


# Certifying the classical simulation cost of a quantum channel

Brian Doolittle<sup>1</sup> and Eric Chitambar<sup>2</sup>

<sup>1</sup>*Department of Physics, University of Illinois at Urbana-Champaign, Urbana, Illinois 61801, USA*

<sup>2</sup>*Department of Electrical and Computer Engineering, Coordinated Science Laboratory, University of Illinois at Urbana-Champaign, Urbana, Illinois 61801, USA*

 (Received 21 April 2021; revised 30 September 2021; accepted 4 October 2021; published 26 October 2021)

A fundamental objective in quantum information science is to determine the cost in classical resources of simulating a particular quantum system. The classical simulation cost is quantified by the signaling dimension which specifies the minimum amount of classical communication needed to perfectly simulate a channel's input-output correlations when unlimited shared randomness is held between encoder and decoder. This paper provides a collection of device-independent tests that place lower and upper bounds on the signaling dimension of a channel. Among them, a single family of tests is shown to determine when a noisy classical channel can be simulated using an amount of communication strictly less than either its input or its output alphabet size. In addition, a family of eight signaling dimension witnesses is presented that completely characterize when any four-outcome measurement channel, such as a Bell measurement, can be simulated using one communication bit and shared randomness. Finally, we bound the signaling dimension for all partial replacer channels in  $d$  dimensions. The bounds are found to be tight for the special case of the erasure channel.

DOI: [10.1103/PhysRevResearch.3.043073](https://doi.org/10.1103/PhysRevResearch.3.043073)

## I. INTRODUCTION

The transmission of quantum states between devices is crucial for many quantum network protocols. In the near-term, quantum memory limitations will restrict quantum networks to “prepare and measure” functionality [1], which allows for quantum communication between separated parties but requires measurement immediately upon reception. Prepare and measure scenarios exhibit quantum advantages for tasks that involve distributed information processing [2] or establishing nonlocal correlations which cannot be reproduced by bounded classical communication and shared randomness [3]. These nonlocal correlations lead to quantum advantages in random access codes [4,5], randomness expansion [6], device self-testing [7], semi-device-independent key distribution [8], and dimensionality witnessing [9,10].

The general communication process is depicted in Fig. 1(a) with Alice (the sender) and Bob (the receiver) connected by some quantum channel  $\mathcal{N}^{A \rightarrow B}$ . Alice encodes a classical input  $x \in \mathcal{X}$  into a quantum state  $\rho_x$  and sends it through the channel to Bob, who then measures the output using a positive-operator valued measure (POVM)  $\{\Pi_y\}_{y \in \mathcal{Y}}$  to obtain a classical message  $y \in \mathcal{Y}$ . The induced classical channel, denoted by  $\mathbf{P}_{\mathcal{N}}$ , has transition probabilities

$$P_{\mathcal{N}}(y|x) = \text{Tr}[\Pi_y \mathcal{N}(\rho_x)]. \quad (1)$$

A famous result by Holevo implies that the communication capacity of  $\mathbf{P}_{\mathcal{N}}$  is limited by  $\log_2 d$ , where  $d$  is the input Hilbert space dimension of  $\mathcal{N}$  [11]; hence, a noiseless classical channel transmitting  $d$  messages has a capacity no less than  $\mathbf{P}_{\mathcal{N}}$ .

However, channel capacity is just one figure of merit, and there may be other features of a  $\mathbf{P}_{\mathcal{N}}$  that do not readily admit a classical simulation. The strongest form of simulation is an exact replication of the transition probabilities  $P_{\mathcal{N}}(y|x)$  for any set of states  $\{\rho_x\}_{x \in \mathcal{X}}$  and POVM  $\{\Pi_y\}_{y \in \mathcal{Y}}$ . This problem falls in the domain of zero-error quantum information theory [12–16], which considers the classical and quantum resources needed to perfectly simulate a given channel. Unlike the capacity, a zero-error simulation of  $\mathbf{P}_{\mathcal{N}}$  typically requires additional communication beyond the input dimension of  $\mathcal{N}$ . For example, a noiseless qubit channel  $\text{id}_2$  can generate channels  $\mathbf{P}_{\text{id}_2}$  that cannot be faithfully simulated using one bit of classical communication [3] (see Fig. 2).

The simulation question becomes more interesting if “static” resources are used for the channel simulation [17,18], in addition to the “dynamic” resource of noiseless classical communication. For example, shared randomness is a relatively inexpensive classical resource that Alice and Bob can use to coordinate their encoding and decoding maps used in the simulation protocol shown in Fig. 1(b). Using shared randomness, a channel can be exactly simulated with a forward noiseless communication rate that asymptotically approaches the channel capacity; a fact known as the Classical Reverse Shannon Theorem [19]. More powerful static resources such as shared entanglement or nonsignaling correlations could also be considered [15,20,21].

While the Classical Reverse Shannon Theorem describes many-copy channel simulation, this work focuses on zero-

*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.*

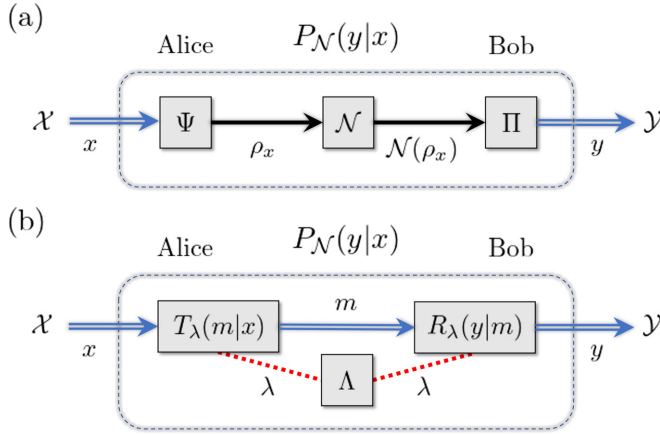


FIG. 1. A general classical communication process. We represent classical information as blue double lines, quantum information as black solid lines, and shared randomness as dotted red lines. (a) A classical channel  $\mathbf{P}_{\mathcal{N}}$  is generated from a quantum channel  $\mathcal{N}$  via Eq. (1). A classical-quantum encoder  $\Psi$  maps the classical input  $x \in \mathcal{X}$  into a quantum state  $\rho_x$ . A quantum-classical decoder  $\Pi$  implements POVM  $\{\Pi_y\}_{y \in \mathcal{Y}}$ . (b) Channel  $\mathbf{P}_{\mathcal{N}}$  is simulated using shared randomness and a noiseless classical channel via Eq. (2). Alice encodes input  $x$  into classical message  $m$  with probability  $T_\lambda(m|x)$  while Bob decodes message  $m$  into output  $y$  with probability  $R_\lambda(y|m)$ . The protocol is coordinated using a shared random value  $\lambda$  drawn from sample space  $\Lambda$  with probability  $q(\lambda)$ .

error channel simulation in the single-copy case. The minimum amount of classical communication (with unlimited shared randomness) needed to perfectly simulate every classical channel  $\mathbf{P}_{\mathcal{N}}$  having the form of Eq. (1) is known as the signaling dimension of  $\mathcal{N}$  [22]. Significant progress in understanding the signaling dimension was made by Frenkel and Weiner who showed that every  $d$ -dimensional quantum channel requires no more than  $d$  classical messages to perfectly simulate [23]. This result is a “fine-grained” version of Holevo’s Theorem for channel capacity mentioned above. However, the Frenkel-Weiner bound is not tight in general. For example, consider the completely depolarizing channel on  $d$  dimensions,  $\mathcal{D}(\rho) = \mathbb{I}/d$ . For any choice of inputs  $\{\rho_x\}_x$  and POVM  $\{\Pi_y\}_y$ , the Frenkel-Weiner protocol yields a simulation of  $\mathbf{P}_{\mathcal{D}}$  that uses a forward transmission of  $d$  messages. However, this is clearly not optimal since  $\mathbf{P}_{\mathcal{D}}$  can be reproduced with no forward communication whatsoever; Bob just samples from the distribution  $P(y) = \text{Tr}[\Pi_y]/d$ . A fundamental problem is then to understand when a noisy classical channel sending  $d$  messages from Alice to Bob actually requires  $d$  noiseless classical messages for zero-error simulation. As a main result of this paper, we provide a family of simple tests that determine when this amount of communication is needed. In other words, we characterize the conditions in which the simulation protocol of Frenkel and Weiner is optimal for the purposes of sending  $d$  messages over a  $d$ -dimensional quantum channel.

This work pursues a device-independent certification of signaling dimension similar to previous approaches used for the device-independent dimensionality testing of classical and quantum devices [24–28]. Specifically, we obtain signaling dimension witnesses that stipulate necessary conditions on

the signaling dimension of  $\mathcal{N}$  in terms of the probabilities  $P_{\mathcal{N}}(y|x)$ , with no assumptions made about the quantum states  $\{\rho_x\}_x$ , POVM  $\{\Pi_y\}_y$ , or channel  $\mathcal{N}$  [29]. Complementary results have been obtained by Dall’Arno *et al.* who approached the simulation problem from the quantum side and characterized the set of channels  $\mathbf{P}_{\mathcal{N}}$  that can be obtained using binary encodings for special types of quantum channels  $\mathcal{N}$  [29]. In this paper, we compute a wide range of signaling dimension witnesses using the adjacency decomposition technique [30], recovering prior results of Frenkel and Weiner [23] and generalizing work by Heinosaari and Kerppo [31]. For certain cases we prove that these inequalities are complete, i.e., providing both necessary and sufficient conditions for signaling dimension. As a further application, we compute bounds for the signaling dimension of partial replacer channels. Proofs for our main results are found in the Appendix while our supporting software is found on Github [32]. For convenience, we provide a glossary of this work’s notation in Appendix A.

## II. PRELIMINARIES

We begin our investigation by reviewing the structure of channels that use noiseless classical communication and shared randomness. Let  $\mathcal{P}^{n \rightarrow n'}$  denote the family of channels having input set  $\mathcal{X} = [n] := \{1, \dots, n\}$  and output set  $\mathcal{Y} = [n']$ . A channel  $\mathbf{P} \in \mathcal{P}^{n \rightarrow n'}$  is represented by an  $n' \times n$  column stochastic matrix, and we thus identify  $\mathcal{P}^{n \rightarrow n'}$  as a subset of  $\mathbb{R}^{n' \times n}$ , the set of all  $n' \times n$  real matrices. In general, we refer to a column (or row) of a matrix as being stochastic if its elements are nonnegative and sum to unity, and a column (respectively, row) stochastic matrix has only stochastic columns (respectively, rows). The elements of a real matrix  $\mathbf{G} \in \mathbb{R}^{n' \times n}$  are denoted by  $G_{y,x}$ , while those of a column stochastic matrix  $\mathbf{P} \in \mathcal{P}^{n \rightarrow n'}$  are denoted by  $P(y|x)$  to reflect their status as conditional probabilities. The Euclidean inner product between  $\mathbf{G}, \mathbf{P} \in \mathbb{R}^{n' \times n}$  is expressed as  $\langle \mathbf{G}, \mathbf{P} \rangle := \sum_{x,y} G_{y,x} P(y|x)$ , and for any  $\mathbf{G} \in \mathbb{R}^{n' \times n}$  and  $\gamma \in \mathbb{R}$ , we let the tuple  $(\mathbf{G}, \gamma)$  denote the linear inequality  $\langle \mathbf{G}, \mathbf{P} \rangle \leq \gamma$ .

### A. Signaling polytopes

Consider now a scenario in which Alice and Bob have access to a noiseless channel capable of sending  $d$  distinct messages. They can use this channel to simulate a noisy channel by applying pre- and post-processing maps. If they coordinate these maps using a shared random variable  $\lambda$  with probability mass function  $q(\lambda)$ , then they can simulate any channel  $\mathbf{P}$  that decomposes as

$$P(y|x) = \sum_{\lambda} q(\lambda) \sum_{m \in [d]} R_{\lambda}(y|m) T_{\lambda}(m|x), \quad (2)$$

where  $m \in [d]$  is the message sent from Alice to Bob and  $T_{\lambda}(m|x)$  [respectively,  $R_{\lambda}(y|m)$ ] is an element of Alice’s encoder  $\mathbf{T}_{\lambda} \in \mathcal{P}^{n \rightarrow d}$  (respectively, Bob’s decoder  $\mathbf{R}_{\lambda} \in \mathcal{P}^{d \rightarrow n'}$ ).

**Definition 1.** The *signaling polytope*  $\mathcal{C}_d^{n \rightarrow n'}$  is the set of all channels satisfying Eq. (2) for any positive integers  $n, n'$ , and  $d$  (see Fig. 2).

The signaling polytope  $\mathcal{C}_d^{n \rightarrow n'}$  is convex due to the fact that any randomness in the encoding or decoding maps of Eq. (2) can be absorbed into the shared randomness distribution  $q(\lambda)$ .

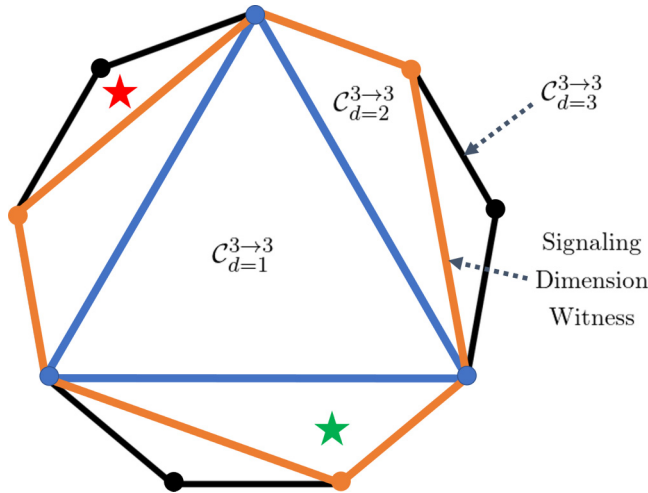


FIG. 2. A graphical analogy illustrating key features of signaling polytopes. Note that the geometry has been simplified by removing vertices and projecting the polytope onto a plane. The example shows a hierarchy of three signaling polytopes  $\mathcal{C}_d^{3 \rightarrow 3}$  with  $d \in [1, 3]$ . Each signaling polytope is a convex set where hierarchy  $\mathcal{C}_{d=1}^{3 \rightarrow 3} \subset \mathcal{C}_{d=2}^{3 \rightarrow 3} \subset \mathcal{C}_{d=3}^{3 \rightarrow 3}$  holds for any  $n$  and  $n'$ . The vertices of each polytope are depicted as circles while the facets are lines. The  $\mathcal{C}_{d=1}^{3 \rightarrow 3}$  polytope is blue, the  $\mathcal{C}_{d=2}^{3 \rightarrow 3}$  polytope is orange, and the  $\mathcal{C}_{d=3}^{3 \rightarrow 3} = \mathcal{P}^{3 \rightarrow 3}$  polytope is black. A signaling dimension witness constitutes a facet of the signaling polytope. The channel  $\mathbf{P}_{\text{Red}}$  (red star) has  $\kappa(\mathbf{P}_{\text{Red}}) = 3$  while the channel  $\mathbf{P}_{\text{Green}}$  (green star) has  $\kappa(\mathbf{P}_{\text{Green}}) = 2$ .

As a result, the extreme points or vertices of the signaling polytope are deterministic channels  $\mathbf{V} \in \mathcal{P}^{n \rightarrow n'}$  such that  $\mathbf{V}$  has 0/1 matrix elements and  $\text{rank}(\mathbf{V}) \leq d$  where  $d$  is the number of distinct classical messages. We see that  $\dim(\mathcal{C}_d^{n \rightarrow n'}) = n(n' - 1)$  when  $d \geq 2$  as a result of the  $n$  normalization constraints on  $\mathcal{P}^{n \rightarrow n'}$ . For  $d = 1$ ,  $\dim(\mathcal{C}_{d=1}^{n \rightarrow n'}) = n'$  due to the independence between input and output,  $P(y|x) = P(y|x')$  for all  $x, x' \in \mathcal{X}$  and  $y \in \mathcal{Y}$ . By the Weyl-Minkowski Theorem [33], the signaling polytope can be described as the intersection of a finite set of linear inequalities describing half-spaces  $\{(\mathbf{G}_k, \mathbf{P}) \leq \gamma_k\}_{k=1}^r$ . For a channel  $\mathbf{P}$ , it follows that  $\mathbf{P} \in \mathcal{C}_d^{n \rightarrow n'}$  iff it satisfies all inequalities in this set. The signaling polytope is previously described in part by references [22,23]. In the main body we highlight key features of its structure while a more detailed characterization is found in Appendix B.

### B. Communication cost of simulating a channel

Having introduced signaling polytopes, we can now define the signaling dimension of quantum and classical channels within our framework. This terminology is adopted from recent work by Dall'Arno *et al.* [22] who defined the signaling dimension of a system in generalized probabilistic theories; an analogous quantity without shared randomness has also been studied by Heinosaari *et al.* [34]. In what follows, we assume that  $\mathcal{N} : \mathcal{S}(A) \rightarrow \mathcal{S}(B)$  is a completely positive trace-preserving (CPTP) map, with  $\mathcal{S}(A)$  denoting the set of density operators (i.e., trace-one positive operators) on system  $A$ , and similarly for  $\mathcal{S}(B)$ .

*Definition 2.*

(i) The *signaling dimension of a classical channel*  $\mathbf{P}$ , expressed as  $\kappa(\mathbf{P})$ , is the zero-error communication cost sim-

ulating  $\mathbf{P}$ . In other words, for  $\mathbf{P} \in \mathcal{P}^{n \rightarrow n'}$ ,  $\kappa(\mathbf{P})$  is the smallest integer  $d$  such that  $\mathbf{P} \in \mathcal{C}_d^{n \rightarrow n'}$ .

(ii) For a quantum channel  $\mathcal{N} : \mathcal{S}(A) \rightarrow \mathcal{S}(B)$ , let  $\mathcal{P}_{\mathcal{N}}^{n \rightarrow n'}$  denote the set of all classical channels  $\mathbf{P}_{\mathcal{N}} \in \mathcal{P}^{n \rightarrow n'}$  generated from  $\mathcal{N}$  via Eq. (1). The  $n \rightarrow n'$  *signaling dimension of a quantum channel*, expressed as  $\kappa^{n \rightarrow n'}(\mathcal{N})$ , is defined as the smallest integer  $d$  such that  $\mathcal{P}_{\mathcal{N}}^{n \rightarrow n'} \subset \mathcal{C}_d^{n \rightarrow n'}$ .

(iii) The *signaling dimension of a quantum channel* is expressed as  $\kappa(\mathcal{N})$  where  $\kappa(\mathcal{N})$  is the smallest integer  $d$  such that  $\mathcal{P}_{\mathcal{N}}^{n \rightarrow n'} \subset \mathcal{C}_d^{n \rightarrow n'}$  for all  $n, n'$ .

For any classical channel  $\mathbf{P} \in \mathcal{P}^{n \rightarrow n'}$  or quantum channel  $\mathcal{N}$  with fixed  $n$  and  $n'$ , a trivial upper bound on their respective signaling dimensions are given by

$$\kappa(\mathbf{P}) \leq \min\{n, n'\} \quad \text{and} \quad \kappa^{n \rightarrow n'}(\mathcal{N}) \leq \min\{n, n'\}. \quad (3)$$

Indeed, when this bound is attained, Alice and Bob can simulate any  $\mathbf{P} \in \mathcal{P}^{n \rightarrow n'}$ : either Alice applies channel  $\mathbf{P}$  on her input and sends the output to Bob, or she sends the input to Bob and he applies  $\mathbf{P}$  on his end. In Theorem 1 we provide necessary and sufficient conditions for when this trivial upper bound is attained. For a quantum channel  $\mathcal{N}$ , a stronger upper bound is found with respect to Hilbert space dimension,

$$\kappa(\mathcal{N}) \leq \min\{d_A, d_B\}, \quad (4)$$

where  $d_A$  and  $d_B$  are the Hilbert space dimensions of Alice and Bob's systems. This bound is a direct consequence of Frenkel and Weiner's result [23], which can be restated in our terminology as  $\kappa(\text{id}_d) = d$ , where  $\text{id}_d$  is the noiseless channel on a  $d$ -dimensional quantum system. To prove Eq. (4), Alice can either send the states  $\{\rho_x\}_x$  to Bob who then performs the POVM  $\{\mathcal{N}^\dagger(\Pi_y)\}_y$ , or she can send the states  $\{\mathcal{N}(\rho_x)\}_x$  to Bob who then performs the POVM  $\{\Pi_y\}_y$ . Here  $\mathcal{N}^\dagger$  denotes the adjoint map of  $\mathcal{N}$ . Another relationship we observe is

$$\kappa^{n \rightarrow n'}(\mathcal{N}) = \kappa^{n \rightarrow d_B^2}(\mathcal{N}) \quad \forall n' \geq d_B^2. \quad (5)$$

This follows from Carathéodory's Theorem [35], which implies that every POVM on a  $d_B$ -dimensional system can be expressed as a convex combination of POVMs with no more than  $d_B^2$  outcomes [36]. Since shared randomness is free, Alice and Bob can always restrict their attention to POVMs with no more than  $d_B^2$  outcomes for the purposes of simulating any channel in  $\mathcal{P}_{\mathcal{N}}^{n \rightarrow n'}$  when  $n' \geq d_B^2$ .

The signaling dimension of quantum and classical channels can be unified through the following observation. A classical channel from set  $\mathcal{X}$  to  $\mathcal{Y}$  can be represented by a CPTP map  $\mathcal{N} : \mathcal{S}(\mathbb{C}^{|\mathcal{X}|}) \rightarrow \mathcal{S}(\mathbb{C}^{|\mathcal{Y}|})$  that completely dephases its input and output in fixed orthonormal bases  $\{|x\rangle\}_{x \in \mathcal{X}}$  and  $\{|y\rangle\}_{y \in \mathcal{Y}}$ , respectively. The transition probabilities of  $\mathcal{N}$  are then given by Eq. (1) as  $P_{\mathcal{N}}(y|x) = \text{Tr}[|y\rangle\langle y| \mathcal{N}(|x\rangle\langle x|)]$ . The channel  $\mathcal{N}$  can be used to generate another channel  $\overline{\mathcal{N}}$  with input and output alphabets  $\overline{\mathcal{X}}$  and  $\overline{\mathcal{Y}}$  by performing a pre-processing map  $\mathbf{T} : \overline{\mathcal{X}} \rightarrow \mathcal{X}$  and post-processing map  $\mathbf{R} : \mathcal{Y} \rightarrow \overline{\mathcal{Y}}$ , thereby yielding the channel  $\mathbf{P}_{\overline{\mathcal{N}}} = \mathbf{R} \mathbf{P}_{\mathcal{N}} \mathbf{T}$ . When this relationship holds,  $\mathbf{P}_{\overline{\mathcal{N}}}$  is said to be *ultraweakly majorized* by  $\mathbf{P}_{\mathcal{N}}$  [31,34], and the signaling dimension of  $\mathbf{P}_{\overline{\mathcal{N}}}$  is no greater than that of  $\mathbf{P}_{\mathcal{N}}$  [15]. Thus,  $\kappa(\mathbf{P}_{\mathcal{N}})$  can always be obtained from the



transition probabilities  $P_{\mathcal{N}}(y|x)$  directly with no need for pre/post-processing.

### C. Witnessing signaling dimension

The signaling dimension is a device-independent quantity that can be ascertained from input-output correlations of a channel. To certify the signaling dimension of a classical channel  $\mathbf{P}_{\mathcal{N}}$ , one must find the smallest  $d$  such that  $\mathbf{P}_{\mathcal{N}} \in \mathcal{C}_d^{n \rightarrow n'}$ . Hence, we can apply the structure of the signaling polytope to develop device-independent tests of signaling dimension. Within this framework, the linear inequalities bounding a signaling polytope  $\mathcal{C}_d^{n \rightarrow n'}$  are used to witness a channel's inclusion in or exclusion from  $\mathcal{C}_d^{n \rightarrow n'}$ . This approach is taken by Dall'Arno *et al.* to demonstrate a violation of the No-Hypersignaling Principle [22]. These linear witnesses are similar to those applied in classical and quantum dimensionality witnessing [24–28].

**Definition 3.** A *signaling dimension witness* of the signaling polytope  $\mathcal{C}_d^{n \rightarrow n'}$  is a linear inequality  $\langle \mathbf{G}, \mathbf{P} \rangle \leq \gamma$  that satisfies  $\mathcal{C}_d^{n \rightarrow n'} \subset \{\mathbf{P} \in \mathcal{P}^{n \rightarrow n'} \mid \langle \mathbf{G}, \mathbf{P} \rangle \leq \gamma\}$ . A signaling dimension witness is “tight” if the equality  $\langle \mathbf{G}, \mathbf{P} \rangle = \gamma$  is satisfied by  $\dim(\mathcal{C}_d^{n \rightarrow n'}) = n(n' - 1)$  affinely independent vertices. In other words, a tight signaling dimension witness describes a facet of  $\mathcal{C}_d^{n \rightarrow n'}$  (see Fig. 2).

