I - WW^\dagger)$ for all $0 \leq i \leq n-1$. Then $(M_0, M_1, \ldots, M_{n-1})$ is a feasible point of the SDP (2) because:

- Each M_i is positive semidefinite. To see this note that $WW^\dagger$ is the orthogonal projection onto $\mathrm{range}(W) = \mathrm{span}(S)$, so $I - WW^\dagger$ is positive semidefinite and thus M_i is as well.
- If we recall the pseudoinverse property $(W^\dagger)^* W^* W = W$ then we see that

$$\begin{aligned}
\sum_{i=0}^{n-1} M_i &= \sum_{i=0}^{n-1} \left((W^\dagger)^* F_i W^\dagger + \frac{1}{n}\left(I - WW^\dagger\right) \right) \\
&= (W^\dagger)^* \left(\sum_{i=0}^{n-1} F_i \right) W^\dagger + \left(I - WW^\dagger\right) \\
&= (W^\dagger)^* G W^\dagger + \left(I - WW^\dagger\right) \\
&= (W^\dagger)^* W^* W W^\dagger + \left(I - WW^\dagger\right) \\
&= WW^\dagger + \left(I - WW^\dagger\right) = I.
\end{aligned}$$

Furthermore, these feasible points give the same objective function values in their respective SDPs since

$$\begin{aligned}
\sum_{i=0}^{n-1} \langle \psi_i | M_i | \psi_i \rangle &= \sum_{i=0}^{n-1} \langle \psi_i | \left((W^\dagger)^* F_i W^\dagger + \frac{1}{n}(I - WW^\dagger) \right) | \psi_i \rangle \\
&= \sum_{i=0}^{n-1} \langle \psi_i | (W^\dagger)^* F_i W^\dagger | \psi_i \rangle \\
&= \sum_{i=0}^{n-1} \langle i | (W^\dagger W)^* F_i (W^\dagger W) | i \rangle \\
&= \sum_{i=0}^{n-1} \langle i | F_i | i \rangle,
\end{aligned}$$

where the final equality follows from $W^\dagger W$ being the orthogonal projection onto $\mathrm{range}(W^*) \supseteq \mathrm{range}(F_i)$, so $(W^\dagger W)^* F_i (W^\dagger W) = F_i$. □

Thanks to the above theorem, the dimension d that the set is embedded in is completely irrelevant when considering the antidistinguishability of pure states; all that matters is how many states there are and their inner products. We thus ignore the dimension d in the remaining sections.

3.2 Antidistinguishability in terms of $(n-1)$-incoherence

We now show that if we only care about antidistinguishability itself, and not the optimal error probability when performing state exclusion, the SDP (6) can be simplified even further, to the point that it coincides with $(n-1)$-incoherence of the states' Gram matrix:

Theorem 3.2. *Let G be the Gram matrix of a set of n pure states. Then the set is antidistinguishable if and only if G is $(n-1)$-incoherent.*

Proof. The primal version of the semidefinite program (6) says that the set of states is antidistinguishable if and only if there exist $F_1, \ldots, F_n \in \mathrm{Pos}(\mathbb{C}^n)$ with $\sum_{i=0}^{n-1} F_i = G$ and $\langle i|F_i|i\rangle = 0$ for all $0 \leq i \leq n-1$. Since $\langle i|F_i|i\rangle = 0$ is equivalent to the i-th row and column of F_i being equal to 0, this is equivalent to $(n-1)$-incoherence of G. □

Thanks to Theorem 3.2, we can now show that a set of pure states is antidistinguishable by finding an $(n-1)$-incoherent decomposition of their Gram matrix G (i.e., a way of writing $G = \sum_i F_i$, where each $F_i \in \mathrm{Pos}(\mathbb{C}^n)$ has at least one row and column equal to 0), and we can show that it is not antidistinguishable by finding an $(n-1)$-locally PSD matrix Y for which $\mathrm{Tr}(YG) < 0$. Both of these tasks can be carried out straightforwardly by semidefinite programming. While we could already determine antidistinguishability via semidefinite programming, this new SDP based on $(n-1)$-incoherence is a bit simpler and lets us derive several new explicit bounds on antidistinguishability in the upcoming sections.

We illustrate how to make use of Theorem 3.2 with an example that determines exactly which equiangular bases of $\mathbb{C}^n$ are antidistinguishable.

Example 3.3. *Let $0 \leq \gamma \leq 1$ be a real number and let $S = \{|\psi_0\rangle, |\psi_1\rangle, \ldots, |\psi_{n-1}\rangle\}$ be such that $\langle\psi_i|\psi_j\rangle = \gamma$ whenever $i \neq j$. In other words, if $\mathbf{1}$ is the all-ones vector then the Gram matrix of S is*

$$G = I + \gamma(\mathbf{1}\mathbf{1}^T - I) = \begin{bmatrix} 1 & \gamma & \gamma & \cdots & \gamma \\ \gamma & 1 & \gamma & \cdots & \gamma \\ \gamma & \gamma & 1 & \cdots & \gamma \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \gamma & \gamma & \gamma & \cdots & 1 \end{bmatrix}.$$

We claim that S is antidistinguishable if and only if $\gamma \leq (n-2)/(n-1)$. To demonstrate this claim, we show that G is $(n-1)$-incoherent if and only if $\gamma \leq (n-2)/(n-1)$ and then apply Theorem 3.2.

