Simple communication complexity separation from quantum state antidistinguishability

Vojtěch Havlíček* and Jonathan Barrett

Department of Computer Science, University of Oxford, Wolfson Building, Parks Road, Oxford OX1 3QD, United Kingdom

(Received 27 November 2019; accepted 15 February 2020; published 17 March 2020)

A set of n pure quantum states is called antidististinguishable if there exists an n-outcome measurement that never outputs the outcome 'k' on the kth quantum state. We describe sets of quantum states for which any subset of three states is antidistinguishable and use this to produce a two-player communication task that can be solved with $\log d$ qubits, but requires one-way communication of at least $\log(4/3)(d-1)-1 \approx 0.415(d-1)-1$ classical bits. The advantages of the approach are that the proof is simple and self-contained – not needing, for example, to rely on hard-to-establish prior results in combinatorics – and that with slight modifications, nontrivial bounds can be established in any dimension $\geqslant 3$. The task can be framed in terms of the separated parties solving a relation. We show, however, that for this particular task, the separation disappears if two-way classical communication is allowed, or if the task need only be solved with bounded error. Finally, we state a conjecture regarding antidistinguishability of sets of states, and provide some supporting numerical evidence. If the conjecture holds, then there is a two-player communication task that can be solved with $\log d$ qubits, but requires exact one-way communication of $\Omega(d \log d)$ classical bits.

DOI: 10.1103/PhysRevResearch.2.013326

I. INTRODUCTION

How difficult is it to communicate classically the identity of a quantum state in an entanglement-unassisted scenario? Specifying a pure state of a qubit requires two real numbers, so communicating its identity seemingly needs an infinite amount of classical information [1]. This suspicion is confirmed by the results of Ref. [2], which show that if the two communicating parties do not share random data, then an unbounded amount of classical communication is needed to exactly simulate results of quantum experiments. Assuming shared randomness, however, only two bits suffice to exactly reproduce results of any projective qubit measurement [3].

Here we derive a lower bound for the classical communication cost of simulating the transmission of a d-dimensional quantum state. This is done by describing a communication problem based on a relation and proving an exponential separation between the classical and quantum communication complexities. The proof uses quantum state antidistinguishability, a concept that has been studied in the foundations literature [4–8], and lies behind the theorem of Ref. [4], which rules out Ψ-epistemic ontological models of quantum theory.

It is already well known that there can be exponential separation between classical and quantum communication complexities. Reference [9] (see also Ref. [10]), for example, presents an $\Omega(d)$ versus $O(\log d)$ separation between classical and quantum zero-error communication complexities for the task of deciding whether two d-bit inputs are either equal or have Hamming distance $d/2$. The proof presented involves a highly nontrivial combinatorial result [11] and results in a classical lower bound of the form cd, for a constant $c = 0.01$. (Slightly strengthened, the same proof yields a lower bound of cd for any $c < 0.02$, which means that a nontrivial separation between the number of classical bits that must be communicated and the number of qubits can be established for any $d \geqslant 512$.) Subsequent works [12–19] established exponential separations between zero-error quantum and bounded-error classical protocols. The separations of Refs. [17,18], in particular, are strong in the sense that the separation holds between zero-error one-way quantum protocols and bounded-error classical protocols that allow two-way communication. In none of Refs. [12–19], however, is a classical lower bound of $\Omega(d)$ established: varying separations are presented of which the strongest is $\Omega(\sqrt{d})$ vs $O(\log d)$. Reference [20], by considering a task based on distributed Fourier sampling, derives an $\Omega(d)$ versus $O(\log d)$ separation, which is robust against constant additive error, and which holds when two-way classical communication is allowed. For a 2010 review, see Ref. [21].

Montina [22] considers the scenario in which Alice's input can be any pure state of a d-dimensional quantum system, and Bob's input can be any two-outcome measurement consisting of a rank 1 projector and the orthogonal projector. Assuming zero-error, one-way classical communication, Montina derives a classical lower bound of cd, for $c \approx 0.293$, where the proof uses a result concerning volumes of subsets of a hypersphere due to Raigorodskii [23]. It is also shown that a classical lower bound of $d-1$ follows from (a complex generalization of) a mathematical conjecture known as the *double cap conjecture*.

Finally, other works have had slightly different aims from that of establishing quantum-classical separations in the

[*] vojtech.havlicek@keble.ox.ac.uk

Published by the American Physical Society under the terms of the Creative Commons Attribution 4.0 International license. Further distribution of this work must maintain attribution to the author(s) and the published article's title, journal citation, and DOI.

standard communication complexity setting, but nonetheless contain techniques related to those that we use. These include Ref. [24], which presents quantum fingerprinting protocols, and Refs. [25,26], where the notion of antidistinguishability is used to give separations between one-way communication and information complexities in exclusion games. They also include Ref. [27], where lower bounds on the size of a classical memory needed to simulate quantum processes are derived, and applied to the stabilizer subtheory of quantum theory. Reference [28] defines and studies tasks of communicating "partial ignorance," including communication tasks using antidistinguishable quantum states that are similar to those used here.

One of the main motivations for our work is to present a proof of exponential separation between classical and quantum communication complexity that is very simple, and self-contained. Aside from this, the advantages of the approach include (i) a lower bound for zero-error one way classical communication of cd, with $c \approx 0.415$, which is the strongest that we have seen, and (ii) a separation between quantum and classical one-way communication complexity for any $d \geqslant 3$. On the negative side, we show that the classical communication lower bound disappears if two-way classical communication is allowed. Although the result is robust against a limited amount of additive noise, the lower bound also disappears if bounded error classical protocols are allowed.

We use asymptotic O-notation throughout [29]. All logarithms are base 2, $[n]$ denotes the set $\{1, 2, \dots, n\}$, and $\{0, 1\}^*$ is the set of all finite bit-strings.