It follows for a channel  $\mathbf{P} \in \mathcal{P}^{n \rightarrow n'}$  that if  $\langle \mathbf{G}, \mathbf{P} \rangle \not\leq \gamma$ , then  $\mathbf{P} \notin \mathcal{C}_d^{n \rightarrow n'}$ . That is, if the correlations  $P(y|x)$  violate a signaling dimension witness of  $\mathcal{C}_d^{n \rightarrow n'}$ , then the signaling dimension is lower bounded as  $\kappa(\mathbf{P}) > d$ . Alternatively, if  $\mathbf{P}$  satisfy all signaling dimension witnesses belonging to the complete set of signaling polytope facets, then the signaling dimension is upper bounded as  $\kappa(\mathbf{P}) \leq d$ . It then becomes our objective to procure signaling dimension witnesses that can be applied in the device-independent certification of signaling dimension.

### III. WITNESSES FOR SIGNALING DIMENSION

In this section we discuss the signaling dimension witnesses that bound signaling polytopes. Since signaling polytopes are invariant under the relabelling of inputs and outputs, all discussed inequalities describe a family of inequalities where each element is obtained by a permutation of the inputs and/or outputs. Additionally, a signaling dimension witness for one signaling polytope can be lifted to a polytope having more inputs and/or outputs [37,38]. Formally, a signaling dimension witness  $\langle \mathbf{G}, \mathbf{P} \rangle \leq \gamma$  is said to be input lifted to  $\langle \mathbf{G}', \mathbf{P} \rangle \leq \gamma$  if  $\mathbf{G}' \in \mathbb{R}^{n' \times m}$  is obtained from  $\mathbf{G} \in \mathbb{R}^{n' \times n}$  by padding it with  $(m - n)$  all-zero columns. However, a signaling dimension witness  $\langle \mathbf{G}, \mathbf{P} \rangle \leq \gamma$  is said to be output lifted to  $\langle \mathbf{G}', \mathbf{P} \rangle \leq \gamma$  if  $\mathbf{G}' \in \mathbb{R}^{m' \times n}$  is obtained from  $\mathbf{G} \in \mathbb{R}^{n' \times n}$  by copying rows; i.e., there exists a surjective function  $f: [m'] \rightarrow [n']$  such that  $G'_{y,x} = G_{f(y),x}$  for all  $y \in [m']$  and  $x \in [n]$ . Note that these descriptions of input/output liftings requires that  $m' > n'$  and  $m > n$ . As an example, we demonstrate liftings on the identity matrix  $\mathbf{G} = \mathbb{I}_3$ ,

$$\mathbf{G} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \xrightarrow[\text{Lifting}]{\text{Input}} \mathbf{G}' = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \quad (6)$$

$$\mathbf{G} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \xrightarrow[\text{Lifting}]{\text{Output}} \mathbf{G}' = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}. \quad (7)$$

To obtain polytope facets, it is typical to first enumerate the vertices, then use a transformation technique such as Fourier-Motzkin elimination to derive the facets [33]. Software such as PORTA [39,40] assists in this computation, but the large number of vertices leads to impractical run times. To improve efficiency, we utilize the adjacency decomposition technique which heavily exploits the permutation symmetry of signaling polytopes [30] (see Appendix C). Our software and computed facets are publicly available on Github [32] while a catalog of general tight signaling dimension witnesses is provided in Appendix D. We now turn to a specific family of signaling dimension witnesses motivated by our computational results.

#### A. Ambiguous guessing games

For  $k \in [0, n']$  and  $d \leq \min\{n, n'\}$ , let  $\mathbf{G}_{k,d}^{n,n'}$  be any  $n' \times n$  matrix such that (i)  $k$  rows are stochastic with 0/1 elements, and (ii) the remaining  $(n' - k)$  rows have  $1/(n - d + 1)$  in each column. As explained below, it will be helpful to refer to rows of type (i) as “guessing rows” and rows of type (ii) as “ambiguous rows.” For example, if  $n = n' = 6$ ,  $k = 5$ , and  $d = 2$ , then up to a permutation of rows and columns we have

$$\mathbf{G}_{5,2}^{6,6} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ \frac{1}{5} & \frac{1}{5} & \frac{1}{5} & \frac{1}{5} & \frac{1}{5} & \frac{1}{5} \end{bmatrix}. \quad (8)$$

Note that the example matrix in Eq. (8) is nonunique and represents a member of the family of ambiguous guessing games with five guessing rows. For any channel  $\mathbf{P} \in \mathcal{C}_d^{n \rightarrow n'}$ , the signaling dimension witness

$$\langle \mathbf{G}_{k,d}^{n,n'}, \mathbf{P} \rangle \leq d \quad (9)$$

is satisfied. To prove this bound, suppose without loss of generality that the first  $k$  rows of  $\mathbf{G}_{k,d}^{n,n'}$  are guessing rows. Let  $\mathbf{V}$  be any vertex of  $\mathcal{C}_d^{n \rightarrow n'}$  where  $t$  of its first  $k$  rows are nonzero. If  $t = d$ , then clearly Eq. (9) holds. Otherwise, if  $t < d$ , then  $\langle \mathbf{G}_{k,d}^{n,n'}, \mathbf{V} \rangle \leq t + (n - t)/(n - d + 1) \leq d$ , where the last inequality follows after some algebraic manipulation.

Equation (9) can be interpreted as the score of a guessing game that Bob plays with Alice. Suppose that Alice chooses a channel input  $x \in [n]$  with uniform probability and sends it through a channel  $\mathbf{P}$ . Based on the channel output  $y$ , Bob guesses the value of  $x$ . Formally, Bob computes  $\hat{x} = f(y)$  for some guessing function  $f$ , and if  $\hat{x} = x$  then he receives one point. In this game, Bob may also declare Alice's input as being ambiguous or indistinguishable, meaning that  $f: [d] \rightarrow [n] \cup \{?\}$  with “?” denoting Bob's declaration of the ambiguous input. However, whenever Bob declares “?” he only receives  $1/(n - d + 1)$  points. Then, Eq. (9) says that

whenever  $\mathbf{P} \in \mathcal{C}_d^{n \rightarrow n'}$  Bob's average score is bounded by  $\frac{d}{n}$ . Note, there is a one-to-one correspondence between each  $\mathbf{G}_{k,d}^{n,n'}$  and the particular guessing function  $f$  that Bob performs. If  $y$  labels a guessing row of  $\mathbf{G}_{k,d}^{n,n'}$ , then  $f(y) = \hat{x}$ , where  $\hat{x}$  labels the only nonzero column of row  $y$ . However, if  $y$  labels an ambiguous row, then  $f(y) = "?"$ .

We define the  $(k, d)$ -ambiguous polytope  $\mathcal{A}_{k,d}^{n \rightarrow n'}$  as the collection of all channels  $\mathbf{P} \in \mathcal{P}^{n \rightarrow n'}$  satisfying Eq. (9) for every  $\mathbf{G}_{k,d}^{n,n'}$ . Naturally,  $\mathcal{C}_d^{n \rightarrow n'} \subset \mathcal{A}_{k,d}^{n \rightarrow n'}$  for all  $k \in [0, n']$ , therefore, if  $\mathbf{P} \notin \mathcal{A}_{k,d}^{n \rightarrow n'}$ , then  $\mathbf{P} \notin \mathcal{C}_d^{n \rightarrow n'}$ . Based on the discussion of the previous paragraph, it is easy to decide membership of  $\mathcal{A}_{k,d}^{n \rightarrow n'}$ .

**Proposition 1.** A channel  $\mathbf{P} \in \mathcal{P}^{n \rightarrow n'}$  belongs to  $\mathcal{A}_{k,d}^{n \rightarrow n'}$  iff

$$\max_{\pi \in \mathcal{S}_{n'}} \sum_{i=1}^k \|\mathbf{r}_{\pi(i)}\|_{\infty} + \frac{1}{n-d+1} \sum_{i=k+1}^{n'} \|\mathbf{r}_{\pi(i)}\|_1 \leq d, \quad (10)$$

where the maximization is taken over all permutations on  $[n']$ ,  $\mathbf{r}_i$  denotes the  $i^{\text{th}}$  row of  $\mathbf{P}$ ,  $\|\mathbf{r}_i\|_{\infty}$  is the largest element in  $\mathbf{r}_i$ , and  $\|\mathbf{r}_i\|_1$  is the row sum of  $\mathbf{r}_i$ .

The maximization on the left-hand side (LHS) of Eq. (10) can be performed efficiently using the following procedure. For each row  $\mathbf{r}_i$  we assign a pair  $(a_i, b_i)$  where  $a_i = \|\mathbf{r}_i\|_{\infty}$  and  $b_i = \frac{1}{n-d+1} \|\mathbf{r}_i\|_1$ . Define  $\delta_i = a_i - b_i$ , and relabel the rows of  $\mathbf{P}$  in nonincreasing order of the  $\delta_i$ . Then according to this sorting, we have an ambiguous guessing game score of  $\sum_{i=1}^k a_i + \sum_{i=k+1}^{n'} b_i$ , which we claim attains the maximum on the LHS of Eq. (10). Indeed, for any other row permutation  $\pi$ , the guessing game score is given by

$$\begin{aligned} & \sum_{\substack{i \in \{1, \dots, k\} \\ \pi(i) \in \{1, \dots, k\}}} a_i + \sum_{\substack{i \in \{1, \dots, k\} \\ \pi(i) \in \{k+1, \dots, n'\}}} b_i \\ & + \sum_{\substack{i \in \{k+1, \dots, n'\} \\ \pi(i) \in \{1, \dots, k\}}} a_i + \sum_{\substack{i \in \{k+1, \dots, n'\} \\ \pi(i) \in \{k+1, \dots, n'\}}} b_i. \end{aligned} \quad (11)$$

Hence, the difference in these two scores is

$$\sum_{\substack{i \in \{1, \dots, k\} \\ \pi(i) \in \{k+1, \dots, n'\}}} (a_i - b_i) - \sum_{\substack{i \in \{k+1, \dots, n'\} \\ \pi(i) \in \{1, \dots, k\}}} (a_i - b_i) \geq 0, \quad (12)$$

where the inequality follows from the fact that we have ordered the indices in nonincreasing order of  $(a_i - b_i)$ , and the number of terms in each summation is the same since  $\pi$  is a bijection.

A special case of the ambiguous guessing games arises when  $k = n'$ . Then up to a normalization factor  $\frac{1}{n}$ , we interpret the LHS of Eq. (10) as the success probability when Bob performs maximum likelihood estimation of Alice's input value  $x$  given his outcome  $y$  [i.e., he chooses the value  $x$  that maximizes  $P(y|x)$ ]. We hence define  $\mathcal{M}_d^{n \rightarrow n'} := \mathcal{A}_{n',d}^{n \rightarrow n'}$  as the *maximum likelihood (ML) estimation polytope*. Using Proposition 1 we see that

$$\mathbf{P} \in \mathcal{M}_d^{n \rightarrow n'} \iff \sum_{y=1}^{n'} \max_{x \in [n]} P(y|x) \leq d. \quad (13)$$

An important question is whether the ambiguous guessing signaling dimension witnesses of Eq. (9) are tight for a signaling polytope  $\mathcal{C}_d^{n \rightarrow n'}$ . In general, this will not be case. For instance,  $\langle \mathbf{G}_{k,d}^{n,n'}, \mathbf{P} \rangle \leq d$  is trivially satisfied whenever  $k = 0$ . Nevertheless, in many cases we can establish tightness of these inequalities. A demonstration of the following facts is carried out in Appendix E.

**Proposition 2.**

(i) For  $\min\{n, n'\} > d > 1$  and  $k = n'$ , Eq. (9) is a tight signaling dimension witness of  $\mathcal{C}_d^{n \rightarrow n'}$  iff  $\mathbf{G}_{k,d}^{n,n'}$  can be obtained by performing input/output liftings and row/column permutations on an  $m \times m$  identity matrix  $\mathbb{I}_m$ , with  $\min\{n, n'\} \geq m > d$ .

(ii) For  $n' > k \geq n > d > 1$ , Eq. (9) is a tight signaling dimension witness of  $\mathcal{C}_d^{n \rightarrow n'}$  iff  $\mathbf{G}_{k,d}^{n,n'}$  can be obtained from the  $(n+1) \times n$  matrix

$$\begin{bmatrix} \frac{1}{n-d+1} & \dots & \frac{\mathbb{I}_n}{n-d+1} & \dots & \frac{1}{n-d+1} \end{bmatrix} \quad (14)$$

by performing output liftings and row/column permutations.

Note that the input/output liftings are used to manipulate the identity matrix  $\mathbb{I}_m$  and the matrix of Eq. (14) into an  $n' \times n$  matrix  $\mathbf{G}_{k,d}^{n,n'}$ . The tight signaling dimension witnesses described in Proposition 2(i) completely characterize the ML polytope  $\mathcal{M}_d^{n \rightarrow n'}$ . For this reason, we refer to any  $\mathbf{G}_{k,d}^{n,n'}$  satisfying the conditions of Proposition 2(i) as a maximum likelihood (ML) facet (see Appendix D 2). Likewise, we refer to any  $\mathbf{G}_{k,d}^{n,n'}$  satisfying the conditions of Proposition 2(ii) as an ambiguous guessing facet (see Appendix D 3).

## B. Fully characterized signaling polytopes

In general, we are unable to identify the complete set of tight signaling dimension witnesses that bound each signaling polytope  $\mathcal{C}_d^{n \rightarrow n'}$ . However, we analytically solve the problem in special cases.

**Theorem 1.** Let  $n$  and  $n'$  be arbitrary integers.

- (i) If  $d = n' - 1$ , then  $\mathcal{C}_d^{n \rightarrow n'} = \mathcal{M}_d^{n \rightarrow n'}$ .
- (ii) If  $d = n - 1$ , then  $\mathcal{C}_d^{n \rightarrow n'} = \bigcap_{k=n}^{n'} \mathcal{A}_{k,d}^{n \rightarrow n'}$ .

In other words, to decide whether a channel can be simulated by an amount of classical messages strictly less than the input/output alphabets, it suffices to consider the ambiguous guessing games. Moreover, by Eq. (10) it is simple to check if these conditions are satisfied for a given channel  $\mathbf{P}$ . A proof of Theorem 1 is found in Appendix F.

We also characterize the  $\mathcal{C}_2^{n \rightarrow 4}$  signaling polytope. As an application, this case can be used to understand the classical simulation cost of performing Bell measurements on a two-qubit system, since this process induces a classical channel with four outputs.

**Theorem 2.** For any integer  $n$ , a channel  $\mathbf{P} \in \mathcal{P}^{n \rightarrow 4}$  belongs to  $\mathcal{C}_2^{n \rightarrow 4}$  iff it satisfies the eight signaling dimension witnesses depicted in Table I and all their input/output permutations.

Remarkably, this result shows that no new facet classes for  $\mathcal{C}_2^{n \rightarrow 4}$  are found when  $n > 6$ . Consequently, to demonstrate that a channel  $\mathbf{P} \in \mathcal{P}^{n \rightarrow 4}$  requires more than one bit for simulation, it suffices to consider input sets of size no greater than

TABLE I. Generator facets for the  $\mathcal{C}_2^{6 \rightarrow 4}$  signaling polytope. Each inequality is expressed as  $\gamma \geq \mathbf{G}$  where the inner product  $\langle \mathbf{G}, \mathbf{P} \rangle$  is implied. (a) ML facet input/output lifted from  $\mathcal{C}_2^{3,3}$ . (b) ML facet output lifted from  $\mathcal{C}_2^{4 \rightarrow 4}$ . (c) Anti-guessing facet output lifted from  $\mathcal{C}_2^{4 \rightarrow 4}$ . (d)  $k$ -guessing facet of  $\mathcal{C}_2^{6 \rightarrow 4}$ . (e) Ambiguous guessing facet output lifted from  $\mathcal{C}_2^{3 \rightarrow 4}$ . (f–h) Rescalings of the  $\mathcal{C}_2^{3 \rightarrow 4}$  ambiguous guessing facet output lifted to  $\mathcal{C}_2^{6 \rightarrow 4}$ . General forms of these tight signaling dimension witnesses are derived in Appendix D.

(a) $2 \geq$	$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix}$	(b) $2 \geq$	$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}$
(c) $3 \geq$	$\begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}$	(d) $5 \geq$	$\begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$
(e) $4 \geq$	$\begin{bmatrix} 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \end{bmatrix}$	(f) $4 \geq$	$\begin{bmatrix} 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \end{bmatrix}$
(g) $4 \geq$	$\begin{bmatrix} 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \end{bmatrix}$	(h) $4 \geq$	$\begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 \end{bmatrix}$

six. For  $n < 6$ , the facet classes of  $\mathcal{C}_2^{n \rightarrow 4}$  are given by the facets in Table I having  $(6 - n)$  all-zero columns. We conjecture that in general, no more than  $\binom{n'}{d}$  inputs are needed to certify that a channel  $\mathbf{P} \in \mathcal{P}^{n \rightarrow n'}$  has a signaling dimension larger than  $d$ . A proof of Theorem 2 is found in Appendix G.

#### IV. CERTIFYING THE SIGNALING DIMENSION OF A QUANTUM CHANNEL

In practice, the classical or quantum channel connecting Alice and Bob may be unknown or not fully characterized. This is the case in most experimental settings where unpredictable noise affects the encoded signaling states. In such scenarios, it is desirable to ascertain certain properties of the channel without having access to the physical device or pre-established trust in the hardware. A device-independent approach infers properties of the channel by analyzing the observed classical input-output correlations  $P(y|x)$  obtained as sample averages over many uses of the memoryless channel [29].

To certify the device signaling dimension of a quantum channel, Alice and Bob use trusted state preparations and measurements, but make minimal assumptions about the untrusted channel  $\mathcal{N}^{A \rightarrow B}$  (see Fig. 3). Their objective is to bound  $\kappa(\mathcal{N})$  using observed classical input-output correlations  $P_{\mathcal{N}}(y|x)$  and the certification procedure for  $\kappa(\mathbf{P}_{\mathcal{N}})$ . Applying the results of the previous section, if  $\langle \mathbf{G}, \mathbf{P} \rangle \leq \gamma$  is a signaling dimension witness for  $\mathcal{C}_d^{n \rightarrow n'}$  and

$$\max_{\{\rho_x\}_x, \{\Pi_y\}_y} \sum_{y,x} G_{y,x} \text{Tr}[\Pi_y \mathcal{N}(\rho_x)] > \gamma, \quad (15)$$

then  $\min\{d_A, d_B\} \geq \kappa(\mathcal{N}) > d$  where the upper bound comes from Eq. (4). The conic optimization problem in Eq. (15) can be analytically solved only in special cases [41]. Hence, deciding whether a given quantum channel can violate a particular signaling dimension witness is typically quite challenging.

One convenience is that we no longer need to consider permutations of the induced classical channel  $\mathbf{P}_{\mathcal{N}}$  because these permutations can be achieved through selecting appropriate quantum states  $\{\rho_x\}_x$  and measurements  $\{\Pi_y\}_y$ .

The upper bound provided by Eq. (4) draws a connection between the signaling dimension of a quantum channel and the dimension of its input/output Hilbert spaces. Hence, a device-independent certification of signaling dimension leads to a device-independent certification of the physical input/output Hilbert spaces of the channel connecting Alice and Bob.

Despite the general difficulty of computing  $\kappa(\mathcal{N})$ , we nevertheless establish bounds for the signaling dimension of

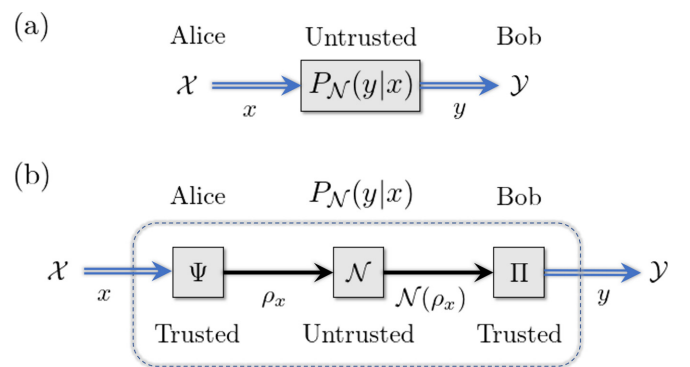


FIG. 3. A depiction of the required device trust to implement the device-independent certification of the signaling dimension for classical and quantum channels. (a) Alice and Bob certify the signaling dimension of an untrusted classical channel  $\mathbf{P}_{\mathcal{N}}$  using only the probabilities  $P_{\mathcal{N}}(y|x)$  for all  $x \in \mathcal{X}$  and  $y \in \mathcal{Y}$ . (b) Alice and Bob certify the signaling dimension of an untrusted quantum channel  $\mathcal{N}$  using trusted state preparation  $\Psi$  and trusted measurement  $\Pi$ . If Alice and Bob do not trust their encode/decode devices, then bounds on the signaling dimension can still be established by treating the quantum communication system as a classical channel.

partial replacer channels. A  $d$ -dimensional partial replacer channel has the form

$$\mathcal{R}_\mu(X) = \mu X + (1 - \mu)\text{Tr}[X]\sigma, \quad (16)$$

where  $1 \geq \mu \geq 0$  and  $\sigma$  is some fixed density matrix. The partial depolarizing channel  $\mathcal{D}_\mu$  corresponds to  $\sigma$  being the maximally mixed state whereas the partial erasure channel  $\mathcal{E}_\mu$  corresponds to  $\sigma$  being an erasure flag  $|E\rangle\langle E|$  with  $|E\rangle$  being orthogonal to  $\{|1\rangle, \dots, |d\rangle\}$ .

**Theorem 3.** The signaling dimension of a partial replacer channel is bounded by

$$\lceil \mu d + 1 - \mu \rceil \leq \kappa(\mathcal{R}_\mu) \leq \min\{d, \lceil \mu d + 1 \rceil\}. \quad (17)$$

Moreover, for the partial erasure channel, the upper bound is tight for all  $\mu \in [0, 1]$ .

*Proof.* We first prove the upper bound in Eq. (17). The trivial bound  $\kappa(\mathcal{R}_\mu) \leq d$  was already observed in Eq. (4). To show that  $\kappa(\mathcal{R}_\mu) \leq \lceil \mu d + 1 \rceil$ , let  $\{\rho_x\}_x$  be any collection of inputs and  $\{\Pi_y\}_y$  a POVM. Then

$$P_{\mathcal{R}_\mu}(y|x) = \mu P(y|x) + (1 - \mu)S(y), \quad (18)$$

where  $P(y|x) = \text{Tr}[\Pi_y \rho_x]$  and  $S(y) = \text{Tr}[\Pi_y \sigma]$ . From Ref. [23], we know that  $P(b|x)$  can be decomposed like Eq. (2). Substituting this into Eq. (18) yields

$$P_{\mathcal{R}_\mu}(u|x) = \sum_{\lambda} q(\lambda) \sum_{m=1}^d R_\lambda(m|x) \times [\mu T_\lambda(y|m) + (1 - \mu)S(y)]. \quad (19)$$

For  $r = \lceil \mu d + 1 \rceil$ , let  $v$  be a random variable uniformly distributed over  $\{\binom{[d]}{r-1}\}$ , which is the collection of all subsets of  $[d]$  having size  $r - 1$ . For a given  $\lambda$ ,  $v$ , and input  $x$ , Alice performs the channel  $\mathbf{T}_\lambda$ . If  $m \in v$ , then Alice sends message  $m' = m$ ; otherwise, Alice sends message  $m' = 0$ . Upon receiving  $m'$ , Bob does the following: if  $m' \neq 0$  he performs channel  $\mathbf{R}_\lambda$  with probability  $\frac{\mu d}{r-1}$  and samples from distribution  $S(y)$  with probability  $1 - \frac{\mu d}{r-1}$ ; if  $m' = 0$  he samples from  $S(y)$  with probability one. Since  $\Pr\{m \in v\} = \frac{r-1}{d}$ , this protocol faithfully simulates  $P_{\mathcal{R}_\mu}$ . To establish the lower bound in Eq. (18), suppose that Alice sends orthogonal states  $\{|1\rangle, \dots, |d\rangle\}$  and Bob measures in the same basis. Then

$$\sum_{i=1}^d \langle i | \mathcal{R}_\mu(|i\rangle\langle i|) | i \rangle = d\mu + (1 - \mu), \quad (20)$$

which will violate Eq. (9) for the ML polytope  $\mathcal{M}_r^{d \rightarrow d}$  whenever  $r < \mu d + (1 - \mu)$ . Hence, any zero-error simulation will require at least  $\lceil \mu d + 1 - \mu \rceil$  classical messages. For the erasure channel, this lower bound can be tightened by considering the score for other ambiguous games, as detailed in Appendix H.

## V. SUMMARY AND DISCUSSION

In this work, we have presented the signaling dimension of a channel as its classical simulation cost. In doing so, we have advanced a device-independent framework for certifying the signaling dimension of quantum and classical channels as well as their input/output dimensions. While this work focuses on

communication systems, our framework also applies to any quantum process including computation and memory tasks.

