






Mutually unbiased balanced functions and generalized random access codesVaisakh M , Ram krishna Patra , Mukta Janpandit , Samrat Sen , and Manik Banik **School of Physics, IISER Thiruvananthapuram, Vithura, Kerala 695551, India*Anubhav Chaturvedi[†]*Institute of Theoretical Physics and Astrophysics, National Quantum Information Centre, Faculty of Mathematics, Physics and Informatics, University of Gdansk, 80-952 Gdansk, Poland**and International Centre for Theory of Quantum Technologies, University of Gdansk, 80-308, Gdansk, Poland*

(Received 13 May 2021; accepted 7 July 2021; published 21 July 2021)

Quantum resources and protocols are known to outperform their classical counterparts in a variety of communication and information processing tasks. Random access codes (RACs) are one such cryptographically significant family of bipartite communication tasks, wherein the sender encodes a data set (typically a string of input bits) onto a physical system of bounded dimension and transmits it to the receiver, who then attempts to guess a randomly chosen part of the sender's data set (typically one of the sender's input bits). In this work, we introduce a generalization of this task wherein the receiver, in addition to the individual input bits, aims to retrieve randomly chosen functions of the sender's input string. Specifically, we employ sets of *mutually unbiased balanced functions*, such that perfect knowledge of any one of the constituent functions yields no knowledge about the others. We investigate and bound the performance of (i) classical, (ii) quantum prepare and measure, and (iii) entanglement assisted classical communication (EACC) protocols for the resultant generalized RACs (GRACs). Finally, we detail the case of GRACs with three input bits and find maximal success probabilities for classical, quantum, and EACC protocols, along with the effect of noisy quantum channels on the performance of quantum protocols. Moreover, with the help of this case study, we reveal several characteristic properties of the GRACs which deviate from the standard RACs.

DOI: [10.1103/PhysRevA.104.012420](https://doi.org/10.1103/PhysRevA.104.012420)**I. INTRODUCTION**

Quantum information theory entails the study of quantum resources and protocols, which are known to enable a plethora of communication and information processing tasks, which otherwise remain unattainable by their classical counterparts governed by Shannon's information theory [1]. For instance, in quantum superdense coding, a sender (say Alice) can transfer two classical bits of information to a distant receiver (say Bob) by transmitting a single two-level quantum system, with the aid of preshared entanglement [2]. Similarly, the counterintuitive feature of quantum entanglement is known to empower several seemingly impossible tasks. However, in the absence of entanglement, the utility of quantum systems in communication tasks is constrained by certain fundamental no-go results. For instance, the Holevo theorem [3] constrains the informational utility of individual quantum systems. Specifically, no more than n classical bits of information can be reliably transmitted using n quantum bits. Recently, a more stringent constraint on quantum communication was established by Frenkel and Weiner; namely, it has been established that the classical information storage capacity of

a d -level quantum system is the same as that of a classical d -state system [4].

These no-go results seem to point towards the conclusion that quantum resources and protocols might not be better than their classical counterparts for transmitting classical information in the absence of entanglement. However, in actuality, even without entanglement, finite-dimensional quantum systems can outperform their classical counterparts in a large variety of stochastic communication tasks. ($n \rightarrow 1$) random access codes (RACs) constitute such a class of communication tasks wherein the sender is tasked with encoding a string of n bits onto a single bit of message, such that the receiver can decode any one of the randomly chosen initial bits with a certain probability of success. It is known that if the message is encoded onto a qubit,¹ the parties can attain higher success probability than any classical strategy entailing a bit of communication [6,7]. RACs utilizing quantum resources (often referred to as QRACs) have a plethora of applications, for instance, in connection with quantum communication complexity (see [8] and references therein), network coding, and locally decodable codes [9–14]. Moreover, RACs have found several foundational implications [15–22], in particular, preshared entanglement assisted random access codes (EARACs)

*manik11ju@gmail.com

†anubhav.chaturvedi@research.iit.ac.in

¹This problem was first studied by Wiesner under the name *conjugate coding* [5].

are closely related to nonlocal games [23,24] and form the basis for the principle of information causality [25,26].

Finally, RACs form a cryptographic primitive and consequently form the basis of quantum key distribution (QKD) schemes [27–29]. One of the features of $(n \rightarrow 1)$ RACs, which makes them a suitable cryptographic primitive, is that in each round the receiver intends to retrieve a single bit of the sender's n bit data and, as these bits are independently distributed, such exclusive decoding reveals no nontrivial information about the other bits. In this work, we propose a generalization of the RAC task, referred to as GRACs, which expands on this property. To this end, we introduce sets of $n \mapsto 1$ bit functions that are *mutually unbiased* (called MUBS) such that perfect knowledge of any one of the constituent functions in a MUBS yields no information about the others. For each such MUBS, the communication task wherein, in each round, the receiver intends to decode a constituent function forms a GRAC.

The manuscript is organized in the following manner: in Sec. II we formally introduce the concept of mutually unbiased balanced functions and their sets; in Sec. III we provide the definition of generalized RAC (GRAC) task, describe (i) classical, (ii) quantum prepare and measure, and (iii) entanglement assisted classical communication (EACC) protocols for GRACs, and derive general bounds on the success probabilities of these protocols. In Sec. IV we provide a detailed study of the case when the sender receives three independently distributed bits as input. Here, we find that majority-encoding-identity-decoding may not be one of the optimal classical strategies for GRAC, which is always the case for RACs. We also report an interesting feature of classical GRACs, namely, the maximal average classical success probability of a GRAC gets increased with the addition of new function(s) to the already existing ones; a phenomenon referred to as “the harder the goal, the greater the payoff.” In the same section, we also analyze the performance quantum prepare and measure protocols, the effect of noisy channels on their performance, and the performance of EACC protocols. In Sec. V we present a brief discussion along with some relevant open questions for further research.

II. MUTUALLY UNBIASED BALANCED FUNCTIONS

This section specifies the definitions of balanced and mutually unbiased balanced functions and sets of mutually unbiased balanced functions, providing key examples along with some notational preliminaries for subsequent use throughout the rest of the manuscript.

Definition 1 (Balanced functions). A Boolean function $f : \{0, 1\}^n \rightarrow \{0, 1\}$ is balanced if its outputs yield as many 0's as 1's over its input set.

In this work, we consider $n \mapsto 1$ bit Boolean functions which take as input an n bit string $\mathbf{x} \equiv \{x_1, x_2, \dots, x_n\} \in \{0, 1\}^n$ to produce a bit of output, i.e., $f : \{0, 1\}^n \rightarrow \{0, 1\}$. Consequently, for such functions to be balanced, the cardinality of the set of inputs mapped to 0, $\mathcal{X}_{f(\mathbf{x})=0} \equiv \{\mathbf{x} \in \{0, 1\}^n \mid f(\mathbf{x}) = 0\}$, must be the same as the cardinality of the set of inputs mapped to 1, $\mathcal{X}_{f(\mathbf{x})=1} \equiv \{\mathbf{x} \in \{0, 1\}^n \mid f(\mathbf{x}) = 1\}$, i.e., $|\mathcal{X}_{f(\mathbf{x})=0}| = |\mathcal{X}_{f(\mathbf{x})=1}| = 2^{n-1}$. Furthermore, this implies that, for such balanced functions, and a uniformly distributed string

of inputs, the probability of obtaining a 0 is the same as the probability of obtaining a 1, i.e., $\forall \mathbf{x} \in \{0, 1\}^n : p(\mathbf{x}) = \frac{1}{2^n}$, $p[f(\mathbf{x}) = 0] = p[f(\mathbf{x}) = 1] = \frac{1}{2}$. Next, we introduce the notion of *mutual unbiasedness* for balanced functions.

Definition 2 (MUBF). A pair of balanced Boolean functions f_1, f_2 is called mutually unbiased if exactly half of the inputs yielding an output for one function yields the same output for the other function.

In particular, for a pair of MUBFs $f_1, f_2 : \{0, 1\}^n \rightarrow \{0, 1\}$, the sets $\mathcal{X}_{f_1(\mathbf{x})=0}, \mathcal{X}_{f_1(\mathbf{x})=1}$ have equal overlaps with the sets $\mathcal{X}_{f_2(\mathbf{x})=0}, \mathcal{X}_{f_2(\mathbf{x})=1}$, i.e., $\forall i, j \in \{0, 1\} : |\mathcal{X}_{f_1(\mathbf{x})=i} \cap \mathcal{X}_{f_2(\mathbf{x})=j}| = 2^{n-2}$. This further implies for a uniformly distributed string of inputs $\forall i, j, k, l \in \{0, 1\} : p[f_2(\mathbf{x}) = i \mid f_1(\mathbf{x}) = j] = p[f_1(\mathbf{x}) = k \mid f_2(\mathbf{x}) = l] = \frac{1}{2}$. Next, we define sets of mutually unbiased balanced functions.

Definition 3 (MUBS). A set of functions $\mathcal{F} \equiv \{f_i\}_{i=1}^{|\mathcal{F}|}$ forms a mutually unbiased balanced set if all of the constituent functions are balanced and pairwise mutually unbiased.

For a n -bit string input, consider the set of $2^n - 1$ functions $\mathcal{F}_{\mathcal{R}}^n \equiv \{f_{\mathbf{r}}(\mathbf{x}) = \bigoplus_{i=1}^n r_i x_i \mid \mathbf{r} \equiv \{r_1, \dots, r_n\} \in \mathcal{R}\}$, where $\mathcal{R} \equiv \{\mathbf{r} \in \{0, 1\}^n \mid \sum_i r_i \geq 1\}$. Notice that all functions in the set are balanced, i.e., $\forall f \in \mathcal{F}_{\mathcal{R}}^n : |\mathcal{X}_{f(\mathbf{x})=0}| = |\mathcal{X}_{f(\mathbf{x})=1}| = 2^{n-1}$. Now any two distinct functions $f_i, f_j \in \mathcal{F}_{\mathcal{R}}^n$ differ by XOR of at least one completely independent bit, and XOR with a random bit obscures all information (one-time pad) about the original bit; all functions in such a set are pairwise mutually unbiased, deeming the set to be MUBS. For instance, for the simplest case of two bit input functions the set $\mathcal{F}_{\mathcal{R}}^2 = \{x_1, x_2, x_1 \oplus x_2\}$ forms a MUBS. Similarly, for the case of three bit input functions the set $\mathcal{F}_{\mathcal{R}}^3 = \{x_1, x_2, x_3, x_1 \oplus x_2, x_2 \oplus x_3, x_1 \oplus x_3, x_1 \oplus x_2 \oplus x_3\}$ forms a MUBS. In general, it is easy to see that any nontrivial subset of $\mathcal{F}_{\mathcal{R}}^n$ forms a MUBS, i.e., the sets $\mathcal{F}_{\mathcal{R}_j}^n \equiv \{f_{\mathbf{r}}(\mathbf{x}) = \bigoplus_{i=1}^n r_i x_i \mid \mathbf{r} \equiv \{r_1, \dots, r_n\} \in \mathcal{R}_j\}$, where $\mathcal{R}_j \subseteq \mathcal{R}$.