II. COMMUNICATION COMPLEXITY

Communication complexity studies the amount of communication needed to solve distributed computational problems [30–33]. In a two-party relational task, Alice and Bob get inputs $x \in X$ and $y \in Y$, respectively, for finite sets X, Y, and do not see the other's input. The aim is for Bob to output $z \in Z$, such that $(x, y, z) \in R$ for a relation $R \subseteq X \times Y \times Z$. Both parties can use unlimited computational power and exchange messages following a shared communication protocol. In this work, we allow shared randomness, meaning that Alice and Bob share a random string $s \in \{0, 1\}^*$ sampled from a distribution $P(s)$. On any run of the protocol, the classical (quantum) communication cost is the number of transmitted bits (qubits). In general, this can depend on both the input and the value of s. The notion of communication complexity we use is the communication cost in the best possible protocol, where the communication cost is averaged over the shared random data, and evaluated on the worst-case input. Note that with this definition, the communication complexity with shared random data can be smaller than the deterministic communication complexity (where no randomness is permitted), even for zero error protocols [32]. The communication cost for the worst-case value of s is always larger than that averaged over s, hence our lower bounds for classical communication complexity still apply if communication complexity is defined with respect to the worst-case value of s. One-way communication complexity assumes a protocol in which Alice is only allowed to send a single message to Bob, after which he announces the result.

III. ANTIDISTINGUISHABILITY

The quantum protocol that we will describe relies on *antidistinguishable* sets of quantum states. A set of n pure quantum states $|\rho_1\rangle, |\rho_2\rangle, \dots, |\rho_n\rangle$ is antidistinguishable if there exists an n-outcome (in general positive operator-valued) measurement $\Pi' = \{\Pi'_z \mid z \in [n]\}$ that never outputs the outcome z on the quantum state $|\rho_z\rangle$, i.e.,

$$\Pi'_z|\rho_z\rangle = 0, \ \forall z \in [n]. \tag{1}$$

A sufficient condition for three pure quantum states $|\rho_j\rangle, |\rho_k\rangle, |\rho_m\rangle$ to be antidistinguishable with a projective measurement is if there exist orthogonal states $|j\rangle, |k\rangle, |m\rangle$, such that

$$\begin{aligned} |\rho_j\rangle &= \cos\theta_i|k\rangle + e^{i\phi_i}\sin\theta_i|m\rangle, \\ |\rho_k\rangle &= \cos\theta_j|m\rangle + e^{i\phi_j}\sin\theta_j|j\rangle, \\ |\rho_m\rangle &= \cos\theta_k|j\rangle + e^{i\phi_k}\sin\theta_k|k\rangle, \end{aligned} \tag{2}$$

for some $\theta_z, \phi_z \in \mathbb{R}$, $z \in \{j, k, m\}$. The notion of antidistinguishability was introduced by Caves, Fuchs and Schack in Ref. [5], where it is shown that that such a basis can be found iff for

$$a = |\langle\rho_j|\rho_k\rangle|^2, \quad b = |\langle\rho_j|\rho_m\rangle|^2, \quad c = |\langle\rho_m|\rho_k\rangle|^2,$$

the following holds [34]:

$$a + b + c < 1, \quad (1 - a - b - c)^2 \geqslant 4abc.$$

As a simple corollary, any triple of pure quantum states is antidistinguishable if

$$a, b, c \leqslant \tfrac{1}{4}. \tag{3}$$

Now consider a finite set S of pure states $|\rho_1\rangle, |\rho_2\rangle, \dots, |\rho_{|S|}\rangle$, for which

$$|\langle\rho_i|\rho_j\rangle| \leqslant \delta; \ \forall\, i \neq j,$$

where $\delta \in [0, 1)$. Such sets are called *complex spherical codes*, and have been much studied, with applications in classical signal processing, error correction, and quantum information [24,35–41]. Our results will be obtained from the following simple observation:

Claim 1. Any triple of states drawn from a complex spherical code S with $\delta \leqslant 1/2$ is antidistinguishable.

IV. SEPARATIONS

The separation between classical and quantum communication complexities that we establish is for solution of a relational task, as follows. For a d-dimensional Hilbert space, let S be a complex spherical code $S = \{|\rho_1\rangle, |\rho_2\rangle, \dots |\rho_{|S|}\rangle\}$, with $\delta = 1/2$. Alice's input is an integer $i \in [|S|]$. Bob's input is a set of three integers $j, k, m \in [|S|]$. Bob must output one of the integers j, k, m, under the constraint that his output must not be equal to Alice's input. Setting $X = Z = [|S|]$, and $Y = \{T | T \subseteq S, |T| = 3\}$, the relation is thus given by

$$\begin{aligned} &R \subseteq X \times Y \times Z: \\ &\quad (i, \{j, k, m\}, z) \in R \text{ iff } z \in \{j, k, m\} \text{ and } z \neq i. \end{aligned} \tag{4}$$

The quantum solution is straightforward (see Fig. 1).

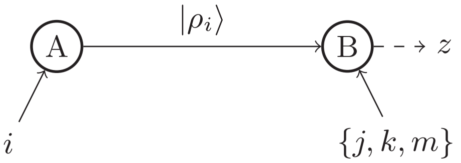

FIG. 1. A quantum protocol. Alice gets an integer $i \in [|S|]$, and Bob gets three integers $j, k, m \in [|S|]$. Alice sends a quantum system in the state $|\rho_i\rangle$ to Bob. Bob performs an antidistinguishing measurement for the states $|\rho_j\rangle, |\rho_k\rangle, |\rho_m\rangle$, and outputs the outcome.

(1) Given input i, Alice prepares a quantum system in the state $|\rho_i\rangle \in S$ and sends it to Bob.

(2) Given input $\{j, k, m\}$, Bob performs an antidistinguishing measurement for the three states $|\rho_j\rangle, |\rho_k\rangle, |\rho_m\rangle$ on the system he receives from Alice. Label the three outcomes Π'_z, for $z \in \{j, k, m\}$, such that $\Pi'_z|\rho_z\rangle = 0$. If Bob obtains outcome Π'_z, then he outputs z. (This means that Bob never outputs an outcome "i.")