In principle, given a classical channel  $\mathbf{P} \in \mathcal{P}^{n \rightarrow n'}$  the signaling dimension  $\kappa(\mathbf{P})$  can be certified incrementally. In each step, the parameter  $d$  is fixed and all signaling dimension witnesses bounding  $\mathcal{C}_d^{n \rightarrow n'}$ ,  $\langle \mathbf{G}_k, \mathbf{P} \rangle \leq \gamma_k$ , are checked for violation. If no violation is found, then  $\mathbf{P} \in \mathcal{C}_d^{n \rightarrow n'}$  and we decrement the integer  $d \rightarrow d - 1$ . The procedure ends when violation to a signaling dimension witness is found thereby placing a tight lower bound on the signaling dimension. Unfortunately, this task becomes intractable as  $n$  and  $n'$  increase because the complete set of facet inequalities of the signaling polytope  $\mathcal{C}_d^{n \rightarrow n'}$  is challenging to computationally obtain and the number of inequalities to test increases dramatically. To address this issue, we apply the Propositions and Theorems of Sec. III.

To efficiently obtain a lower bound for the signaling dimension  $\kappa(\mathbf{P})$  we apply Proposition 1 and employ the bounds of the  $(k, d)$ -ambiguous polytope  $\mathcal{A}_{k,d}^{n \rightarrow n'}$  as signaling dimension witnesses for  $\mathcal{C}_d^{n \rightarrow n'}$ . The most efficient lower bound is obtained when no ambiguous rows are considered ( $k = n'$ ). The lower bound on  $\kappa(\mathbf{P})$  is then found through the maximum-likelihood estimation described by Eq. (13) to find

$$\kappa(\mathbf{P}) \geq \left\lceil \sum_{y=1}^{n'} \max_{x \in [n]} P(y|x) \right\rceil. \quad (21)$$

To improve upon this lower bound, one may perform the maximization in Eq. (10) for each value  $k \in [1, n']$ . Assuming that the rows of  $\mathbf{P}$  have been sorted to maximize Eq. (10), the lower bound on signaling dimension is then witnessed to be

$$\kappa(\mathbf{P}) \geq \left\lceil \max_{k \in [1, n']} \sum_{i=1}^k \|\mathbf{r}_{\pi(i)}\|_\infty + \sum_{i=k+1}^{n'} \frac{\|\mathbf{r}_{\pi(i)}\|_1}{n - d + 1} \right\rceil. \quad (22)$$

An upper bound on the signaling dimension of a classical channel is found using Theorem 1. For the cases  $d = n - 1$  or  $d = n' - 1$  the signaling polytope is fully characterized and the complete set of tight signaling dimension witnesses are known to be ambiguous guessing games. Naturally, if the right-hand side (RHS) of Eq. (22) is found to be greater than  $(n - 1)$  or  $(n' - 1)$ , then  $\kappa(\mathbf{P}) = \min\{n, n'\}$ . Otherwise, the upper bound on the signaling dimension is witnessed to be

$$\kappa(\mathbf{P}) \leq \min\{n, n'\} - 1. \quad (23)$$

If a classical channel  $\mathbf{P} \in \mathcal{P}^{n \rightarrow 4}$  has 4 outputs ( $n' = 4$ ), then the exact signaling dimension can be certified. By Theorem 2 the complete set of tight signaling dimension witnesses are known for the  $\mathcal{C}_{d=2}^{n \rightarrow 4}$  signaling polytope. For a channel  $\mathbf{P} \in \mathcal{P}^{n \rightarrow 4}$ , if  $\mathbf{P} \in \mathcal{C}_{d=2}^{n \rightarrow 4}$ , then the inequality

$$\max_{\pi_A \in S_n, \pi_B \in S_{n'}} \langle \mathbf{G}_k, \pi_B \mathbf{P} \pi_A \rangle \leq \gamma_k \quad (24)$$

must be satisfied for all signaling dimension witnesses  $(\mathbf{G}_k, \gamma_k)$  listed in Table I. Note that the LHS of Eq. (24) is maximized with respect to all row and column permutations of  $\mathbf{P}$ . Hence, for the  $n' = 4$  case, we can easily decide if  $\kappa(\mathbf{P}) = 2$ . If a violation of Eq. (24) is found, then we then apply Theorem 1 to decide whether  $\mathbf{P} \in \mathcal{C}_{d=3}^{n \rightarrow 4}$ . The signaling



dimension is found to be  $\kappa(\mathbf{P}) = 3$  if  $\mathbf{P} \in \mathcal{C}_{d=3}^{n \rightarrow 4}$ , otherwise  $\kappa(\mathbf{P}) = 4$ .

The family of ambiguous guessing games includes the maximum likelihood facets, which say that  $\sum_{y=1}^{n'} \max_{x \in [n]} P(y|x) \leq d$  for all  $\mathbf{P} \in \mathcal{C}_d^{n \rightarrow n'}$ . Since the results of Frenkel and Weiner imply that  $\mathcal{P}_{\mathcal{N}^{A \rightarrow B}}^{n \rightarrow n'} \subset \mathcal{C}_d^{n \rightarrow n'}$  whenever  $d \geq \min\{d_A, d_B\}$  for channel  $\mathcal{N}^{A \rightarrow B}$  [23], it follows that

$$\max_{\{\rho_x\}_{x \in [n]} \{\Pi_y\}_{y \in [n]}} \sum_{x=1}^n \text{Tr}[\Pi_x \mathcal{N}(\rho_x)] \leq d, \quad (25)$$

an observation also made in Ref. [27]. Despite the simplicity of this bound, in general it is too loose to certify the input/output Hilbert space dimensions of a channel. For example, consider the 50 : 50 erasure channel  $\mathcal{E}_{1/2}$  acting on a  $d_A = 3$  system. It can be verified that  $\mathcal{P}_{\mathcal{E}_{1/2}}^{n \rightarrow n'} \subset \mathcal{M}_2^{n \rightarrow n'}$ , i.e.,  $\sum_x \text{Tr}[\Pi_x \mathcal{E}_{1/2}(\rho_x)] \leq 2$  for all  $\{\rho_x\}_x$  and  $\{\Pi_y\}_y$ . Hence, maximum likelihood estimation yields the lower bound  $\kappa(\mathcal{E}_{1/2}) \geq 2$ . However, the classical channel

$$\mathbf{P}_{\mathcal{E}_{1/2}} = \begin{bmatrix} 0.5 & 0 & 0 \\ 0 & 0.5 & 0 \\ 0 & 0 & 0.5 \\ 0.5 & 0.5 & 0.5 \end{bmatrix} \quad (26)$$

generated by orthonormal input states  $\{|1\rangle, |2\rangle, |3\rangle\}$  and a measurement in the orthonormal basis  $\{|1\rangle, |2\rangle, |3\rangle, |E\rangle\}$  violates Eq. (10) for the  $\mathcal{A}_{3,2}^{3 \rightarrow 4}$  ambiguous polytope. Hence,  $\mathbf{P}_{\mathcal{E}_{1/2}} \notin \mathcal{A}_{3,2}^{3 \rightarrow 4}$ , and it follows that  $\kappa^{3 \rightarrow 4}(\mathcal{E}_{1/2}) \geq 3$ . Therefore, the ambiguous guessing game certifies the qutrit nature of the input space whereas maximum likelihood estimation does not.

Our results can be extended in two key directions. First, our characterization of the signaling polytope is incomplete. Novel signaling dimension witnesses, lifting rules, and complete sets of facets can be derived beyond those discussed in this work. Such results would help improve the signaling dimension bounds and the efficiency of computing signaling dimension witnesses. Second, the signaling dimension specifies the classical cost of simulating a quantum channel, but not the protocol that achieves the classical simulation. Such a simulation protocol would apply broadly across the field of quantum information science and technology.

## VI. SUPPORTING SOFTWARE

This work is supported by SignalingDimension.jl [32]. This software package includes our signaling polytope computations, numerical facet verification, and signaling dimension certification examples. SignalingDimension.jl is publicly available on Github and written in the Julia programming language [42]. The software is documented, tested, and reproducible on a laptop computer. The interested reader should review the software documentation as it elucidates many details of our work.

## ACKNOWLEDGMENTS

We thank M. Junge for enlightening discussions during the preparation of this paper. We acknowledge NSF Award No. 2016136 for supporting this work.

## APPENDIX A: NOTATION GLOSSARY

See Table II for a glossary of notation introduced within this work.

## APPENDIX B: SIGNALING POLYTOPE STRUCTURE

In this Appendix we provide details about the structure of signaling polytopes (see Definition 1). The signaling polytope, denoted by  $\mathcal{C}_d^{n \rightarrow n'}$ , is a subset of  $\mathcal{P}^{n \rightarrow n'}$ . Therefore, a channel  $\mathbf{P} \in \mathcal{C}_d^{n \rightarrow n'}$  has matrix elements  $P(y|x)$  subject to the constraints of nonnegativity  $P(y|x) \geq 0$  and normalization  $\sum_{y \in [n']} P(y|x) = 1$  for all  $y \in [n']$  and  $x \in [n]$ . Furthermore, since channels  $\mathbf{P} \in \mathcal{C}_d^{n \rightarrow n'}$  are permitted the use of shared randomness, the set  $\mathcal{C}_d^{n \rightarrow n'}$  is convex.

In the two extremes of communication, the signaling polytope admits a simple structure. For maximum communication,  $d = \min\{n, n'\}$ , any channel  $\mathbf{P} \in \mathcal{P}^{n \rightarrow n'}$  can be realized, hence  $\mathcal{C}_{\min\{n, n'\}}^{n \rightarrow n'} = \mathcal{P}^{n \rightarrow n'}$ . For no communication,  $d = 1$ , Bob's output  $y$  is independent from Alice's input  $x$  meaning that  $P(y|x) = P(y|x')$  for any choice of  $x, x' \in [n]$  and  $y \in [n']$ . This added constraint simplifies the signaling polytope  $\mathcal{C}_1^{n \rightarrow n'}$  to  $\mathcal{P}^{1 \rightarrow n'}$  which is formally an  $n'$ -simplex [33]. For all other cases,  $\min\{n, n'\} > d > 1$ , the signaling polytope  $\mathcal{C}_d^{n \rightarrow n'}$  takes on a more complicated structure.

### 1. Vertices

The vertices of the signaling polytope are denoted by  $\mathcal{V}_d^{n \rightarrow n'}$ . Signaling polytopes are convex and therefore described as the convex hull of their vertices,  $\mathcal{C}_d^{n \rightarrow n'} = \text{conv}(\mathcal{V}_d^{n \rightarrow n'})$ . As noted in the main text, a vertex  $\mathbf{V} \in \mathcal{V}_d^{n \rightarrow n'}$  is an  $n' \times n$  column stochastic matrices with 0/1 elements and rank  $\text{rank}(\mathbf{V}) \leq d$ . For instance,

$$\mathbf{V} = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix} \quad (\text{B1})$$

is a vertex  $\mathbf{V} \in \mathcal{V}_2^{4 \rightarrow 3}$ . Naturally, each vertex  $\mathbf{V} \in \mathcal{V}_d^{n \rightarrow n'}$  has no more than  $d$  nonzero rows. A straightforward counting argument shows that  $\mathcal{V}_d^{n \rightarrow n'}$  contains  $\sum_{c=1}^d \binom{n}{c} \binom{n'}{c} c!$  vertices (see Supplemental Material of Ref. [22]), where  $\binom{n}{c}$  denotes Stirling's number of the second kind and  $\binom{n'}{c}$  a binomial coefficient. An important observation is that number of vertices in  $\mathcal{V}_d^{n \rightarrow n'}$  grows exponentially in the number of inputs,  $n$ , and factorially in the number of outputs,  $n'$ . The large number of vertices represents a key challenge in characterizing the signaling polytope.

### 2. Polytope dimension

The dimension of the signaling polytope  $\dim(\mathcal{C}_d^{n \rightarrow n'}) \leq \dim(\mathcal{P}^{n \rightarrow n'}) = n(n' - 1)$ . This upper bound follows from the facts that  $\mathcal{C}_d^{n \rightarrow n'} \subseteq \mathcal{P}^{n \rightarrow n'}$  and any  $\mathbf{P} \in \mathcal{P}^{n \rightarrow n'}$  must satisfy  $n$  normalization constraints, one for each column of  $\mathbf{P}$ . Naively,  $\mathcal{P}^{n \rightarrow n'} \subset \mathbb{R}^{n' \times n}$  where  $\dim(\mathbb{R}^{n' \times n}) = n(n')$ , however, the  $n$  normalization constraints restrict  $\mathcal{P}^{n \rightarrow n'}$  to  $\dim(\mathcal{P}^{n \rightarrow n'}) = n(n' - 1)$ . To evaluate the dimension of  $\mathcal{C}_d^{n \rightarrow n'}$  with greater precision, the number of affinely independent vertices in  $\mathcal{V}_d^{n \rightarrow n'}$  can be counted where  $\dim(\mathcal{C}_d^{n \rightarrow n'})$  is one less than the



TABLE II. Notation used throughout this work.

Notation	Terminology	Definition
$\mathcal{P}^{n \rightarrow n'}$	Set of Classical Channels	The subset of $\mathbb{R}^{n' \times n}$ containing column stochastic matrices.
$\mathbf{P}$	Classical Channel	An element of $\mathcal{P}^{n \rightarrow n'}$ that represents a classical channel with $n$ inputs and $n'$ outputs.
$\mathcal{N}$	Quantum Channel	A completely positive trace-preserving map.
$\mathcal{P}_{\mathcal{N}}^{n \rightarrow n'}$	Set of Classical Channels Generated from $\mathcal{N}$	The subset of $\mathcal{P}^{n \rightarrow n'}$ which decomposes as Eq. (1) for some quantum channel $\mathcal{N}$ .
$\mathcal{C}_d^{n \rightarrow n'}$	Signaling Polytope	The subset of $\mathcal{P}^{n \rightarrow n'}$ containing channels that decomposes as Eq. (2) (see Def. 1).
$(\mathbf{G}, \gamma)$	Linear Inequality	A tuple describing the linear inequality $\langle \mathbf{G}, \mathbf{P} \rangle \leq \gamma$ where $\mathbf{G} \in \mathbb{R}^{n' \times n}$ , $\gamma \in \mathbb{R}$ , and $\mathbf{P} \in \mathcal{P}^{n \rightarrow n'}$ .
$\kappa^{n \rightarrow n'}(\mathcal{N})$	The $n \rightarrow n'$ Signaling Dimension of $\mathcal{N}$	The smallest integer $d$ such that $\mathcal{P}_{\mathcal{N}}^{n \rightarrow n'} \subset \mathcal{C}_d^{n \rightarrow n'}$ (see Def. 2).
$\kappa(\mathcal{N})$	The Signaling Dimension of $\mathcal{N}$	The smallest integer $d$ such that $\mathcal{P}_{\mathcal{N}}^{n \rightarrow n'} \subset \mathcal{C}_d^{n \rightarrow n'}$ for all positive integers $n$ and $n'$ (see Def. 2).
$(\mathbf{G}_{k,d}^{n,n'}, d)$	Ambiguous Guessing Game	A signaling dimension witness where $\mathbf{G}_{k,d}^{n,n'} \in \mathbb{R}^{n' \times n}$ has $k$ rows that are row stochastic with 0/1 elements and $(n' - k)$ rows with each column containing $1/(n - d + 1)$ .
$\mathcal{A}_{k,d}^{n \rightarrow n'}$	Ambiguous Polytope	The subset of $\mathcal{P}^{n \rightarrow n'}$ which is tightly bound by inequalities of the form $(\mathbf{G}_{k,d}^{n,n'}, d)$ .
$\mathcal{M}_d^{n \rightarrow n'}$	Maximum Likelihood Estimation Polytope	The subset of $\mathcal{P}^{n \rightarrow n'}$ defined as the ambiguous polytope $\mathcal{A}_{k,d}^{n \rightarrow n'}$ where $k = n'$ .
$\mathcal{R}_\mu$	Partial Replacer Channel	A quantum channel that replaces the input state $\rho_x$ with quantum state $\sigma$ with probability $(1 - \mu)$ .
$\mathcal{E}_\mu$	Partial Erasure Channel	A partial replacer channel that replaces the input with $\sigma =  E\rangle\langle E $ where $ E\rangle$ is orthogonal to the input Hilbert space.
$\mathcal{V}_d^{n \rightarrow n'}$	Signaling Polytope Vertices	The subset of $\mathcal{C}_d^{n \rightarrow n'}$ containing classical channels with 0/1 elements.
$\mathcal{F}_d^{n \rightarrow n'}$	Signaling Polytope Facets	The complete set of linear inequalities tightly bounding $\mathcal{C}_d^{n \rightarrow n'}$ .
$\mathcal{G}_d^{n \rightarrow n'}$	Signaling Polytope Generator Facets	The subset of $\mathcal{F}_d^{n \rightarrow n'}$ containing a representative of each facet class in $\mathcal{F}_d^{n \rightarrow n'}$ (see Appendix B 5).
$(\mathbf{G}_K^{n',k}, \gamma_K^{n',k,d})$	$k$ -Guessing Facet	Tight signaling dimension witness (see Appendix D 1).
$(\mathbf{G}_{ML}^{n'}, d)$	Maximum Likelihood Facet	Tight signaling dimension witness (see Appendix D 2).
$(\mathbf{G}_\gamma^{n',d}, \gamma_\gamma^{n',d})$	Ambiguous Guessing Facet	Tight signaling dimension witness (see Appendix D 3).
$(\mathbf{G}_A^{\varepsilon,m'}, \gamma_A^{\varepsilon,d})$	Anti-Guessing Facet	Tight signaling dimension witness (see Appendix D 4).

number of affinely independent vertices. When  $d \geq 2$ , one can count  $n(n' - 1) + 1$  affinely independent vertices in  $\mathcal{V}_d^{n \rightarrow n'}$ , therefore,  $\dim(\mathcal{C}_d^{n \rightarrow n'}) = n(n' - 1)$ . In the remaining case of  $d = 1$ , each of the  $n'$  vertices are affinely independent and  $\dim(\mathcal{C}_1^{n \rightarrow n'}) = n' - 1$ . This result is not surprising because, as noted before,  $\mathcal{C}_1^{n \rightarrow n'} = \mathcal{P}^{1 \rightarrow n'}$  and  $\dim(\mathcal{P}^{1 \rightarrow n'}) = n' - 1$ .

### 3. Facets

A linear inequality is represented as a tuple  $(\mathbf{G}, \gamma)$  with  $\mathbf{G} \in \mathbb{R}^{n' \times n}$  and  $\gamma \in \mathbb{R}$  where the inequality  $\langle \mathbf{G}, \mathbf{P} \rangle = \sum_{x,y} G_{y,x} P(y|x) \leq \gamma$  is formed by the Euclidean inner product with a channel  $\mathbf{P} \in \mathcal{P}^{n \rightarrow n'}$ . For convenience, we identify two polyhedra of channels

$$\mathcal{C}(\mathbf{G}, \gamma) := \{\mathbf{P} \in \mathcal{P}^{n \rightarrow n'} \mid \langle \mathbf{G}, \mathbf{P} \rangle \leq \gamma\}, \quad (\text{B2})$$

$$\mathcal{F}(\mathbf{G}, \gamma) := \{\mathbf{P} \in \mathcal{P}^{n \rightarrow n'} \mid \langle \mathbf{G}, \mathbf{P} \rangle = \gamma\}. \quad (\text{B3})$$

**Lemma 1.** An inequality  $(\mathbf{G}, \gamma)$  is a tight bound of the  $\mathcal{C}_d^{n \rightarrow n'}$  signaling polytope iff

- (1)  $\mathcal{C}_d^{n \rightarrow n'} \subset \mathcal{C}(\mathbf{G}, \gamma)$ ;
- (2)  $\dim[\mathcal{C}_d^{n \rightarrow n'} \cap \mathcal{F}(\mathbf{G}, \gamma)] = \dim(\mathcal{C}_d^{n \rightarrow n'}) - 1$ .

Condition 1 requires that signaling dimension witness  $(\mathbf{G}, \gamma)$  contains all channels  $\mathbf{P} \in \mathcal{C}_d^{n \rightarrow n'}$  while Condition 2 requires that inequality  $(\mathbf{G}, \gamma)$  is both a proper half-space and a *facet* of  $\mathcal{C}_d^{n \rightarrow n'}$ . Tight signaling dimension witnesses and facets are closely related and described by the same inequality  $(\mathbf{G}, \gamma)$ . The key difference is that a tight signaling dimension witness is a half-space inequality  $\langle \mathbf{G}, \mathbf{P} \rangle \leq \gamma$  whereas a facet is the polytope  $\mathcal{C}_d^{n \rightarrow n'} \cap \mathcal{F}(\mathbf{G}, \gamma)$ . The complete set of signaling polytope facets is denoted by  $\mathcal{F}_d^{n \rightarrow n'}$  and the signaling polytope is simply the intersection of all tight signaling dimension witnesses  $(\mathbf{G}_m, \gamma_m) \in \mathcal{F}_d^{n \rightarrow n'}$ ,

$$\mathcal{C}_d^{n \rightarrow n'} = \bigcap_{m=1}^r \mathcal{C}(\mathbf{G}_m, \gamma_m). \quad (\text{B4})$$

The number of facet inequalities  $r$  is typically larger than the set of vertices  $\mathcal{V}_d^{n \rightarrow n'}$  presenting another challenge in the characterization of signaling polytopes.

*Remark* A given signaling dimension witness  $(\mathbf{G}, \gamma) \in \mathcal{F}_d^{n \rightarrow n'}$  does not have a unique form. Therefore, it is convenient to establish a *normal form* for a given facet inequality [30]. First, observe that multiplying an inequality  $(\mathbf{G}, \gamma)$  by a scalar  $a \in \mathbb{R}$  does not change the inequality, that is,  $\mathcal{C}(\mathbf{G}, \gamma) = \mathcal{C}[a\mathbf{G}, a(\gamma)]$ . Second, observe that the vertices in  $\mathcal{V}_d^{n \rightarrow n'}$  have 0/1 elements and the rational arithmetic in Fourier-Motzkin elimination [33,39] results in the matrix coefficients of  $\mathbf{G}$  being rational. Therefore, there exists a rational scalar  $a$  such that  $aG_{y,x}$  and  $a\gamma$  are integers for all  $x \in [n]$  and  $y \in [n']$ . Third, observe that the normalization and nonnegativity constraints for channels  $\mathbf{P} \in \mathcal{P}^{n \rightarrow n'}$  allows the equivalence between the two inequalities

$$\gamma \geq \langle \mathbf{G}, \mathbf{P} \rangle \iff \gamma + 1 \geq \langle \mathbf{G}, \mathbf{P} \rangle + \sum_{y \in [n']} G_{y,x'} P(y|x') \quad (\text{B5})$$

for any  $x' \in [n]$ . Therefore, it is always possible to find a form of inequality  $(\mathbf{G}, \gamma)$  where  $G_{y,x} \geq 0$  for all  $y \in [n']$  and  $x \in [n]$ . Hence, we define a normal form for any tight signaling dimension witness  $(\mathbf{G}, \gamma) \in \mathcal{F}_d^{n \rightarrow n'}$ :

- (1) Inequality  $(\mathbf{G}, \gamma)$  is scaled such that  $\gamma$  and all  $G_{y,x}$  are integers with a greatest common factor of 1.
- (2) Normalization constraints are added or subtracted from all columns using Eq. (B5) such that  $G_{y,x} \geq 0$  and the smallest element in each column of  $\mathbf{G}$  is zero.

#### 4. Permutation symmetry

The input and output values  $x$  and  $y$  are merely labels for a channel  $\mathbf{P} \in \mathcal{P}^{n \rightarrow n'}$ ; therefore, swapping labels  $x \leftrightarrow x'$  and  $y \leftrightarrow y'$  where  $x, x' \in [n]$  and  $y, y' \in [n']$  does not affect  $\mathcal{P}^{n \rightarrow n'}$  [38]. The relabeling operation is implemented using elements from the set of doubly stochastic  $k \times k$  permutation matrices  $S_k$ . For example,

$$\mathbf{P}' = \pi_y \mathbf{P} \pi_x, \quad \text{where } \mathbf{P}, \mathbf{P}' \in \mathcal{P}^{n \rightarrow n'}, \quad (\text{B6})$$

$\pi_x \in S_n$ , and  $\pi_y \in S_{n'}$ . Note that permuting the rows or columns of a matrix cannot change the rank of a matrix, therefore, if  $\mathbf{V} \in \mathcal{V}_d^{n \rightarrow n'}$  and  $\mathbf{V}' = \pi_y \mathbf{V} \pi_x$ , then  $\mathbf{V}' \in \mathcal{V}_d^{n \rightarrow n'}$ . It follows that this permutation symmetry holds for any channel in the signaling polytope,  $\mathbf{P}, \mathbf{P}' \in \mathcal{C}_d^{n \rightarrow n'}$  where  $\mathbf{P}'$  is a permutation of  $\mathbf{P}$ . Likewise, a facet inequality  $(\mathbf{G}, \gamma) \in \mathcal{F}_d^{n \rightarrow n'}$  can be permuted into a new facet inequality  $(\mathbf{G}', \gamma) \in \mathcal{F}_d^{n \rightarrow n'}$  where  $\mathbf{G}' = \pi_y \mathbf{G} \pi_x$ .