To verify that S is antidistinguishable when $\gamma \leq (n-2)/(n-1)$, define

$$F_i := \left(\frac{1}{n-1} - \frac{\gamma}{n-2}\right)\left(I - |i\rangle\langle i|\right) + \frac{\gamma}{n-2}\left(\mathbf{1} - |i\rangle\right)\left(\mathbf{1} - |i\rangle\right)^T \quad \text{for all} \quad 0 \leq i \leq n-1.$$

It is clear that $F_i \in \mathrm{Pos}(\mathbb{C}^n)$ for all i (since $\gamma \leq (n-2)/(n-1)$), and direct calculation shows that

$$\begin{aligned} \sum_{i=1}^n F_i &= \sum_{i=1}^n \left(\left(\frac{1}{n-1} - \frac{\gamma}{n-2}\right)\left(I - |i\rangle\langle i|\right) + \frac{\gamma}{n-2}\left(\mathbf{1} - |i\rangle\right)\left(\mathbf{1} - |i\rangle\right)^T\right) \\ &= \left(1 - \frac{\gamma(n-1)}{n-2}\right) I + \gamma\left(\mathbf{1}\mathbf{1}^T + \frac{1}{n-2} I\right) \\ &= G. \end{aligned} \tag{7}$$

It follows that G is $(n-1)$-incoherent, since each F_i has its i-th row and column equal to 0 (i.e., Equation (7) is a decomposition of G into a sum of $(n-1)\times(n-1)$ PSD blocks).

Now suppose that $\gamma > (n-2)/(n-1)$. To verify that S is not antidistinguishable, let

$$X = (n-2)I - (\mathbf{1}\mathbf{1}^T - I).$$

Since each $(n-1)\times(n-1)$ principal submatrix of X is diagonally dominant, X is $(n-1)$-locally PSD. However,

$$\begin{aligned}\operatorname{Tr}(XG) &= \operatorname{Tr}\Big(\big((n-2)I - (\mathbf{1}\mathbf{1}^T - I)\big)\big(I + \gamma(\mathbf{1}\mathbf{1}^T - I)\big)\Big)\\ &= n(n-2) - n(n-1)\gamma,\end{aligned}$$

which is strictly negative (since $\gamma > (n-2)/(n-1)$). It follows that G is not $(n-1)$-incoherent.

The above calculation shows that the SDP (6) has its optimal value equal to 0 if and only if we have $\gamma \leq (n-2)/(n-1)$. By simply running that SDP numerically (and dividing the result by n), we can furthermore find the optimal (i.e., minimal) error probability when performing state exclusion on this set of states, which is plotted in Figure 2.

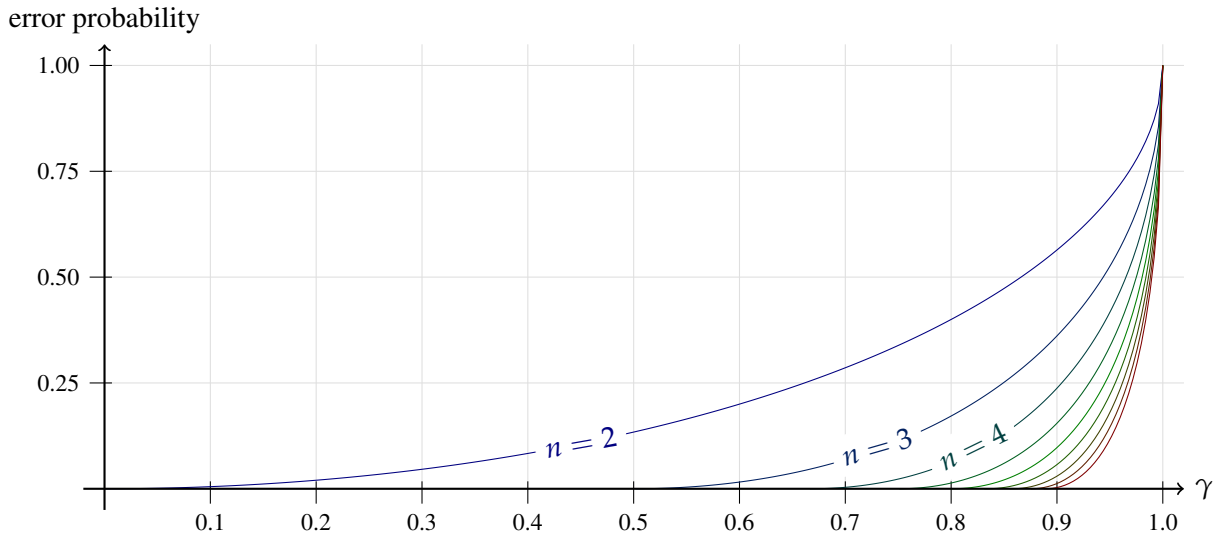

Figure 2: Plot of the relationship between γ and the optimal error probability when performing state exclusion on the set of states described by Example 3.3, for $2 \leq n \leq 10$. This error probability equals 0 if and only if the set is antidistinguishable, which happens exactly when $\gamma \leq (n-2)/(n-1)$.