The communication complexity is the number of qubits transmitted, which is $\lceil \log d \rceil$. A classical protocol is illustrated in Fig. 2.

Claim 2. The zero-error one-way classical communication complexity of the task is at least $\lceil \log |S| - 1 \rceil$.

Proof. To establish the claim, consider first deterministic protocols, in which the message that Alice sends to Bob is a function of her input, and Bob's output is a function of his input and the message. Suppose that there are three distinct values of Alice's input, $|\rho_j\rangle, |\rho_k\rangle, |\rho_m\rangle$, such that the same message λ is sent for each of them. If Bob receives λ, and his input is the triple $\{j, k, m\}$, then there is no output he can give that will not sometimes generate an error. Therefore, Alice needs at least a distinct message per two states of S. This gives

$$|\Lambda| \geqslant \frac{|S|}{2}, \tag{5}$$

where Λ is the set of possible values of Alice's message. It follows that on the worst case input, Alice needs to send at least $\lceil \log |S| - 1 \rceil$ bits.

In the presence of shared randomness s, each value of s defines a deterministic protocol, which in the zero-error case must respect the relation. If communication complexity is evaluated as the communication cost on the worst case values of s, then this concludes the proof. With communication complexity given by the communication cost averaged over s, and evaluated on the worst case input, the following standard manoeuvre (Yao's minimax principle) [32] suffices. For any probability distribution Q over input pairs, the communication complexity is lower bounded by the communication cost, averaged both over values of s and over inputs drawn according to the distribution Q. This is in turn lower bounded by the communication cost, averaged over inputs drawn according to the distribution Q, of the deterministic protocol that achieves the lowest value for this cost. Choosing Q as the uniform distribution over all input pairs, the argument above establishes that the lower bound of $\lceil \log |S| - 1 \rceil$ bits still holds. ■

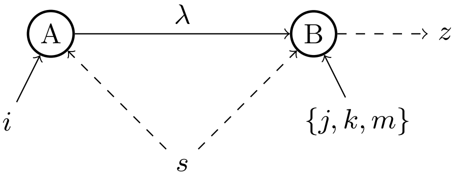

FIG. 2. A classical protocol. Alice gets an integer $i \in [|S|]$, and Bob gets three integers $j, k, m \in [|S|]$. Alice sends a message λ, after which Bob outputs $z \in \{j, k, m\}$. The classical strategy can use a shared random string s, drawn according to a probability distribution $P(s)$.

We remark that the lower bound derived in Claim 2 also straightforwardly applies to multiplicative error sampling. Let S be the set of states defined in Claim 1 and let $\Pi' = \{\Pi'_z | z \in \{j, k, m\}\}$ be a measurement antidistinguishing a triple of states $\{|\rho_j\rangle, |\rho_k\rangle, |\rho_m\rangle\} \subseteq S$, chosen such that $\Pi'_z|\rho_z\rangle = 0$ for all $z \in \{j, k, m\}$. Let $p(z|\Pi', |\rho_i\rangle)$ denote the probability of measuring an outcome "z" by applying Π' to $|\rho_i\rangle$. A ϵ-multiplicative sampling protocol samples from a distribution $\tilde{p}(z|\Pi', |\rho_i\rangle)$, such that

$$|\tilde{p}(z|\Pi', |\rho_i\rangle) - p(z|\Pi', |\rho_i\rangle)| \leqslant \epsilon\, p(z|\Pi', |\rho_i\rangle), \tag{6}$$

for some $\epsilon \geqslant 0$ and all inputs. Notice that

$$p(z|\Pi', |\rho_i\rangle) = 0 \Rightarrow \tilde{p}(z|\Pi', |\rho_i\rangle) = 0 \tag{7}$$

holds for arbitrary ϵ. Even as $\epsilon \to \infty$, the mutliplicative error simulation protocol cannot output an outcome that is assigned zero probability in the exact case and hence also solves the relation R defined in Eq. (4). This means that classical protocols for the sampling task are subject to the same classical lower bounds as the zero-error protocol for R.

The lower bound of Claim 2 is determined by $|S|$, the size of the spherical code S. In contrast, for a fixed dimension d, regardless of the size of $|S|$, the quantum protocol uses only $\lceil \log d \rceil$ qubits. This gives a communication advantage whenever $|S| > 2d$. For the best separation, the problem becomes: how large can a complex spherical code in d dimensions be, with $\delta = 1/2$?

In $d = 3$, the largest such set is given by an equiangular complex spherical code, otherwise known as a symmetric, informationally complete set (SIC) [42–45]. A SIC in dimension 3 consists of 9 unit vectors, such that

$$|\langle \rho_i|\rho_j\rangle|^2 = \tfrac{1}{4}, \quad \forall\, i \neq j. \tag{8}$$

That a larger set cannot be found follows from the Welch bound [35], which states that

$$\max_{i \neq j} |\langle \rho_i|\rho_j\rangle|^2 \geqslant \frac{|S| - d}{d(|S| - 1)}, \tag{9}$$

for any set of d-dimensional pure states $S = \{|\rho_1\rangle, |\rho_2\rangle, \ldots |\rho_{|S|}\rangle\}$. This shows that Alice needs to send at least a 5-valued message versus a 3-dimensional quantum system, or in terms of whole numbers of bits and qubits, at least 3 bits versus 2 qubits.