#### 5. Generator facets

Permutation symmetry motivates the notion of a *facet class* defined as a collection of facet inequalities formed by taking all permutations of a canonical facet  $(\mathbf{G}^*, \gamma) \in \mathcal{F}_d^{n \rightarrow n'}$  which we refer to as a *generator facet*. The canonical facet is arbitrary thus we define the generator facet as the *lexicographic normal form* [30,38] of the facet class. The set of generator facets, denoted by  $\mathcal{G}_d^{n \rightarrow n'} := \{(\mathbf{G}_i^*, \gamma_i)\}_{i=1}^{r'}$ , is the subset of  $\mathcal{F}_d^{n \rightarrow n'}$  containing the generator facet of each facet class bounding  $\mathcal{C}_d^{n \rightarrow n'}$ . Since the number of input and output permutations scale as factorials of  $n$  and  $n'$  respectively, the set of generator facets is considerably smaller than  $\mathcal{F}_d^{n \rightarrow n'}$  and therefore, provides a convenient simplification to  $\mathcal{F}_d^{n \rightarrow n'}$ . To recover the complete set of facets from  $\mathcal{G}_d^{n \rightarrow n'}$ , we take all row

and column permutations of each generator facet  $(\mathbf{G}^*, \gamma) \in \mathcal{G}_d^{n \rightarrow n'}$ . As a final remark, we note that  $\mathcal{V}_d^{n \rightarrow n'}$  can also be reduced to a set of generator vertices, however, this set is not required for our current discussion of signaling polytopes.

### APPENDIX C: ADJACENCY DECOMPOSITION

This Appendix provides an overview of the adjacency decomposition technique [30]. In our work, we use an adjacency decomposition algorithm to compute the generator facets of the signaling polytope. Our implementation can be found in our supporting software [32]. The adjacency decomposition provides a few key advantages in the computation of signaling dimension witnesses:

- (1) The algorithm stores only the generator facets  $\mathcal{G}_d^{n \rightarrow n'}$  instead of the complete set of facets  $\mathcal{F}_d^{n \rightarrow n'}$ . This considerably reduces the required memory.
- (2) New generator facets are derived in each iteration of the computation, hence, the algorithm does not need to run to completion to provide value.
- (3) The algorithm can be widely parallelized [30].

#### 1. Adjacency decomposition algorithm

The adjacency decomposition is an iterative algorithm which requires as input the signaling polytope vertices  $\mathcal{V}_d^{n \rightarrow n'}$  and a seed generator facet  $(\mathbf{G}_{\text{seed}}^*, \gamma_{\text{seed}}) \in \mathcal{G}_d^{n \rightarrow n'}$ . The algorithm maintains a list of generator facets  $\mathcal{G}_{\text{list}}$  where each facet  $(\mathbf{G}^*, \gamma) \in \mathcal{G}_{\text{list}}$  is marked either as *considered* or *unconsidered*. The generator facet is defined as the lexicographic normal form of the facet class [30,38]. Before the algorithm begins,  $(\mathbf{G}_{\text{seed}}^*, \gamma_{\text{seed}})$  is added to  $\mathcal{G}_{\text{list}}$  and marked as *unconsidered*. In each iteration, the algorithm proceeds as follows [30]:

- (1) An *unconsidered* generator facet  $(\mathbf{G}^*, \gamma) \in \mathcal{G}_{\text{list}}$  is selected.
- (2) All facets adjacent to  $(\mathbf{G}^*, \gamma)$  are computed.
- (3) Each adjacent facet is converted into its lexicographic normal form.
- (4) Any new generator facets identified are marked as *unconsidered* and added to  $\mathcal{G}_{\text{list}}$ .
- (5) Facet  $(\mathbf{G}^*, \gamma)$  is marked as *considered*.

The procedure repeats until all facets in  $\mathcal{G}_{\text{list}}$  are marked as *considered*. If run to completion, then  $\mathcal{G}_{\text{list}} = \mathcal{G}_d^{n \rightarrow n'}$  and all generator facets of the signaling polytope  $\mathcal{C}_d^{n \rightarrow n'}$  are identified. The algorithm is guaranteed to find all generator facets due to the permutation symmetry of the signaling polytope. By this symmetry, any representative of a given facet class has the same fixed set of facet classes adjacent to it. For the permutation symmetry to hold for all facets in the signaling polytope, there cannot be two disjoint sets of generator facets where the members of one set do not lie adjacent to the members of the other.

The inputs of the adjacency decomposition are easy to produce computationally. A seed facet can always be constructed using the lifting rules for signaling polytopes [see Eqs. (6) and (7)] and the signaling polytope vertices  $\mathcal{V}_d^{n \rightarrow n'}$  can be easily computed (see supporting software [32]). Note, however, that the exponential growth of  $\mathcal{V}_d^{n \rightarrow n'}$  eventually hinders the performance of the adjacency decomposition algorithm.

## 2. Facet adjacency

A key step in the adjacency decomposition algorithm is to compute the set of facets adjacent to a given facet  $(\mathbf{G}, \gamma)$ . In this section, we define facet adjacency and outline the method used to compute the adjacent facets.

**Lemma 2.** Two facets  $(\mathbf{G}_1, \gamma_1), (\mathbf{G}_2, \gamma_2) \in \mathcal{F}_d^{n \rightarrow n'}$  are adjacent iff they share a ridge  $\mathcal{H}$  defined as:

- (1)  $\mathcal{H} := \mathcal{F}(\mathbf{G}_1, \gamma_1) \cap \mathcal{F}(\mathbf{G}_2, \gamma_2) \cap \mathcal{C}_d^{n \rightarrow n'}$ ,
- (2) where  $\dim(\mathcal{H}) = \dim(\mathcal{C}_d^{n \rightarrow n'}) - 2$ .

A ridge can be understood as a facet of the facet polytope  $\mathcal{C}_d^{n \rightarrow n'} \cap \mathcal{F}(\mathbf{G}, \gamma)$ . Therefore, to compute the ridges of a given facet  $(\mathbf{G}, \gamma) \in \mathcal{F}_d^{n \rightarrow n'}$  we take the typical approach for computing facets. Namely, the set of vertices  $\{\mathbf{V} \in \mathcal{V}_d^{n \rightarrow n'} \mid \langle \mathbf{G}, \mathbf{V} \rangle = \gamma\}$  is constructed and PORTA [39,40] is used to compute the ridges of  $(\mathbf{G}, \gamma)$ . A facet adjacent to  $(\mathbf{G}, \gamma)$  is computed from each ridge using a *rotation algorithm* described by Christof and Reinelt [30]. Given the signaling polytope vertices  $\mathcal{V}_d^{n \rightarrow n'}$ , this procedure computes the complete set of facets adjacent to  $(\mathbf{G}, \gamma)$ .

## APPENDIX D: TIGHT SIGNALING DIMENSION WITNESSES

In this Appendix we discuss the general forms for each of the signaling polytope facets in Table I. Each facet class is described by a generator facet (see Appendix B 4) where all permutations and input/output liftings of these generator facets are also tight signaling dimension witnesses. To prove that an inequality  $(\mathbf{G}, \gamma)$  is a facet of  $\mathcal{C}_d^{n \rightarrow n'}$ , both conditions of Lemma 1 must hold. The proofs contained by this Appendix verify Condition 2 of Lemma 1 by constructing a set of  $\dim(\mathcal{C}_d^{n \rightarrow n'}) = n(n' - 1)$  affinely independent  $\{\mathbf{V} \in \mathcal{V}_d^{n \rightarrow n'} \mid \langle \mathbf{G}, \mathbf{V} \rangle = \gamma\}$ . These enumerations are verified numerically in our supporting software [32]. To assist with the enumeration of affinely independent vertices, we introduce a simple construction for affinely independent vectors with 0/1 elements.

**Lemma 3.** Consider an  $n$ -element binary vector  $\vec{b}_k \in \{0, 1\}^n$  with  $n_0$  null elements and  $n_1$  unit elements where  $n_0 + n_1 = n$ . A set of  $n$  affinely independent vectors  $\{\vec{b}_k\}_{k=1}^n$  is constructed as follows:

- (1) Let  $\vec{b}_1$  be the binary vector where the first  $n_0$  elements are null and the next  $n_1$  elements are unit values.

- (2) For  $k \in [2, n_0 + 1]$ ,  $\vec{b}_k$  is derived from  $\vec{b}_1$  by swapping the unit element at index  $(n_0 + 1)$  with the null element at index  $(k - 1)$ .

- (3) For  $k \in [n_0 + 2, n]$ ,  $\vec{b}_k$  is derived from  $\vec{b}_1$  by swapping the null element at index  $n_0$  with the unit element at index  $k$ .

For example, when  $n = 5$ ,  $n_0 = 2$ , and  $n_1 = 3$  the enumeration yields

$$\begin{aligned} \vec{b}_1 &= [0, 0, 1, 1, 1], & \vec{b}_2 &= [1, 0, 0, 1, 1], \\ \vec{b}_3 &= [0, 1, 0, 1, 1], & \vec{b}_4 &= [0, 1, 1, 0, 1], \\ \vec{b}_5 &= [0, 1, 1, 1, 0]. \end{aligned} \quad (\text{D1})$$

*Proof.* To verify the affine independence of  $\{\vec{b}_k\}_{k=1}^n$  it is sufficient to show the linear independence of  $\{\vec{b}_1 - \vec{b}_k\}_{k=2}^n$ . Note that each  $(\vec{b}_1 - \vec{b}_k)$  has two nonzero elements, one of which occurs at an index that is zero for all  $(\vec{b}_1 - \vec{b}_{k'})$  where  $k \neq k'$ . Therefore, the vectors in  $\{\vec{b}_1 - \vec{b}_k\}_{k=2}^n$  are linearly independent and  $\{\vec{b}_k\}_{k=1}^n$  is affinely independent. ■

### 1. $k$ -Guessing facets

Consider a guessing game with  $k$  correct answers out of  $n'$  possible answers. In this game, Alice has  $n = \binom{n'}{k}$  inputs where each value  $x$  corresponds to a unique set of  $k$  correct answers. Given an input  $x \in [n]$ , Alice signals to Bob using a message  $m \in [d]$  and Bob makes a guess  $y \in [n']$ . A correct guess scores 1 point while an incorrect guess scores 0 points. This type of guessing game is described by Heinosaari *et al.* [31,34] and used to test the communication performance of a particular theory. In this work, we treat this  $k$ -guessing game as a signaling dimension witness  $(\mathbf{G}_K^{n',k}, \gamma_K^{n',k,d})$  of the signaling polytope  $\mathcal{C}_d^{n \rightarrow n'}$  where

$$\gamma_K^{n',k,d} = \binom{n'}{k} - \binom{n' - d}{k} \quad (\text{D2})$$

and  $\mathbf{G}_K^{n',k} \in \mathbb{R}^{n' \times \binom{n'}{k}}$  is a matrix with each column containing a unique distribution of  $k$  unit elements and  $(n' - k)$  null elements. For example,

$$\mathbf{G}_K^{6,2} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \end{pmatrix}. \quad (\text{D3})$$

This general signaling dimension witness was identified by Frenkel and Weiner [23], who showed that given a channel  $\mathbf{P} \in \mathcal{C}_d^{n \rightarrow n'}$ , the bounds of this inequality are

$$\binom{n'}{k} - \binom{n' - d}{k} \geq \langle \mathbf{G}_K^{n',k}, \mathbf{P} \rangle \geq \binom{n' - d}{n' - k}. \quad (\text{D4})$$

However, we only focus on the upper bound  $\gamma_K^{n',k,d}$ . We now show conditions for which  $(\mathbf{G}_K^{n',k}, \gamma_K^{n',k,d}) \in \mathcal{F}_d^{n \rightarrow n'}$ .

**Proposition 3.** The inequality  $(\mathbf{G}_K^{n',k}, \gamma_K^{n',k,d})$  is a facet of  $\mathcal{C}_d^{n \rightarrow n'}$  with  $n = \binom{n'}{k}$ ,  $n' - 2 \geq k \geq 1$ , and  $d = n' - k$ .

*Proof.* To prove that  $(\mathbf{G}_K^{n',k}, \gamma_K^{n',k,d})$  is a facet of  $\mathcal{C}_d^{n \rightarrow n'}$  we construct a set of  $\dim(\mathcal{C}_d^{n \rightarrow n'}) = (n' - 1)\binom{n'}{k}$  affinely independent vertices  $\{\mathbf{V} \in \mathcal{V}_d^{n \rightarrow n'} \mid \gamma_K^{n',k,d} = \langle \mathbf{G}_K^{n',k}, \mathbf{V} \rangle\}$ . Observe that separating the first row from the rest of  $\mathbf{G}_K^{n',k}$  results in a block matrix of form,

$$\mathbf{G}_K^{n',k} = \left[ \begin{array}{c|c} \bar{\mathbf{1}} & \bar{\mathbf{0}} \\ \hline \mathbf{G}_K^{(n'-1),(k-1)} & \mathbf{G}_K^{(n'-1),k} \end{array} \right], \quad \text{e.g.,} \quad \mathbf{G}_K^{5,2} = \left[ \begin{array}{cccc|cccc} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \end{array} \right] = \left[ \begin{array}{c|c} \bar{\mathbf{1}} & \bar{\mathbf{0}} \\ \hline \mathbf{G}_K^{4,1} & \mathbf{G}_K^{4,2} \end{array} \right], \quad (\text{D5})$$

where  $\bar{\mathbf{0}}$  and  $\bar{\mathbf{1}}$  are row vectors containing zeros and ones, and we refer to  $\mathbf{G}_K^{(n'-1),(k-1)}$  and  $\mathbf{G}_K^{(n'-1),k}$  as left and right  $k$ -guessing blocks respectively. The left and right  $k$ -guessing blocks suggest a recursive approach to our construction of affinely independent vertices. Namely, we construct  $\binom{n'}{k}$  vertices by targeting the first row of  $\mathbf{G}_K^{n',k}$  while Proposition 3 is recursively applied to enumerate the remaining vertices using the left and right  $k$ -guessing blocks. The recursion requires two base cases to be addressed:

- (1) When  $d = 2$  and  $n' = k + d$ , the construction of affinely independent vertices is described in Proposition 4.
- (2) When  $k = 1$ , the construction of affinely independent vertices is described in Proposition 5.

An iteration of this recursive construction proceeds as follows.

First, we construct an affinely independent vertex for each of the  $\binom{n'}{k}$  elements in the first row of  $\mathbf{G}_K^{n',k}$ . For each index  $x'_1$  in the  $\bar{\mathbf{1}}$  block, a vertex  $\mathbf{V}_1$  is constructed by setting all  $V_1(1|x) = 1$  where  $x \neq x'_1$  and  $V_1(y|x'_1) = 1$  where  $y > 1$  is the smallest row index such that  $G_{y,x'_1} = 1$ . The remaining rows of  $\mathbf{V}_1$  are filled to maximize the right  $k$ -guessing block. Then, for each index  $x'_0$  in the  $\bar{\mathbf{0}}$  block, a vertex  $\mathbf{V}_0$  is constructed by setting  $V_0(1|x'_0) = 1$  and all  $V_0(1|x) = 1$  where  $G_{1,x} = 1$ . The remaining  $(d - 1)$  rows of  $\mathbf{V}_0$  are filled to maximize the right  $k$ -guessing block. This procedure enumerates  $\binom{n'}{k}$  affinely independent vertices.

Then, the remaining  $(n' - 2)\binom{n'}{k}$  vertices are found by individually targeting the left and right  $k$ -guessing blocks. To construct a vertex  $\mathbf{V}_L$  using the left block  $\mathbf{G}_K^{(n'-1),(k-1)}$ , the first row of  $\mathbf{V}_L$  is not used. The left block is then a  $(k - 1)$ -guessing game with  $(n' - 1)$  outputs where  $d = (n' - 1) - (k - 1) = n' - k$ , hence, Proposition 3 holds and  $(n' - 2)\binom{n'-1}{k-1}$  affinely independent vertices are enumerated using the described recursive process. Note that for each vertex of form  $\mathbf{V}_L$ , the remaining elements are filled to maximize the right  $k$ -guessing block  $\mathbf{G}_K^{(n'-1),k}$ . Similarly, to construct a vertex  $\mathbf{V}_R$  using the right block  $\mathbf{G}_K^{(n'-1),k}$ , we set all elements  $V_R(1|x) = 1$  where  $G_{1,x} = 1$ . The remaining  $(d - 1)$  rows of  $\mathbf{V}_R$  are filled by optimizing the  $\mathbf{G}_K^{(n'-1),k}$  block. Since  $d = n' - k$  and  $(d - 1) = (n' - 1) - k$ , Proposition 3 holds, and recursively applying this procedure constructs  $(n' - 2)\binom{n'-1}{k}$  vertices of form  $\mathbf{V}_R$  using the right  $k$ -guessing block.

Finally, vertices of forms  $\mathbf{V}_0$ ,  $\mathbf{V}_1$ ,  $\mathbf{V}_L$ , and  $\mathbf{V}_R$  are easily verified to be affinely independent. Summing these

vertices yields  $(n' - 2)\binom{n'-1}{k-1} + (n' - 2)\binom{n'-1}{k} + \binom{n'}{k} = (n' - 1)\binom{n'}{k}$  affinely independent vertices, therefore, the  $k$ -guessing signaling dimension witness is proven to be tight when  $n' = k + d$ . ■

**Proposition 4.** The  $k$ -guessing game signaling dimension witness  $(\mathbf{G}_K^{n',k}, \gamma_K^{n',k,d})$  is a tight bound for all signaling polytopes  $\mathcal{C}_d^{n \rightarrow n'}$  with  $n = \binom{n'}{k}$ ,  $d = 2$ , and  $k = n' - 2$ .

*Proof.* To prove the tightness we construct a set containing  $(n' - 1)\binom{n'}{k}$  affinely independent vertices  $\{\mathbf{V} \in \mathcal{V}_2^{n \rightarrow n'} \mid \langle \mathbf{G}_K^{n',n'-2}, \mathbf{V} \rangle = \binom{n'}{n'-2} - 1\}$ . To help illustrate this proof, we use the example of  $(\mathbf{G}_K^{5,3}, \gamma_K^{5,3,2})$ , where

$$\mathbf{G}_K^{5,3} = \left[ \begin{array}{cccccc|cccc} 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \end{array} \right], \quad (\text{D6})$$

and  $\gamma_K^{5,3,2} = \binom{5}{3} - 1$ . Since  $d = 2$ , we consider vertices  $\mathbf{V} \in \mathcal{V}_2^{n \rightarrow n'}$  with  $\text{rank}(\mathbf{V}) = 2$  where each vertex uses two rows  $y$  and  $y'$  where  $y < y'$ . In general, each of the  $\binom{n'}{2}$  two-row selections from  $\mathbf{G}_K^{n',(n'-2)}$  have a unique column  $x_0$  containing null elements both rows  $y$  and  $y'$ . Therefore, for each unique pair  $y$  and  $y'$ , two affinely independent vertices  $\mathbf{V}_1$  and  $\mathbf{V}_2$  are constructed by setting  $V_1(y|x_0) = 1$  and  $V_2(y'|x_0) = 1$  while the remaining terms are arranged such that all unit elements in row  $y$  and the remaining elements in row  $y'$  are selected to achieve the optimal score. Performing this procedure for the first two rows of  $\mathbf{G}_K^{5,3}$  ( $y = 1$  and  $y' = 2$ ) constructs the vertices

$$\mathbf{V}_1 = \left[ \begin{array}{cccccc|cccc} 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array} \right],$$

$$\mathbf{V}_2 = \left[ \begin{array}{cccccc|cccc} 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array} \right], \quad (\text{D7})$$

where  $x_0 = 10$  in this example. Repeating this procedure for each of the  $\binom{n'}{2}$  row selections produces,  $2\binom{n'}{2} = 2\binom{n'}{k}$  affinely independent vertices, one for each null element in  $\mathbf{G}_K^{n',(n'-2)}$ .



The remaining vertices are constructed by selecting a target row  $y \in [n' - 1]$ . In the target row, for each  $x'$  where  $G_{y,x'} = 1$  a vertex  $\mathbf{V}_3$  is constructed by setting  $V_3(y|x) = 1$  for all  $x \neq x'$  that satisfy  $G_{y,x} = 1$ . A secondary row  $y' > y$  of  $\mathbf{V}_3$  is chosen where  $y'$  is the smallest index satisfying  $G_{y',x'} = 1$ . We then set  $V(y'|x') = 1$  while the remaining elements of  $\mathbf{V}_3$  are set to achieve the optimal score. For selected rows  $y$  and  $y'$ , the null column at index  $x_0$  is set in the target row as  $V_3(y|x_0) = 1$ . For example, consider  $\mathbf{G}_K^5$  with the target row as  $y = 1$  and  $x' = 4$  we construct the vertex

$$\mathbf{V}_3 = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}. \quad (\text{D8})$$

Note that all secondary row indices  $y' \leq y + 3$  are required to construct a vertex  $\mathbf{V}_3$  for each unit element in the target row  $y$ . Let  $\Delta y = y' - y$ , then  $\sum_{\Delta y=1}^3 \binom{n'-1-\Delta y}{d+1-\Delta y}$  vertices are constructed for target row  $y$ . For  $y = n' - 2$  and  $y = n' - 1$ , the sum terminates at  $\Delta y = 2$  and  $\Delta y = 1$  respectively because the vertices are only affinely independent if the secondary row has index  $y' > y$ . Thus, this process produces

$$\sum_{\Delta y=1}^3 (n' - \Delta y) \binom{n' - 1 - \Delta y}{d + 1 - \Delta y} = (n' - 3) \binom{n'}{d}, \quad (\text{D9})$$

affinely independent vertices where the identities  $\frac{l}{m} \binom{l}{m} = \binom{l-1}{m-1}$  and  $\frac{l+1-m}{m} \binom{l}{m} = \binom{l}{m-1}$  are used to convert the binomial coefficients to the form  $\binom{n'}{d} = \binom{n'}{k}$ . Combining the vertices of form  $\mathbf{V}_1$ ,  $\mathbf{V}_2$ , and  $\mathbf{V}_3$  yields a set of  $2 \binom{n'}{k} + (n' - 3) \binom{n'}{k} = (n' - 1) \binom{n'}{k}$  affinely independent vertices. Therefore, when  $d = 2$  and  $k = n' - 2$ ,  $[\mathbf{G}_K^{n', (n'-2)}, \binom{n'}{n'-2} - 1]$  is a tight signaling dimension witness of the  $\mathcal{C}_2^{(n') \rightarrow n'}$  signaling polytope. ■

## 2. Maximum likelihood facets

In this section, we discuss the conditions for which maximum likelihood games (see main text) are tight signaling dimension witnesses. The maximum likelihood signaling dimension witness  $(\mathbf{G}_{\text{ML}}^{n'}, d)$  is a  $(k = 1)$ -guessing game where  $\mathbf{G}_{\text{ML}}^{n'} = \mathbf{G}_K^{n', 1}$ . For simplicity, this section considers unlifted forms of  $\mathbf{G}_{\text{ML}}^{n'}$  is a  $n' \times n'$  doubly stochastic matrix with 0/1 elements such as the  $n' \times n'$  identity matrix. For any vertex  $\mathbf{V} \in \mathcal{V}_d^{n' \rightarrow n'}$ ,

$$\langle \mathbf{G}_{\text{ML}}^{n'}, \mathbf{V} \rangle \leq d, \quad (\text{D10})$$

is satisfied because  $\text{rank}(\mathbf{V}) \leq d$  and  $\mathbf{G}_{\text{ML}}^{n'}$  is doubly stochastic. By the convexity of  $\mathcal{C}_d^{n' \rightarrow n'}$ , inequality Eq. (D10) must hold for all  $\mathbf{P} \in \mathcal{C}_d^{n' \rightarrow n'}$ . We now discuss the conditions for which  $(\mathbf{G}_{\text{ML}}^{n'}, d)$  is a tight signaling dimension witness.

**Proposition 5.** The maximum likelihood (ML) signaling dimension witness  $(\mathbf{G}_{\text{ML}}^{n'}, d)$  is a facet of all signaling polytopes  $\mathcal{C}_d^{n' \rightarrow n'}$  with  $n = n'$  and  $n' > d > 1$ .