4 Necessary conditions for antidistinguishability

While antidistinguishability of a set can be checked via semidefinite programming, it is useful to have necessary and/or sufficient conditions for antidistinguishability that are even easier to make use of (e.g., conditions that rely only on elementary linear algebra, or on quantities that have a natural physical interpretation). In this section, we present a pair of necessary conditions for antidistinguishability that involve just inequalities of the inner products of the pure states. In particular, if these inner products are sufficiently large then the set cannot be antidistinguishable:

Theorem 4.1. *Let $n \geq 2$ be an integer and let $S = \{|\psi_0\rangle, |\psi_1\rangle, \ldots, |\psi_{n-1}\rangle\}$. If*

$$\sum_{i \neq j = 0}^{n-1} \big|\langle \psi_i | \psi_j \rangle\big| > n(n-2) \tag{8}$$

then S is not antidistinguishable.

We note that the above theorem was originally proved in [BJOP14], but the proof is rather long and technical. We re-prove it here via Theorem 3.2 in just a couple of lines, to demonstrate how simple antidistinguishability is to work with via our $(n-1)$-incoherence machinery:

Proof of Theorem 4.1. This result follows via an argument that is similar to the one used in the latter half of Example 3.3. Define

$$Y = (n-1)I - E,$$

where, for all $0 \leq i, j \leq n-1$ (even if $i = j$), the (i, j)-entry of E is the complex number with modulus 1 and phase equal to that of $\langle \psi_i | \psi_j \rangle$. Since each $(n-1) \times (n-1)$ principal submatrix of Y is diagonally dominant, Y is $(n-1)$-locally PSD. However,

$$\mathrm{Tr}(YG) = \mathrm{Tr}\Big(\big((n-1)I - E\big)G\Big) = n(n-2) - \sum_{i \neq j = 0}^{n-1} \big|\langle \psi_i | \psi_j \rangle\big|,$$

which is strictly negative whenever Inequality (8) holds. It follows that G is not $(n-1)$-incoherent, so Theorem 3.2 tells us that S is not antidistinguishable. □

By noting that there are $n(n-1)$ terms in the sum (8), the above theorem immediately implies the following special case:

Corollary 4.2. *Let $n \geq 2$ be an integer and let $S = \{|\psi_0\rangle, |\psi_1\rangle, \ldots, |\psi_{n-1}\rangle\}$. If*

$$\big|\langle \psi_i | \psi_j \rangle\big| > \frac{n-2}{n-1} \quad \text{for all} \quad 0 \leq i \neq j \leq n-1 \tag{9}$$

then S is not antidistinguishable.

We note that Example 3.3 demonstrates that the inequalities described by Theorem 4.1 and Corollary 4.2 are both tight: for all n, there is an antidistinguishable set with $\big|\langle \psi_i | \psi_j \rangle\big| = (n-2)/(n-1)$ and thus $\sum_{i \neq j = 0}^{n-1} \big|\langle \psi_i | \psi_j \rangle\big| = n(n-2)$. In the $n = 3$ case, the trine states from Example 2.1 also demonstrate tightness of these bounds, as they are antidistinguishable with $\big|\langle \psi_i | \psi_j \rangle\big| = (n-2)/(n-1) = 1/2$ for all $i \neq j$.

5 Sufficient conditions for antidistinguishability

We now present some sufficient conditions for antidistinguishability that are simpler to make use of than any of the semidefinite programs that we have described. Much like the results of Section 4 showed that if the states' inner products are sufficiently large then the set cannot be antidistinguishable, in this section we show that if the inner products are sufficiently small then the set *must* be antidistinguishable. In particular, one of these sufficient conditions (Corollary 5.5) can be thought of as a "corrected version" of the recently-disproved conjecture from [HB20]. For completeness, we state this conjecture here:

Conjecture 5.1 ([HB20]). *Let $n \geq 2$ be an integer and let $S = \{|\psi_0\rangle, |\psi_1\rangle, \ldots, |\psi_{n-1}\rangle\}$. If*

$$\big|\langle\psi_i|\psi_j\rangle\big| \leq \frac{n-2}{n-1} \quad \text{for all} \quad 0 \leq i \neq j \leq n-1 \tag{10}$$

then S is antidistinguishable.

As our first step towards correcting this conjecture (in particular, placing a correct quantity on the right-hand-side of Inequality (10)), we present a sufficient condition for antidistinguishability in terms of the eigenvalues of the set's Gram matrix. Remarkably, this sufficient condition is also necessary for circulant sets:

Theorem 5.2. *Let $n \geq 2$ be an integer and let $G \in \mathrm{Pos}(\mathbb{C}^n)$ be the Gram matrix of a set S of n pure states, and let $\lambda_0 \geq \lambda_1 \geq \cdots \geq \lambda_{n-1}$ be the eigenvalues of G. If*

$$\sqrt{\lambda_0} \leq \sum_{j=1}^{n-1} \sqrt{\lambda_j} \tag{11}$$

then S is antidistinguishable. Furthermore, if G is circulant then Inequality (11) is both necessary and sufficient for the antidistinguishability of S.