In $d \geqslant 4$, mutually unbiased bases (MUBs) yield larger sets than SICs. It is known that for d power prime, there exist $d + 1$ distinct MUBs [46], which satisfy $|\langle \rho_i|\rho_j\rangle|^2 \leqslant 1/d$. Taking S as the union of the vectors in the MUBs gives $|S| = d(d + 1)$, hence a $\lceil \log(d^2 + d) - 1 \rceil$ lower bound on classical communication. In $d = 4$, Alice needs to send at least a 10-valued message versus a 4-dimensional quantum system, or in terms of whole numbers of bits and qubits, at least 4 bits versus 2 qubits. A bound due to Levenshtein

[36,37,40] implies that in $d = 4$, the 20-element set of vectors given by MUBs is the largest that can be achieved with $\delta = 1/2$. In $d \geqslant 5$, larger sets than those given by MUBs have been found numerically [40,41].

For general d, the following supplies a classical lower bound of $\lceil \log(4/3)(d-1) - 1 \rceil \approx 0.415(d-1) - 1$ bits.

Claim 3. For any d, there exists a complex spherical code, with $\delta = 1/2$, such that $|S| \geqslant (\frac{4}{3})^{d-1}$.

Proof. The claim is established by generalizing a well known result of Chabauty, Shannon and Wyner [47–50] to the case of complex vector spaces. Consider, for each vector $|e\rangle \in S$, the complex spherical cap A^d_θ, defined as the set of all vectors $|\psi\rangle$ in the Hilbert space satisfying $|\langle e|\psi\rangle|^2 \geqslant \cos^2\theta$, for some $0 \leqslant \theta \leqslant \pi/2$. If S is as large as possible under the constraint $\delta = 1/2$, then for $\theta = \pi/3$, these caps must cover the whole of the complex unit sphere—otherwise, there is room to add another vector to S. Therefore, a simple lower bound on the achievable $|S|$ is given by

$$|S| \geqslant \frac{V^d}{V^d_{\pi/3}}, \tag{10}$$

where V^d_θ is the volume of a spherical cap A^d_θ, and $V^d = V^d_{\pi/2}$ is the volume of the unit sphere in d complex dimensions, volumes being evaluated according to some suitable measure.

The following calculation (with different θ, in the context of a different method for establishing a communication complexity separation) appears in Ref. [22]. In keeping with our main motivation of providing a simple and self-contained proof of exponential separation, we reproduce the reasoning here.

The points of the unit sphere in d complex dimensions are in $1-1$ correspondence with the points of the unit sphere in $2d$ real dimensions, under the obvious mapping that takes the real and imaginary parts of each complex coordinate to two independent classical coordinates. Volumes of subsets of the complex unit sphere can therefore be defined as the volumes of the corresponding subsets of the real unit sphere in $2d$ dimensions. Letting $|e\rangle = (1, 0, \ldots, 0) \in \mathbb{C}^d$, the complex spherical cap A^d_θ maps to the set of real vectors of the form

$$\cos\phi\, \hat{u}_1 + \sin\phi\, \hat{u}_2, \tag{11}$$

where $\hat{u}_1 \in \mathbb{R}^{2d}$ is a unit vector in the subspace spanned by $(1, 0, 0, \ldots, 0)$ and $(0, 1, 0, \ldots, 0)$, $\hat{u_2}$ is a unit vector in the orthogonal subspace, and $0 \leqslant \phi \leqslant \theta$. The volume of this set is given by

$$V^d_\theta = \int_0^\theta 2\pi \cos\phi\, \tilde{V}^{2d-2}(\sin\phi)\, d\phi, \tag{12}$$

where $\tilde{V}^{2d-2}(\sin\phi)$ is the volume of a $(2d-3)$-sphere in $(2d-2)$ real dimensions of radius $\sin\phi$. Combining Eqs. (10) and (12), with $\theta = \pi/3$, yields

$$|S| \geqslant \left(\tfrac{4}{3}\right)^{d-1}.$$

■

An alternative proof that there exist sets S with $|S|$ exponentially large, which results in a worse bound, but which some may find even simpler, is given in Refs. [24,51], and reproduced in the Appendix.

V. TWO-WAY CLASSICAL COMMUNICATION

Claim 4. Assuming $|S| = 2^q$, for integer q, the two-way classical communication complexity of R is at most $\lceil \log\log|S| \rceil + 1$ bits.

Proof. The assumption that $|S| = 2^q$ is not essential, but allows a short statement of the proof. The protocol has two rounds and starts with a message from Bob to Alice. Let Bob's input be $\{j, k, m\}$, and assume without loss of generality that $j < k < m$. Bob determines the largest integer $r \leqslant q = \log|S|$, such that for some integer $s \geqslant 0$, either

$$\begin{aligned} s\,2^r &< j, k \leqslant (s+1)\,2^r \text{ and} \\ (s+1)\,2^r &< m \leqslant (s+2)\,2^r \end{aligned} \tag{13}$$

or

$$\begin{aligned} s\,2^r &< j \leqslant (s+1)\,2^r \text{ and} \\ (s+1)2^r &< k, m \leqslant (s+2)2^r. \end{aligned} \tag{14}$$

Bob sends r to Alice using $\lceil \log\log|S| \rceil$ bits. Note that r determines a subset $Y_r \subseteq Y$ of Bob's possible inputs. For input $i \in [|S|]$, Alice computes the parity p of $\lceil \frac{i}{2^r} \rceil$, and sends it to Bob. Note that the set X of Alice's inputs is partitioned by p and r into subsets $X_{r,p} \subseteq X$. By Eqs. (13) and (14), at least one of j, k, m is not in $X_{r,p}$. Bob chooses such a value for his output. Communicating $\lceil \log\log|S| \rceil + 1$ bits hence suffices in the two-way scenario. Figure 3 illustrates the protocol for $|S| = 8$. ■

Claim 4 implies that the exponential complexity gap vanishes if we allow interactive protocols.