**Proof.** To prove that  $(\mathbf{G}_{\text{ML}}^{n'}, d)$  is a tight bound of  $\mathcal{C}_d^{n' \rightarrow n'}$  we construct a set of  $\dim(\mathcal{C}_d^{n' \rightarrow n'}) = n'(n' - 1)$  affinely independent vertices  $\{\mathbf{V} \in \mathcal{V}_d^{n' \rightarrow n'} \mid \langle \mathbf{G}_{\text{ML}}^{n'}, \mathbf{P} \rangle = d\}$ . Taking  $\mathbf{G}_{\text{ML}}^{n'}$  to be

the  $n' \times n'$  identity matrix, a vertex  $\mathbf{V}$  satisfies  $d = \langle \mathbf{G}_{\text{ML}}^{n'}, \mathbf{V} \rangle$  when  $d$  unit elements of  $\mathbf{V}$  lie along the diagonal. In this case,  $(n' - d)$  unit elements of  $\mathbf{V}$  can be freely distributed in the remaining columns of the  $d$  selected rows. For simplicity, we place all free elements in a single row with index  $y \in [n']$  which we refer to as the target row. In the target row, we set  $V(y|y) = 1$  while the off-diagonals,  $V(y|x \neq y)$  with  $x \in [n']$  contain  $(n' - d)$  unit elements and  $(d - 1)$  null elements. Lemma 3 describes a construction of  $(n' - 1)$  affinely independent vectors  $\{\tilde{b}_k\}_{k \in [n'-1]}$  to set as the off-diagonals in the target row. Then, for each  $x \in [n']$  where  $V(y|x \neq y) = 0$ , we set  $V(x|x) = 1$ . This procedure obtains the upper bound in Eq. (D10) and constructs an affinely independent vertex for each of the  $(n' - 1)$  binary vectors in  $\{\tilde{b}_k\}_{k \in [n'-1]}$ . For example, targeting row  $y = 3$  of  $\mathbf{G}_{\text{ML}}^5$  when  $d = 3$  yields four vertices,

$$\mathbf{V} \in \left\{ \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \right. \\ \left. \times \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \right\}. \quad (\text{D11})$$

Repeating the procedure for each  $y \in [n']$  results in  $n'(n' - 1)$  affinely independent vertices. The vertices enumerated for each target row  $y$  are affinely independent from all other target rows because the free unit elements are only allowed in the target row. As a final note, this procedure does not work in the case where  $d = 1$  because there are only  $n'$  vertices in  $\mathcal{V}_d^{n' \rightarrow n'}$  or the case where  $d = n'$  because only one vertex  $\mathbf{V} = \mathbf{G}_{\text{ML}}^{n'}$  maximizes Eq. (D10). Since  $n'(n' - 1) = \dim(\mathcal{C}_d^{n' \rightarrow n'})$  affinely independent vertices are constructed,  $(\mathbf{G}_{\text{ML}}^{n'}, d)$  is proven to be a tight bound of all signaling polytopes with  $n' > d > 1$ . ■

## 3. Ambiguous guessing facets

In this section we discuss the conditions for which ambiguous guessing games (see main text) are tight signaling dimension witnesses. Consider the ambiguous guessing signaling dimension witness  $(\mathbf{G}_\gamma^{n', d}, \gamma_\gamma^{n', d})$  where  $\mathbf{G}_\gamma^{n', d} \in \mathbb{R}^{n' \times (n'-1)}$ ,

$$\mathbf{G}_\gamma^{n', d} = \sum_{x \in [n'-1]} (n' - d) |x\rangle \langle x| + |n'\rangle \langle x|, \\ \text{and } \gamma_\gamma^{n', d} = d(n' - d). \quad (\text{D12})$$

This signaling dimension witness is best considered as a combination between a 1-guessing game for which a correct answer provides  $(n' - d)$  points extended with an ambiguous row for which 1 point is scored for choosing the ambiguous

output. For example, when  $n' = 6$  and  $d = 2$  we have

$$\mathbf{G}_\gamma^{n',d} = \begin{bmatrix} (n'-d)\mathbf{G}_{\text{ML}}^{(n'-1)} \\ \bar{\mathbf{1}} \end{bmatrix}, \text{ e.g., } \mathbf{G}_\gamma^{6,2} = \begin{bmatrix} 4 & 0 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 & 0 \\ 0 & 0 & 4 & 0 & 0 \\ 0 & 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 0 & 4 \\ 1 & 1 & 1 & 1 & 1 \end{bmatrix}, \quad (\text{D13})$$

where we refer to rows of the  $\mathbf{G}_{\text{ML}}^{(n'-1)}$  block as *guessing rows* and  $\bar{\mathbf{1}}$  is a row vector of ones which we refer to as the *ambiguous row*. Note that  $\mathbf{G}_\gamma^{n',d}$  is a special case of the ambiguous guessing game  $\mathbf{G}^{(k)}$  (see main text), and without loss of generality, we express  $\mathbf{G}_\gamma^{n',d}$  in a normal form where all elements  $G_{y,x}$  are nonnegative integers. For any vertex  $\mathbf{V} \in \mathcal{V}_d^{n \rightarrow n'}$ , the inequality

$$\langle \mathbf{G}_\gamma^{n',d}, \mathbf{V} \rangle \leq d(n' - d) \quad (\text{D14})$$

is satisfied. We now prove the conditions for which inequality  $(\mathbf{G}_\gamma^{n',d}, \gamma_\gamma^{n',d})$  is a facet of  $\mathcal{C}_d^{n \rightarrow n'}$ .

**Proposition 6.** The inequality  $(\mathbf{G}_\gamma^{n',d}, \gamma_\gamma^{n',d})$  is a facet of  $\mathcal{C}_d^{n \rightarrow n'}$  when  $n = n' - 1$  and  $n' - 2 \geq d \geq 2$ .

*Proof.* To prove that  $(\mathbf{G}_\gamma^{n',d}, \gamma_\gamma^{n',d})$  is a facet of  $\mathcal{C}_d^{n \rightarrow n'}$  we construct a set of  $\dim(\mathcal{C}_d^{(n'-1) \rightarrow n'}) = (n' - 1)^2$  affinely independent vertices  $\{\mathbf{V} \in \mathcal{V}_d^{(n'-1) \rightarrow n'} \mid d(n' - d) = \langle \mathbf{G}_\gamma^{n',d}, \mathbf{V} \rangle\}$ . Using Proposition D 2 we can easily enumerate  $(n' - 1)(n' - 2)$  affinely independent vertices that optimize the  $\mathbf{G}_{\text{ML}}^{(n'-1)}$  block. The remaining vertices are constructed using the ambiguous row and  $(d - 1)$  guessing rows. In these vertices, the ambiguous row has  $(d - 1)$  null elements and  $(n' - d)$  unit elements, hence, Lemma 3 can be used to  $(n' - 1)$  affinely independent arrangements of the ambiguous row. For each of the  $(n' - 1)$  arrangements, a vertex  $\mathbf{V}_\gamma$  is constructed by setting each  $V_\gamma(x|x) = 1$  where  $x \in [n' - 1]$  and  $V_\gamma(n'|x) = 0$ . Combining the  $(n' - 1)(n' - 2)$  vertices from the  $\mathbf{G}_{\text{ML}}^{(n'-1)}$  block and the  $(n' - 1)$  vertices from the ambiguous row, a total of  $(n' - 1)^2$  affinely independent vertices are found. Therefore,  $(\mathbf{G}_\gamma^{n',d}, \gamma_\gamma^{n',d})$  is a tight signaling dimension witness of  $\mathcal{C}_d^{(n'-1) \rightarrow n'}$ . The upper bound  $n' - 2 \geq d$  follows from the fact that if  $d \geq (n' - 1)$ , then no optimal vertices would ever use the ambiguous row resulting in an insufficient number of vertices to justify the facet. ■

#### a. Rescalings of ambiguous guessing facets

An ambiguous guessing facet  $(\mathbf{G}_\gamma^{n',d}, \gamma_\gamma^{n',d})$  as defined in Proposition 6 can be rescaled to  $\mathbf{G}_\gamma^{5,2} \in \mathbb{R}^{n' \times (n+1)}$  by taking a guessing row  $y$  where  $G_{y,x} = (n' - d)$  distributing the value between between two columns such that  $G'_{y,x} = 1$  and  $G'_{y,x'} = (n' - d) - 1$  where  $x' = n'$  is a new column. This rescaling is a nontrivial input lifting rule. The bound of the input-lifted facet is the same as the unlifted version. For example, when

$n' = 5$  and  $d = 2$ , the  $\mathbf{G}_\gamma^{5,2}$  is rescaled along the fourth row as

$$\mathbf{G}_\gamma^{5,2} = \begin{bmatrix} 3 & 0 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 & 0 \\ 0 & 0 & 3 & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 \\ 1 & 1 & 1 & 1 & 1 \end{bmatrix} \rightarrow \mathbf{G}_\gamma^{5,2} = \begin{bmatrix} 3 & 0 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 & 0 \\ 0 & 0 & 3 & 0 & 0 \\ 0 & 0 & 0 & 1 & 2 \\ 1 & 1 & 1 & 1 & 0 \end{bmatrix}. \quad (\text{D15})$$

This rescaling input lifting is a general trend observed in our computed signaling polytope facets [32], however, it is not clear how broadly this lifting rule applies or generalizes.

#### 4. Antiguessing facets

Another special case of the  $k$ -guessing game is the *antiguessing game* signaling dimension witness  $(\mathbf{G}_A^{n'}, n')$  where  $\mathbf{G}_A^{n'} = \mathbf{G}_K^{n',(n'-1)}$ . For any channel  $\mathbf{P} \in \mathcal{P}^{n \rightarrow n'}$  with  $n = n'$  The antiguessing signaling dimension witness  $\langle \mathbf{G}_A^{n'}, \mathbf{P} \rangle \leq n'$  is satisfied; therefore, antiguessing games are not very useful for witnessing signaling dimension. That said, the antiguessing game is significant because it can be combined with a maximum likelihood game in block form to construct a facet of the  $d = (n' - 2)$  signaling polytope  $\mathcal{C}_{(n'-2)}^{n \rightarrow n'}$ . We denote these antiguessing facets by  $\mathbf{G}_A^{\varepsilon, m'}$  where the facet is constructed as

$$\mathbf{G}_A^{\varepsilon, m'} = \left[ \begin{array}{c|c} \mathbf{G}_A^\varepsilon & \hat{0} \\ \hline \hat{0} & \mathbf{G}_{\text{ML}}^{m'} \end{array} \right], \text{ e.g., } \mathbf{G}_A^{4,2} = \left[ \begin{array}{cccc|cc} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{array} \right], \quad (\text{D16})$$

where  $\mathbf{G}_A^{\varepsilon, m'} \in \mathbb{R}^{n' \times n'}$ ,  $n' = \varepsilon + m'$ , and  $\hat{0}$  is a matrix block of zeros. For channel  $\mathbf{P} \in \mathcal{C}_d^{n' \rightarrow n'}$ ,

$$\langle \mathbf{G}_A^{\varepsilon, m'}, \mathbf{P} \rangle \leq \varepsilon + d - 2 = \gamma_A^{\varepsilon, d}. \quad (\text{D17})$$

This upper bound follows from the fact that no more than two rows are required to score  $\varepsilon$  in the  $\mathbf{G}_A^\varepsilon$  block and the remaining  $d - 2$  rows score one point each against the  $\mathbf{G}_{\text{ML}}^{m'}$  block.

**Proposition 7.** The inequality  $(\mathbf{G}_A^{\varepsilon, m'}, \gamma_A^{\varepsilon, d})$  is a facet of  $\mathcal{C}_d^{n \rightarrow n'}$ , where  $n = n'$ ,  $n' - 2 \geq d \geq 2$ , and  $n' - d + 1 \geq \varepsilon \geq 3$ .

*Proof.* To prove the tightness of the antiguessing signaling dimension witness we show a row-by-row construction of  $\dim(\mathcal{C}_d^{n \rightarrow n'}) = n'(n' - 1)$  affinely independent vertices  $\{\mathbf{V} \in \mathcal{V}_d^{n \rightarrow n'} \mid \langle \mathbf{G}_A^{\varepsilon, m'}, \mathbf{V} \rangle = \gamma_A^{\varepsilon, d}\}$ . For convenience, we refer to the first  $\varepsilon$  rows of  $\mathbf{G}_A^{\varepsilon, m'}$  as *antiguessing rows* and the remaining  $m'$  rows as *guessing rows*. We treat antiguessing and guessing rows individually because each admits its own vertex construction. To help illustrate this proof, we draw upon the

example where  $\varepsilon = m' = d = 3$ ,

$$\mathbf{G}_A^{3,3} = \left[ \begin{array}{ccc|ccc} 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{array} \right] \text{ and } \gamma^{3,3} = 4. \quad (\text{D18})$$

For a target antiguessing row  $y \in [1, \varepsilon]$  we construct  $(n' - 1)$  vertices where  $(\varepsilon - 1)$  vertices are constructed using the  $\mathbf{G}_A^\varepsilon$  block and  $m'$  vertices are constructed using the  $\hat{0}$  block in the top right. Note that a vertex achieves the upper bound  $\gamma_A^{\varepsilon,d}$  only if two or less antiguessing rows are used. A vertex  $\mathbf{V}_A$  is constructed using the  $\mathbf{G}_A^{\varepsilon,m'}$  block by setting  $V_A(y|x) = 1$  for all  $x$  that satisfy  $G_{y,x}^{\varepsilon,m'} = 1$  and selecting a secondary row  $y' \neq y$  with  $y' \in [1, \varepsilon]$  and setting  $V_A(y'|x') = 1$  where  $x'$  is the index of the null element in the target row  $G_{y,x'}^{\varepsilon,m'} = 0$ . All remaining elements of  $\mathbf{V}_A$  are set so that the first  $(d - 2)$  diagonal elements of the  $\mathbf{G}_{ML}^{m'}$  block are selected and any remaining terms are set as unit elements in the target row. An affinely independent vertex is constructed for each of the  $(\varepsilon - 1)$  choices of secondary row  $y'$ . For example, when targeting row  $y = 1$  we enumerate two vertices

$$\mathbf{V}_A \in \left\{ \left[ \begin{array}{ccc|ccc} 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array} \right], \left[ \begin{array}{ccc|ccc} 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array} \right] \right\}. \quad (\text{D19})$$

For a target antiguessing row  $y$ , an additional  $m'$  vertices with form  $\mathbf{V}_{A,0}$  are constructed using the  $\hat{0}$  block in the top right. If  $m' > (d - 1)$ , then we set the target row as  $V_{A,0}(y|x) = 1$  where  $x \in [1, \varepsilon]$ . The remaining  $(d - 1)$  rows are then used to maximize the  $\mathbf{G}_{ML}^{m'}$  block. Using Lemma 3 a set of  $m'$  affinely independent vectors  $\{\tilde{b}_k\}_{k=1}^{m'}$  with  $(d - 1)$  null elements and  $(m' - d + 1)$  unit elements can be constructed and used in the  $\hat{0}$  block of  $\mathbf{V}_{A,0}$  by setting  $V_{A,0}(y|[\varepsilon + 1, n']) = \tilde{b}_k$ . All remaining null elements in the target row of  $\mathbf{V}_{A,0}$  are then set along the diagonal of the  $\mathbf{G}_{ML}^{m'}$  block. Since there are  $m'$  choices of  $\tilde{b}_k$ , that many affinely independent vertices can be constructed. For example, when targeting row  $y = 1$  we enumerate three vertices,

$$\mathbf{V}_{A,0} \in \left\{ \left[ \begin{array}{ccc|ccc} 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array} \right], \right.$$

$$\times \left[ \begin{array}{ccc|ccc} 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{array} \right], \left. \left[ \begin{array}{ccc|ccc} 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{array} \right] \right\}. \quad (\text{D20})$$

If  $m' = (d - 1)$ , then a secondary antiguessing row  $y'$  is selected where the antiguessing rows are set as  $V_{A,0}(y|x) = 1$  and  $V_{A,0}(y'|x')$ , where  $x, x' \in [1, \varepsilon]$  and  $G_{y,x}^{\varepsilon,m'} = 1$  and  $G_{y',x'}^{\varepsilon,m'} = 0$ . The remainder of the procedure is the same as the  $m' > (d - 1)$  case. Note that in the  $m' = (d - 1)$  case one of the  $\mathbf{V}_{A,0}$  vertices is redundant of a  $\mathbf{V}_A$  vertex. To reconcile this conflict another vertex must be added which maximizes  $\mathbf{G}_{ML}^{m'}$  with  $V(y|x) = 1$  for all  $x \in [1, \varepsilon]$  and  $V(x'|x') = 1$  for all  $x' \in [\varepsilon + 1, n']$ . By this procedure  $(\varepsilon - 1) + m' = (n' - 1)$  affinely independent vertices are constructed for each target row  $y \in [1, \varepsilon]$ . Thus,  $\varepsilon(n' - 1)$  affinely independent vertices are constructed for the antiguessing rows of  $\mathbf{G}_A^{\varepsilon,m'}$ .

For a target guessing row  $y \in [\varepsilon + 1, n']$  we construct  $(n' - 1)$  vertices where  $\varepsilon$  are constructed using the  $\hat{0}$  block in the lower left and  $(m' - 1)$  vertices using the  $\mathbf{G}_{ML}^{m'}$  block. Starting with the lower left  $\hat{0}$  block we construct a vertex  $\mathbf{V}_{ML,0}$  for each  $x \in [1, \varepsilon]$  by setting  $V_{ML,0}(y|x) = 1$  and  $V_{ML,0}(y|y) = 1$ . Of the remaining  $(d - 1)$  rows one is used to maximize the  $\mathbf{G}_A^\varepsilon$  block and  $(d - 2)$  rows maximize the  $\mathbf{G}_{ML}^{m'}$  block. Any unspecified unit terms of  $\mathbf{V}_{ML,0}$  are set in the target row  $y$ . Since there are  $\varepsilon$  values of  $x$  to consider, this procedure produces  $\varepsilon$  affinely independent vertices. For example, when targeting row  $y = 4$  we enumerate three vertices,

$$\mathbf{V}_{ML,0} \in \left\{ \left[ \begin{array}{ccc|ccc} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ \hline 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array} \right], \right.$$

$$\times \left[ \begin{array}{ccc|ccc} 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array} \right],$$

$$\times \left[ \begin{array}{ccc|ccc} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array} \right] \right\}. \quad (\text{D21})$$

Next, we use the  $\mathbf{G}_{ML}^{m'}$  block to a vertex  $\mathbf{V}_{ML}$ . If  $m' > (d - 1)$ , then we set  $V_{ML}(1|x) = 1$  for all  $x \in [1, \varepsilon]$  and use the procedure in Proposition 5 to enumerate  $(m' - 1)$  affinely

independent vertices that optimize the  $\mathbf{G}_{\text{ML}}^{m'}$  block in the target row. If  $m' = (d - 1)$ , then two antiguessing rows are selected to maximize the  $\mathbf{G}_A^\varepsilon$  block while the procedure in Proposition 5 is used for the remaining  $(d - 2)$  rows are used to construct  $(m' - 1)$  affinely independent vertices that optimize the  $\mathbf{G}_{\text{ML}}^{m'}$  block in the target row. For example, when targetting row  $y = 4$  we enumerate two vertices,

$$\mathbf{V}_{\text{ML}} \in \left\{ \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \right. \\ \left. \times \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \right\}. \quad (\text{D22})$$

Each guessing row produces  $\varepsilon + (m' - 1) = (n' - 1)$  affinely independent vertices, thus in total, we have  $m'(n' - 1)$  vertices enumerated for the guessing rows.

Combining the procedures for the guessing and antiguessing rows, we construct a total of  $\varepsilon(n' - 1) + m'(n' - 1) = n'(n' - 1)$  affinely independent vertices. Therefore, we prove that  $(\mathbf{G}_A^{\varepsilon, m'}, \gamma_A^{\varepsilon, d})$  is a tight bound. We now address the bounds on  $d$  and  $\varepsilon$ . The lower bound  $\varepsilon \geq 3$  follows from the fact that  $\mathbf{G}_A^2 = \mathbf{G}_{\text{ML}}^2$  meaning the antiguessing game is indistinguishable from the maximum likelihood game. The upper bound  $n' - d + 1 \geq \varepsilon$  follows from the fact that  $m' \geq (d - 1)$  must be satisfied or  $n'(n' - 1)$  affinely independent vertices cannot be found because the entire diagonal of the  $\mathbf{G}_{\text{ML}}^{m'}$  block must be used by every vertex to satisfy  $\langle \mathbf{G}_A^{\varepsilon, m'}, \mathbf{V} \rangle = \varepsilon + d - 2$ . The upper bound  $n' - 2 \geq d$  results from the lower bound on  $\varepsilon$  and the fact that  $d$  cannot be so large the  $n' - d + 1 < 3$ . ■

## APPENDIX E: PROOF OF PROPOSITION 2

In this Appendix we prove the conditions for which the ambiguous guessing game  $(\mathbf{G}_{k,d}^{n,n'}, d)$  is a facet of  $\mathcal{C}_d^{n \rightarrow n'}$ .

### 1. Proof of Proposition 2(i)

*Proof.* To prove Proposition 2(i), we consider the general form of an ambiguous guessing signaling dimension witness  $(\mathbf{G}_{k,d}^{n,n'}, d)$  where  $\mathbf{G}_{k,d}^{n,n'} \in \mathbb{R}^{n' \times n}$  is row stochastic and contains  $k = n'$  guessing rows (see main text). Note that matrix  $\mathbf{G}_{k,d}^{n,n'}$  is row stochastic and therefore describes any input/output lifting and permutation of the maximum likelihood game  $\mathbf{G}_{\text{ML}}^{m'} = \mathbb{I}_{m'}$  where  $\min\{n, n'\} \geq m' \geq 1$ . For example,

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix},$$

$$\times \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}, \quad \text{and} \quad \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}, \quad (\text{E1})$$

are all instances of  $\mathbf{G}_{5,d}^{5,5}$ . By Proposition 5,  $(\mathbf{G}_{\text{ML}}^{m'}, d)$  is a facet of  $\mathcal{C}_d^{m' \rightarrow m'}$  iff  $m' > d > 1$ , that is,  $\text{rank}(\mathbf{G}_{\text{ML}}^{m'}) > d$ . When the trivial lifting rules [see Eqs. (6) and (7)] are applied to  $\mathbf{G}_{\text{ML}}^{m'}$ , the rank of the lifted matrix does not change. Therefore, any signaling dimension witness  $(\mathbf{G}_{n',d}^{n,n'}, d)$  with  $\text{rank}(\mathbf{G}_{n',d}^{n,n'}) > d$  is a facet of  $\mathcal{C}_d^{n \rightarrow n'}$  that has been lifted from  $\mathcal{C}_d^{m' \rightarrow m'}$  where  $\min\{n, n'\} \geq m' > d$ . Conversely, if  $\text{rank}(\mathbf{G}_{n',d}^{n,n'}) < d$ , then  $\langle \mathbf{G}_{n',d}^{n,n'}, \mathbf{V} \rangle < d$  for any  $\mathbf{V} \in \mathcal{V}_d^{n \rightarrow n'}$ . Likewise, if  $\text{rank}(\mathbf{G}_{n',d}^{n,n'}) = d$ , then there are an insufficient number of affinely independent vertices  $\mathbf{V} \in \mathcal{V}_d^{n \rightarrow n'}$  which satisfy  $\langle \mathbf{G}_{n',d}^{n,n'}, \mathbf{V} \rangle = d$  because  $d$  columns must have fixed values in  $\mathbf{V}$ . Thus, we conclude that when  $\min\{n, n'\} > d > 1$   $(\mathbf{G}_{n',d}^{n,n'}, d)$  is a tight bound of  $\mathcal{C}_d^{n \rightarrow n'}$  iff  $\text{rank}(\mathbf{G}_{n',d}^{n,n'}) > d$ . ■

*Remark* Proposition 2(i) is significant because it allows one to easily find a facet of any signaling polytope  $\mathcal{C}_d^{n \rightarrow n'}$ . This enables the use of adjacency decomposition for any signaling polytope (see Appendix C).

### 2. Proof of Proposition 2(ii)

*Proof.* To prove Proposition 2(ii), we consider the ambiguous guessing game signaling dimension witnesses  $(\mathbf{G}_{k,d}^{n,n'}, d)$  with  $k$  guessing rows and  $(n' - k)$  ambiguous rows (see main text). Note that the ambiguous rows of  $\mathbf{G}_{k,d}^{n,n'}$  span the entire width of the matrix. For example,

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ \frac{1}{3} & \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \end{bmatrix}, \\ \times \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ \frac{1}{3} & \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \end{bmatrix}, \quad \text{and} \quad \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ \frac{1}{3} & \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \end{bmatrix}, \quad (\text{E2})$$

are all instances of  $\mathbf{G}_{4,2}^{4,6}$ . Furthermore, any ambiguous guessing facet described by Proposition 6  $(\mathbf{G}_{n',d}^{n',d}, d(n' - d))$  of  $\mathcal{C}_d^{(n'-1) \rightarrow n'}$  can be converted into an inequality  $(\mathbf{G}_{(n'-1),d}^{(n'-1),n'}, d)$  simply by dividing the inequality by  $(n' - d)$ , hence, these two matrices describe the same inequality. It follows that any ambiguous guessing facet  $\mathbf{G}_{n',d}^{m',d}$  can be input lifted from  $\mathcal{C}_d^{(m'-1) \rightarrow m'}$  to  $\mathcal{C}_d^{(m'-1) \rightarrow n'}$  where  $n' \geq m'$ . Since the rank of the  $(m' - 1)$  guessing rows of  $\mathbf{G}_{n',d}^{m',d}$  is  $(m' - 1)$  and input liftings do not affect the matrix rank, any  $\mathbf{G}_{k,d}^{(m'-1),n'}$  with  $n' > k \geq (m' - 1)$  with a similar rank for its guessing rows must be a facet of  $\mathcal{C}_d^{(m'-1) \rightarrow n'}$ . Finally, if the rank of the guessing rows



of  $\mathbf{G}_{k,d}^{n,n'}$ ) is less than  $n$ , then  $\mathbf{G}_{k,d}^{n,n'}$  cannot be a facet of  $\mathcal{C}_d^{n \rightarrow n'}$  because there is an insufficient number of affinely independent vertices in  $\{\mathbf{V} \in \mathcal{V}_d^{n \rightarrow n'} \mid \langle \mathbf{G}_{k,d}^{n,n'}, \mathbf{V} \rangle = d\}$ . This is true because Proposition 5 implies that we can enumerate  $(k-1)n$  affinely independent vertices using only guessing rows of  $\mathbf{G}_{k,d}^{n,n'}$ . This requires that the remaining  $(n'-k)n$  affinely independent vertices are enumerated using  $(d-1)$  guessing rows and one ambiguous row. However, as exemplified in the proof of Proposition 6, this cannot be done unless there is a nonzero element in each column of the  $k$  guessing rows of  $\mathbf{G}_{k,d}^{n,n'}$ . Thus, we conclude that for  $n' > k \geq n$  and  $n > d$   $\mathbf{G}_{k,d}^{n,n'}$  is a facet of  $\mathcal{C}_d^{n \rightarrow n'}$  iff the rank of the guessing rows is  $n$ . ■

**Remark** In our proof, we do not consider input liftings of  $\mathbf{G}_{\gamma}^{n,n'}$  because it results in matrices which deviate in form from  $\mathbf{G}_{k,d}^{n,n'}$ . Input lifting append an all-zero column to  $\mathbf{G}_{\gamma}^{n,n'}$  while  $\mathbf{G}_{k,d}^{n,n'}$  is defined to have a nonzero element in each column of an ambiguous row ambiguous. Therefore, input liftings of ambiguous guessing facets  $\mathbf{G}_{\gamma}^{n,n'}$  are incompatible with the ambiguous guessing games  $\mathbf{G}_{k,d}^{n,n'}$  described in the main text.