III. GENERALIZED RANDOM ACCESS CODES

In this section, we start by introducing generalized random access codes which utilize mutually unbiased balanced functions defined above.

Definition 4 ((n, \mathcal{R}_i) -GRAC). An (n, \mathcal{R}_i) generalized random access code (GRAC) is a bipartite one-way communication task, wherein in each round the sender (Alice) receives a uniformly distributed input n -bit string $\mathbf{x} \in \{0, 1\}^n$ which they encode onto a message, which is transmitted to the receiver (Bob). Bob, upon receiving the transmission from Alice, decodes the message based on her uniformly distributed input $\mathbf{y} \in \mathcal{R}_i$, where $\mathcal{R}_i \subseteq \mathcal{R} \equiv \{\mathbf{r} \in \{0, 1\}^n \mid \sum_i r_i \geq 1\}$ and produces an output bit $z \in \{0, 1\}$. They win a round if $z = f_{\mathbf{y}}(\mathbf{x}) = \bigoplus_{i=1}^n x_i y_i$. They gauge their performance on the basis of their average success probability $s^{(n, \mathcal{R}_i)} = \frac{1}{2^n |\mathcal{R}_i|} \sum_{\mathbf{x}, \mathbf{y}} p(z = f_{\mathbf{y}}(\mathbf{x}) \mid \mathbf{x}, \mathbf{y})$.

We note here that the standard $(n \rightarrow 1)$ random access codes (RACs) form restricted cases of GRACs, specifically when Bob's input \mathbf{y} is uniformly sampled from $\mathcal{R}_{\text{RAC}} \equiv \{\mathbf{r} \in \{0, 1\}^n \mid \sum_i r_i = 1\}$. We denote the success probability of $(n \rightarrow 1)$ RACs by $s^{(n \rightarrow 1)}$.

In this work, we study three distinct classes of communication protocols for (n, \mathcal{R}_i) GRAC.

(i) A classical communication protocol \mathcal{C} for (n, \mathcal{R}_i) GRAC is one wherein Alice encodes their input string \mathbf{x} onto a bit $\omega \in \{0, 1\}$, based on an encoding scheme \mathcal{E} entailing conditional probability distributions of the form $\{p_{\mathcal{E}}(\omega|\mathbf{x})\}$. Bob decodes the message based on their input to produce the output z employing a decoding scheme \mathcal{D} entailing conditional probability distributions of the form $\{p_{\mathcal{D}}(z|\omega, \mathbf{y})\}$. The average success probability for such a protocol is $s_{\mathcal{C}}^{(n, \mathcal{R}_i)} = \frac{1}{2^n |\mathcal{R}_i|} \sum_{\mathbf{x}, \mathbf{y}, \omega} p_{\mathcal{E}}(\omega|\mathbf{x}) p_{\mathcal{D}}[z = f_{\mathbf{y}}(\mathbf{x})|\omega, \mathbf{y}]$. The maximal classical success probability of (n, \mathcal{R}_i) GRAC, $S_{\mathcal{C}}^{(n, \mathcal{R}_i)}$, has the expression

$$S_{\mathcal{C}}^{(n, \mathcal{R}_i)} = \max_{\mathcal{E}, \mathcal{D}} \left\{ \frac{1}{2^n |\mathcal{R}_i|} \sum_{\mathbf{x}, \mathbf{y}, \omega} p_{\mathcal{E}}(\omega|\mathbf{x}) p_{\mathcal{D}}[z = f_{\mathbf{y}}(\mathbf{x})|\omega, \mathbf{y}] \right\}. \quad (1)$$

We note here that, as we are considering average success probability, the parties gain no advantage even if they have access to an arbitrary amount of shared randomness [30]. Moreover, it is straightforward to see that, for average success probability, it is enough to consider only deterministic encoding and decoding schemes. Consequently, the optimal classical protocols for (n, \mathcal{R}_i) GRAC, without loss of generality, comprise a deterministic encoding scheme such that $\omega = f_{\mathcal{E}}(\mathbf{x})$ and a deterministic decoding scheme such that $z = f_{\mathcal{D}}(\mathbf{y}, \omega)$.

(ii) A quantum prepare and measure protocol \mathcal{Q} for (n, \mathcal{R}_i) GRAC entails Alice encoding her input onto a qubit $\rho_{\mathbf{x}}$, which is transmitted to Bob. Bob, upon receiving the qubit, performs the measurement $\{M_z^{\mathbf{y}}|\forall \mathbf{y} : \sum_z M_z^{\mathbf{y}} = \mathbb{I}\}$ based on his input \mathbf{y} to produce the outcome z . The average success probability for such a protocol has the expression $s_{\mathcal{Q}}^{(n, \mathcal{R}_i)} = \frac{1}{2^n |\mathcal{R}_i|} \sum_{\mathbf{x}, \mathbf{y}} \text{Tr}(\rho_{\mathbf{x}} M_{z=f_{\mathbf{y}}(\mathbf{x})}^{\mathbf{y}})$. The maximal quantum success probability of (n, \mathcal{R}_i) GRAC $S_{\mathcal{Q}}^{(n, \mathcal{R}_i)}$ has the expression

$$S_{\mathcal{Q}}^{(n, \mathcal{R}_i)} = \max_{\{\rho_{\mathbf{x}}\}, \{M_z^{\mathbf{y}}\}} \left\{ \frac{1}{2^n |\mathcal{R}_i|} \sum_{\mathbf{x}, \mathbf{y}} \text{Tr}(\rho_{\mathbf{x}} M_{z=f_{\mathbf{y}}(\mathbf{x})}^{\mathbf{y}}) \right\}, \quad (2)$$

where the maximization is over all two-dimensional states $\{\rho_{\mathbf{x}}\}$ and two-dimensional binary outcome measurements $\{M_z^{\mathbf{y}}\}$. For maximal average success probability it is enough to consider pure states, i.e., $\forall \mathbf{x} : \rho_{\mathbf{x}} \equiv |\psi_{\mathbf{x}}\rangle\langle\psi_{\mathbf{x}}|$, and the measurement operators to be projectors, i.e., $\{M_z^{\mathbf{y}} \equiv \Pi_z^{\mathbf{y}}|\forall \mathbf{y} : \sum_z \Pi_z^{\mathbf{y}} = \mathbb{I}\}$. This allows us to reexpress (2) as

$$S_{\mathcal{Q}}^{(n, \mathcal{R}_i)} = \max_{\{\mathbf{r}_{\mathbf{x}}\}, \{\mathbf{v}_{\mathbf{y}}\}} \left\{ \frac{1}{2^n |\mathcal{R}_i|} \sum_{\mathbf{x}, \mathbf{y}} \frac{1}{2} (1 + (-1)^{f_{\mathbf{y}}(\mathbf{x})} \mathbf{r}_{\mathbf{x}} \cdot \mathbf{v}_{\mathbf{y}}) \right\}, \quad (3)$$

where we have used Bloch vector notation for states $\rho_{\mathbf{x}} = \frac{\mathbb{I} + \mathbf{r}_{\mathbf{x}} \cdot \boldsymbol{\sigma}}{2}$ and for measurements $M_z^{\mathbf{y}} = \frac{\mathbb{I} + (-1)^z \mathbf{v}_{\mathbf{y}} \cdot \boldsymbol{\sigma}}{2}$, where $\mathbf{r}_{\mathbf{x}} \in \mathbb{R}_3$, $\mathbf{v}_{\mathbf{y}} \in \mathbb{R}_3$ are unit vectors, such that $\forall \mathbf{x} : \|\mathbf{r}_{\mathbf{x}}\| = 1$, $\forall \mathbf{y} : \|\mathbf{v}_{\mathbf{y}}\| = 1$, and $\boldsymbol{\sigma}$ is the vector of Pauli matrices.

(iii) An entanglement assisted classical communication protocol (EACC) entails Alice and Bob presharing an entangled quantum state ρ_{AB} of arbitrary local dimension. Alice based on her input measures her part of the entangled state employing the binary outcome measurement $\{M_{\omega}^{\mathbf{x}}|\forall \mathbf{x} : \sum_{\omega} M_{\omega}^{\mathbf{x}} = \mathbb{I}\}$ and transmits the outcome ω to Bob. Bob upon receiving the message ω and his input \mathbf{y} performs the binary outcome measurements $\{M_z^{\omega, \mathbf{y}}|\forall \mathbf{y}, \omega : \sum_z M_z^{\omega, \mathbf{y}} =$

$\mathbb{I}\}$ to produce the outcome z . The average success probability for such a protocol has the expression $s_{EACC} = \frac{1}{2^n |\mathcal{R}_i|} \sum_{\mathbf{x}, \mathbf{y}, \omega} \text{Tr}(\rho_{AB} M_{\omega}^{\mathbf{x}} \otimes M_{z=f_{\mathbf{y}}(\mathbf{x})}^{\omega, \mathbf{y}})$. The maximal success probability of EACC protocols in (n, \mathcal{R}_i) GRAC, S_{EACC} , has the expression

$$S_{EACC} = \max_{\rho_{AB}, \{M_{\omega}^{\mathbf{x}}\}, \{M_z^{\omega, \mathbf{y}}\}} \left\{ \frac{1}{2^n |\mathcal{R}_i|} \sum_{\mathbf{x}, \mathbf{y}, \omega} \text{Tr}(\rho_{AB} M_{\omega}^{\mathbf{x}} \otimes M_{z=f_{\mathbf{y}}(\mathbf{x})}^{\omega, \mathbf{y}}) \right\}. \quad (4)$$

Bounding success of GRACs

Now we are prepared to present our results for bounding the average success probability of (n, \mathcal{R}_i) GRACs.

Theorem 1. The maximal success probability of (n, \mathcal{R}_i) GRACs, $S_{\mathcal{O}}^{(n, \mathcal{R}_i)}$, is lower bounded by that of $(|\mathcal{R}_i| \rightarrow 1)$ RAC, $S_{\mathcal{O}}^{(|\mathcal{R}_i| \rightarrow 1)}$, i.e.,

$$S_{\mathcal{O}}^{(n, \mathcal{R}_i)} \geq S_{\mathcal{O}}^{(|\mathcal{R}_i| \rightarrow 1)}, \quad (5)$$

where $\mathcal{O} \in \{\mathcal{C}, \mathcal{Q}, EACC\}$.

Proof. To prove the desired thesis we provide a viable strategy for (n, \mathcal{R}_i) GRAC which utilizes an optimal $(|\mathcal{R}_i| \rightarrow 1)$ RAC as a subroutine and achieves success $s_{\mathcal{O}}^{(n, \mathcal{R}_i)} \geq S_{\mathcal{O}}^{(|\mathcal{R}_i| \rightarrow 1)}$.