VI. BOUNDED ERROR

The separation almost trivially disappears if the classical players need only solve the relation with bounded error. We show this by reduction to equality testing. Suppose that Alice's input was i and Bob's input was $\{j, k, m\}$. The parties repeat the following in several runs: they generate a uniformly random shared string $s \in \{0, 1\}^{|S|}$. Alice computes the parity p_i of $\sum_{r=1}^{|S|} i_r s_r$, where i_r, s_r are the rth bits of her input and shared randomness, respectively. She sends p_i to Bob. Bob similarly computes parities p_j, p_k, p_m of $\sum_{r=1}^{|S|} j_r s_r$, $\sum_{r=1}^{|S|} k_r s_r$ and $\sum_{r=1}^{|S|} m_r s_r$. Without loss of generality, suppose that $i = j$. Then $p_j = p_i$ with certainty, and $p_k = p_i$ with probability $1/2$ (similarly $p_m = p_i$ with probability $1/2$), as s was chosen uniformly at random. If the parties repeat this $\lceil \log(1/\epsilon) \rceil$ times, then Bob concludes that $i = j$ with probability greater than $1 - \epsilon$. In this case, he outputs m or k, making a mistake with probability less than ϵ. However, if i is not equal to any of j, k, m, then Bob can output any of j, k, m without error.

VII. ANTIDISTINGUISHABILITY CONJECTURE

Reference [52] considers, among other things, exact classical simulation of a scenario in which Alice chooses an arbitrary quantum pure state, and sends it to Bob who performs an arbitrary two-outcome von Neumann measurement. A lower bound of $\Omega(d \log d)$ bits is shown to follow from two mathematical conjectures. Such a bound would be asymptotically

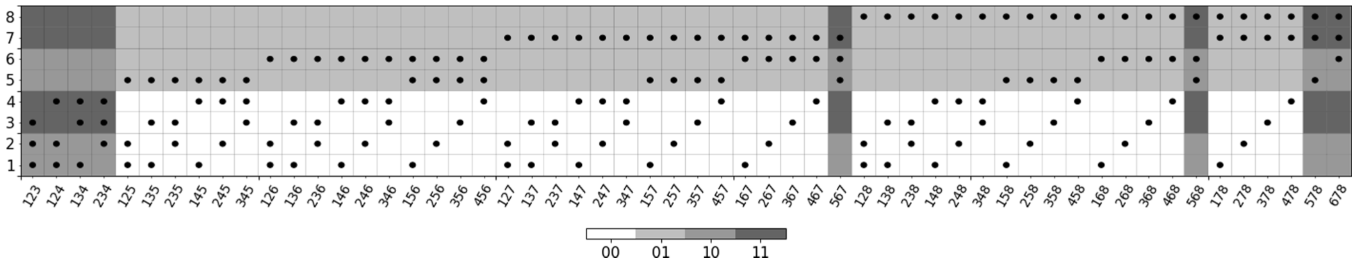

FIG. 3. An illustration of the two-way classical protocol with $|S| = 8$. Rows correspond to different values of Alice's input, columns to different values of Bob's input. In single run of the protocol, Bob sends an integer r to Alice, and Alice sends an integer p to Bob. Each value of the conversation (r, p) is compatible with a subset of the joint inputs, where the subset is of the form $X_{r,p} \times Y_r$ for $X_{r,p} \subset X$ and $Y_r \subset Y$, and is known as a combinatorial rectangle. In the $|S| = 8$ example, there are four possible conversations, hence four rectangles, which cover $X \times Y$ as illustrated. No rectangle contains three dots in the same column, which implies that Bob can always produce a suitable output without error.

stronger than all existing established lower bounds. See also Ref. [53] for an application to the foundations of quantum theory, in which the conjectured $\Omega(d \log d)$ lower bound is used to strengthen the theorem of Ref. [4].

Here we observe that the following conjecture concerning antidistinguishability would also give a separation of $\log d$ qubits versus $\Omega(d \log d)$ bits for exact simulation. Our argument is very different from those of Ref. [52], and our conjecture concerning antidistinguishability is very different from the two conjectures of Ref. [52].

Conjecture 1. Let $|\rho_1\rangle, \dots, |\rho_d\rangle$ be d pure states. If $|\langle\rho_i|\rho_j\rangle| \leqslant (d-2)/(d-1)$ for all $i \neq j$, then the states are antidistinguishable.

The $\log d$ versus $\Omega(d \log d)$ separation is established using Conjecture 1, along with essentially the same proof of zero-error one-way separation that we have given above. We omit the details of this step, and instead provide some discussion of the conjecture itself.

It is obvious that the conjecture holds with $d = 2$, and it follows from the results of Ref. [5] that the conjecture holds with $d = 3$. To gain some intuition for why the conjecture might be true in all dimensions, first consider a generic set of states $|\rho_1\rangle, \dots, |\rho_d\rangle$. Reference [6] shows that if any triple of the states is antidistinguishable, then it follows that the set of d states is antidistinguishable. However, it does not follow that if the set of d states is antidistinguishable, then any triple must be antidistinguishable. Hence the condition that d states is antidistinguishable is logically weaker than the condition that any triple of them is antidistinguishable. If the states satisfy $|\langle\rho_i|\rho_j\rangle| \leqslant 1/2$ for all $i \neq j$, then the stronger condition holds [5], hence it is natural to suppose that a similar statement, with $1/2$ on the right-hand side replaced by a larger number, suffices for the weaker condition.

Second, consider the set of d-dimensional states:

$$
\begin{aligned}
|\rho_1\rangle &= \frac{1}{\sqrt{d-1}}(|e_2\rangle + |e_3\rangle + \cdots + |e_d\rangle),\\
|\rho_2\rangle &= \frac{1}{\sqrt{d-1}}(|e_1\rangle + |e_3\rangle + \cdots + |e_d\rangle),\\
&\dots\\
|\rho_d\rangle &= \frac{1}{\sqrt{d-1}}(|e_1\rangle + |e_2\rangle + \cdots + |e_{d-1}\rangle),
\end{aligned}
$$

where $\{|e_i\rangle\}$ is an orthonormal basis. This set is antidistinguishable by construction and satisfies $|\langle\rho_i|\rho_j\rangle| = (d-2)/(d-1)$ for all $i \neq j$, which motivates the particular choice of function on the right-hand side of the conjectured sufficient condition.