Proof. Define $q := \sum_{j=1}^{n-1} \sqrt{\lambda_j}$ and suppose that $\sqrt{\lambda_0} \leq q$. Our goal is to show that S is antidistinguishable. It was shown in [JMPP22, Theorem 8] that if there exists a real matrix $\Lambda \in \mathrm{Pos}(\mathbb{R}^n)$ such that

$$\lambda_0 = -\Lambda_{0,0} - \sum_{i=1}^{n-1} (\Lambda_{0,i} + \Lambda_{i,0}) \quad \text{and} \quad \lambda_j = \Lambda_{j,j} \quad \text{for } 1 \leq j \leq n-1 \tag{12}$$

then G is $(n-1)$-incoherent, so (by Theorem 3.2) S is antidistinguishable. It thus suffices to find such a Λ.

To this end, define a vector $\mathbf{v} \in \mathbb{R}^n$ by

$$v_0 = -q - \sqrt{q^2 - \lambda_0} \quad \text{and} \quad v_j = \sqrt{\lambda_j} \quad \text{for } 1 \leq j \leq n-1$$

(the hypothesis $\sqrt{\lambda_0} \leq q$ was used here to ensure that v_0 is real). It is then straightforward to check that the positive semidefinite matrix $\Lambda = \mathbf{v}\mathbf{v}^T$ satisfies Equation (12), which completes the proof that Inequality (11) implies antidistinguishability of S.

For the "furthermore" statement, suppose that G is circulant. Our goal is to show that S being antidistinguishable is equivalent to Inequality (11) holding. To this end, recall from Theorem 3.2 that S is antidistinguishable if and only if G is $(n-1)$-incoherent, which (by Lemma 2.6) is equivalent to

$$\mathrm{Tr}(GY) \geq 0 \tag{13}$$

for all circulant $(n-1)$-locally PSD matrices Y. Well, Proposition 2.3(c) tells us that a matrix Y is circulant if and only if $Y = F\mathrm{diag}(\mathbf{d})F^*$, where $\mathbf{d}$ is the vector of eigenvalues of Y. Furthermore, it was shown in [JMPP22, Theorem 2] that a circulant matrix Y is $(n-1)$-locally PSD if and only if $S_k(\mathbf{d}) \geq 0$ for all $1 \leq k \leq n-1$, where S_k is the k-th elementary symmetric polynomial

$$S_k(\mathbf{d}) := \sum_{0 \leq j_1 < \cdots < j_k < n} d_{j_1} d_{j_2} \cdots d_{j_k}.$$

Since G is circulant, we can write $G = F\mathrm{diag}(\boldsymbol{\lambda})F^*$ for some vector $\boldsymbol{\lambda} = (\lambda_0, \lambda_1, \ldots, \lambda_{n-1})$ whose entries are the eigenvalues of G. It follows that Inequality (13) is equivalent to

$$0 \leq \mathrm{Tr}(GY) = \mathrm{Tr}\left((F\mathrm{diag}(\boldsymbol{\lambda})F^*)(F\mathrm{diag}(\mathbf{d})F^*)\right) = \mathrm{Tr}\left(\mathrm{diag}(\boldsymbol{\lambda})\mathrm{diag}(\mathbf{d})\right) = \boldsymbol{\lambda} \cdot \mathbf{d}.$$

In other words, S is antidistinguishable if and only if $\boldsymbol{\lambda}$ is in the dual cone of the set of vectors $\mathbf{d}$ satisfying $S_k(\mathbf{d}) \geq 0$ for all $1 \leq k \leq n-1$. This dual cone was characterized in [Zin08, Proposition 4.2], and $\boldsymbol{\lambda}$ being in this dual cone implies the existence of $\Lambda \in \mathrm{Pos}(\mathbb{R}^n)$ satisfying Equation (12). Since Λ is positive semidefinite, so are all of its 2×2 principal submatrices, so $\Lambda_{0,0}\Lambda_{j,j} \geq \Lambda_{0,j}^2$ for all $1 \leq j \leq n-1$. Substituting this into Equation (12) gives

$$\Lambda_{0,0} = -\lambda_0 - 2\sum_{j=1}^{n-1} \Lambda_{0,j} \leq -\lambda_0 + 2\sqrt{\Lambda_{0,0}} \sum_{j=1}^{n-1} \sqrt{\lambda_j}.$$

This is a quadratic inequality in $\sqrt{\Lambda_{0,0}}$, which (via the discriminant of the quadratic formula) has a real solution if and only if

$$\left(\sum_{j=1}^{n-1} \sqrt{\lambda_j}\right)^2 - \lambda_0 \geq 0,$$

which implies $\sqrt{\lambda_0} \leq \sum_{j=1}^{n-1} \sqrt{\lambda_j}$. □

Remark 5.3. *The proof of Theorem 5.2 shows something that was overlooked in [Zin08, JMPP22]: the existence of $\Lambda \in \mathrm{Pos}(\mathbb{R}^n)$ satisfying the constraints (12) can be determined without semidefinite programming. Inequality (11) is both necessary and sufficient for the existence of such a Λ.*

Our first corollary of Theorem 5.2 gives a sufficient condition for antidistinguishability in terms of the Frobenius norm $\|G\|_{\mathrm{F}}$ of G, which is slightly easier to compute than its eigenvalues.