Given a (n, \mathcal{R}_i) GRAC with the input string $\mathbf{x} \equiv \{x_1, \dots, x_n\} \in \{0, 1\}^n$, consider the bit string $[f_{\mathbf{r}}(\mathbf{x})]_{\mathbf{r} \in \mathcal{R}_i}$. Notice that $[f_{\mathbf{r}}(\mathbf{x})]_{\mathbf{r} \in \mathcal{R}_i}$ may not be uniformly distributed. Now, consider a $(|\mathcal{R}_i| \rightarrow 1)$ RAC with the input string $\tilde{\mathbf{x}} \equiv \{\tilde{x}_1, \dots, \tilde{x}_{|\mathcal{R}_i|}\} \in \{0, 1\}^{|\mathcal{R}_i|}$ with maximal success probability $S_{\mathcal{O}}^{(|\mathcal{R}_i|)} = \frac{1}{2^{|\mathcal{R}_i|} |\mathcal{R}_i|} \sum_{\mathbf{x}, \tilde{\mathbf{y}} \in \{1, \dots, |\mathcal{R}_i|\}} p(\tilde{z} = \tilde{x}_{\tilde{\mathbf{y}}}|\tilde{\mathbf{x}}, \tilde{\mathbf{y}})$, where $\mathcal{O} \in \{\mathcal{C}, \mathcal{Q}, EACC\}$ specifies the particular type of the protocol. We use the string $[f_{\mathbf{r}}(\mathbf{x})]_{\mathbf{r} \in \mathcal{R}_i}$ as the input string for the $(|\mathcal{R}_i| \rightarrow 1)$ RAC, up to optimal reordering, i.e., $\tilde{\mathbf{x}} = \text{Perm}\{[f_{\mathbf{r}}(\mathbf{x})]_{\mathbf{r} \in \mathcal{R}_i}\}$. It is easy to see that this protocol achieves success probability $s_{\mathcal{O}}^{(n, \mathcal{R}_i)} \geq S_{\mathcal{O}}^{(|\mathcal{R}_i| \rightarrow 1)}$, where the inequality is saturated when the optimal strategy of $(|\mathcal{R}_i| \rightarrow 1)$ RAC has equal success for all inputs, $\forall \tilde{\mathbf{x}} \in \{0, 1\}^{|\mathcal{R}_i|} : \frac{1}{2^{|\mathcal{R}_i|} |\mathcal{R}_i|} \sum_{\tilde{\mathbf{y}} \in \{1, \dots, |\mathcal{R}_i|\}} p(\tilde{z} = \tilde{x}_{\tilde{\mathbf{y}}}|\tilde{\mathbf{x}}, \tilde{\mathbf{y}}) = S_{\mathcal{O}}^{(|\mathcal{R}_i| \rightarrow 1)}$. ■

Theorem 2. The maximal success probability of a prepare and measure protocol in an (n, \mathcal{R}_i) GRAC, $S_{\mathcal{Q}}^{(n, \mathcal{R}_i)}$, is upper bounded as follows:

$$S_{\mathcal{Q}}^{(n, \mathcal{R}_i)} \leq \frac{1}{2} \left(1 + \frac{1}{\sqrt{|\mathcal{R}_i|}} \right). \quad (6)$$

Proof. We start by recalling that the maximal success probability of prepare and measure protocol for an (n, \mathcal{R}_i) GRAC has the expression (3)

$$S_{\mathcal{Q}}^{(n, \mathcal{R}_i)} = \max_{\{\mathbf{r}_{\mathbf{x}}\}, \{\mathbf{v}_{\mathbf{y}}\}} \left\{ \frac{1}{2^n |\mathcal{R}_i|} \sum_{\mathbf{x}, \mathbf{y}} \frac{1}{2} (1 + (-1)^{f_{\mathbf{y}}(\mathbf{x})} \mathbf{r}_{\mathbf{x}} \cdot \mathbf{v}_{\mathbf{y}}) \right\} = \frac{1}{2} \left(1 + \frac{1}{2^n |\mathcal{R}_i|} \max_{\{\mathbf{r}_{\mathbf{x}}\}, \{\mathbf{v}_{\mathbf{y}}\}} \left\{ \sum_{\mathbf{x}, \mathbf{y}} (-1)^{f_{\mathbf{y}}(\mathbf{x})} \mathbf{r}_{\mathbf{x}} \cdot \mathbf{v}_{\mathbf{y}} \right\} \right). \quad (7)$$

Consequently, finding maximal success probability of prepare and measure protocols in (n, \mathcal{R}_i) GRACs effectively boils down to solving the following optimization problem:

$$\begin{aligned} \Phi(n, |\mathcal{R}_i|) &= \max_{\{\mathbf{r}_x\}, \{\mathbf{v}_y\}} \left\{ \Phi_{n, |\mathcal{R}_i|}(\{\mathbf{r}_x\}, \{\mathbf{v}_y\}) \right\}, \\ &= \max_{\{\mathbf{v}_y\}} \left\{ \sum_{\mathbf{x}} \max_{\{\mathbf{r}_x\}} \left\{ \mathbf{r}_x \cdot \sum_y (-1)^{f_y(\mathbf{x})} \mathbf{v}_y \right\} \right\}. \end{aligned} \quad (8)$$

Defining $\mathbf{V}_x = \sum_y (-1)^{f_y(\mathbf{x})} \mathbf{v}_y$, we notice that the scalar product $\mathbf{r}_x \cdot \mathbf{V}_x$ is maximized when \mathbf{r}_x has the same direction as \mathbf{V}_x , i.e., when $\mathbf{r}_x = \mathbf{V}_x / \|\mathbf{V}_x\|$, which implies $\mathbf{r}_x \cdot \mathbf{V}_x = \|\mathbf{V}_x\|$. This observation allows us to reexpress (8) as

$$\Phi(n, |\mathcal{R}_i|) = \max_{\{\mathbf{v}_y\}} \left\{ \sum_{\mathbf{x}} \left\| \sum_y (-1)^{f_y(\mathbf{x})} \mathbf{v}_y \right\| \right\}. \quad (9)$$

We now further rewrite Eq. (9) as

$$\Phi(n, |\mathcal{R}_i|) = \max_{\{\mathbf{v}_y\}} \left\{ \underbrace{\sum_{\mathbf{x}} \left\| \sum_y g_y(\mathbf{x}) \mathbf{v}_y \right\|}_{\Phi_{n, |\mathcal{R}_i|}(\{\mathbf{v}_y\})} \right\}, \quad (10)$$

where $g_y(\mathbf{x}) = (-1)^{f_y(\mathbf{x})}$. Now, $\Phi_{n, |\mathcal{R}_i|}(\{\mathbf{v}_y\})$ can be thought of as the dot product between $\mathbf{z} = (1, 1, \dots, 1) \in \mathbb{R}^{2^n}$ and $\mathbf{w} = (\|\sum_y g_y(\mathbf{x}_1) \mathbf{v}_y\|, \dots, \|\sum_y g_y(\mathbf{x}_{2^n}) \mathbf{v}_y\|) \in \mathbb{R}^{2^n}$, where $\mathbf{x}_1 \equiv (x_0 = 0, \dots, x_n = 0), \dots, \mathbf{x}_{2^n} \equiv (x_0 = 1, \dots, x_n = 1)$. Now recall that Cauchy-Schwarz inequality implies

$$\Phi_{n, |\mathcal{R}_i|}(\{\mathbf{v}_y\}) = \mathbf{z} \cdot \mathbf{w} \leq \|\mathbf{z}\| \|\mathbf{w}\|. \quad (11)$$

Now observe that

$$\begin{aligned} \|\mathbf{w}\|^2 &= \sum_{\mathbf{x}} \left\| \sum_y g_y(\mathbf{x}) \mathbf{v}_y \right\|^2 \\ &= \sum_{\mathbf{x}} \left(\sum_y g_y(\mathbf{x}) \mathbf{v}_y \cdot \sum_{y'} g_{y'}(\mathbf{x}) \mathbf{v}_{y'} \right). \end{aligned} \quad (12)$$

There are two types of terms that appear in the sum in (12): (i) whenever $\mathbf{y} = \mathbf{y}'$, in this case $\forall \mathbf{y} \in \mathcal{R}_i : g_y(\mathbf{x}) \mathbf{v}_y \cdot g_{y'}(\mathbf{x}) \mathbf{v}_{y'} = \|\mathbf{v}_y\|^2$, and (ii) whenever $\mathbf{y} \neq \mathbf{y}'$, we have terms of the form $g_y(\mathbf{x}) g_{y'}(\mathbf{x}) \mathbf{v}_y \cdot \mathbf{v}_{y'}$. Now, as all functions in our MUBS are balanced and pairwise mutually unbiased, there exists 2^{n-1} strings $\mathbf{x} \in (\mathcal{X}_{f_y=0} \cap \mathcal{X}_{f_{y'}=0}) \cup (\mathcal{X}_{f_y=1} \cap \mathcal{X}_{f_{y'}=1})$ for which the coefficients $g_y(\mathbf{x}) g_{y'}(\mathbf{x}) = 1$, and there exists 2^{n-1} strings $\mathbf{x} \in (\mathcal{X}_{f_y=0} \cap \mathcal{X}_{f_{y'}=1}) \cup (\mathcal{X}_{f_y=1} \cap \mathcal{X}_{f_{y'}=0})$ for which the coefficients $g_y(\mathbf{x}) g_{y'}(\mathbf{x}) = -1$. Consequently, all terms of the form (ii) cancel out, and we are left with

$$\begin{aligned} \|\mathbf{w}\|^2 &= \sum_{\mathbf{x} \in \{0,1\}^n, \mathbf{y} \in \mathcal{R}_i} \|\mathbf{v}_y\|^2 = 2^n |\mathcal{R}_i| \\ \Rightarrow \|\mathbf{w}\| &= \sqrt{2^n |\mathcal{R}_i|}. \end{aligned} \quad (13)$$

Since $\|\mathbf{z}\| = \sqrt{2^n}$, we have $\Phi_{n, |\mathcal{R}_i|}(\{\mathbf{v}_y\}) \leq 2^n \sqrt{|\mathcal{R}_i|}$, which when plugged back in (10) and (7) yields the desired thesis,

$$S_{\mathcal{Q}}^{(n, \mathcal{R}_i)} \leq \frac{1}{2} \left(1 + \frac{2^n \sqrt{|\mathcal{R}_i|}}{2^n |\mathcal{R}_i|} \right) = \frac{1}{2} \left(1 + \frac{1}{\sqrt{|\mathcal{R}_i|}} \right). \quad (14)$$

Theorem 3. The maximal success probability of an EACC protocol in an (n, \mathcal{R}_i) GRAC, $S_{EACC}^{(n, \mathcal{R}_i)}$, is upper bounded by the maximum quantum value of the following Bell expression $B_{\mathcal{Q}}^{(n, \mathcal{R}_i)}$, i.e., $S_{EACC}^{(n, \mathcal{R}_i)} \leq B_{\mathcal{Q}}^{(n, \mathcal{R}_i)}$:

$$B_{\mathcal{Q}}^{(n, \mathcal{R}_i)} \equiv \frac{1}{2^n |\mathcal{R}_i|} \sum_{\mathbf{x}, \mathbf{y}, y_0 \in \{0,1\}} p[u = y_0, v = f_y(\mathbf{x}) | \mathbf{x}, y_0, \mathbf{y}], \quad (15)$$

where $\mathbf{x} \in \{0, 1\}^n$ is Alice's input, $(y_0 \in \{0, 1\}, \mathbf{y} \in |\mathcal{R}_i|)$ are Bob's input, and $u, v \in \{0, 1\}$ are outputs of Alice and Bob, respectively.