## APPENDIX F: PROOF OF THEOREM 1

Our proofs to parts (i) and (ii) of Theorem 1 follow the same approach. In both cases we want to show that the signaling polytope  $\mathcal{C}_d^{n \rightarrow n'}$  is equivalent to some convex polytope defined by certain signaling dimension witnesses. We establish this by showing that the extreme points of the latter are also extreme points of the former; the converse has already been shown in Eq. (9). Recall that the extreme points of  $\mathcal{C}_d^{n \rightarrow n'}$  consist of all extreme points of  $\mathcal{P}^{n \rightarrow n'}$  having rank no greater than  $d$ . In other words,  $\mathbf{P}$  is extremal in  $\mathcal{C}_d^{n \rightarrow n'}$  iff it is column stochastic with 0/1 elements and at most  $d$  nonzero rows.

We rely heavily on the following general characterization of extreme points.

**Proposition 8.** Let  $\mathcal{S} \subset \mathbb{R}^{n' \times n}$  be some convex polytope in  $\mathbb{R}^{n' \times n}$ . Then  $\mathbf{P}$  is an extreme point of  $\mathcal{S}$  iff there does not exist some  $\mathbf{D} \in \mathbb{R}^{n' \times n}$  such that  $\mathbf{P} \pm \mathbf{D} \in \mathcal{S}$ .

In our application of Proposition 8, we will refer to  $\mathbf{D} \in \mathbb{R}^{n' \times n}$  as a “valid” perturbation of  $\mathbf{P}$  if  $\mathbf{P} \pm \mathbf{D} \in \mathcal{S}$ ; hence, if  $\mathbf{D}$  is a valid perturbation, then  $\mathbf{P}$  cannot be extremal.

Some other terminology used in our proofs is the following. For a channel  $\mathbf{P} \in \mathcal{P}^{n \rightarrow n'}$ , an element  $P(y|x)$  is called *nonextremal* if it lies in the open interval  $(0,1)$ . We say that  $P(y|x)$  is a *row maximizer* if it attains the largest value in row  $y$  of  $\mathbf{P}$ . It is further called a *unique row maximizer* if there are no other elements in row  $y$  having this value. Finally, we define the maximum likelihood estimation (ML) sum

$$\phi(\mathbf{P}) := \sum_{x=1}^{n'} \|\mathbf{r}_y\|_{\infty}, \quad (\text{F1})$$

where  $\mathbf{r}_y$  denotes row  $y$  of  $\mathbf{P}$  and  $\|\mathbf{r}_y\|_{\infty}$  is its row maximizer. Then the maximum likelihood estimation (ML) polytope can be expressed as

$$\mathcal{M}_d^{n \rightarrow n'} = \{\mathbf{P} \in \mathcal{P}^{n \rightarrow n'} \mid \phi(\mathbf{P}) \leq d\}. \quad (\text{F2})$$

Note that  $\phi$  is a convex function so that if  $\phi(\mathbf{P}) = d$  with  $\mathbf{P} = \sum_{\lambda} p_{\lambda} \mathbf{V}_{\lambda}$  for extreme points  $\mathbf{V}_{\lambda} \in \mathcal{M}_d^{n \rightarrow n'}$  and nonnegative numbers  $p_{\lambda}$ , then necessarily  $\phi(\mathbf{V}_{\lambda}) = d$  for every  $\lambda$ .

### 1. Proof of Theorem 1(i)

The proof of Theorem 1(i) follows immediately from the following lemma due to the convexity of the ML and signaling polytopes.

**Lemma 4.** For arbitrary  $n$  and  $n'$ , the extreme points of  $\mathcal{M}_{n'-1}^{n \rightarrow n'}$  are extreme points of  $\mathcal{C}_{n'-1}^{n \rightarrow n'}$ .

**Proof.** We first show the conclusion of Lemma 4 is true for any extreme point  $\mathbf{V}$  of  $\mathcal{M}_{n'-1}^{n \rightarrow n'}$  having ML sum  $\phi(\mathbf{V}) < n' - 1$ . If  $\mathbf{V}$  is not extremal in  $\mathcal{P}^{n \rightarrow n'}$ , then  $\mathbf{V}$  must have at least one column  $x$  with two nonextremal elements  $V(y_1|x)$  and  $V(y_2|x)$ . However, we could then take two perturbations  $V(y_1|x) \rightarrow V(y_1|x) \pm \epsilon$  and  $V(y_2|x) \rightarrow V(y_2|x) \mp \epsilon$  with  $\epsilon$  chosen sufficiently small so that the ML sum remains  $< n' - 1$  and the numbers remain nonnegative. Hence, by contradiction,  $\mathbf{V}$  must be extremal in  $\mathcal{P}^{n \rightarrow n'}$  with rank clearly  $< n' - 1$ .

Let us then consider an extremal point  $\mathbf{V}$  of  $\mathcal{M}_{n'-1}^{n \rightarrow n'}$  for which  $\phi(\mathbf{V}) = n' - 1$ . Since  $\phi(\mathbf{V}) = n' - 1$  is an integer and  $\mathbf{V}$  has  $n'$  rows, then  $\mathbf{V}$  must have at least two nonextremal row maximizers (possibly in different columns). We will again introduce perturbations, but care is needed to ensure that the perturbations are valid; i.e., the perturbed channels must remain in  $\mathcal{M}_{n'-1}^{n \rightarrow n'}$ . There are two cases to consider.

**Case (a):** Suppose that two nonextremal row maximizers occur in the same column: say  $V(y_1|x)$  and  $V(y_2|x)$  are both row maximizers in column  $x$ . Since these values will account for the contributions of rows  $y_1$  and  $y_2$  in the ML sum, and since there are only  $n'$  total rows in this sum, we must have that all other row maximizers are  $+1$ . Hence, we introduce perturbations  $V(y_1|x) \rightarrow V(y_1|x) \pm \epsilon$  and  $V(y_2|x) \rightarrow V(y_2|x) \mp \epsilon$ . If  $V(y_1|x)$  and  $V(y_2|x)$  are unique row maximizers, then this perturbation is valid. However, if there are columns  $x'$ ,  $x''$  such that  $V(y_1|x) = V(y_1|x')$  and/or  $V(y_2|x) = V(y_2|x'')$  (with possibly  $x' = x''$ ), then we must also introduce a corresponding perturbation  $V(y_1|x') \rightarrow V(y_1|x') \pm \epsilon$  and/or  $V(y_2|x'') \rightarrow V(y_2|x'') \mp \epsilon$ . To preserve normalization in columns  $x'$  and/or  $x''$ , we will have to introduce an offsetting perturbation to some other row in  $x'$  and/or  $x''$ . This can always be done since either  $x' = x''$ , or  $x'$  and/or  $x''$  have a nonextremal element in some other row which is not a row maximizer (since all other row maximizers are  $+1$ ).

**Case (b):** No column has two nonextremal row maximizers, and  $\mathbf{V}$  has at least two nonextremal row maximizers that belong to different columns. For each row  $y$  with a nonextremal row maximizer, add perturbations  $\pm \epsilon_y$  to all the row maximizers in that row. Since each column has at most one row maximizer, a normalization-preserving perturbation  $\mp \epsilon_y$  can be added to another nonextremal element in any column having a row maximizer in row  $y$ . Finally, choose the  $\epsilon_y$  so that  $\sum_{y=1}^{n'} \epsilon_y = 0$ . ■

### 2. Proof of Theorem 1(ii)

We now turn to the ambiguous polytopes  $\mathcal{A}_{\cap}^{n \rightarrow n'} := \cap_{k=n}^{n'} \mathcal{A}_{k,n-1}^{n \rightarrow n'}$ . Recall that  $\mathcal{A}_{k,n-1}^{n \rightarrow n'}$  is the polytope of channels  $\mathbf{P} \in \mathcal{P}^{n \rightarrow n'}$  satisfying all signaling dimension witnesses of the

form

$$\langle \mathbf{G}_{k,n-1}^{n,n'}, \mathbf{P} \rangle \leq n-1, \quad (\text{F3})$$

with  $\mathbf{G}_{k,n-1}^{n,n'}$  having  $k$  guessing rows and  $(n'-k)$  ambiguous rows. In this case, all the elements in an ambiguous row are equal to  $\frac{1}{n-d+1} = \frac{1}{2}$ .

To prove Theorem 1(ii) we apply the following lemma to show that the extreme points of  $\mathcal{A}_{\cap}^{n \rightarrow n'}$  are the same as those of  $\mathcal{C}_{n-1}^{n \rightarrow n'}$ . Then by convexity of  $\mathcal{A}_{\cap}^{n \rightarrow n'}$  and  $\mathcal{C}_{n-1}^{n \rightarrow n'}$  we must have  $\mathcal{A}_{\cap}^{n \rightarrow n'} = \mathcal{C}_{n-1}^{n \rightarrow n'}$ .

**Lemma 5.** For arbitrary  $n' \geq n$ , the extreme points of  $\mathcal{A}_{\cap}^{n \rightarrow n'}$  are extreme points of  $\mathcal{C}_{n-1}^{n \rightarrow n'}$ .

*Proof.* We first argue that the conclusion of Lemma 5 is true for any extreme point  $\mathbf{V}$  of  $\mathcal{A}_{\cap}^{n \rightarrow n'}$  such that  $\langle \mathbf{G}_{k,n-1}^{n,n'}, \mathbf{V} \rangle < n-1$  for all  $\mathbf{G}_{k,n-1}^{n,n'}$  and all integers  $k \in [n, n']$ . Analogous to Lemma 4, if  $\mathbf{V}$  has at least one column  $x$  with two nonextremal elements  $V(y_1|x)$  and  $V(y_2|x)$ , we can take two sufficiently small perturbations  $V(y_1|x) \rightarrow V(y_1|x) \pm \epsilon$  and  $V(y_2|x) \rightarrow V(y_2|x) \mp \epsilon$  and still satisfy all the constraints of Eq. (F3). Hence,  $\mathbf{V}$  must be an extreme element of  $\mathcal{P}^{n \rightarrow n'}$ . In this case,  $\text{rank}(\mathbf{V}) < n-1$  since  $\phi(\mathbf{P}) < n-1$ , and so  $\mathbf{V} \in \mathcal{C}_{n-1}^{n \rightarrow n'}$ .

It remains to prove the conclusion of Lemma 5 whenever Eq. (F3) is tight for some  $\mathbf{A}_{k,n-1}^{n \rightarrow n'}$ . The lengthiest part of this argument is when  $k = n'$  and tightness in Eq. (F3) corresponds to the ML sum equaling  $n-1$ . In this case, Proposition 10 below shows that  $\mathbf{V}$  must be an extreme point of  $\mathcal{C}_{n-1}^{n \rightarrow n'}$ . However, before proving this result, we apply it to show that Lemma 5 holds whenever Eq. (F3) is tight for some other  $\mathbf{G}_{k,n-1}^{n,n'}$  with

$$\mathbf{r}_y \rightarrow \begin{bmatrix} V(y|x_1) & 0 & \cdots & 0 \\ 0 & V(y|x_2) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & V(y|x_{k-1}) \\ 0 & 0 & \cdots & 0 \end{bmatrix}$$

Notice that we can obtain  $\mathbf{V}$  from  $\tilde{\mathbf{V}}$  by coarse-graining over these rows. Moreover, this decomposition was constructed so that

$$\sum_{i=1}^k \|\tilde{\mathbf{r}}_{y_i}\|_{\infty} = \sum_{i=1}^{k-1} V(y|x_i) + \lambda V(y|x_k) = \|\mathbf{r}_y\|_1, \quad (\text{F8})$$

where the  $\tilde{\mathbf{r}}_{y_i}$  are the rows in Eq. (F7). Essentially this transformation allows us to replace an ambiguous row with a collection of guessing rows so that the overall guessing score does not change.

We perform this row splitting process on all ambiguous rows of  $\mathbf{V}$  thereby obtaining a new matrix  $\tilde{\mathbf{V}}$  such that  $\phi(\tilde{\mathbf{V}}) = n-1$ . If  $m$  is the total number of rows in  $\tilde{\mathbf{V}}$ , then  $\tilde{\mathbf{V}}$  will be an element of  $\mathcal{A}_{\cap}^{n \rightarrow m}$ . We decompose  $\tilde{\mathbf{V}}$  into a convex combination of extremal points of  $\mathcal{A}_{\cap}^{n \rightarrow m}$  as  $\tilde{\mathbf{V}} = \sum_{\lambda} p_{\lambda} \tilde{\mathbf{V}}_{\lambda}$ . By the convexity of  $\phi$ , it follows that  $\phi(\tilde{\mathbf{V}}_{\lambda}) = n-1$ , and we can therefore apply Proposition 10 below on the channels  $\tilde{\mathbf{V}}_{\lambda}$  to conclude that they are extreme points of  $\mathcal{C}_{n-1}^{n \rightarrow m}$ . Consequently,

$k < n'$ . Specifically, we will perform a lifting technique on any vertex  $\mathbf{V}$  satisfying  $\langle \mathbf{G}_{k,n-1}^{n,n'}, \mathbf{V} \rangle = n-1$  and reduce it to the case of the ML sum equaling  $(n-1)$ .

Suppose that  $\phi(\mathbf{V}) < n-1$  yet there exists some  $\mathbf{G}_{k,n-1}^{n,n'}$  such that  $\langle \mathbf{G}_{k,n-1}^{n,n'}, \mathbf{V} \rangle = n-1$ . The matrix  $\mathbf{G}_{k,n-1}^{n,n'}$  identifies  $(n'-k)$  ambiguous rows, and suppose that  $y$  is an ambiguous row such that  $\frac{1}{2}\|\mathbf{r}_y\|_1 > \|\mathbf{r}_y\|_{\infty}$ , with  $\mathbf{r}_y$  being the  $y$ th row of  $\mathbf{V}$ . To be concrete, let us suppose without loss of generality that the components of row  $\mathbf{r}_y$  are arranged in nonincreasing order [i.e.,  $V(y|x_i) \geq V(y|x_{i+1})$ ], and let  $k$  be the smallest index such that

$$\frac{1}{2} \left[ -\sum_{i=1}^{k-1} V(y|x_i) + \sum_{i=k}^n V(y|x_i) \right] \leq V(y|x_k). \quad (\text{F4})$$

By the assumption  $\frac{1}{2}\|\mathbf{r}_y\|_1 > \|\mathbf{r}_y\|_{\infty}$ , we have  $k > 1$ . Also, since  $k$  is the smallest integer satisfying Eq. (F4), we have

$$\frac{1}{2} \left[ -\sum_{i=1}^{k-2} V(y|x_i) + \sum_{i=k-1}^n V(y|x_i) \right] > V(y|x_{k-1}). \quad (\text{F5})$$

Subtracting  $V(y|x_{k-1})$  from both sides of this equation implies that the LHS of Eq. (F4) is strictly positive. Hence, there exists some  $\lambda \in (0, 1]$  such that

$$\lambda V(y|x_k) = \frac{1}{2} \left[ -\sum_{i=1}^{k-1} V(y|x_i) + \sum_{i=k}^n V(y|x_i) \right]. \quad (\text{F6})$$

Consider then the new matrix  $\tilde{\mathbf{V}}$  formed from  $\mathbf{V}$  by splitting row  $y$  into  $k$  rows as follows:

$$\begin{bmatrix} (1-\lambda)V(y|x_k) & V(y|x_{k+1}) & \cdots & V(y|x_n) \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \\ \lambda V(y|x_k) & 0 & \cdots & 0 \end{bmatrix}. \quad (\text{F7})$$

each  $\tilde{\mathbf{V}}_{\lambda}$  has only one nonzero element per row. Let  $\mathbf{R}$  denote the coarse-graining map such that  $\mathbf{V} = \mathbf{R}\tilde{\mathbf{V}}$ , and apply

$$\mathbf{V} = \mathbf{R}\tilde{\mathbf{V}} = \sum_{\lambda} p_{\lambda} \mathbf{R}\tilde{\mathbf{V}}_{\lambda}. \quad (\text{F9})$$

However, by the assumption that  $\mathbf{V}$  is extremal, this is only possible if  $\mathbf{R}\tilde{\mathbf{V}}_{\lambda}$  is the same for every  $\lambda$ . As a result, any two  $\tilde{\mathbf{V}}_{\lambda}$  and  $\tilde{\mathbf{V}}_{\lambda'}$  can differ only in rows that coarse-grain into the same rows by  $\mathbf{R}$ . From this it follows that  $\mathbf{V}$  can have no more than one nonzero element per column and  $\text{rank}(\mathbf{V}) \leq n-1$ . Hence, we have shown that the extreme points of  $\mathcal{A}_{\cap}^{n \rightarrow n'}$  are indeed extreme points of the signaling polytope  $\mathcal{C}_{n-1}^{n \rightarrow n'}$ .

To complete the proof of Lemma 5, we establish the case when  $\phi(\mathbf{V}) = n-1$ , as referenced above. We begin by proving the partial result provided by Proposition 9 and then use this result to prove Proposition 10.

**Proposition 9.** If  $\mathbf{V}$  is an extreme point of  $\mathcal{A}_{\cap}^{n \rightarrow n'}$  satisfying  $\phi(\mathbf{V}) = n-1$ , then each column of  $\mathbf{V}$  must have at least one unique row maximizer or it has only one nonzero element.

*Proof.* Suppose on the contrary that some column  $x$  has more than one nonzero element yet no unique row maximizer. Let  $\mathcal{S}_x \subset [n']$  be the set of rows for which column  $x$  contains a row maximizer. Since only one row maximizer per row contributes to the ML sum, and the elements of column  $x$  sum to one, we can satisfy  $\phi(\mathbf{V}) = n - 1$  iff both conditions hold:

- (i) each row  $y$  in  $\mathcal{S}_x$  has only two nonzero elements  $V(y|x)$  and  $V(y|x_y)$  for some column  $x_y \neq x$ ;
- (ii) every other nonzero element in  $\mathbf{V}$  outside of column  $x$  and the rows in  $\mathcal{S}_x$  are unique row maximizers.

With this structure, we introduce three cases of valid perturbations.

**Case (a):**  $V(y_1|x)$  and  $V(y_2|x)$  are nonextremal elements in column  $x$  with  $y_1, y_2 \notin \mathcal{S}_x$ . Then  $V(y_1|x) \rightarrow V(y_1|x) \pm \epsilon$  and  $V(y_2|x) \rightarrow V(y_2|x) \mp \epsilon$  is a valid perturbation. Indeed, even if we consider  $y_1$  or  $y_2$  as ambiguous rows, there is at most one other element in each of these rows (property (i) above), and so this perturbation would not violate any of the inequalities in Eq. (F3).

**Case (b):**  $V(y_1|x)$  and  $V(y_2|x)$  are nonextremal elements in column  $x$  with  $y_1 \in \mathcal{S}_x$  and  $y_2 \notin \mathcal{S}_x$ . Then  $V(y_1|x) = V(y_1|x_{y_1})$  for some other column  $x_{y_1} \neq x$ . By normalization, there will be another element  $V(y_3|x_{y_1})$  in column  $x_{y_1}$  that by property (ii) is a unique row maximizer. Hence, we introduce perturbations

$$\begin{aligned} V(y_1|x) &\rightarrow V(y_1|x) \pm \epsilon, & V(y_1|x_{y_1}) &\rightarrow V(y_1|x_{y_1}) \pm \epsilon, \\ V(y_2|x) &\rightarrow V(y_2|x) \mp \epsilon, & V(y_3|x_{y_1}) &\rightarrow V(y_3|x_{y_1}) \mp \epsilon. \end{aligned} \quad (\text{F10})$$

For clarity, the line spacing is chosen here so that elements on the same vertical line correspond to elements in the same row of  $\mathbf{V}$ . By properties (i) and (ii), these perturbations do not increase the ML sum, nor are they able to violate any of the other inequalities in Eq. (F3).

**Case (c):**  $V(y_1|x)$  and  $V(y_2|x)$  are nonextremal elements in column  $x$  with  $y_1, y_2 \in \mathcal{S}_x$ . Then  $V(y_1|x) = V(y_1|x_{y_1})$  and  $V(y_2|x) = V(y_2|x_{y_2})$  for some other columns  $x_{y_1}, x_{y_2} \neq x$  (with possibly  $x_{y_1} = x_{y_2}$ ). By normalization, there will be elements  $V(y_3|x_{y_1})$  and  $V(y_4|x_{y_2})$  in columns  $x_{y_1}$  and  $x_{y_2}$  respectively that are unique row maximizers [again by property (ii)]. Note this requires that  $y_1, y_2, y_3, y_4$  are all distinct rows. Hence, we introduce perturbations

$$\begin{aligned} V(y_1|x) &\rightarrow V(y_1|x) \pm \epsilon, & V(y_1|x_{y_1}) &\rightarrow V(y_1|x_{y_1}) \pm \epsilon, \\ V(y_2|x) &\rightarrow V(y_2|x) \mp \epsilon, & V(y_2|x_{y_2}) &\rightarrow V(y_2|x_{y_2}) \mp \epsilon, \\ V(y_3|x_{y_1}) &\rightarrow V(y_3|x_{y_1}) \mp \epsilon, & V(y_4|x_{y_2}) &\rightarrow V(y_4|x_{y_2}) \pm \epsilon, \end{aligned} \quad (\text{F11})$$

Normalization is preserved under these perturbations and all the inequalities in Eq. (F3) are satisfied.

As we have shown valid perturbations in all three cases under the assumption that some column has nonextremal elements with no unique row maximizer, the proposition follows.

**Proposition 10.** If  $\mathbf{V}$  is an extreme point of  $\mathcal{A}_{\cap}^{n \rightarrow n'}$  satisfying  $\phi(\mathbf{V}) = n - 1$ , then  $\mathbf{V}$  is an extreme point of  $\mathcal{C}_d^{n \rightarrow n'}$ .

*Proof.* Suppose that  $\mathbf{V}$  has some column  $x_1$  containing more than one nonzero element (if no such column can be found, then the proposition is proven). Let  $V(y_1|x_1) \in (0, 1)$

denote a unique row maximizer, which is assured to exist by Proposition 9. We again proceed by considering two cases.

**Case (a):** Column  $x_1$  contains only one row maximizer  $V(y_1|x_1)$  and all other elements in the column are not row maximizers. Then there must exist another column  $x'_1$  that also contains at least two nonzero elements. Indeed, if on the contrary all other columns only had one nonzero element each, then it would be impossible for  $\phi(\mathbf{V}) = n - 1$ . If  $x'_1$  only contains row maximizers, then proceed to case (b) and replace  $x_1$  with  $x'_1$ . Otherwise,  $x'_1$  does not only contain row maximizers; rather it has a unique row maximizer  $V(y_3|x'_1)$  in row  $y_3$  and a nonzero element  $V(y_4|x'_1)$  in row  $y_4$  that is not a row maximizer. Thus, we can introduce the valid perturbations

$$\begin{aligned} V(y_1|x_1) &\rightarrow V(y_1|x_1) \pm \epsilon, & V(y_2|x_1) &\rightarrow V(y_2|x_1) \mp \epsilon, \\ V(y_3|x'_1) &\rightarrow V(y_3|x'_1) \mp \epsilon, & V(y_4|x'_1) &\rightarrow V(y_4|x'_1) \mp \epsilon, \end{aligned} \quad (\text{F12})$$

where  $V(y_2|x_1)$  denotes another nonzero element in  $x_1$  (with possibly  $y_2 = y_3, y_4$  and/or  $y_3 = y_1$ ). It can be verified that all inequalities in Eq. (F3) are preserved under these perturbations.