Corollary 5.4. *Let $n \geq 2$ be an integer and let G be the Gram matrix of a set S of n pure states. If*

$$\|G\|_{\mathrm{F}} \leq \frac{n}{\sqrt{2}}$$

then S is antidistinguishable.

It is perhaps worth noting that for all Gram matrices G we have $\sqrt{n} \leq \|G\|_{\mathrm{F}} \leq n$, with the lower bound being saturated when the states in the set are mutually orthogonal and the upper bound being saturated when the states in the set are all equal to each other. Corollary 5.4 thus says that if the states in a set are "close enough" to being mutually orthogonal then they must be antidistinguishable.

Proof of Corollary 5.4. Define $x_j = \sqrt{\lambda_j / n}$ for all $0 \leq j \leq n-1$, so that the conditions $\mathrm{Tr}(G) = n$ and $\|G\|_{\mathrm{F}} \leq n/\sqrt{2}$ are equivalent to

$$\sum_{j=0}^{n-1} x_j^2 = 1 \quad \text{and} \quad \sum_{j=0}^{n-1} x_j^4 \leq \frac{1}{2}, \tag{14}$$

respectively. If we can show that these conditions imply $\sqrt{\lambda_0} \leq \sum_{j=1}^{n-1} \sqrt{\lambda_j}$ (i.e., $x_0 \leq \sum_{j=1}^{n-1} x_j$) then Theorem 5.2 will imply the present corollary.

To this end, we note that the constraints (14) imply $x_0^2 = 1 - \sum_{j=1}^{n-1} x_j^2$ and thus

$$\left(1 - \sum_{j=1}^{n-1} x_j^2\right)^2 + \sum_{j=1}^{n-1} x_j^4 \leq \frac{1}{2}.$$

Multiplying through by 2 and rearranging slightly shows that the above inequality is equivalent to

$$\left(1 - 2\sum_{j=1}^{n-1} x_j^2\right)^2 \leq 4 \sum_{\substack{i,j=1 \\ i>j}}^{n-1} x_i^2 x_j^2.$$

Using the fact that $1 = \sum_{j=0}^{n-1} x_j^2$ on the left-hand-side, and then square-rooting both sides (noting that the right-hand-side is non-negative, so the direction of the inequality is preserved) then shows that

$$x_0^2 - \sum_{j=1}^{n-1} x_j^2 \leq 2\sqrt{\sum_{\substack{i,j=1 \\ i>j}}^{n-1} x_i^2 x_j^2} \leq 2 \sum_{\substack{i,j=1 \\ i>j}}^{n-1} x_i x_j, \tag{15}$$

where the second inequality follows since the 2-norm is at most the 1-norm. In particular, the outermost inequality in (15) can be rearranged as

$$x_0^2 \leq \sum_{j=1}^{n-1} x_j^2 + 2 \sum_{\substack{i,j=1 \\ i>j}}^{n-1} x_i x_j,$$

which can be factored as

$$x_0^2 \leq \left(\sum_{j=1}^{n-1} x_j\right)^2.$$

This implies $x_0 \leq \sum_{j=1}^{n-1} x_j$, as desired. □

Our final sufficient condition for antidistinguishability arises simply by noting that if each off-diagonal entry of a Gram matrix G has $|g_{i,j}| \leq \sqrt{(n-2)/(2n-2)}$, then $\|G\|_{\mathrm{F}} \leq n/\sqrt{2}$, so Corollary 5.4 tells us that the set is antidistinguishable. In other words, we have the following corrected version of Conjecture 5.1:

Corollary 5.5. *Let $n \geq 2$ be an integer and let $S = \{|\psi_0\rangle, |\psi_1\rangle, \ldots, |\psi_{n-1}\rangle\}$. If*

$$\left|\langle\psi_i|\psi_j\rangle\right| \leq \frac{1}{\sqrt{2}}\sqrt{\frac{n-2}{n-1}} \quad \textit{for all} \quad 0 \leq i \neq j \leq n-1 \tag{16}$$

then S is antidistinguishable.

6 Tightness of these bounds

We already noted that the bounds of Section 4 are tight, as demonstrated by Example 3.3 (which is circulant). The bound of Theorem 5.2 is also tight, as demonstrated by the fact that it is both necessary and

sufficient for circulant matrices. Corollary 5.4 can also be seen to be tight via circulant matrices: if $\varepsilon > 0$ is small and G is a circulant Gram matrix with eigenvalues $\lambda_0 = n/2 + \varepsilon$, $\lambda_1 = n/2 - \varepsilon$, and $\lambda_j = 0$ for $j \geq 2$, then

$$\sum_{j=1}^{n-1} \sqrt{\lambda_j} = \sqrt{\frac{n}{2} - \varepsilon} < \sqrt{\frac{n}{2} + \varepsilon} = \sqrt{\lambda_0},$$

so any set of pure states with Gram matrix G must not be antidistinguishable, by Theorem 5.2. However, in this case, we also have

$$\|G\|_{\mathrm{F}} = \sqrt{\left(\frac{n}{2} + \varepsilon\right)^2 + \left(\frac{n}{2} - \varepsilon\right)^2} = \sqrt{\frac{n^2}{2} + 2\varepsilon^2} \leq \frac{n}{\sqrt{2}} + \sqrt{2}\varepsilon,$$

demonstrating that the quantity $n/\sqrt{2}$ in Corollary 5.4 cannot be increased at all.