Proof. To prove the above thesis all we need to demonstrate is that, for an EACC (n, \mathcal{R}_i) GRAC achieving success probability $S_{EACC}^{(n, \mathcal{R}_i)} = \frac{1}{2^n |\mathcal{R}_i|} \sum_{\mathbf{x}, \mathbf{y}, \omega} \text{Tr}(\rho_{AB} M_{\omega}^{\mathbf{x}} \otimes M_{z=f_y(\mathbf{x})}^{\omega, \mathbf{y}})$, a quantum correlation can be obtained that achieves the same value for the Bell expression in (15), so that the maximum value of the Bell expression caps the success probability of the EACC protocol. To this end we recall that an EACC protocol for (n, \mathcal{R}_i) GRAC entails a preshared entangled state ρ_{AB} , local measurements for Alice $\{M_{\omega}^{\mathbf{x}}\}$, and local measurements for Bob $\{M_z^{\omega, \mathbf{y}}\}$, where Alice's output ω is transmitted to Bob. Now instead of transmitting the output of her measurement, Alice simply relabels it as her local output, i.e., $u = \omega$. On the other hand, Bob obtains an additional uniformly sampled input bit $y_0 \in \{0, 1\}$, utilizing it instead of the message from Alice to decide on the measurement $\{M_z^{\omega, \mathbf{y}}\}$ he performs on his part of the entangled state. Finally, Bob relabels his output as $v = z$. As a result, they obtain the correlation $p(u, v | \mathbf{x}, y_0, \mathbf{y}) = \text{Tr}(\rho_{AB} M_u^{\mathbf{x}} \otimes M_v^{y_0, \mathbf{y}})$. Clearly, this correlation because of the construction achieves the Bell value

$$\begin{aligned} B_{\mathcal{Q}}^{(n, \mathcal{R}_i)} &= \frac{1}{2^n |\mathcal{R}_i|} \sum_{\mathbf{x}, \mathbf{y}, y_0 \in \{0,1\}} \text{Tr}(\rho_{AB} M_{u=y_0}^{\mathbf{x}} \otimes M_{v=f_y(\mathbf{x})}^{y_0, \mathbf{y}}) \\ &= \frac{1}{2^n |\mathcal{R}_i|} \sum_{\mathbf{x}, \mathbf{y}, \omega} \text{Tr}(\rho_{AB} M_{\omega}^{\mathbf{x}} \otimes M_{z=f_y(\mathbf{x})}^{\omega, \mathbf{y}}) = S_{EACC}^{(n, \mathcal{R}_i)}. \end{aligned}$$

Therefore, the maximum Bell value of the Bell expression (15), $B_{\mathcal{Q}}^{(n, \mathcal{R}_i)}$, caps the success probability of EACC protocols in (n, \mathcal{R}_i) GRAC, $S_{EACC}^{(n, \mathcal{R}_i)}$. \blacksquare

IV. $n = 3$: A CASE STUDY

In this section, we study and characterize $(n = 3, \mathcal{R}_i)$ GRACs, finding out optimal classical and quantum protocol and success probabilities, as well as noise tolerance of the latter.

A. Classical protocols

We recall that, in classical $(n = 3, \mathcal{R}_i)$ GRACs, Alice encodes her input string $\mathbf{x} \in \{0, 1\}^3$ onto a classical bit message $\omega \in \{0, 1\}$, based on a deterministic encoding scheme \mathcal{E} , $\omega = f_{\mathcal{E}}(\mathbf{x})$. On the other end, Bob, upon receiving ω from Alice,

²We note here that this thesis and the proof thereof builds on the observations contained in [24,31].

TABLE I. Explicit comparison of classical strategies: (i) majority encoding and identity decoding [$\omega = \text{maj}(x_1, x_2, x_3)$] and (ii) an encoding strategy entailing $\omega = x_1 \wedge \neg(x_2 \wedge x_3)$, along with the decoding scheme wherein Bob outputs $z = \omega \oplus 1$ whenever he is asked to guess x_2, x_3 , or $x_1 \oplus x_2 \oplus x_3$, and $z = \omega$ otherwise, for ($n = 3, \mathcal{R}$) GRAC. We also enlist the guessing probabilities $s_C^{(n=3, \mathcal{R})}(\mathbf{y})$ for the functions $f_i \in \mathcal{F}_{\mathcal{R}}^3$; the upper row denotes the success probabilities corresponding to the majority-encoding and identity-decoding strategy (i) and the bottom row with the strategy (ii). The asterisk (\star) indicates the use of inverse identity decoding, i.e., $z = \omega \oplus 1$ for the particular function. The arrows indicate the change in success probabilities of strategy (ii) in comparison with strategy (i).

\mathbf{x}	$0\omega = \text{maj}(x_1, x_2, x_3)$	$\omega = x_1 \wedge \neg(x_2 \wedge x_3)$	x_1	x_2	x_3	$x_1 \oplus x_2$	$x_1 \oplus x_3$	$x_2 \oplus x_3$	$x_1 \oplus x_2 \oplus x_3$
(000)	0	0	0	0	0	0	0	0	0
(001)	0	0	0	0	1	0	1	1	1
(010)	0	0	0	1	0	1	0	1	1
(011)	1	0	0	1	1	1	1	0	0
(100)	0	1	1	0	0	1	1	0	1
(101)	1	1	1	0	1	1	0	1	0
(110)	1	1	1	1	0	0	1	1	0
(111)	1	0	1	1	1	0	0	0	1
	$s_C^{(n=3, \mathcal{R})}(\mathbf{y})$		06/8 7/8[↑]	06/8 5/8[*][↓]	06/8 5/8[*][↓]	04/8 5/8[↑]	04/8 5/8[↑]	04/8 5/8[↑]	06/8[*] 5/8[*][↓]

decodes it to produce his output $z = f_{\mathcal{D}}(\mathbf{y}, \omega)$ based on a deterministic decoding scheme \mathcal{D} . The optimal classical strategy for ($n \rightarrow 1$) RACs, without loss of generality, turns out to be majority encoding, i.e., $\omega = \text{maj}(x_1, \dots, x_n)$, and identity decoding, i.e., $z = \omega$ [30,32]. However, as we demonstrate below, this strategy may not be optimal for ($n = 3, \mathcal{R}_i$) GRACs.

Observation 1. Unlike ($n \rightarrow 1$) RAC, majority encoding and identity decoding is not optimal for all ($n = 3, \mathcal{R}_i$) GRACs.³

Proof. To prove this thesis, we shall consider the ($n = 3, \mathcal{R}$) GRAC which entails the entire MUBS $\mathcal{F}_{\mathcal{R}}^3$. For this task, the majority encoding, i.e., $\omega = \text{maj}(x_1, x_2, x_3)$, and identity decoding, i.e., $z = \omega$, strategy yields a success probability of $s_C^{(n, \mathcal{R})} = \frac{32}{56}$. Moreover, even if we allow for an inverse identity decoding, for the function $x_1 \oplus x_2 \oplus x_3$, i.e., $z = \omega \oplus 1$, we obtain success probability of $s_C^{(3, \mathcal{R})} = \frac{36}{56}$ (see Table I). However, employing a straightforward linear program, we find that the optimal success probability of ($n = 3, \mathcal{R}$) GRAC turns out to be $S_C^{(3, \mathcal{R})} = \frac{37}{56}$. Specifically, Alice’s encoding strategy entails $\omega = x_1 \wedge \neg(x_2 \wedge x_3)$, whereas Bob’s decoding scheme entails producing $z = \omega \oplus 1$ whenever he is asked to guess x_2, x_3 , or $x_1 \oplus x_2 \oplus x_3$, and $z = \omega$ otherwise. We note that this strategy is not unique, as there exists other strategies that saturate the classical optimal success probability.

Moving on, we used straightforward linear programs to obtain the optimal classical success probabilities for all non-trivial ($n = 3, \mathcal{R}_i$) GRACs (see Table II). We find that the optimal strategies for all cases are (equivalent up to rebelling) to either majority encoding and identity decoding, or the strategy entailing the encoding $\omega = x_1 \wedge \neg(x_2 \wedge x_3)$. While for $|\mathcal{R}_i| \in \{2, 3\}$, we find the maximal classical success probability of the ($n = 3, \mathcal{R}_i$) GRACs remains the same as that of the ($|\mathcal{R}_i| \rightarrow 1$) RACs. For $|\mathcal{R}_i| = \{5, 6\}$, the maximal classical success probability of the ($n = 3, \mathcal{R}_i$) GRACs exceeds that of the ($|\mathcal{R}_i| \rightarrow 1$) RACs. The case of four questions, $|\mathcal{R}_i| = 4$,

presents a peculiarity, and forms the basis of the following observation.

Observation 2. The maximum average success probability of ($n = 3, \mathcal{R}_i$) GRAC depends on the list of functions that Bob needs to guess, when $|\mathcal{R}_i| = 4$.

Proof. Consider the case when Bob is required to guess $\mathcal{F}_{\mathcal{R}_i}^3 \equiv \{x_1, x_2, x_3, x_1 \oplus x_2 \oplus x_3\} \in \mathcal{F}_{\mathcal{R}}^3$; then majority encoding and identity decoding yields the optimal success proba-

TABLE II. Maximal classical success probability of ($3, \mathcal{R}_i$) GRACs, $S_C^{(3, \mathcal{R}_i)}$, listed along with the number of MUBFs Bob is required to guess. These values are contrasted against the maximal success probability of standard ($n = |\mathcal{R}_i| \rightarrow 1$) RACs, $S_C^{(|\mathcal{R}_i| \rightarrow 1)}$, which form lower bounds for the former according to Theorem 1. These were obtained via linear programming and by retrieving explicit classical strategies. The case of four MUBFs presents a peculiarity, i.e., when the four functions $\{f_i, f_j, f_k, f_l\}$ as such that $f_i \oplus f_j = f_k \oplus f_l$, the classical protocols can attain a success probability of 0.75, whereas, in the other cases, classical protocols cannot go beyond $\frac{11}{16}$, which is also the maximal success probability of ($4 \rightarrow 1$) RAC (see Observation 2). Moreover, notice that, for the latter case, adding any MUBF to the latter increases the maximal classical average success probability, demonstrating a surprising feature of GRACs termed harder the task, greater the payoff (see Observation 3).