**Case (b):** Column  $x_1$  only contains row maximizers, with  $V(y_2|x_1)$  being another one in addition to  $V(y_1|x_1)$ . If  $V(y_2|x_1)$  is a unique row maximizer, then valid perturbations can be made to both  $V(y_1|x_1)$  and  $V(y_2|x_1)$ . However, suppose that  $V(y_2|x_1)$  is a nonunique row maximizer, and let  $V(y_2|x_2) = V(y_2|x_1)$  be another row maximizer in column  $x_2$ . There can be no other nonzero elements in row  $y_2$ . Indeed, if there were another column, say  $x_3$ , such that  $V(y_2|x_3) > 0$ , then we would have

$$\begin{aligned} \frac{1}{2} \|\mathbf{r}_{y_2}\|_1 &\geq \frac{1}{2} [V(y_2|x_1) + V(y_2|x_2) + V(y_2|x_3)] \\ &> V(y_2|x_2) = \|\mathbf{r}_{y_2}\|_\infty, \end{aligned} \quad (\text{F13})$$

and so

$$\langle \mathbf{G}_{n'-1, n-1}^{n, n'}, \mathbf{V} \rangle > \phi(\mathbf{V}) = n - 1, \quad (\text{F14})$$

where the one ambiguous row in  $\mathbf{G}_{n'-1, n-1}^{n, n'}$  is  $y_2$ . Hence, the only nonzero elements in row  $y_2$  are  $V(y_2|x_1)$  and  $V(y_2|x_2)$ . Let  $V(y_3|x_2)$  be a unique row maximizer in column  $x_2$ .

We must be able to find another column  $x_3$  with more than one nonzero element, one of which is a unique row maximizer and the other which is a nonunique row maximizer. For if this were not the case, then any other column in  $\mathbf{V}$  would either have a unique row maximizer equaling one, or it would have at least two elements, one being a unique row maximizer and the others not being row maximizers. However, the latter possibility was covered in case (a) and was shown to be impossible for an extremal  $\mathbf{V}$ . For the former, if all the other  $n - 2$  columns outside of  $x_1$  and  $x_2$  contain unique row maximizers equaling one, then they would collectively contribute an amount of  $n - 2$  to the ML sum. Since every element in column  $x_1$  is a row maximizer, and  $V(y_3|x_2)$  is a row maximizer in column  $x_2$ , we would have  $\phi(\mathbf{V}) > (n - 2) + 1 + V(y_3|x_2) > n - 1$ . Hence, there must exist another column  $x_3$  with a nonunique row maximizer  $V(y_5|x_3)$  that is shared with column  $x_4$  (which may be equivalent to either  $x_1$  or  $x_2$ ). Letting  $V(y_4|x_3)$  and  $V(y_6|x_4)$  denote unique row maximizers in columns  $x_3$  and  $x_4$ ,

respectively, we can perform the valid perturbations

$$\begin{aligned} V(y_1|x_1) &\rightarrow V(y_1|x_1) \pm \epsilon, & V(y_2|x_1) &\rightarrow V(y_2|x_1) \mp \epsilon, \\ V(y_2|x_2) &\rightarrow V(y_2|x_2) \mp \epsilon, & V(y_3|x_2) &\rightarrow V(y_3|x_2) \pm \epsilon, \\ V(y_4|x_3) &\rightarrow V(y_4|x_3) \pm \epsilon, & V(y_5|x_3) &\rightarrow V(y_5|x_3) \mp \epsilon, \\ V(y_5|x_4) &\rightarrow V(y_5|x_4) \mp \epsilon, & V(y_6|x_4) &\rightarrow V(y_6|x_4) \pm \epsilon. \end{aligned} \quad (\text{F15})$$

Note that  $y_1, y_2, y_3, y_4, y_5, y_6$  are all distinct rows since each row in  $\mathbf{V}$  can have at most one pair of nonunique row maximizers while rows  $y_1, y_3, y_4, y_6$  contain unique row maximizers. This assures that the perturbations do not violate the inequalities in Eq. (F3).

As cases (a) and (b) exhaust all possibilities, we see that  $\mathbf{V}$  can only have one nonzero element per column. From this the conclusion of Proposition 10 follows. ■

This completes the proof of Lemma 5. ■

## APPENDIX G: PROOF OF THEOREM 2

In this Appendix we analyze the  $\mathcal{C}_2^{n \rightarrow 4}$  signaling polytope to prove the Theorem 2. To begin we define the polyhedron of channels

$$\mathcal{C}(\mathbf{G}, \gamma) := \{\mathbf{P} \in \mathcal{P}^{n \rightarrow n'} \mid \langle \mathbf{G}, \mathbf{P} \rangle = \sum_{x=1}^n \sum_{y=1}^{n'} G_{y,x} P(y|x) \leq \gamma\} \quad (\text{G1})$$

for any signaling dimension witness  $(\mathbf{G}, \gamma)$  with  $\mathbf{G} \in \mathbb{R}^{n' \times n}$  and  $\gamma \in \mathbb{R}$ . Since  $\mathcal{C}_d^{n \rightarrow n'}$  is a convex polytope, there exists a finite number of polyhedra  $\{\mathcal{C}(\mathbf{G}_m, \gamma_m)\}_{m=1}^r$  such that

$$\mathcal{C}_d^{n \rightarrow n'} = \bigcap_{m=1}^r \mathcal{C}(\mathbf{G}_m, \gamma_m). \quad (\text{G2})$$

*Remark* Without loss of generality, we can assume that the matrices  $\mathbf{G}_m$  contain nonnegative elements. Indeed, if  $G_{y,x} < 0$  is the smallest element in column  $x$  of  $\mathbf{G}_m$ , then we replace each element in column  $x$  as  $G_{y',x} \rightarrow G_{y',x} + G_{y,x}$  and shift  $\gamma \rightarrow \gamma + G_{y,x}$ . Hence, the smallest element in column  $x$  of  $\mathbf{G}_m$  becomes  $G_{y,x} = 0$ .

The proof of Theorem 2 is a consequence of Lemmas 6 and 7 below and our numerical results for the  $\mathcal{C}_2^{n \rightarrow 4}$  signaling polytope [32] (see Table I). First, by Lemma 6 we can reduce any signaling dimension witness  $(\mathbf{G}, \gamma)$  bounding  $\mathcal{C}_2^{n \rightarrow 4}$  to a new signaling dimension witness  $(\hat{\mathbf{G}}, \hat{\gamma})$  having at most 2 nonzero elements in each column. The reduced inequality  $(\hat{\mathbf{G}}, \hat{\gamma})$  satisfies  $\mathcal{C}_2^{n \rightarrow 4} \subset \mathcal{C}(\hat{\mathbf{G}}, \hat{\gamma}) \subset \mathcal{C}(\mathbf{G}, \gamma)$  and thus bounds  $\mathcal{C}_2^{n \rightarrow 4}$  more tightly than  $(\mathbf{G}, \gamma)$ . Next, we use Lemma 7 to show that for any integer  $n$  a tight signaling dimension witness of  $\mathcal{C}_2^{n \rightarrow 4}$  has at most six nonzero columns. The presence of

all-zero columns implies that this inequality is simply an input lifting of a tight signaling dimension witness of  $\mathcal{C}_2^{6 \rightarrow 4}$ . Therefore, the complete set of tight signaling dimension witnesses bounding  $\mathcal{C}_2^{n \rightarrow 4}$  is the set of all input liftings and permutations of the generator facets of  $\mathcal{C}_2^{6 \rightarrow 4}$  shown in Table I.

*Lemma 6.* If  $\mathcal{C}_d^{n \rightarrow n'} \subset \mathcal{C}(\mathbf{G}, \gamma)$ , then there exists a polyhedron  $\mathcal{C}(\hat{\mathbf{G}}, \hat{\gamma})$  with  $\hat{\mathbf{G}}$  having at most  $(n' - d)$  nonzero elements in each column and satisfying

$$\mathcal{C}_d^{n \rightarrow n'} \subset \mathcal{C}(\hat{\mathbf{G}}, \hat{\gamma}) \subset \mathcal{C}(\mathbf{G}, \gamma). \quad (\text{G3})$$

*Proof.* Suppose  $\mathcal{C}_d^{n \rightarrow n'} \subset \mathcal{C}(\mathbf{G}, \gamma)$  and consider an arbitrary  $x \in [n]$ . For convenience, let us relabel the elements of the  $x^{\text{th}}$  column of  $\mathbf{G}$  in nonincreasing order; i.e.,  $G_{y,x} \geq G_{y+1,x}$ . Every vertex  $\mathbf{V}$  of  $\mathcal{C}_d^{n \rightarrow n'}$  will satisfy

$$\begin{aligned} \gamma &\geq \sum_{x',y} G_{y,x'} V(y|x') \\ &= \sum_y G_{y,x} V(y|x) + \sum_{x' \neq x, y} G_{y,x'} V(y|x') \\ &= \sum_y G_{y,x} V(y|x) + f(\mathbf{G}, \mathbf{V}, x), \end{aligned} \quad (\text{G4})$$

where  $f(\mathbf{G}, \mathbf{V}, x) := \sum_{x' \neq x, y} G_{y,x'} V(y|x')$ . A key observation is

$$\gamma \geq G_{d,x} + f(\mathbf{G}, \mathbf{V}, x) \quad \text{for every vertex } \mathbf{V} \text{ of } \mathcal{C}_d^{n \rightarrow n'}. \quad (\text{G5})$$

We prove this observation using Eq. (G4). First consider any vertex  $\mathbf{V}$  such that  $V(y|x) = \delta_{d'y}$  with  $d' \geq d$ . Then Eq. (G4) shows that  $\gamma \geq G_{d',x} + f(\mathbf{G}, \mathbf{V}, x) \geq G_{d,x} + f(\mathbf{G}, \mathbf{V}, x)$ , since we have labeled the elements in nonincreasing order. However, consider a vertex  $\mathbf{V}$  for which  $V(y|x) = \delta_{d'y}$  with  $d' < d$ . Since vertices can be formed with  $d$  nonzero rows, we can choose another vertex  $\mathbf{V}'$  that is identical to  $\mathbf{V}$  in all columns  $x' \neq x$ , and yet for column  $x$  it satisfies  $V'(y|x) = \delta_{d''y}$  with  $d \leq d''$ . Hence, applying Eq. (G4) to vertex  $\mathbf{V}'$  yields

$$\begin{aligned} \gamma &\geq G_{d'',x} + f(\mathbf{V}', x) \geq G_{d,x} + f(\mathbf{G}, \mathbf{V}', x) \\ &= G_{d,x} + f(\mathbf{G}, \mathbf{V}, x), \end{aligned} \quad (\text{G6})$$

where the last line follows from the fact that  $\mathbf{V}$  and  $\mathbf{V}'$  only differ in column  $x$ .

Having established Eq. (G5), we next form a new matrix  $\hat{\mathbf{G}}$  which is obtained from  $\mathbf{G}$  by replacing its  $x$ th column with

$$(\hat{\mathbf{G}}_{y,x})_y^T := (\overbrace{0, 0, \dots, 0}^d, G_{d+1,x} - G_{d,x}, \dots, G_{n',x} - G_{d,x})^T. \quad (\text{G7})$$

Letting  $\hat{\gamma} = \gamma - G_{d,x}$ , for any vertex  $\mathbf{V}$  we have

$$\sum_{x',y} \hat{G}_{y,x'} V(y|x') = \sum_y \hat{G}_{y,x} V(y|x) + f(\mathbf{G}, \mathbf{V}, x) = \begin{cases} f(\mathbf{G}, \mathbf{V}, x) & \text{if } V(y|x) = \delta_{d'y} \text{ with } d' \leq d, \\ G_{d',x} - G_{d,x} + f(\mathbf{G}, \mathbf{V}, x) & \text{if } V(y|x) = \delta_{d'y} \text{ with } d' > d, \end{cases} \leq \hat{\gamma}, \quad (\text{G8})$$

where the last inequality follows from Eq. (G5) (in the first case) and Eq. (G4) (in the second case). Hence, we have that  $\mathcal{C}_d^{n \rightarrow n'} \subset \mathcal{C}(\hat{\mathbf{G}}, \hat{\gamma})$ . Conversely, if  $\mathbf{P} \in \mathcal{C}(\hat{\mathbf{G}}, \hat{\gamma})$ , then

$$\gamma - G_{d,x} \geq \sum_{x',y} \hat{G}_{y,x'} P(y|x') = \sum_y \hat{G}_{y,x} P(y|x) + \sum_{x' \neq x, y} \hat{G}_{y,x'} P(y|x')$$



$$\begin{aligned}
 &= \sum_{y=d+1}^{n'} (G_{y,x} - G_{d,x})P(y|x) + \sum_{x' \neq x, y} \hat{G}_{y,x'}P(y|x') \\
 &= -G_{d,x}(1 - \sum_{y=1}^d P(y|x)) + \sum_{y=d+1}^{n'} G_{y,x}P(y|x) + \sum_{x' \neq x, y} \hat{G}_{y,x'}P(y|x') \\
 &\geq -G_{d,x} + \sum_{y=1}^{n'} G_{y,x}P(y|x) + \sum_{x' \neq x, y} \hat{G}_{y,x'}P(y|x') \\
 &= -G_{d,x} + \sum_{x', y} G_{y,x'}P(y|x'). \tag{G9}
 \end{aligned}$$

Therefore,  $\mathbf{P} \in \mathcal{C}(\mathbf{G}, \gamma)$  and so  $\mathcal{C}_2^{n \rightarrow n'} \subset \mathcal{C}(\hat{\mathbf{G}}, \hat{\gamma}) \subset \mathcal{C}(\mathbf{G}, \gamma)$ . Note that if  $\mathbf{G}$  has only nonnegative elements then so will  $\hat{\mathbf{G}}$ . ■

*Lemma 7.* For any finite number of inputs  $n$ ,

$$\mathcal{C}_2^{n \rightarrow 4} = \bigcap_{m=1}^s \mathcal{C}(\mathbf{G}_m, \gamma_m), \tag{G10}$$

with each  $\mathbf{G}_m$  having at most six nonzero columns.

*Proof.* As a consequence of Lemma 6, we can always find a complete set of polyhedra  $\{\mathcal{C}(\hat{\mathbf{G}}_m, \hat{\gamma}_m)\}_{m=1}^s$  such that

$$\mathcal{C}_2^{n \rightarrow 4} = \bigcap_{m=1}^s \mathcal{C}(\hat{\mathbf{G}}_m, \hat{\gamma}_m),$$

such that each  $\hat{\mathbf{G}}_m$  has no more than positive elements in each column and the rest being zero. Our goal is to show that the number of such columns can be reduced to six. The key steps in our reduction are given by the following two propositions. ■

*Proposition 11.* Consider the matrices

$$\begin{aligned}
 \hat{\mathbf{G}} &= \begin{bmatrix} a & b & \cdot & \cdots \\ c & d & \cdot & \cdots \\ 0 & 0 & \cdot & \cdots \\ 0 & 0 & \cdot & \cdots \end{bmatrix}, \\
 \hat{\mathbf{G}}' &= \begin{bmatrix} a-c & b+c & \cdot & \cdots \\ 0 & d+c & \cdot & \cdots \\ 0 & 0 & \cdot & \cdots \\ 0 & 0 & \cdot & \cdots \end{bmatrix}, \quad a \geq c \geq 0, \tag{G11}
 \end{aligned}$$

which differ only in the first two columns. Then  $\mathcal{C}_2^{n \rightarrow 4} \in \mathcal{C}(\hat{\mathbf{G}}, \hat{\gamma})$  iff  $\mathcal{C}_2^{n \rightarrow 4} \in \mathcal{C}(\hat{\mathbf{G}}', \hat{\gamma})$ .

*Proof.* Every vertex  $\mathbf{V}$  of  $\mathcal{C}_2^{n \rightarrow 4}$  will have support in only two rows. If  $\mathbf{V}$  has support in the first two rows, then its upper left corner will have one of the forms  $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ ,  $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ ,  $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ ,  $\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$ . In each of these cases,  $\langle \hat{\mathbf{G}}, \mathbf{V} \rangle \leq \hat{\gamma} \Leftrightarrow \langle \hat{\mathbf{G}}', \mathbf{V} \rangle \leq \hat{\gamma}$ .

The other possibility is that  $\mathbf{V}$  has support in only one of the first two rows. This leads to upper left corners of the form  $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ ,  $\begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$ ,  $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ ,  $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ ,  $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ ,  $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ . Suppose now that  $\mathcal{C}_2^{n \rightarrow 4} \in \mathcal{C}(\hat{\mathbf{G}}, \hat{\gamma})$ . If a vertex  $\mathbf{V}$  of  $\mathcal{C}_2^{n \rightarrow 4}$  has form  $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$  in the upper left corner, then nonnegativity of  $c$  implies that  $\langle \hat{\mathbf{G}}', \mathbf{V} \rangle \leq \hat{\gamma}$ . A somewhat less trivial case is any vertex  $\mathbf{V}_1$  having form  $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$  in the upper left corner. Here we need to use the fact that there exists a vertex  $\mathbf{V}_2$  with  $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$  in the upper left corner but is identical to  $\mathbf{V}_1$  in all other columns.

Hence, we have

$$\begin{aligned}
 \hat{\gamma} &\geq \langle \hat{\mathbf{G}}, \mathbf{V}_2 \rangle = a + b + \kappa \Rightarrow \langle \hat{\mathbf{G}}', \mathbf{V}_1 \rangle \\
 &= b + c + \kappa \leq a + b + \kappa \leq \hat{\gamma}, \tag{G12}
 \end{aligned}$$

where  $\kappa$  is the contribution of the other columns to the inner product, and we have used the assumption that  $a \geq c$ . Similar reasoning shows that  $\langle \hat{\mathbf{G}}', \mathbf{V} \rangle \leq \hat{\gamma}$  for all other vertices  $\mathbf{V}$ . Conversely, by an analogous case-by-case consideration, we can establish that  $\mathcal{C}_2^{n \rightarrow 4} \in \mathcal{C}(\hat{\mathbf{G}}', \hat{\gamma})$  implies  $\langle \hat{\mathbf{G}}, \mathbf{V} \rangle \leq \hat{\gamma}$  for all vertices  $\mathbf{V}$  of  $\mathcal{C}_2^{n \rightarrow 4}$ . ■

*Proposition 12.* Consider the matrices

$$\begin{aligned}
 \hat{\mathbf{G}} &= \begin{bmatrix} a & b & \cdot & \cdots \\ 0 & 0 & \cdot & \cdots \\ 0 & 0 & \cdot & \cdots \\ 0 & 0 & \cdot & \cdots \end{bmatrix}, \quad \hat{\mathbf{G}}' = \begin{bmatrix} a+b & 0 & \cdot & \cdots \\ 0 & 0 & \cdot & \cdots \\ 0 & 0 & \cdot & \cdots \\ 0 & 0 & \cdot & \cdots \end{bmatrix}, \\
 \hat{\mathbf{G}}'' &= \begin{bmatrix} 0 & a+b & \cdot & \cdots \\ 0 & 0 & \cdot & \cdots \\ 0 & 0 & \cdot & \cdots \\ 0 & 0 & \cdot & \cdots \end{bmatrix}, \tag{G13}
 \end{aligned}$$

which differ only in the first two columns. Then  $\mathcal{C}_2^{n \rightarrow 4} \in \mathcal{C}(\hat{\mathbf{G}}, \hat{\gamma})$  iff  $\mathcal{C}_2^{n \rightarrow 4} \in \mathcal{C}(\hat{\mathbf{G}}', \hat{\gamma}) \cap \mathcal{C}(\hat{\mathbf{G}}'', \hat{\gamma})$ . ■

*Proof.* This proof considers the vertices of  $\mathcal{C}_2^{n \rightarrow 4}$  and applies the same reasoning as the proof of Proposition 11.

Continuing with the proof of Lemma 7, suppose that  $\mathcal{C}_2^{n \rightarrow 4} \in \mathcal{C}(\hat{\mathbf{G}}_m, \hat{\gamma}_m)$  with each column of  $\hat{\mathbf{G}}_m$  having no more than two nonzero rows. We can group the columns into six groups according to which two rows have zero (it may be that a column has more than two zeros, in which case we just select one group to place it in). By repeatedly applying Proposition 11, we can replace  $\hat{\mathbf{G}}_m$  with a matrix  $\hat{\mathbf{G}}'_m$  such that each group has at most one column with two nonzero elements; the rest of the columns in that group have at most just one nonzero element. We then repeatedly apply Proposition 12 to remove multiple columns with the same single nonzero row. In the end, we arrive at the following:

$$\mathcal{C}_2^{n \rightarrow 4} \in \mathcal{C}(\hat{\mathbf{G}}_m, \hat{\gamma}_m) \Leftrightarrow \mathcal{C}_2^{n \rightarrow 4} \in \bigcap_j \mathcal{C}(\hat{\mathbf{G}}_{m,j}, \hat{\gamma}_m), \tag{G14}$$

where each  $\hat{\mathbf{G}}_{m,j}$  has at most ten nonzero columns corresponding to the different ways that no more than two nonzero elements can occupy a column. That is, up to a permutation of

columns, each  $\hat{\mathbf{G}}_{m,j}$  will have the form

$$\hat{\mathbf{G}}_{m,j} = \begin{bmatrix} a_1 & b_1 & c_1 & 0 & 0 & 0 & g & 0 & 0 & 0 & 0 & \dots \\ a_2 & 0 & 0 & d_1 & e_1 & 0 & 0 & h & 0 & 0 & 0 & \dots \\ 0 & b_2 & 0 & d_2 & 0 & f_1 & 0 & 0 & i & 0 & 0 & \dots \\ 0 & 0 & c_2 & 0 & e_2 & f_2 & 0 & 0 & 0 & j & 0 & \dots \end{bmatrix}. \quad (\text{G15})$$

The final step is to remove the block of diagonal elements  $[g, h, i, j]$ . To do this, observe that we absorb any of these diagonal elements into an earlier column, provided that the row contains the largest element in that column. For example, if  $f_2 > f_1$ , then we can replace  $\hat{\mathbf{G}}_{m,j}$  with

$$\hat{\mathbf{G}}'_{m,j} = \begin{bmatrix} a_1 & b_1 & c_1 & 0 & 0 & 0 & g & 0 & 0 & 0 & 0 & \dots \\ a_2 & 0 & 0 & d_1 & e_1 & 0 & 0 & h & 0 & 0 & 0 & \dots \\ 0 & b_2 & 0 & d_2 & 0 & f_1 & 0 & 0 & i & 0 & 0 & \dots \\ 0 & 0 & c_2 & 0 & e_2 & f_2 + j & 0 & 0 & 0 & 0 & 0 & \dots \end{bmatrix}, \quad (\text{G16})$$

and we can easily see that  $\mathcal{C}_2^{n \rightarrow 4} \in \mathcal{C}(\hat{\mathbf{G}}_{m,j}, \hat{\gamma}_m)$  iff  $\mathcal{C}_2^{n \rightarrow 4} \in \mathcal{C}(\hat{\mathbf{G}}'_{m,j}, \hat{\gamma}_m)$ . By considering the maximum element in each of the first six columns, we can perform this replacement for at least three of the four elements  $[g, h, i, j]$ . If we can do this for all four elements, then the proof is complete. However, if we can only remove three of these elements, then we will obtain a matrix  $\hat{\mathbf{G}}''_{m,j}$  of the form (up to row/column permutations)

$$\hat{\mathbf{G}}''_{m,j} = \begin{bmatrix} a_1 & b_1 & c_1 & 0 & 0 & 0 & g & 0 & 0 & 0 & 0 & \dots \\ a_2 & 0 & 0 & d_1 & e_1 & 0 & 0 & 0 & 0 & 0 & 0 & \dots \\ 0 & b_2 & 0 & d_2 & 0 & f_1 & 0 & 0 & 0 & 0 & 0 & \dots \\ 0 & 0 & c_2 & 0 & e_2 & f_2 & 0 & 0 & 0 & 0 & 0 & \dots \end{bmatrix}, \quad (\text{G17})$$

with  $a_1, b_1, c_2$  not having the largest values in their respective columns. In this case, we construct the matrix

$$\hat{\mathbf{G}}'''_{m,j} = \begin{bmatrix} a_1 + g & b_1 + g & c_1 + g & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots \\ a_2 + g & 0 & 0 & d_1 & e_1 & 0 & 0 & 0 & 0 & 0 & 0 & \dots \\ 0 & b_2 + g & 0 & d_2 & 0 & f_1 & 0 & 0 & 0 & 0 & 0 & \dots \\ 0 & 0 & c_2 + g & 0 & e_2 & f_2 & 0 & 0 & 0 & 0 & 0 & \dots \end{bmatrix}, \quad (\text{G18})$$

from which it can be verified that  $\mathcal{C}_2^{n \rightarrow 4} \subset \mathcal{C}(\hat{\mathbf{G}}'''_{m,j}, \hat{\gamma}_m)$  iff  $\mathcal{C}_2^{n \rightarrow 4} \subset \mathcal{C}(\hat{\mathbf{G}}'''_{m,j}, \hat{\gamma}_m + 2g)$ . ■

## APPENDIX H: PROOF OF THEOREM 3

In this Appendix we provide two propositions that support the proof of Theorem 3. Recall that a  $d$ -dimensional partial replacer channel is a quantum channel having the form

$$\mathcal{R}_\mu(X) = \mu X + (1 - \mu)\text{Tr}[X]\sigma, \quad (\text{H1})$$

where  $1 \geq \mu \geq 0$ ,  $\sigma$  is some fixed density matrix, and  $X$  is a quantum state on a  $d$ -dimensional Hilbert space. Note that the partial erasure channel  $\mathcal{E}_\mu$  corresponds to  $\sigma$  being an erasure flag  $|E\rangle\langle E|$ , where  $|E\rangle$  is orthogonal to  $\{|1\rangle, \dots, |d\rangle\}$ . We first show that the lower bound of  $\kappa(\mathcal{R}_\mu) \geq \lceil \mu d + (1 - \mu) \rceil$  [see Eq. (17)] is not improved by any choice of states  $\{\rho_x\}_x$ , POVM  $\{\Pi_y\}_y$ , or ambiguous guessing game  $\mathbf{G}_{n',d}^{n,n'}$  with  $k = n'$ .