The only question remaining is whether or not the bound established by Corollary 5.5 is also tight. It is trivially tight when $n = 2$ or $n = 3$ since it matches the corresponding necessary condition provided by Corollary 4.2. The situation is less clear when $n \geq 4$, since when $n = 4$, for example, we have the following situation:

- If $|\langle \psi_i | \psi_j \rangle| > 2/3 \approx 0.6667$ for all $i \neq j$ then the set is not antidistinguishable (Corollary 4.2).
- If $|\langle \psi_i | \psi_j \rangle| \leq 2/3$ for all $i \neq j$ then the set *may* be antidistinguishable (Example 3.3), so Corollary 4.2 is tight.
- If $|\langle \psi_i | \psi_j \rangle| \leq 1/\sqrt{3} \approx 0.5774$ for all $i \neq j$ then the set is antidistinguishable (Corollary 5.5).
- It is currently only known that the set *may* not be antidistinguishable when $|\langle \psi_i | \psi_j \rangle| > 0.6451$ [RS23]. Our next example improves this bound to $1/\sqrt{3}$, thus showing that Corollary 5.5 is tight, at least when $n = 4$:

Example 6.1. *Let $c = 1/\sqrt{3}$ and consider the matrix*

$$G := \begin{bmatrix} 1 & c & c & c \\ c & 1 & ci & (1+ci)/2 \\ c & -ci & 1 & (1-ci)/2 \\ c & (1-ci)/2 & (1+ci)/2 & 1 \end{bmatrix}.$$

It is straightforward to check that G is positive semidefinite and is thus the Gram matrix of some set S of $n = 4$ pure states. Since $|g_{i,j}| = 1/\sqrt{3}$ for all $i \neq j$, Corollary 5.5 tells us that S is antidistinguishable.

Now let $\varepsilon > 0$ be small, let $\mathbf{v} = [1, (-\sqrt{3}+i)/2, (-\sqrt{3}-i)/2, 0]^T$ and $\mathbf{w} = [0,0,0,1]^T$, and define

$$G_\varepsilon = \frac{1}{1-2\varepsilon}\big(G + \varepsilon(\mathbf{v}\mathbf{v}^* + \mathbf{w}\mathbf{w}^* - 3I)\big).$$

A straightforward computation shows that G_ε is positive semidefinite if $0 < \varepsilon < 1/10$ and its diagonal entries all equal 1, so it is the Gram matrix of some set S_ε of $n = 4$ pure states. Furthermore, $\lim_{\varepsilon \to 0^+} G_\varepsilon = G$, so the inner products of the members of S_ε can be made to have modulus as close to $1/\sqrt{3}$ as we like by choosing $\varepsilon > 0$ sufficiently small.

We claim that G_ε is not $(n-1) = 3$-incoherent, so (by Theorem 3.2), S_ε is not antidistinguishable. To verify this claim, we need to find a 3-locally PSD matrix X for which $\mathrm{Tr}(XG_\varepsilon) < 0$. To this end, consider

the matrices

$$Y = \begin{bmatrix} 2 & -\sqrt{3}-i & -\sqrt{3}+i & 0 \\ -\sqrt{3}+i & 2 & 1-\sqrt{3}i & 0 \\ -\sqrt{3}-i & 1+\sqrt{3}i & 2 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \quad \textit{and}$$

$$Z = \begin{bmatrix} 0 & 1+\sqrt{3}i & 1-\sqrt{3}i & -2 \\ 1-\sqrt{3}i & 0 & -\sqrt{3}+i & -\sqrt{3}-i \\ 1+\sqrt{3}i & -\sqrt{3}-i & 0 & -\sqrt{3}+i \\ -2 & -\sqrt{3}+i & -\sqrt{3}-i & 2\sqrt{3}(1+5\varepsilon) \end{bmatrix}.$$

The following claims are all straightforward (albeit somewhat tedious) to verify:

- $\mathrm{Tr}(YG_\varepsilon) = 0$ *for all* $0 < \varepsilon < 1/2$.
- $\mathrm{Tr}(ZG_\varepsilon) = -(20\sqrt{3})\varepsilon^2/(1-2\varepsilon) < 0$ *for all* $0 < \varepsilon < 1/2$.
- *The matrix* $X = Y + \delta Z$ *is* 3*-locally PSD when* $0 < \varepsilon < 1/2$ *and* $0 < \delta \leq 5\sqrt{3}\varepsilon/(1+5\varepsilon)$.

It follows that, for these choices of δ *and* ε*,* X *is a* 3*-locally positive semidefinite matrix with*

$$\mathrm{Tr}(XG_\varepsilon) = -(20\sqrt{3})\delta\varepsilon^2/(1-2\varepsilon) < 0,$$

proving our claim.

We summarize the above example and related theorems in Figure 3.