$ \mathcal{R}_i $	$S_C^{(\mathcal{R}_i \rightarrow 1)}$	$S_C^{(3, \mathcal{R}_i)}$
2	$\frac{3}{4} = 0.75$	$\frac{3}{4} = 0.75$
3	$\frac{3}{4} = 0.75$	$\frac{3}{4} = 0.75$ $\frac{3}{4} = 0.75$
4	$\frac{11}{16} = 0.6875$	(if $f_i \oplus f_j = f_k \oplus f_l$) $\frac{11}{16} = 0.6875$ (if $f_i \oplus f_j \neq f_k \oplus f_l$)
5	$\frac{11}{16} = 0.6875$	$\frac{7}{10} = 0.7$
6	$\frac{21}{32} = 0.65625$	$\frac{2}{3} \approx 0.6667$
7	$\frac{21}{32} = 0.65625$	$\frac{37}{56} \approx 0.6607$

³We note that a similar thesis was observed in [33,34] in the context of multipartite RACs.

TABLE III. Maximal quantum success probability of prepare and measure qubit protocols for $(3, \mathcal{R}_i)$ GRACs, $S_{\mathcal{Q}}^{(3, \mathcal{R}_i)}$, listed along with the number of MUBFs Bob is required to guess. These values are contrasted against the maximal quantum success probability of standard $(n = |\mathcal{R}_i| \rightarrow 1)$ RACs, $S_{\mathcal{Q}}^{(|\mathcal{R}_i| \rightarrow 1)}$, which form lower bounds for the former according to Theorem 1. All values were obtained upon coincidence (up to numerical precision) of lower bounds obtained from the seesaw semidefinite programming method and upper bounds obtained via *Navascues-Vertesi* hierarchy of semidefinite programming relaxations, along with retrieval of explicit quantum protocols. In all cases except when $|\mathcal{R}_i| = 4$, notice that the maximal quantum success probabilities saturate the upper bounds, $\frac{1}{2}(1 + \frac{1}{\sqrt{|\mathcal{R}_i|}})$, which follow from Theorem 2. In particular, for the case of four MUBFs, when the four functions $\{f_i, f_j, f_k, f_l\}$ are such that $f_i \oplus f_j = f_k \oplus f_l$, the qubit prepare and measure protocols cannot exceed the classical maximum success probability 0.75, whereas in the remaining cases the qubit protocols can go beyond the classical bound, $\frac{11}{16} = 0.6875$, but saturate the maximal success probability of qubits for $(4 \rightarrow 1)$ RAC, $\frac{1}{2}(1 + \frac{\sqrt{2} + \sqrt{6}}{8}) \approx 0.7415$.

$ \mathcal{R}_i $	$S_{\mathcal{Q}}^{(\mathcal{R}_i \rightarrow 1)}$	$S_{\mathcal{Q}}^{(3, \mathcal{R}_i)}$
2	$\frac{1}{2}(1 + \frac{1}{\sqrt{2}}) \approx 0.8536$	$\frac{1}{2}(1 + \frac{1}{\sqrt{2}}) \approx 0.8536$
3	$\frac{1}{2}(1 + \frac{1}{\sqrt{3}}) \approx 0.7887$	$\frac{1}{2}(1 + \frac{1}{\sqrt{3}}) \approx 0.7887$
4	$\frac{1}{2}(1 + \frac{\sqrt{2} + \sqrt{6}}{8}) \approx 0.7415$	$\frac{3}{4} = 0.75$ (if $f_i \oplus f_j \neq f_k \oplus f_l$) (if $f_i \oplus f_j = f_k \oplus f_l$) $\frac{1}{2}(1 + \frac{\sqrt{2} + \sqrt{6}}{8}) \approx 0.7415$
5	≈ 0.7135	$\frac{1}{2}(1 + \frac{1}{\sqrt{5}}) \approx 0.7236$
6	≈ 0.6940	$\frac{1}{2}(1 + \frac{1}{\sqrt{6}}) \approx 0.7041$
7	≈ 0.6786	$\frac{1}{2}(1 + \frac{1}{\sqrt{7}}) \approx 0.6890$

bility, $S_C^{(n=3, \mathcal{R}_i)} = \frac{3}{4}$. In general, whenever Bob has to guess $\mathcal{F}_{\mathcal{R}_i}^3 \equiv \{f_i, f_j, f_k, f_l \in \mathcal{F}_{\mathcal{R}_i}^3\}$ such that $\forall \mathbf{x} \in \{0, 1\}^3 : f_i(\mathbf{x}) \oplus f_j(\mathbf{x}) = f_k(\mathbf{x}) \oplus f_l(\mathbf{x})$, a strategy equivalent up to relabeling majority encoding and identity decoding yields the optimal success probability, $S_C^{(n=3, \mathcal{R}_i)} = \frac{3}{4}$.

Now consider the case when Bob is required to guess $\mathcal{F}_{\mathcal{R}_i}^3 \equiv \{x_1, x_2, x_3, x_1 \oplus x_2\} \in \mathcal{F}_{\mathcal{R}_i}^3$. In this case the strategy entailing the encoding scheme $\omega = x_1 \wedge \neg(x_2 \wedge x_3)$, and the decoding scheme $z = \omega$ when Bob is asked to guess x_1 or $x_1 \oplus x_2$, and $z = \omega \oplus 1$ otherwise, attains the optimal success probability $S_C^{(n=3, \mathcal{R}_i)} = \frac{11}{16}$. In fact, whenever $\exists \mathbf{x} \in \{0, 1\}^3 : f_i(\mathbf{x}) \oplus f_j(\mathbf{x}) \neq f_k(\mathbf{x}) \oplus f_l(\mathbf{x})$, a strategy equivalent up to relabeling to the aforementioned strategy attains the optimal success probability, $S_C^{(n=3, \mathcal{R}_i)} = \frac{11}{16}$.

The case of $(n = 3, \mathcal{R}_i)$ GRAC with four questions, i.e., when $|\mathcal{R}_i| = 4$, presents yet another peculiarity.

Observation 3. (Harder the task, greater the payoff.) In the case of four questions, $|\mathcal{R}_i| = 4$, and $\exists \mathbf{x} \in \{0, 1\}^3 : f_i(\mathbf{x}) \oplus f_j(\mathbf{x}) \neq f_k(\mathbf{x}) \oplus f_l(\mathbf{x})$, the maximal average success probability increases from $\frac{11}{16} = 0.6875$ to $\frac{7}{10} = 0.7$ when Bob is asked to guess any additional mutually unbiased balanced function of Alice's input.

This is especially surprising as, in general, for $(n \rightarrow 1)$ RAC and generic communication complexity tasks, increasing the number of questions that Bob is required to guess, n , decreases the maximal average success probability (see Table II).

B. Quantum prepare and measure protocols

We now investigate the performance of qubit prepare and measure protocols in $(n = 3, \mathcal{R}_i)$ GRACs. We employed a standard *seesaw* semidefinite programming technique to obtain lower bounds on maximal success probability of such

protocols. Additionally, we employed the *Navascues-Vertesi* hierarchy of semidefinite programming relaxations to obtain tight upper bounds. Whenever the lower and upper bounds coincide (up to machine precision), they yield a proof of optimality. The consequent optimal values are listed in Table III. Additionally, we retrieve explicit quantum protocols which saturate these values (see the Appendix).

Noisy channels

In this section, we investigate the effect of noisy channels on the performance of qubit prepare and measure protocols in $(n = 3, \mathcal{R}_i)$ GRACs. Recall that a quantum channel is mathematically described by a completely positive trace preserving map $\Lambda : L(\mathcal{H}_{\text{in}}) \rightarrow L(\mathcal{H}_{\text{out}})$, where $L(\mathcal{X})$ is the set of linear operators acting on the Hilbert space \mathcal{X} ; \mathcal{H}_{in} and \mathcal{H}_{out} respectively denote input and output Hilbert space of the map Λ [35]. Since we are considering qubit communication therefore we have $\mathcal{H}_{\text{in}} \equiv \mathcal{H}_{\text{out}} \equiv \mathbb{C}^2$. Furthermore, a channel is known to be unital if completely mixed state remains invariant under it. In the following we analyze the effect of the following two unital qubit channels on the performance of $(n = 3, \mathcal{R}_i)$ GRACs.

(a) *Depolarizing channel.* The effect of a depolarizing channel $\Phi_{\text{Depol}}^\lambda$ is to keep the input state intact with probability $(1 - \lambda)$, while with probability λ an ‘‘error’’ occurs entirely replacing the input state by white noise, i.e., a generic initial state $\rho_{\text{in}} = \frac{\mathbb{I} + \mathbf{n} \cdot \boldsymbol{\sigma}}{2}$ is distorted to

$$\rho_{\text{out}} = \Phi_{\text{Depol}}^\lambda(\rho_{\text{in}}) = \lambda \frac{\mathbb{I}}{2} + (1 - \lambda)\rho_{\text{in}}, \quad (16)$$

where $\lambda \in [0, 1]$ is the noise parameter. Now, for qubits, increasing the noise parameter λ shrinks the Bloch sphere uniformly, so it is enough to consider the noisy versions of the optimal preparations we recovered above. In Table IV we

TABLE IV. Threshold value of the noise parameter λ_{crit} for depolarizing channel, such that we continue to retrieve the quantum advantage in $n = 3$, \mathcal{R}_i GRACs. Note that for $|\mathcal{R}_i| = 4$ we considered only the cases for which $f_i \oplus f_j \neq f_k \oplus f_l$. Consequently, we observe that for $|\mathcal{R}_i| = 3$ the noise tolerance is lower than that of $|\mathcal{R}_i| = 5, 6, 7$, which forms yet another instance of harder the task, greater the payoff.

$ \mathcal{R}_i $	2	3	4	5	6	7
λ_{crit}	0.29289	0.13396	0.22354	0.10555	0.18349	0.14957

list the threshold value of the noise parameter λ such that we continue to retrieve a quantum advantage in $(n = 3, \mathcal{R}_i)$ GRACs. Yet again, we witness the reappearance of the characteristic phenomenon of GRACs, namely, harder the task, greater the payoff, as the noise threshold λ_{crit} in the cases with $|\mathcal{R}_i| = 5, 6, 7$ MUBFs exceeds that of $|\mathcal{R}_i| = 3$.