Finally, Fig. 4 displays numerical evidence for Conjecture 1. Note that for a given set of states in d dimensions, determining whether they are antidistinguishable or not corresponds to solving a semidefinite program (SDP) [54]. For each $d = 2, 3, 4, 5$, we generated a set of 1 50 000 sets of d vectors in d dimensions, where each vector is chosen independently, and uniformly according to the Haar measure. For each set of vectors, the SDP is solved, to determine whether the set is antidistinguishable. For those sets that are not antidistinguishable, the quantity $\alpha = \max_{i\neq j} |\langle\rho_i|\rho_j\rangle|$ is recorded. The shaded region of the graph shows, for each dimension, the minimum value of α obtained, and the dashed line shows the value of $(d-2)/(d-1)$, with lines rather than points used for clarity. A counterexample to the conjecture would appear as the dashed line crossing the nonshaded region. The evidence for the conjecture consists in the fact that the shaded region cleaves fairly closely to the dashed line, yet no counterexamples were found.

VIII. CONCLUSION

We have used quantum state antidistinguishability to give simple proofs of separation between classical and quantum

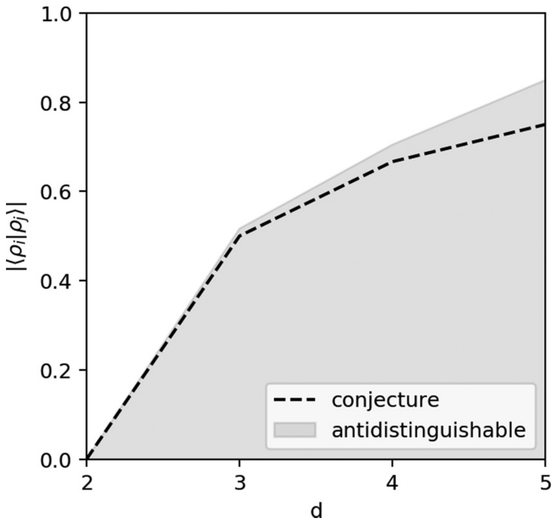

FIG. 4. Numerical evidence for Conjecture 1.

zero-error one-way communication complexities. Using SICs and MUBs, we proved separations in any $d \geqslant 3$. Using a lower bound on the achievable size of a suitable complex spherical code, we showed an exponential separation of $\log d$ qubits versus $0.415(d-1)-1$ bits. For the relation considered, however, the separation disappears if two-way classical communication is allowed or if one-way classical communication is allowed with bounded error.

The results are stated in terms of quantum and classical players solving a relation, which is defined on finite sets of possible inputs for Alice and Bob. Seeing as expanding the sets of inputs can only make things more difficult for classical players, the lower bounds also apply to the one-way classical communication cost of simulating an experiment in which Alice prepares an arbitrary pure state of a d-dimensional quantum system and sends it to Bob, who performs an arbitrary projective measurement. (Naturally, the same can be said for the results of any of Refs. [9,10,12–20,22].) In this more general scenario, if error ϵ is tolerated in the measurement outcome probabilities in the classical simulation, then it is easy to see that transmission of $O(\log(1/\epsilon)\, d)$ classical bits is sufficient, simply by approximating the real and imaginary parts of the complex entries in the d-dimensional state vector. As discussed in Ref. [20], this means that the results of Ref. [20] are asymptotically optimal for bounded error simulation. If exact simulation is required, however, then Ref. [2] shows that without shared randomness, bounded classical communication is insufficient. If exact simulation is required, and shared random data permitted, then surprisingly little is known apart from the exponential lower bounds. Ref. [3] shows that for $d = 2$, transmission of two bits is sufficient (see also Ref. [1] which considers positive operator-valued measurements). But we are unaware of any demonstration, even for $d = 3$, that classical simulation of arbitrary preparations and projective measurements is possible with bounded communication cost, let alone a demonstration of a specific protocol with bounded communication, or a finite upper bound. A lower bound of $\Omega(d \log d)$, as implied by Conjecture 1, would be particularly interesting given the $O(\log(1/\epsilon)d)$ upper bound for the bounded-error case.

The exponential lower bounds are of interest for the foundations of quantum theory, as well as for communication complexity per se. As Montanaro writes [20]: "On a fundamental, conceptual level, the question asks: Are quantum states 'really' like an exponentially long string of numbers, or do they have a more efficient representation?" Restated in different language, any lower bound on the size of the classical message in a simulation of the transmission of a quantum state becomes a lower bound on the size of the set of ontic states that the system must have available to it in an ontological model for quantum theory [4,55]. For further discussion of the relevance of communication complexity results to quantum foundations, see Ref. [56].

The importance of the exponential separation between quantum and classical communication, both for foundations and for complexity theory, underpins one of the motivations of this work, which is to present as simple as possible proof of this fact, and to obtain as strong a lower bound as possible. In future work, it would be interesting to prove a stronger separation, for example by finding a modification of the presented problem that makes our proof technique work for bounded error.

ACKNOWLEDGMENTS

We thank John-Mark Allen, Matthew Pusey, Matthew Jenssen, and Ashley Montanaro for useful discussions. The numerical investigations were carried out by the authors. Some similar investigations were carried out by Matthew Pusey, and we thank him for sharing the results with us. V.H. is supported by the Clarendon and Keble de Breyne scholarships at the University of Oxford and an IBM Ph.D. Fellowship. This work was supported by the EPSRC National Quantum Technology Hub in Networked Quantum Information Technologies and by the Perimeter Institute for Theoretical Physics. Research at Perimeter Institute is supported by the Government of Canada through the Department of Innovation, Science, and Economic Development Canada and by the Province of Ontario through the Ministry of Research, Innovation, and Science. This project/publication was made possible through the support of a grant from the John Templeton Foundation. The opinions expressed in this publication are those of the author(s) and do not necessarily reflect the views of the John Templeton Foundation.