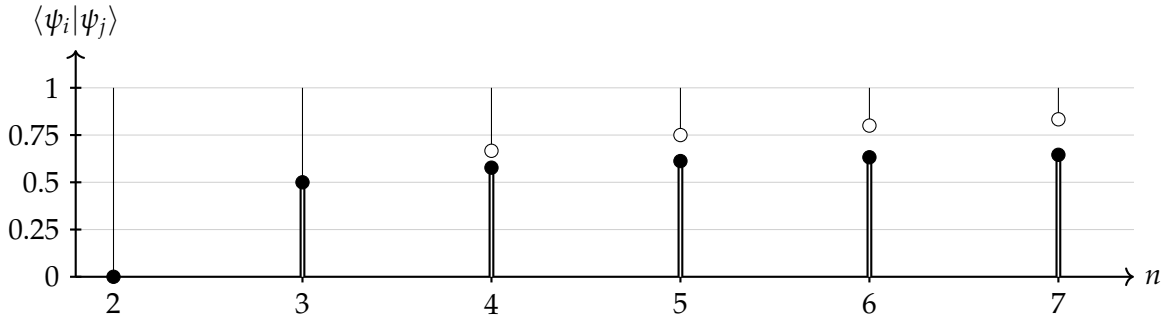

Figure 3: How inner products between n pure states determine their antidistinguishability. If all inner products are on or below the filled-in circles then the states are antidistinguishable (Corollary 5.5) and if all inner products are strictly above the hollow circles then the states are not antidistinguishable (Corollary 4.2). In between those circles, the states might be antidistinguishable (Example 3.3), and when $n = 4$ at least they might also be not antidistinguishable (Example 6.1).

We still do not know whether or not Corollary 5.5 is tight when $n \geq 5$. The difficulty here is that the circulant matrices that we used to show that Corollary 5.4 is tight only have the property that their off-diagonal entries all have absolute value equal to each other when $n \leq 3$. When $n \geq 4$ we must explore non-circulant matrices like the one from Example 6.1, and this seems much more difficult.

Software. Companion software that implements the SDPs from Equation (2) in addition to Examples 2.1, 3.3, and 6.1 can be found at the GitHub repository [JRS23]. This repository contains Python code that

makes use of the toqito quantum information package [Rus21] as well as the PICOS package [SS22] which invokes the CVXOPT solver [ADV20] for solving the SDPs.

Acknowledgements. The authors thank Mark Hamilton, who provided a key insight that significantly simplified the proof of Theorem 5.2, as well as Debbie Leung, Robert Spekkens, Iman Marvian, and Vojtěch Havlíček for helpful conversations. N.J. was supported by NSERC Discovery Grant RGPIN-2022-04098. J.S. is partially supported by Commonwealth Cyber Initiative SWVA grant 467489.

References

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

[ASR+21] Ryan Amiri, Robert Stárek, David Reichmuth, Ittoop V. Puthoor, Michal Mičuda, Jr. Mišta, Ladislav, Miloslav Dušek, Petros Wallden, and Erika Andersson. Imperfect 1-Out-of-2 Quantum Oblivious Transfer: Bounds, a Protocol, and its Experimental Implementation. *PRX Quantum*, 2(1):010335, March 2021.

[BC09] Stephen M Barnett and Sarah Croke. Quantum state discrimination. *Advances in Optics and Photonics*, 1(2):238–278, 2009.

[BCPT05] E. G. Boman, D. Chen, O. Parekh, and S. Toledo. On factor width and symmetric H-matrices. *Linear Algebra and its Applications*, 405:239–248, 2005.

[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.

[BDSS22] Grigoriy Blekherman, Santanu S Dey, Kevin Shu, and Shengding Sun. Hyperbolic relaxation of k-locally positive semidefinite matrices. *SIAM Journal on Optimization*, 32(2):470–490, 2022.

[Ber10] János A Bergou. Discrimination of quantum states. *Journal of Modern Optics*, 57(3):160–180, 2010.

[BJOP14] Somshubhro Bandyopadhyay, Rahul Jain, Jonathan Oppenheim, and Christopher Perry. Conclusive exclusion of quantum states. *Physical Review A*, 89(2):022336, February 2014.

[BK15] Joonwoo Bae and Leong-Chuan Kwek. Quantum state discrimination and its applications. *Journal of Physics A: Mathematical and Theoretical*, 48(8):083001, 2015.

[BV04] S. Boyd and L. Vandenberghe. *Convex Optimization*. Cambridge University Press, 2004.

[CFS02] Carlton M. Caves, Christopher A. Fuchs, and Rüdiger Schack. Conditions for compatibility of quantum-state assignments. *Physical Review A*, 66(6):062111, December 2002.

[Che00] Anthony Chefles. Quantum state discrimination. *Contemporary Physics*, 41(6):401–424, 2000.

[DA12] Vedran Dunjko and Erika Andersson. Transformations between symmetric sets of quantum states. *Journal of Physics A: Mathematical and Theoretical*, 45(36):365304, aug 2012.

[Dav79] P.J. Davis. *Circulant Matrices*. Monographs and textbooks in pure and applied mathematics. Wiley, 1979.

[DM16] Louis Deaett and Seth A. Meyer. The minimum rank problem for circulants. *Linear Algebra and its Applications*, 491:386–418, 2016. Proceedings of the 19th ILAS Conference, Seoul, South Korea 2014.

[DWA14] Vedran Dunjko, Petros Wallden, and Erika Andersson. Quantum digital signatures without quantum memory. *Physical Review Letters*, 112(4):040502, 2014.