(b) *Dephasing channel.* The effect of a qubit dephasing channel $\Phi_{\text{Dephase}}^\lambda$ along a given spin direction \mathbf{n} is given by

$$\rho_{\text{out}} = \Phi_{\text{Dephase}}^\lambda(\rho_{\text{in}}) = \lambda(\mathbf{n} \cdot \boldsymbol{\sigma})\rho_{\text{in}}(\mathbf{n} \cdot \boldsymbol{\sigma}) + (1 - \lambda)\rho_{\text{in}}, \quad (17)$$

where $\lambda \in [0, \frac{1}{2}]$ is the noise parameter. Unlike the depolarizing channel, here, the optimal quantum strategy always performs as well as the optimal classical strategy. Therefore, in Fig. 1 we plot the ratio optimal quantum success probability to that of maximal classical success probability, $\mathfrak{R}_{Q/C} = \frac{S_Q^{(n=3, \mathcal{R}_i)}}{S_C^{(n=3, \mathcal{R}_i)}}$, for different numbers of MUBFs, wherein we employed a *bit-flip* channel, i.e., $\mathbf{n} \equiv [1, 0, 0]^T$, and numerically optimized over qubit preparations and measurements for all $\lambda \in [0, 1]$. Moreover, even in this case we find the reappearance of the phenomenon, harder the task, greater the payoff, as for a range of the noise parameter $1 - \lambda \in (0.5, 0.871)$ the maximal quantum success probability ($n = 3, \mathcal{R}_i$) GRAC with four MUBFs exceeds that of ($n = 3, \mathcal{R}_i$) GRAC with five MUBFs (see Fig. 2).

C. Entanglement assisted classical communication

Finally, we investigate the performance of shared entanglement and cbt communication protocols. Again, we employ

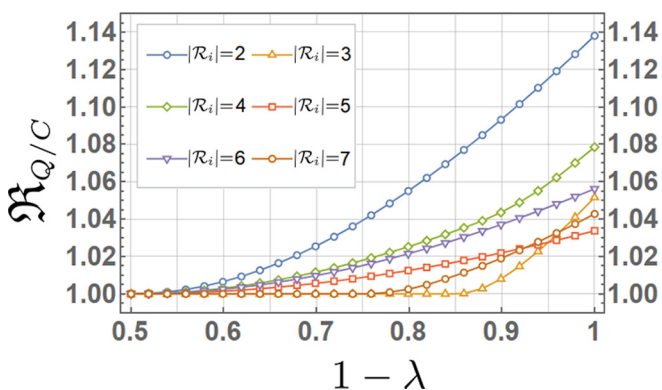


FIG. 1. Ratio of maximal quantum success probability to maximal classical success probability, $\mathfrak{R}_{Q/C} = \frac{S_Q^{(n=3, \mathcal{R}_i)}}{S_C^{(n=3, \mathcal{R}_i)}}$, for $(n = 3, \mathcal{R}_i)$ GRACs with $|\mathcal{R}_i| = [2, 7]$ plotted against $1 - \lambda$, where λ is the noise parameter of the dephasing channel.

the standard *seesaw* semidefinite programming technique to obtain dimension dependent lower bounds on maximal success probability of such protocols. Moreover, we employ *Navascues-Pironio-Acin* hierarchy of semidefinite programming relaxations to obtain upper bounds on the quantum violation of associated (Theorem 3) Bell inequalities. Yet again, a coincidence (up to machine precision) implies the optimality of these bounds, listed in Table V. It is known that entanglement assistance can increase classical capacity of a quantum channel as established in the seminal superdense coding protocol [2] (see also [36]). Moreover, it has also been shown that entanglement, more generally nonlocal correlations, can increase the zero-error capacity [37,38] of a noisy classical channel [39,40]. More strikingly, as established recently, entanglement can empower even a noiseless classical channel [41]. It is known that EACC protocols can outperform qubit prepare and measure protocols in standard ($n \rightarrow 1$) RACs when the number of input bits to the sender exceeds three, i.e., for $n > 3$ [23]. However, as we will report in the following observation, EACC protocols can outperform quantum prepare and measure even with three inputs to the sender in GRACs.

Observation 4. For the case of four MUBFs $\{f_i, f_j, f_k, f_l\}$, such that $\exists \mathbf{x} : f_i(\mathbf{x}) \oplus f_j(\mathbf{x}) \neq f_k(\mathbf{x}) \oplus f_l(\mathbf{x})$, entanglement assisted classical communication protocols can outperform the prepare and measure qubit protocols.

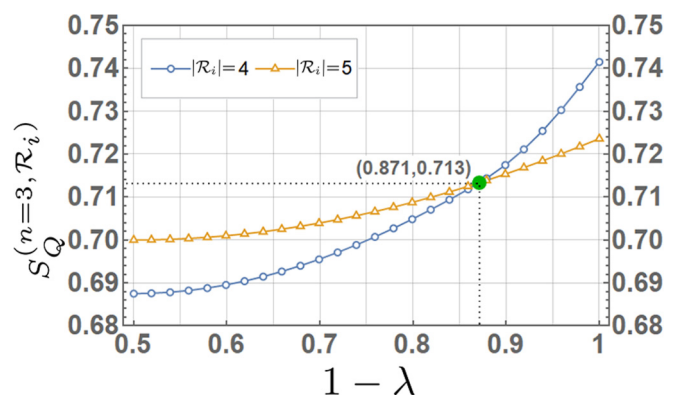


FIG. 2. Maximal quantum success probability of $(n = 3, \mathcal{R}_i)$ GRAC with $|\mathcal{R}_i| = \{4, 5\}$ in the presence of dephasing channel with noise parameter λ . Note that for $|\mathcal{R}_i| = 4$ we considered only the cases for which $f_i \oplus f_j \neq f_k \oplus f_l$. Moreover, we find that for a range of the noise parameter $1 - \lambda \in (0.5, 0.871)$ the maximal quantum success probability ($n = 3, \mathcal{R}_i$) GRAC with four MUBFs (curve with circles) exceeds that of ($n = 3, \mathcal{R}_i$) GRAC with five MUBFs (curve with triangles), which is yet another instance of harder the task, greater the payoff.

TABLE V. Maximal quantum success probability of entanglement assisted one bit communication protocols for $(3, \mathcal{R}_i)$ GRACs, $S_{EACC}^{(3, \mathcal{R}_i)}$, listed along with the number of MUBFs Bob is required to guess. These values are contrasted against the maximal quantum success probability of standard ($n = |\mathcal{R}_i| \rightarrow 1$) RACs from [23], $S_{EACC}^{(|\mathcal{R}_i| \rightarrow 1)}$, which form lower bounds for the former according to Theorem 1. All values were obtained upon coincidence of lower bounds obtained from the seesaw semidefinite programming method and upper bounds obtained from Navascues-Pironio-Acin hierarchy of semidefinite programming relaxations. For all cases, shared entanglement and one bit of classical communication can achieve a maximal success probability of $\frac{1}{2}(1 + \frac{1}{\sqrt{|\mathcal{R}_i|}})$.

$ \mathcal{R}_i $	$S_{EACC}^{(\mathcal{R}_i \rightarrow 1)}$	$S_{EACC}^{(3, \mathcal{R}_i)}$
2	$\frac{1}{2}(1 + \frac{1}{\sqrt{2}}) \approx 0.8536$	$\frac{1}{2}(1 + \frac{1}{\sqrt{2}}) \approx 0.8535$
3	$\frac{1}{2}(1 + \frac{1}{\sqrt{3}}) \approx 0.7887$	$\frac{1}{2}(1 + \frac{1}{\sqrt{3}}) \approx 0.7887$
4	$\frac{1}{2}(1 + \frac{1}{\sqrt{4}}) = \frac{3}{4} = 0.75$	$\frac{1}{2}(1 + \frac{1}{\sqrt{4}}) = \frac{3}{4} = 0.75$
5	$\frac{1}{20}(12 + \sqrt{6}) \approx 0.7225$	$\frac{1}{2}(1 + \frac{1}{\sqrt{5}}) \approx 0.7236$
6	$\frac{1}{2}(1 + \frac{1}{\sqrt{6}}) \approx 0.7041$	$\frac{1}{2}(1 + \frac{1}{\sqrt{6}}) \approx 0.7041$
7	$\frac{1}{21}(12 + \sqrt{6}) \approx 0.6880$	$\frac{1}{2}(1 + \frac{1}{\sqrt{7}}) \approx 0.6890$

V. DISCUSSIONS AND OUTLOOK

We introduced a generalization of a widely studied family of communication tasks, namely, the random access codes. At this point, it is worth mentioning the recent work of [42], wherein the authors also consider a generalization of RACs, referred to as f -RACs. In these tasks, the receiver intends to recover the value of a given Boolean function f of any subset of a fixed size of the sender's input bits. Manifestly, the generalization considered in this work differs from that considered in [42]. The generalization of RACs introduced in this work, namely, GRACs, entail the receiver intending to recover certain Boolean functions of the sender's input bits. These functions belong to sets of mutually unbiased functions (MUBS) with the cryptographic property that recovering the value of any one such function does not yield any information about the values of the rest of the functions in the set. We study three distinct classes of protocols for GRACs: (i) classical, (ii) quantum prepare and measure, and (iii) entanglement assisted classical communication protocols. Along with finding general bounds on the success probability of these protocols in GRACs, we have detailed the specific case of GRACs with the sender's input data comprised of three independently distributed bits.

This work motivates several possible directions for future research. While we have studied only classical and quantum strategies, it is also possible to explore more generalized strategies. Note that for the axiomatic derivation of Hilbert space quantum mechanics research has initiated the study of generalized probability theories (GPT) [43–47]. The seminal two-party-two-input-two-output ($2 - 2 - 2$) Popescu-Rohrlich (PR) correlation [48] that exhibits stronger nonlocal behavior than quantum theory can be studied in this GPT framework. In [16], it has been shown that the ($2 \rightarrow 1$) RAC task can be perfectly accomplished in a particular GPT model called box world that can be thought of as the marginal state space of the set of all $2 - 2 - 2$ no-signaling correlations. A particular generalization of this box world is the polygon model where state spaces are described by symmetric polygons [49] which has been studied

extensively in the recent past [50–57]. The performance of these polygonal models in GRACs is worth exploring.

Moreover, researchers have generalized the study of RAC-QRAC with larger input-output alphabets, wherein Alice is given random string $\mathbf{x} \equiv x_1 \cdots x_n \in \{0, 1, \dots, d-1\}^n$ [21,32,58]. Indeed, it is possible to generalize MUBF-MUBS and GRACs with larger input-output alphabets. However, we leave this for future study. Finally, as we have demonstrated, GRACs allow for quantum over classical advantage; hence GRACs may be used for certification of private randomness and quantum key distribution schemes. It remains to be seen whether GRACs provide an advantage over RACs in such tasks.

ACKNOWLEDGMENTS

M.B. acknowledges the research grant of INSPIRE-faculty fellowship from the Department of Science and Technology, Government of India. A.C. acknowledges financial support by NCN grant SHENG 2018/30/Q/ST2/00625. The numerical optimization was carried out using Ncpol2sdpa [59], YALMIP [60], and SDPT3 [61]. A.C. is grateful to M. Pawłowski for fruitful discussions. R.K.P. acknowledges support from the CSIR project 09/997(0079)/2020-EMR-I.