APPENDIX: ALTERNATIVE SIMPLE PROOF FOR THE EXISTENCE OF EXPONENTIAL-SIZED COMPLEX SPHERICAL CODES

The following argument, from Refs. [24,51], shows that complex spherical codes exist that are exponentially large in the dimension. Take two random d-dimensional pure states:

$$|v\rangle = \frac{1}{\sqrt{d}}\sum_{i=1}^{d} v_i|i\rangle, \quad |w\rangle = \frac{1}{\sqrt{d}}\sum_{i=1}^{d} w_i|i\rangle, \tag{A1}$$

where w_i, v_i are Rademacher random variables with $\Pr(v_i = \pm 1) = \Pr(w_i = \pm 1) = 1/2$. Their inner product is

$$\langle v|w\rangle = \frac{1}{d}\sum_{i=1}^{d} v_i w_i = \frac{1}{d}\sum_{i=1}^{d} X_i, \tag{A2}$$

where X_i is again a Rademacher random variable with $\Pr(X_i = \pm 1) = 1/2$. The probability that $|\langle v|w\rangle| > 1/2$ is upper bounded by the Chernoff-Hoeffding inequality:

$$\Pr\left(|\langle v|w\rangle| > \frac{1}{2}\right) = \Pr\left(\left|\sum_i^d X_i\right| > \frac{d}{2}\right) \leqslant 2e^{-\frac{d}{8}}. \tag{A3}$$

The probability that a set S of such random vectors contains a pair $|v_i\rangle, |w_j\rangle \in S$, $i \neq j$ with overlap greater than $1/2$ is given by

$$\Pr\left(|\langle v_i|w_j\rangle| > \frac{1}{2}\right) \leqslant 2\binom{|S|}{2}e^{-\frac{d}{8}} < |S|^2 e^{-\frac{d}{8}}. \tag{A4}$$

As soon as this probability falls below 1, there exists a set S of such random states, so that $|\langle v_i|w_j\rangle| \leqslant 1/2$ for any pair. From Eq. (A4), $|S| = e^{\frac{d}{16}}$. Using such a set S for the task defined in the main text, the classical one-way communication complexity is at least $\lceil 0.09\, d - 1 \rceil$ bits.

[1] N. J. Cerf, N. Gisin, and S. Massar, Classical Teleportation of a Quantum Bit, Phys. Rev. Lett. **84**, 2521 (2000).

[2] L. Hardy, Quantum ontological excess baggage, Studies History Philos. Sci. Part B: Studies History Philos. Modern Phys. **35**, 267 (2004).

[3] B. F. Toner and D. Bacon, Communication Cost of Simulating Bell Correlations, Phys. Rev. Lett. **91**, 187904 (2003).

[4] M. F. Pusey, J. Barrett, and T. Rudolph, On the reality of the quantum state, Nat. Phys. **8**, 476 (2012).

[5] C. M. Caves, C. A. Fuchs, and R. Schack, Conditions for compatibility of quantum-state assignments, Phys. Rev. A **66**, 062111 (2002).

[6] T. Heinosaari and O. Kerppo, Antidistinguishability of pure quantum states, J. Phys. A: Math. Gen. **51**, 365303 (2018).

[7] M. Leifer, Is the quantum state real? An extended review of ψ-ontology theorems, Quanta **3**, 67 (2014).

[8] J. Barrett, E. G. Cavalcanti, R. Lal, and O. J. E. Maroney, No ψ-Epistemic Model can Fully Explain the Indistinguishability of Quantum States, Phys. Rev. Lett. **112**, 250403 (2014).

[9] H. Buhrman, R. Cleve, and A. Wigderson, Quantum vs classical communication and computation, in *Proceedings of the 30th Annual ACM Symposium on Theory of Computing (STOC'09)* (ACM, New York, 1998), pp. 63–68.

[10] G. Brassard, R. Cleve, and A. Tapp, Cost of Exactly Simulating Quantum Entanglement with Classical Communication, Phys. Rev. Lett. **83**, 1874 (1999).

[11] P. Frankl and V. Rödl, Forbidden intersections, Trans. Amer. Math. Soc. **300**, 259 (1987).

[12] R. Raz, Exponential separation of quantum and classical communication complexity, in *Proceedings of the 31st Annual ACM Symposium on Theory of Computing (STOC'99)* (ACM, New York, 1999), pp. 358–367.

[13] A. Ambainis, L. J. Schulman, A. Ta-Shma, U. V. Vazirani, and A. Wigderson, The quantum communication complexity of sampling, SIAM J. Comput. **32**, 1570 (2003).

[14] Z. Bar-Yossef, T. S. Jayram, and I. Kerenidis. Exponential separation of quantum and classical one-way communication complexity, SIAM J. Comput. **38**, 366 (2008).

[15] I. Kerenidis and R. Raz, The one-way communication complexity of the Boolean hidden matching problem, arXiv:quant-ph/0607173.

[16] D. Gavinsky, J. Kempe, I. Kerenidis, R. Raz, and R. de Wolf, Exponential separations for one-way quantum communication complexity, with applications to cryptography, in *Proceedings of the 39th Annual ACM Symposium on Theory of Computing (STOC'07)* (ACM, New York, 2007), pp. 516–525.

[17] D. Gavinsky, Classical interaction cannot replace a quantum message, in *Proceedings of the 40th Annual ACM Symposium on Theory of Computing (STOC'08)* (ACM, New York, 2008), pp. 95–102.

[18] O. Regev and B. Klartag, Quantum one-way communication can be exponentially stronger than classical communication, in *Proceedings of the 43rd Annual ACM Symposium on Theory of Computing (STOC'11)* (ACM, New York, 2011), pp. 31–40.