[GKR+01] Sibasish Ghosh, Guruprasad Kar, Anirban Roy, Aditi Sen, and Ujjwal Sen. Distinguishability of Bell states. *Physical Review Letters*, 87(27):277902, 2001.

[HB20] Vojtvech Havlívcek and Jonathan Barrett. Simple communication complexity separation from quantum state antidistinguishability. *Physical Review Research*, 2(1):013326, 2020.

[HK18] Teiko Heinosaari and Oskari Kerppo. Antidistinguishability of pure quantum states. *Journal of Physics A: Mathematical and Theoretical*, 51(36):365303, 2018.

[HK19] Teiko Heinosaari and Oskari Kerppo. Communication of partial ignorance with qubits. *Journal of Physics A: Mathematical and Theoretical*, 52(39):395301, 2019.

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

[JMPP22] Nathaniel Johnston, Shirin Moein, Rajesh Pereira, and Sarah Plosker. Absolutely k-incoherent quantum states and spectral inequalities for factor width of a matrix. *Physical Review A*, 106:052417, 2022.

[Joh21] N. Johnston. *Advanced Linear and Matrix Algebra*. Springer, 2021.

[JRS23] Nathaniel Johnston, Vincent Russo, and Jamie Sikora. circulant_antidist: A Python toolkit for studying the antidistinguishability of circulant pure states. https://github.com/vprusso/circulant_antidist, July 2023.

[LBT19] Z.W. Liu, K. Bu, and R. Takagi. One-shot operational quantum resource theory. *Physical Review Letters*, 123(2):020401, 2019.

[Lei14] Matthew Saul Leifer. Is the quantum state real? An extended review of ψ-ontology theorems. *arXiv preprint arXiv:1409.1570*, 2014.

[LM14a] F. Levi and F. Mintert. A quantitative theory of coherent delocalization. *New Journal of Physics*, 16(3):033007, 2014.

[LM14b] Federico Levi and Florian Mintert. A quantitative theory of coherent delocalization. *New Journal of Physics*, 16(3):033007, mar 2014.

[LSLL21] J.W. Liu, S.Q. Shen, M. Li, and L. Li. Lower bounds for the robustness of multilevel coherence. *International Journal of Theoretical Physics*, 60(5):1712–1719, 2021.

[MNW23] Hemant K Mishra, Michael Nussbaum, and Mark M Wilde. On the optimal error exponents for classical and quantum antidistinguishability. *arXiv preprint arXiv:2309.03723*, 2023.

[MW14a] Alberto Montina and Stefan Wolf. Lower bounds on the communication complexity of two-party (quantum) processes. In *2014 IEEE International Symposium on Information Theory*, pages 1484–1488. IEEE, 2014.

[MW14b] Alberto Montina and Stefan Wolf. Necessary and sufficient optimality conditions for classical simulations of quantum communication processes. *Physical Review A*, 90(1):012309, 2014.

[NC00] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[PBR12] Matthew F Pusey, Jonathan Barrett, and Terry Rudolph. On the reality of the quantum state. *Nature Physics*, 8(6):475–478, 2012.

[PJO15] Christopher Perry, Rahul Jain, and Jonathan Oppenheim. Communication tasks with infinite quantum-classical separation. *Physical Review Letters*, 115(3):030504, 2015.

[QL10] Daowen Qiu and Lvjun Li. Minimum-error discrimination of quantum states: Bounds and comparisons. *Physical Review A*, 81(4):042329, 2010.

[RBC+18] M. Ringbauer, T. R. Bromley, M. Cianciaruso, L. Lami, W. Y..S. Lau, G. Adesso, A. G. White, A. Fedrizzi, and M. Piani. Certification and quantification of multilevel quantum coherence. *Physical Review X*, 8:041007, 2018.

[RS23] Vincent Russo and Jamie Sikora. Inner products of pure states and their antidistinguishability. *Physical Review A*, 107(3), 2023.

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

[SBC+16] Gael Sentís, Emilio Bagan, John Calsamiglia, Giulio Chiribella, and Ramon Munoz-Tapia. Quantum change point. *Physical Review Letters*, 117(15):150502, 2016.

[SCMT17] Gael Sentís, John Calsamiglia, and Ramon Munoz-Tapia. Exact identification of a quantum change point. *Physical Review Letters*, 119(14):140506, 2017.

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

[SV15] J Sperling and W Vogel. Convex ordering and quantification of quantumness. *Physica Scripta*, 90(7):074024, jun 2015.

[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.

[Wat05] John Watrous. Bipartite subspaces having no bases distinguishable by local operations and classical communication. *Physical Review Letters*, 95(8):080505, 2005.

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

[Wei18] Graeme Weir. *Optimal discrimination of quantum states*. PhD thesis, University of Glasgow, 2018.

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

[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.

[ZGY21] L. M. Zhang, T. Gao, and F. L. Yan. Transformations of multilevel coherent states under coherence-preserving operations. *Science China Physics, Mechanics & Astronomy*, 64(6):1–6, 2021.

[Zin08] Y. Zinchenko. On hyperbolicity cones associated with elementary symmetric polynomials. *Optimization Letters*, 2:389–402, 2008.