APPENDIX: EXPLICIT QUBIT PREPARE AND MEASURE PROTOCOLS FOR $(n = 3, \mathcal{R}_i)$ GRACs

In this section, we present qubit states and measurements that attain maximal quantum success probability in $(n = 3, \mathcal{R}_i)$ GRACs.

(A) $|\mathcal{R}_i| = 2$. All choices of $\mathcal{R}_i \subset \mathcal{R}$ ($|\mathcal{R}_i| = 2$) are equivalent up to a reordering of the input strings. We give an explicit example using $\mathcal{F}_{\mathcal{R}_i}^3 = \{x_1, x_2\}$. If Bob is asked to evaluate one of the functions from a MUBS of cardinality 2 then they can have the optimal quantum success by following a strategy similar to the standard ($2 \mapsto 1$) RAC. Recall that optimal

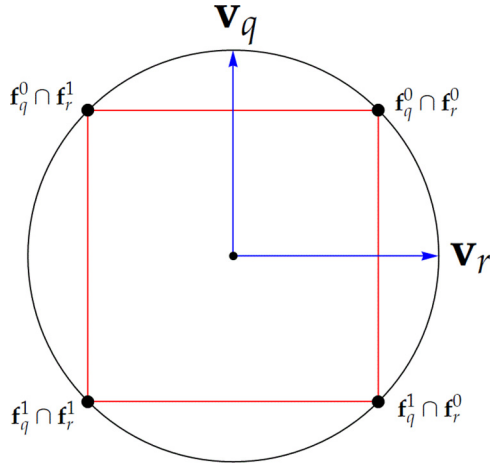


FIG. 3. Optimal quantum protocol for GRAC ($|\mathcal{R}_i| = 2$). Optimal quantum protocol for any ($n = 3, \mathcal{R}_i$) GRAC with $\mathcal{F}_{\mathcal{R}_i}^3 \equiv \{f_q, f_r\}$. Shown in the figure is a projection of the Bloch sphere onto a plane with the black dots denoting the encoded states and blue arrows representing the measurement basis. The set of strings $\mathbf{f}_q^i \cap \mathbf{f}_r^j \subset \{0, 1\}^3$ are encoded in one of the black dots representing a quantum state, where \mathbf{f}_q^i denote the set of strings whose output value under the function f_q is i ; $\mathbf{f}_q^i = \{\mathbf{x} \in \{0, 1\}^3 | f_q(\mathbf{x}) = i, i \in \{0, 1\}\}$. For evaluating the function f_q (f_r) von Neumann measurement along \mathbf{v}_q (\mathbf{v}_r) is performed and function value is reported as 0 (1) if the “+1” (“-1”) outcome clicks.

quantum protocol for ($2 \mapsto 1$) RAC is given by

Alice’s encoding: $\{0, 1\}^2 \ni x_1 x_2 \mapsto \rho_{x_1 x_2}$,

$$\text{e.g.} \begin{cases} 00 \mapsto \frac{1}{2}(\mathbf{I} + \frac{1}{\sqrt{2}}\sigma_x + \frac{1}{\sqrt{2}}\sigma_y), \\ 01 \mapsto \frac{1}{2}(\mathbf{I} + \frac{1}{\sqrt{2}}\sigma_x - \frac{1}{\sqrt{2}}\sigma_y), \\ 10 \mapsto \frac{1}{2}(\mathbf{I} - \frac{1}{\sqrt{2}}\sigma_x + \frac{1}{\sqrt{2}}\sigma_y), \\ 11 \mapsto \frac{1}{2}(\mathbf{I} - \frac{1}{\sqrt{2}}\sigma_x - \frac{1}{\sqrt{2}}\sigma_y), \end{cases}$$

Bob’s decoding: $M_i \equiv \{\frac{1}{2}(\mathbf{I} + \mathbf{v}_i \cdot \sigma), \frac{1}{2}(\mathbf{I} - \mathbf{v}_i \cdot \sigma)\}$,

$$\text{e.g.} \begin{cases} \text{1st function} \rightarrow \mathbf{v}_1 \equiv (1, 0, 0), \\ \text{2nd function} \rightarrow \mathbf{v}_2 \equiv (0, 1, 0). \end{cases}$$

Bob will guess the bit value as 0 whenever he obtains +1 outcome; otherwise, he guesses the value as 1. To make this protocol work for an arbitrary $\mathcal{F}_{\mathcal{R}_i}^n = \{f_q, f_r\}$, Alice follows the encoding $\mathbf{f}_q^{x_1} \cap \mathbf{f}_r^{x_2} \mapsto |\psi\rangle_{x_1 x_2}$ and Bob performs the measurement M_1 for evaluating the function f_q and performs the measurement M_2 for f_r (see Fig. 3). Importantly, in this case both the worst case success probability as well as the average success probability turns out to be $\frac{1}{2}(1 + \frac{1}{\sqrt{2}})$.

(B) $|\mathcal{R}_i| = 3$. Unlike the previous case, all choices of $\mathcal{R}_i \subset \mathcal{R}$ ($|\mathcal{R}_i| = 3$) are not equivalent under a permutation of the input strings. If $\mathcal{F}_{\mathcal{R}_i}^3 = \{f_q, f_r, f_s\}$, then the two possible equivalence classes are defined by $f_q \oplus f_r \neq f_s$ and $f_q \oplus f_r = f_s$.

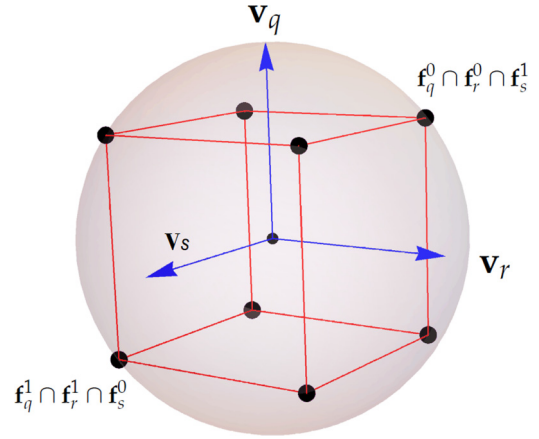


FIG. 4. Optimal quantum protocol for GRAC $\mathcal{F}^n\{3\} \equiv \{f_q, f_r, f_s\}$, where $f_q \oplus f_r \neq f_s$. The set of strings $\mathbf{f}_q^i \cap \mathbf{f}_r^j \cap \mathbf{f}_s^k \subset \{0, 1\}^n$ are encoded in qubit state $\rho_{ijk} := \frac{1}{2}(\mathbf{I} + (-1)^i \frac{1}{\sqrt{3}}\sigma_x + (-1)^j \frac{1}{\sqrt{3}}\sigma_y + (-1)^k \frac{1}{\sqrt{3}}\sigma_z)$, where the decoding measurements are along $\mathbf{v}_q \equiv (1, 0, 0)$, $\mathbf{v}_r \equiv (0, 1, 0)$, and $\mathbf{v}_s \equiv (0, 0, 1)$.

Case (i). If $f_q \oplus f_r \neq f_s$, then every such set is equivalent to the set $\mathcal{F}_{\mathcal{R}_i}^3 = \{x_1, x_2, x_3\}$. Employing the standard ($3 \mapsto 1$) RAC protocol (see Fig. 4) on this set attains the optimal quantum success probability of $\frac{1}{2}(1 + 1/\sqrt{3})$.

Alice’s encoding:

$$\text{e.g.} \begin{cases} x_1 x_2 x_3 \mapsto \rho_{x_1 x_2 x_3} \\ = \frac{1}{2}(\mathbf{I} + (-1)^{x_1} \frac{1}{\sqrt{3}}\sigma_x + (-1)^{x_2} \frac{1}{\sqrt{3}}\sigma_y + (-1)^{x_3} \frac{1}{\sqrt{3}}\sigma_z). \end{cases}$$

Bob’s decoding: $M_i \equiv \{\frac{1}{2}(\mathbf{I} + \mathbf{v}_i \cdot \sigma), \frac{1}{2}(\mathbf{I} - \mathbf{v}_i \cdot \sigma)\}$,

$$\text{e.g.} \begin{cases} x_1 \rightarrow \mathbf{v}_1 \equiv (1, 0, 0), \\ x_2 \rightarrow \mathbf{v}_2 \equiv (0, 1, 0), \\ x_3 \rightarrow \mathbf{v}_3 \equiv (0, 0, 1). \end{cases}$$

Case (ii). If $f_q \oplus f_r = f_s$, then every such set is equivalent to the set $\mathcal{F}_{\mathcal{R}_i}^3 = \{x_1, x_2, x_1 \oplus x_2\}$. (See Fig. 5.)

Alice’s encoding:

$$\text{e.g.} \begin{cases} \{000, 001\} \mapsto \frac{1}{2}(\mathbf{I} + \frac{1}{\sqrt{3}}\sigma_x + \frac{1}{\sqrt{3}}\sigma_y + \frac{1}{\sqrt{3}}\sigma_z), \\ \{010, 011\} \mapsto \frac{1}{2}(\mathbf{I} + \frac{1}{\sqrt{3}}\sigma_x - \frac{1}{\sqrt{3}}\sigma_y - \frac{1}{\sqrt{3}}\sigma_z), \\ \{100, 101\} \mapsto \frac{1}{2}(\mathbf{I} - \frac{1}{\sqrt{3}}\sigma_x + \frac{1}{\sqrt{3}}\sigma_y - \frac{1}{\sqrt{3}}\sigma_z), \\ \{110, 111\} \mapsto \frac{1}{2}(\mathbf{I} - \frac{1}{\sqrt{3}}\sigma_x - \frac{1}{\sqrt{3}}\sigma_y + \frac{1}{\sqrt{3}}\sigma_z). \end{cases} \quad (\text{A1})$$

Bob’s decoding: $M_i \equiv \{\frac{1}{2}(\mathbf{I} + \mathbf{v}_i \cdot \sigma), \frac{1}{2}(\mathbf{I} - \mathbf{v}_i \cdot \sigma)\}$,

$$\text{e.g.} \begin{cases} x_1 \rightarrow \mathbf{v}_1 \equiv (1, 0, 0), \\ x_2 \rightarrow \mathbf{v}_2 \equiv (0, 1, 0), \\ x_1 \oplus x_2 \rightarrow \mathbf{v}_{12} \equiv (0, 0, 1). \end{cases}$$

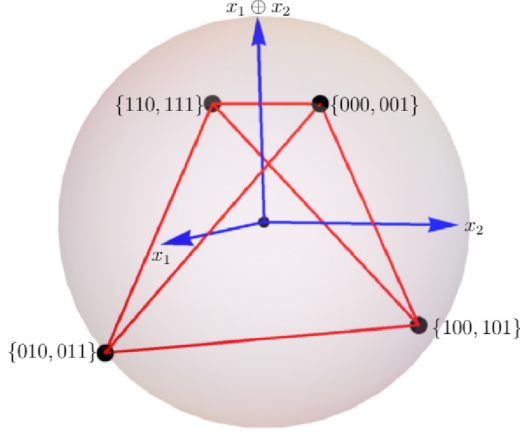


FIG. 5. ($|\mathcal{R}_i|=3$) Optimal encoding protocol for $\mathcal{F}_{\mathcal{R}_i}^3 = \{f_q, f_r, f_s\}$ with $f_q \oplus f_r = f_s$. Black dots denote the encoded states of Eq. (A1). They form the vertices of a regular tetrahedron. For evaluating the function $x_\alpha \in \{x_1, x_2, x_1 \oplus x_2\}$, Bob performs the measurement $M_\alpha \equiv \{\frac{1}{2}(\mathbf{I} + \mathbf{v}_\alpha \cdot \sigma), \frac{1}{2}(\mathbf{I} - \mathbf{v}_\alpha \cdot \sigma)\}$ on the received state and guesses the function value as “+1” if he obtains outcome “+1”; otherwise, he guesses the value as “-1”. He chooses $\mathbf{v}_1 = (1, 0, 0) = \mathbf{v}_2$ and $\mathbf{v}_{12} = (0, 0, 1)$.