[19] A. Montanaro, A new exponential separation between quantum and classical one-way communication complexity, Quant. Info. Comput. **11**, 574 (2011).

[20] A. Montanaro, Quantum states cannot be transmitted efficiently classically, Quantum **3**, 154 (2019).

[21] H. Buhrman, R. Cleve, S. Massar, and R. de Wolf, Nonlocality and communication complexity, Rev. Mod. Phys. **82**, 665 (2010).

[22] A. Montina, Communication cost of classically simulating a quantum channel with subsequent rank-1 projective measurement, Phys. Rev. A **84**, 060303(R) (2011).

[23] A. M. Raigorodskii, On a bound in borsuk's problem, Russian Math. Surveys **54**, 453 (1999).

[24] H. Buhrman, R. Cleve, J. Watrous, and R. de Wolf, Quantum Fingerprinting, Phys. Rev. Lett. **87**, 167902 (2001).

[25] C. Perry, R. Jain, and J. Oppenheim, Communication Tasks with Infinite Quantum-Classical Separation, Phys. Rev. Lett. **115**, 030504 (2015).

[26] Z. Liu, C. Perry, Y. Zhu, D. E. Koh, and S. Aaronson, Doubly infinite separation of quantum information and communication, Phys. Rev. A **93**, 012347 (2016).

[27] A. Karanjai, J. J. Wallman, and S. D. Bartlett, Contextuality bounds the efficiency of classical simulation of quantum processes, arXiv:1802.07744.

[28] T. Heinosaari and O. Kerppo, Communication of partial ignorance with qubits, J. Phys. A: Math. Theor. **52**, 395301 (2019).

[29] T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein, *Introduction to Algorithms*, 3rd ed. (MIT Press, Cambridge, MA, 2009).

[30] A. Chi-Chih Yao, Some complexity questions related to distributive computing (preliminary report), in *Proceedings of the 11th Annual ACM Symposium on Theory of Computing* (ACM, New York, 1979), pp. 209–213.

[31] A. Chi-Chih Yao, Quantum circuit complexity, in *Proceedings of the IEEE 34th Annual Foundations of Computer Science* (IEEE, New York, 1993), pp. 352–361.

[32] E. Kushilevitz and N. Nisan, *Communication Complexity* (Cambridge University Press, New York, 1997).

[33] A. Rao and A. Yehudayoff, *Communication Complexity and Applications* (Cambridge University Press, Cambridge, 2019).

[34] As also noted in Ref. [45], Ref. [5] contains a minor error, in which $>$ instead of $\geqslant$ appears in the second part of the condition.

[35] L. Welch, Lower bounds on the maximum cross correlation of signals, IEEE Trans. Inf. Theory **20**, 397 (1974).

[36] G. A. Kabatiansky and V. I. Levenshtein, On bounds for packings on a sphere and in space, Problems Inform. Transmission **14**, 3 (1978).

[37] V. I. Levenshtein, Bounds for packings of metric spaces and some of their applications, Probl. Kibern. **40**, 43 (1983).

[38] J. M. Renes, Frames, designs, and spherical codes in quantum information theory, Ph.D. thesis, The University of New Mexico, 2004.

[39] A. Roy and S. Suda, Complex spherical designs and codes, J. Combinat. Designs **22**, 105 (2014).

[40] H. Zorlein and M. Bossert, Coherence optimization and best complex antipodal spherical codes, IEEE Trans. Signal Process. **63**, 6606 (2015).

[41] M. Heredia Conde and O. Loffeld, Fast approximate construction of best complex antipodal spherical codes, arXiv:1705.03280.

[42] J. M. Renes, R. Blume-Kohout, A. J. Scott, and C. M. Caves, Symmetric informationally complete quantum measurements, J. Math. Phys. **45**, 2171 (2004).

[43] A. J. Scott and M. Grassl, Symmetric informationally complete positive-operator-valued measures: A new computer study, J. Math. Phys. **51**, 042203 (2010).

[44] A. J. Scott, SICs: Extending the list of solutions, arXiv:1703.03993 (2017).

[45] B. C. Stacey, SIC-POVMs and compatibility among quantum states, Mathematics **4**, 36 (2016).

[46] W. K. Wootters and B. D. Fields, Optimal state-determination by mutually unbiased measurements, Ann. Phys. **191**, 363 (1989).

[47] C. Chabauty, Résultats sur l'empilement de calottes égales sur une périsphère de $\mathbb{R}^n$ et correction à un travail antérieur, C. R. Acad. Sci. Ser. A **236**, 1462 (1953).

[48] C. E. Shannon, Probability of error for optimal codes in a gaussian channel, Bell Syst. Tech. J. **38**, 611 (1959).

[49] A. D. Wyner, Capabilities of bounded discrepancy decoding, Bell Syst. Tech. J. **44**, 1061 (1965).

[50] M. Jenssen, F. Joos, and W. Perkins, On kissing numbers and spherical codes in high dimensions, Adv. Math. **335**, 307 (2018).

[51] N. Alon and J. H. Spencer, *The Probabilistic Method*, 4th ed. (Wiley Publishing, New York, 2016).

[52] A. Montina and S. Wolf, Necessary and sufficient optimality conditions for classical simulations of quantum communication processes, Phys. Rev. A **90**, 012309 (2014).

[53] A. Montina, Communication complexity and the reality of the wave function, Mod. Phys. Lett. A **30**, 1530001 (2015).

[54] S. Bandyopadhyay, R. Jain, J. Oppenheim, and C. Perry, Conclusive exclusion of quantum states, Phys. Rev. A **89**, 022336 (2014).

[55] N. Harrigan and R. W. Spekkens, Einstein, incompleteness, and the epistemic view of quantum states, Found. Phys. **40**, 125 (2010).

[56] A. Montina, Epistemic View of Quantum States and Communication Complexity of Quantum Channels, Phys. Rev. Lett. **109**, 110501 (2012).