**Proposition 13.** The maximum likelihood score for any classical channel  $\mathbf{P}_{\mathcal{R}_\mu}$  generated using a partial replacer channel  $\mathcal{R}_\mu$  is bounded as

$$\langle \mathbf{G}_{\text{ML}}, \mathbf{P}_{\mathcal{R}_\mu} \rangle \leq \mu d + (1 - \mu), \quad (\text{H2})$$

where  $\mathbf{G}_{\text{ML}}$  is any maximum likelihood facet satisfying Proposition 2(i).

*Proof.* In this proof, we first consider the unlifted maximum likelihood  $\mathbf{G}_{\text{ML}}^{n'} = \mathbb{I}_{n'}$  where  $n = n'$  (see Appendix D 2), and then generalize across all input/output liftings taking  $\mathbf{G}_{\text{ML}}^{n'} \rightarrow \mathbf{G}_{\text{ML}} \in \mathbb{R}^{m' \times m}$  where  $m', m \geq n'$ . To begin we maximize  $\langle \mathbf{G}_{\text{ML}}^{n'}, \mathbf{P}_{\mathcal{R}_\mu} \rangle$  over the quantum states  $\{\rho_x\}_x$  and POVM

$\{\Pi_y\}_y$ ,

$$\begin{aligned} & \max_{\{\rho_x\}_x, \{\Pi_y\}_y} \langle \mathbf{G}_{\text{ML}}^{n'}, \mathbf{P}_{\mathcal{R}_\mu} \rangle \\ &= \max_{\{\rho_x\}_x, \{\Pi_y\}_y} \sum_{x=y} \text{Tr}[\Pi_y \mathcal{R}_\mu(\rho_x)] \end{aligned} \quad (\text{H3})$$

$$= \max_{\{\rho_x\}_x, \{\Pi_y\}_y} \sum_{x=y} \mu \text{Tr}[\Pi_y \rho_x] + (1 - \mu) \text{Tr}[\Pi_y \sigma] \quad (\text{H4})$$

$$\leq \max_{\{\Pi_y\}_y} \sum_y \mu \text{Tr}[\Pi_y] + (1 - \mu) \text{Tr}[\Pi_y \sigma] \quad (\text{H5})$$

$$= \mu d + (1 - \mu), \quad (\text{H6})$$

where Eq. (H5) uses the fact that  $\text{Tr}[\Pi_y \rho_x] \leq \text{Tr}[\Pi_y]$  for any choice of  $\Pi_y$  and  $\rho_x$  while Eq. (H6) results from  $\sum_y \text{Tr}[\Pi_y] = d$  and  $\sum_y \text{Tr}[\Pi_y \sigma] = \text{Tr}[\sigma] = 1$ . A simple example that achieves this bound is the scenario where Alice sends orthogonal states  $\{|x\rangle\}_{x=1}^d$  and Bob measures with a similar POVM  $\{|y\rangle\}_{y=1}^d$ , then

$$\begin{aligned} & \langle \mathbf{G}_{\text{ML}}^d, \mathbf{P}_{\mathcal{R}_\mu} \rangle \\ &= \sum_{y=x=1}^d \text{Tr}[|y\rangle\langle y| \mathcal{R}_\mu(|x\rangle\langle x|)] \end{aligned} \quad (\text{H7})$$

$$= \mu \sum_{y=1}^d \text{Tr}[|y\rangle\langle y| \mathcal{R}_\mu(|y\rangle\langle y|)] + (1 - \mu) \sum_{y=1}^d \text{Tr}[|y\rangle\langle y| \sigma] \quad (\text{H8})$$

$$= \mu d + (1 - \mu). \quad (\text{H9})$$

In general, the upper bound is achieved whenever  $\Pi_y \rho_x = \Pi_y$  for all  $x \in [n]$  and  $y \in [n']$ . Note that this requires  $\text{rank}(\Pi_y) = \text{rank}(\rho_x) = 1$  and  $\Pi_y \Pi_x = \rho_x$ .

To extend the bound  $\langle \mathbf{G}'_{\text{ML}}, \mathbf{P}_{\mathcal{R}_\mu} \rangle \leq \mu d + (1 - \mu)$  to all liftings of  $\mathbf{G}'_{\text{ML}}$ , we make two observations. First, note that the input lifting taking  $\mathbf{G}'_{\text{ML}} \rightarrow \mathbf{G}''_{\text{ML}} \in \mathbb{R}^{n' \times m}$  contains  $(m - n)$  all-zero columns. These all-zero columns of  $\mathbf{G}''_{\text{ML}}$  do not contribute to the inner product  $\langle \mathbf{G}'_{\text{ML}}, \mathbf{P}_{\mathcal{R}_\mu} \rangle$ , and therefore, cannot increase the inner product beyond  $\mu d + (1 - \mu)$ . Second, observe that the output lifting taking  $\mathbf{G}'_{\text{ML}} \rightarrow \mathbf{G}''_{\text{ML}} \in \mathbb{R}^{(n'+1) \times n}$  requires a new POVM  $\{\Pi'_y\}_{y=1}^{n'+1}$  which must satisfy  $\sum_{y=1}^{n'+1} \Pi'_y = \mathbb{I}_d$ . Furthermore, one column  $x$  of  $\mathbf{G}'_{\text{ML}}$  has two nonzero elements in rows  $y$  and  $y'$  where  $G'_{y,x} = G'_{y',x} = 1$ . In this case, two POVM elements  $\Pi'_y$  and  $\Pi'_{y'}$  are both optimized against the state  $\rho_x$ . However, the constraint  $\text{Tr}[\Pi'_y \rho_x] + \text{Tr}[\Pi'_{y'} \rho_x] \leq 1$  holds for any choice of  $\rho_x$  and POVM. Therefore, the inner product  $\langle \mathbf{G}'_{\text{ML}}, \mathbf{P}_{\mathcal{R}_\mu} \rangle \leq \mu d + (1 - \mu)$ . The argument applied for the output lifting holds in general where one or more columns  $x$  contain at least two nonzero elements. Thus, the upper bound in Eq. (H6) holds for any input/output lifting taking  $\mathbf{G}'_{\text{ML}} \rightarrow \mathbf{G}''_{\text{ML}} \in \mathbb{R}^{m' \times m}$ , where  $\min\{m, m'\} \geq n'$ . This concludes the proof. ■

The upper bound on the maximum likelihood score from Proposition 13 serves as a lower bound on the signaling dimension of the partial replacer channel  $\kappa(\mathcal{R}_\mu)$ . This follows from the fact that if  $\mathbf{P}_{\mathcal{R}_\mu} \notin \mathcal{M}_r^{n \rightarrow n'}$ , then  $\kappa(\mathcal{R}_\mu) > r$ . Furthermore, the integer nature of the signaling dimension implies that  $\kappa(\mathcal{R}_\mu) \geq \lceil \mu d + (1 - \mu) \rceil$ . We now turn to certify the signaling dimension of the partial erasure channel.

**Proposition 14.** The signaling dimension of a  $d$ -dimensional partial erasure channel is

$$\kappa(\mathcal{E}_\mu) = \min\{d, \lceil \mu d + 1 \rceil\}. \quad (\text{H10})$$

*Proof.* Let the classical channel  $\mathbf{P}_{\mathcal{E}_\mu}$  be induced by the partial erasure channel  $\mathcal{E}_\mu$  via Eq. (1) for any collection of quantum states  $\{\rho_x\}_x$  and POVM  $\{\Pi_y\}_y$ . The transition probabilities are then expressed

$$P_{\mathcal{E}_\mu}(y|x) = \mu P_{\text{id}_d}(y|x) + (1 - \mu) P_{|E\rangle}(y), \quad (\text{H11})$$

where  $P_{\text{id}_d}(y|x) = \text{Tr}[\Pi_y \rho_x]$  and  $P_{|E\rangle}(y) = \text{Tr}[\Pi_y |E\rangle\langle E|]$ . Since the simulation protocol for partial replacer channels can faithfully simulate  $\mathbf{P}_{\mathcal{E}_\mu}$ , the upper bound  $\kappa(\mathcal{R}_\mu) \leq \lceil \mu d + 1 \rceil$  holds (see the proof of Theorem 3 in the main text). Therefore,  $\min\{d, \lceil \mu d + 1 \rceil\} \geq \kappa(\mathcal{E}_\mu)$ . To establish a lower bound on  $\kappa(\mathcal{E}_\mu)$  we consider the channel  $\mathbf{P}_{\mathcal{E}_\mu} \in \mathcal{P}^{d \rightarrow (d+1)}$  generated by the scenario where Alice sends the computational basis states  $\{|x\rangle\}_{x=1}^d$  and Bob measures with the POVM  $\{|y\rangle\}_{y=1}^{d+1}$ , where  $|d+1\rangle = |E\rangle$ ,

$$\begin{aligned} \mathbf{P}_{\mathcal{E}_\mu} &= \sum_{x=1}^d \sum_{y=1}^{d+1} \text{Tr}[|y\rangle\langle y| \mathcal{E}_\mu(|x\rangle\langle x|)] |y\rangle\langle x| \\ &= \sum_{x=1}^d \sum_{y=1}^{d+1} (\mu \text{Tr}[|y\rangle\langle y|x\rangle\langle x|] \\ &\quad + (1 - \mu) \text{Tr}[|y\rangle\langle y|E\rangle\langle E|]) |y\rangle\langle x| \end{aligned} \quad (\text{H12})$$

$$+ (1 - \mu) \text{Tr}[|y\rangle\langle y|E\rangle\langle E|] |y\rangle\langle x| \quad (\text{H13})$$

$$= \mu \sum_{x=1}^d |x\rangle\langle x| + (1 - \mu) \sum_{x=1}^d |E\rangle\langle x|. \quad (\text{H14})$$

As demonstrated in Proposition 13,  $\mathbf{P}_{\mathcal{E}_\mu}$  achieves the maximum likelihood upper bound for partial replacer channels,  $\langle \mathbf{G}_{\text{ML}}, \mathbf{P}_{\mathcal{E}_\mu} \rangle = \mu d + (1 - \mu)$ . In fact, this bound also holds for nonorthogonal quantum states  $\{\rho_x\}_{x \in [n]}$ , where  $n > d$ .

To improve the lower bound on  $\kappa(\mathcal{E}_\mu)$  beyond Proposition 13, we consider the ambiguous polytope  $\mathcal{A}_{(n'-1),r}^{(n'-1) \rightarrow n'}$  with ambiguous guessing facets  $\mathbf{G}_{\eta}^{n',r}$  that are tight signaling dimension witnesses of  $\mathcal{C}_r^{n \rightarrow n'}$  (see Appendix D3). Our goal is to find the smallest integer  $r$  such that  $\mathbf{P}_{\mathcal{E}_\mu} \in \mathcal{A}_{(n'-1),r}^{(n'-1) \rightarrow n'}$ , that is,  $\langle \mathbf{G}_{\eta}^{n',r}, \mathbf{P}_{\mathcal{E}_\mu} \rangle \leq r(n' - r)$  is satisfied. Consider the erasure channel  $\mathbf{P}_{\mathcal{E}_\mu} \in \mathcal{P}^{d \rightarrow (d+1)}$  described by Eq. (H14). We find that the inequality

$$r(n' - r) \geq \langle \mathbf{G}_{\eta}^{n',r}, \mathbf{P}_{\mathcal{E}_\mu} \rangle = (n' - r)\mu d + (1 - \mu)(n' - 1) \quad (\text{H15})$$

is violated if  $\mathbf{P}_{\mathcal{E}_\mu} \notin \mathcal{A}_{(n'-1),r}^{(n'-1) \rightarrow n'}$  for  $n' - 2 \geq r \geq 2$ . Note that in our example  $n' = d + 1$ ; however, this procedure holds for any  $n' > d$ . Rearranging inequality Eq. (H15) into the form

$$0 \geq r^2 - r(\mu d + n') + \mu d n' + (1 - \mu)(n' - 1) \quad (\text{H16})$$

allows us to find the values of  $r$  for which inequality Eq. (H15) is satisfied by solving for the zeros  $r_{\pm}$  of the quadratic on the RHS of Eq. (H16),

$$r_{\pm} = \frac{1}{2}(\mu d + n') \pm \frac{1}{2}\sqrt{(n' - \mu d)^2 - 4(1 - \mu)(n' - 1)}. \quad (\text{H17})$$

Since the parabola of Eq. (H16) is concave up, all integer values of  $r \in [r_-, r_+]$  satisfy inequality Eq. (H15). Furthermore, the smallest integer for which the inequality is satisfied is  $r = \lceil r_- \rceil$ . Therefore, the signaling dimension is bounded as

$$\begin{aligned} \kappa(\mathcal{E}_\mu) \geq r &= \left\lceil \frac{1}{2}(\mu d + n') \right. \\ &\quad \left. - \frac{1}{2}\sqrt{(n' - \mu d)^2 - 4(1 - \mu)(n' - 1)} \right\rceil. \end{aligned} \quad (\text{H18})$$

The value of  $r$  in Eq. (H18) satisfies the facet inequality Eq. (H15) for all allowed values of  $n'$ ,  $\mu$ , and  $d$ . Note that  $n'$  is a free parameter which we can choose as any integer  $n' \geq d + 1$ . In our example,  $\mathbf{P}_{\mathcal{E}_\mu}$  has  $n' = (d + 1)$  which obtains the lower bound  $\kappa(\mathcal{E}_\mu) \geq \lceil \mu d + 1 \rceil$ . To see this, we substitute  $n' = (d + 1)$  into Eq. (H18) and perform some algebra,

$$r = \left\lceil \frac{1}{2}(\mu d + d + 1) - \frac{1}{2}\sqrt{(d(1 - \mu) + 1)^2 - 4d(1 - \mu)} \right\rceil$$

$$= \left\lceil \frac{1}{2}(\mu d + d + 1) - \frac{1}{2}\sqrt{(d(1 - \mu) - 1)^2} \right\rceil \quad (\text{H19})$$

$$= \left\lceil \frac{1}{2}(\mu d + d + 1) - \frac{1}{2}(d(1 - \mu) - 1) \right\rceil \quad (\text{H20})$$

$$= \left\lceil \frac{1}{2}(\mu d + 1) + \frac{1}{2}(\mu d + 1) \right\rceil \quad (\text{H21})$$

$$= \lceil \mu d + 1 \rceil. \quad (\text{H22})$$

Hence,  $\kappa(\mathcal{E}_\mu) \geq r = \lceil \mu d + 1 \rceil$ . Additionally, substituting  $n' > d + 1$  into Eq. (H18) results in a necessarily smaller value or  $r$  therefore  $n' = d + 1$  is a maximum.

It is important to note that the lower bound  $\kappa(\mathcal{E}_\mu) \geq \lceil \mu d + 1 \rceil$  only holds for  $r \leq n' - 2$  because  $\mathbf{G}_{\eta}^{n',r}$  is not a facet

for signaling polytopes  $\mathcal{C}_r^{(n'-1) \rightarrow n'}$  with  $r > n' - 2$ . Therefore, we must consider the edge case where  $r = n' - 1 = n$ , that is, the case where the trivial upper bound of Eq. (3) is obtained. From Theorem 1 Condition (ii) we know that  $\mathcal{C}_{n-1}^{n \rightarrow n'} = \cap k = n' \mathcal{A}_{k, n-1}^{n \rightarrow n'}$ . It follows for the edge case  $r = n' - 1 = n$  that if a channel  $\mathbf{P}_{\mathcal{E}_\mu} \notin \mathcal{A}_{(n'-1), r}^{(n'-1) \rightarrow n'}$ , then  $\kappa^{n \rightarrow n'}(\mathcal{E}_\mu) = \min\{n, n'\} = (n' - 1)$ . Hence,  $\kappa(\mathcal{E}_\mu)$  is proven to be tight with the upper bound. To illustrate this case we consider inequality Eq. (H16) and substitute  $r = n' - 2$ ,

$$0 \geq (n'^2 - 4n' + 4) - (n' - 2)(\mu d + n') + \mu d n' + (1 - \mu)(n' - 1) \quad (\text{H23})$$

$$\geq -4n' + 4 + 2\mu d + 2n' + (1 - \mu)n' - (1 - \mu). \quad (\text{H24})$$

Next, we substitute  $d = n' - 1$  into Eq. (H24) as this is the edge case we wish to consider,

$$0 \geq -4n' + 4 + 2\mu(n' - 1) + 2n' + (1 - \mu)n' - (1 - \mu) \quad (\text{H25})$$

$$\geq n'(\mu - 1) + 3 - \mu \quad (\text{H26})$$

$$\geq 3 - n' + \mu(n' - 1). \quad (\text{H27})$$

Rearranging inequality Eq. (H27), we find that it is satisfied iff,  $\frac{n'-3}{n'-1} \geq \mu$ . Therefore, when  $\mu > \frac{n'-3}{n'-1}$ , inequality Eq. (H15) is violated, and by Theorem 1(ii) we certify that  $\kappa(\mathcal{E}_\mu) = d$ . Considering this edge case, we arrive at the conclusion that  $\kappa(\mathcal{E}_\mu) \geq \min\{d, \lceil \mu d + 1 \rceil\}$ , which is exactly the upper bound  $\min\{d, \lceil \mu d + 1 \rceil\} \geq \kappa(\mathcal{E}_\mu)$ . That is, the signaling dimension of the erasure channel is bounded tightly from above and below from which it follows,  $\kappa(\mathcal{E}_\mu) = \min\{d, \lceil \mu d + 1 \rceil\}$ . ■

- 
- [1] S. Wehner, D. Elkouss, and R. Hanson, Quantum internet: A vision for the road ahead, *Science* **362**, eaam9288 (2018).
  - [2] H. Buhrman, R. Cleve, S. Massar, and R. de Wolf, Nonlocality and communication complexity, *Rev. Mod. Phys.* **82**, 665 (2010).
  - [3] J. I. de Vicente, Shared randomness and device-independent dimension witnessing, *Phys. Rev. A* **95**, 012340 (2017).
  - [4] A. Ambainis, D. Leung, L. Mancinska, and M. Ozols, Quantum random access codes with shared randomness, [arXiv:0810.2937](https://arxiv.org/abs/0810.2937).
  - [5] A. Tavakoli, A. Hameedi, B. Marques, and M. Bourennane, Quantum Random Access Codes Using Single  $d$ -Level Systems, *Phys. Rev. Lett.* **114**, 170502 (2015).
  - [6] H.-W. Li, Z.-Q. Yin, Y.-C. Wu, X.-B. Zou, S. Wang, W. Chen, G.-C. Guo, and Z.-F. Han, Semi-device-independent random-number expansion without entanglement, *Phys. Rev. A* **84**, 034301 (2011).
  - [7] A. Tavakoli, J. Kaniewski, T. Vértesi, D. Rosset, and N. Brunner, Self-testing quantum states and measurements in the prepare-and-measure scenario, *Phys. Rev. A* **98**, 062307 (2018).
  - [8] M. Pawłowski and N. Brunner, Semi-device-independent security of one-way quantum key distribution, *Phys. Rev. A* **84**, 010302(R) (2011).
  - [9] N. Brunner, S. Pironio, A. Acín, N. Gisin, A. A. Méthot, and V. Scarani, Testing the Dimension of Hilbert Spaces, *Phys. Rev. Lett.* **100**, 210503 (2008).
  - [10] M. Hendrych, R. Gallego, M. Mičuda, N. Brunner, A. Acín, and J. P. Torres, Experimental estimation of the dimension of classical and quantum systems, *Nat. Phys.* **8**, 588 (2012).
  - [11] A. S. Holevo, Bounds for the quantity of information transmitted by a quantum communication channel, *Prob. Peredachi Info.* **9**, 3 (1973).
  - [12] J. Körner and A. Orlitsky, Zero-error information theory, *IEEE Trans. Info. Theory* **44**, 2207 (1998).
  - [13] R. Duan, Super-activation of zero-error capacity of noisy quantum channels, [arXiv:0906.2527](https://arxiv.org/abs/0906.2527).
  - [14] T. S. Cubitt, J. Chen, and A. W. Harrow, Superactivation of the asymptotic zero-error classical capacity of a quantum channel, *IEEE Trans. Info. Theory* **57**, 8114 (2011).
  - [15] T. S. Cubitt, D. Leung, W. Matthews, and A. Winter, Zero-error channel capacity and simulation assisted by non-local correlations, *IEEE Trans. Info. Theory* **57**, 5509 (2011).
  - [16] R. Duan and A. Winter, No-Signalling-Assisted Zero-Error Capacity of Quantum Channels and an Information Theoretic Interpretation of the Lovász Number, *IEEE Trans. Info. Theory* **62**, 891 (2016).
  - [17] I. Devetak and A. Winter, Distilling common randomness from bipartite quantum states, *IEEE Trans. Info. Theory* **50**, 3183 (2004).
  - [18] I. Devetak, A. W. Harrow, and A. J. Winter, A Resource Framework for Quantum Shannon Theory, *IEEE Trans. Info. Theory* **54**, 4587 (2008).
  - [19] C. H. Bennett, P. W. Shor, J. A. Smolin, and A. V. Thapliyal, Entanglement-assisted capacity of a quantum channel and the reverse Shannon theorem, *IEEE Trans. Info. Theory* **48**, 2637 (2002).
  - [20] X. Wang and M. M. Wilde, Cost of Quantum Entanglement Simplified, *Phys. Rev. Lett.* **125**, 040502 (2020).
  - [21] K. Fang, X. Wang, M. Tomamichel, and M. Berta, Quantum Channel simulation and the channel's smooth max-information, *IEEE Trans. Info. Theory* **66**, 2129 (2020).
  - [22] M. Dall'Arno, S. Brandsen, A. Tosini, F. Buscemi, and V. Vedral, No-Hypersignaling Principle, *Phys. Rev. Lett.* **119**, 020401 (2017).
  - [23] P. E. Frenkel and M. Weiner, Classical information storage in an  $n$ -level quantum system, *Commun. Math. Phys.* **340**, 563 (2015).
  - [24] R. Gallego, N. Brunner, C. Hadley, and A. Acín, Device-Independent Tests of Classical and Quantum Dimensions, *Phys. Rev. Lett.* **105**, 230501 (2010).
  - [25] M. Dall'Arno, E. Passaro, R. Gallego, and A. Acín, Robustness of device-independent dimension witnesses, *Phys. Rev. A* **86**, 042312 (2012).
  - [26] J. Ahrens, P. Badziąg, A. Cabello, and M. Bourennane, Experimental device-independent tests of classical and quantum dimensions, *Nat. Phys.* **8**, 592 (2012).
  - [27] N. Brunner, M. Navascués, and T. Vértesi, Dimension Witnesses and Quantum State Discrimination, *Phys. Rev. Lett.* **110**, 150501 (2013).



- [28] M. Dall’Arno, S. Brandsen, F. Buscemi, and V. Vedral, Device-Independent Tests of Quantum Measurements, *Phys. Rev. Lett.* **118**, 250501 (2017).
- [29] M. Dall’Arno, S. Brandsen, and F. Buscemi, Device-independent tests of quantum channels, *Proc. Roy. Soc. A: Math. Phys. Eng. Sci.* **473**, 20160721 (2017).
- [30] T. Christof and G. Reinelt, Decomposition and parallelization techniques for enumerating the facets of combinatorial polytopes, *Int. J. Comput. Geom. Appl.* **11**, 423 (2001).
- [31] T. Heinosaari and O. Kerppo, Communication of partial ignorance with qubits, *J. Phys. A: Math. Theor.* **52**, 395301 (2019).
- [32] B. Doolittle, SignalingDimension.jl, <https://github.com/ChitambarLab/SignalingDimension.jl>.
- [33] G. Ziegler, *Lectures on Polytopes*, Graduate Texts in Mathematics (Springer, New York, 2012).
- [34] T. Heinosaari, O. Kerppo, and L. Leppäjärvi, Communication tasks in operational theories, *J. Phys. A: Math. Theor.* **53**, 435302 (2020).
- [35] A. Barvinok, *A Course in Convexity* (American Mathematical Society, Providence, RI, 2002).
- [36] E. Davies, Information and quantum measurement, *IEEE Trans. Info. Theory* **24**, 596 (1978).
- [37] S. Pironio, Lifting Bell inequalities, *J. Math. Phys.* **46**, 062112 (2005).
- [38] D. Rosset, J.-D. Bancal, and N. Gisin, Classifying 50 years of Bell inequalities, *J. Phys. A: Math. Theor.* **47**, 424022 (2014).
- [39] T. Christof and A. Löbel, Porta, <http://porta.zib.de/>.
- [40] B. Doolittle and B. Legat, XPORTA.jl, <https://github.com/JuliaPolyhedra/XPORTA.jl>.
- [41] E. Chitambar, I. George, B. Doolittle, and M. Junge, The communication value of a quantum channel, [arXiv:2109.11144](https://arxiv.org/abs/2109.11144) (2021).
- [42] J. Bezanson, A. Edelman, S. Karpinski, and V. B. Shah, Julia: A fresh approach to numerical computing, *SIAM Rev.* **59**, 65 (2017).