(C) $\mathcal{F}_{\mathcal{R}_i}^3$ ($|\mathcal{R}_i|=4$). If $\mathcal{F}_{\mathcal{R}_i}^3 = \{f_i, f_j, f_k, f_l\}$, such that $f_i \oplus f_j = f_k \oplus f_l$, then the optimal classical success is the same as the optimal possible quantum success. So in those cases there is no question of quantum advantage. However, when $f_i \oplus f_j \neq f_k \oplus f_l$ optimal classical success is 11/16, whereas the optimal possible quantum success can go up to 3/4. We have found that for these cases the optimal quantum success indeed is higher than the classical value. For instance, consider $\mathcal{F}_{\mathcal{R}_i}^3 \equiv \{x_1, x_2, x_3, x_1 \oplus x_2\}$. (See Fig. 6.)

Alice’s encoding:

$$\text{e.g.} \begin{cases} 000 \mapsto \frac{1}{2}(\mathbf{I} + \sqrt{\frac{2}{3}}\sigma_x + \frac{1}{\sqrt{6}}\sigma_y + \frac{1}{\sqrt{6}}\sigma_z), \\ 001 \mapsto \frac{1}{2}(\mathbf{I} + \sqrt{\frac{2}{3}}\sigma_x - \frac{1}{\sqrt{6}}\sigma_y + \frac{1}{\sqrt{6}}\sigma_z), \\ \{010, 100\} \mapsto \frac{1}{2}(\mathbf{I} + \frac{1}{\sqrt{2}}\sigma_y - \frac{1}{\sqrt{2}}\sigma_z), \\ \{011, 101\} \mapsto \frac{1}{2}(\mathbf{I} - \frac{1}{\sqrt{2}}\sigma_y - \frac{1}{\sqrt{2}}\sigma_z), \\ 110 \mapsto \frac{1}{2}(\mathbf{I} - \sqrt{\frac{2}{3}}\sigma_x + \frac{1}{\sqrt{6}}\sigma_y + \frac{1}{\sqrt{6}}\sigma_z), \\ 111 \mapsto \frac{1}{2}(\mathbf{I} - \sqrt{\frac{2}{3}}\sigma_x - \frac{1}{\sqrt{6}}\sigma_y + \frac{1}{\sqrt{6}}\sigma_z). \end{cases} \quad (\text{A2})$$

Bob’s decoding: $M_i \equiv \{\frac{1}{2}(\mathbf{I} + \mathbf{v}_i \cdot \sigma), \frac{1}{2}(\mathbf{I} - \mathbf{v}_i \cdot \sigma)\}$,

$$\text{e.g.} \begin{cases} x_1 \rightarrow \mathbf{v}_1 \equiv (1, 0, 0), \\ x_2 \rightarrow \mathbf{v}_2 \equiv \mathbf{v}_1, \\ x_3 \rightarrow \mathbf{v}_3 \equiv (0, 1, 0), \\ x_1 \oplus x_2 \rightarrow \mathbf{v}_{12} \equiv (0, 0, 1). \end{cases}$$

This protocol yields the average success probability $\frac{1}{2}(1 + \frac{\sqrt{2} + \sqrt{6}}{8})$. Note that the average success is still less than 3/4. However, up to numerical precision, the lower bound obtained from the seesaw semidefinite programming method and the upper bounds obtained via *Navascues-Vertesi* hierarchy of

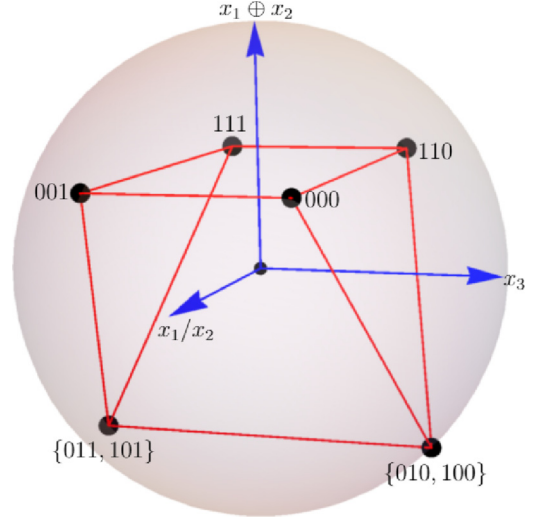


FIG. 6. ($|\mathcal{R}_i|=4$) Black dots denote the encoded states of Eq. (A2). For evaluating the function $x_\alpha \in \{x_1, x_2, x_3, x_1 \oplus x_2\}$, Bob performs the measurement $M_\alpha \equiv \{\frac{1}{2}(\mathbf{I} + \mathbf{v}_\alpha \cdot \sigma), \frac{1}{2}(\mathbf{I} - \mathbf{v}_\alpha \cdot \sigma)\}$ on the received state and guesses the function value as “0” if he obtains outcome “+1”; otherwise, he guesses the value as “-1”. He chooses $\mathbf{v}_1 = (1, 0, 0) = \mathbf{v}_2$, $\mathbf{v}_3 = (0, 1, 0)$, and $\mathbf{v}_{12} = (0, 0, 1)$.

semidefinite programming relaxations is the same as the value obtained with the present explicit protocol (see Table III).

(D) $|\mathcal{R}_i|=5$. Let us consider a particular case $\mathcal{F}_{\mathcal{R}_i}^3 \equiv \{x_1, x_2, x_3, x_1 \oplus x_2, x_1 \oplus x_3\}$.

Alice’s encoding (nonplanar):

$$\text{e.g.} \begin{cases} 000 \mapsto \frac{1}{2}(\mathbf{I} + \frac{1}{\sqrt{5}}\sigma_x + \frac{2}{\sqrt{5}}\sigma_z), \\ 001 \mapsto \frac{1}{2}(\mathbf{I} + \frac{1}{\sqrt{5}}\sigma_x + \frac{2}{\sqrt{5}}\sigma_y), \\ 010 \mapsto \frac{1}{2}(\mathbf{I} + \frac{1}{\sqrt{5}}\sigma_x - \frac{2}{\sqrt{5}}\sigma_y), \\ 011 \mapsto \frac{1}{2}(\mathbf{I} + \frac{1}{\sqrt{5}}\sigma_x - \frac{2}{\sqrt{5}}\sigma_z), \\ 100 \mapsto \frac{1}{2}(\mathbf{I} - \frac{1}{\sqrt{5}}\sigma_x + \frac{2}{\sqrt{5}}\sigma_y), \\ 101 \mapsto \frac{1}{2}(\mathbf{I} - \frac{1}{\sqrt{5}}\sigma_x - \frac{2}{\sqrt{5}}\sigma_z), \\ 110 \mapsto \frac{1}{2}(\mathbf{I} - \frac{1}{\sqrt{5}}\sigma_x + \frac{2}{\sqrt{5}}\sigma_z), \\ 111 \mapsto \frac{1}{2}(\mathbf{I} - \frac{1}{\sqrt{5}}\sigma_x - \frac{2}{\sqrt{5}}\sigma_y). \end{cases}$$

Bob’s decoding: $M_i \equiv \{\frac{1}{2}(\mathbf{I} + \mathbf{v}_i \cdot \sigma), \frac{1}{2}(\mathbf{I} - \mathbf{v}_i \cdot \sigma)\}$,

$$\text{e.g.} \begin{cases} x_1 \rightarrow \mathbf{v}_1 \equiv (1, 0, 0), \\ x_2 \rightarrow \mathbf{v}_2 \equiv (0, 1, 0), \\ x_3 \rightarrow \mathbf{v}_3 \equiv (0, 0, 1), \\ x_1 \oplus x_2 \rightarrow \mathbf{v}_{12} \equiv \mathbf{v}_3, \\ x_1 \oplus x_3 \rightarrow \mathbf{v}_{13} \equiv -\mathbf{v}_2. \end{cases}$$

A straightforward calculation yields the average success probability $\frac{1}{2}(1 + \frac{1}{\sqrt{5}})$ for this particular encoding decoding, which turns out to be the optimal quantum success (see Table III). Note that the encoded states form a rectangular box (see Fig. 7). We, however, find a different strategy where the encoded states lie on a great circle (Fig. 8) but yield the

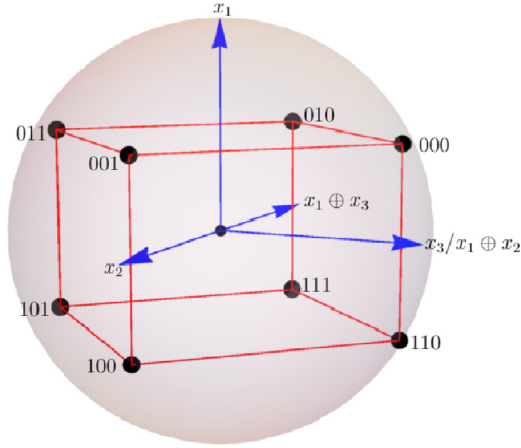


FIG. 7. ($|\mathcal{R}_i| = 5$) Optimal quantum protocol (nonplanar) for a GRAC with $\mathcal{F}_{\mathcal{R}_i}^3 \equiv \{x_1, x_2, x_3, x_1 \oplus x_2, x_1 \oplus x_3\}$.

maximum success.

Alice's encoding (planar):

$$\text{e.g.} \begin{cases} \{000, 001\} \mapsto \frac{1}{2}(\mathbf{I} + \frac{1}{\sqrt{5}}\sigma_x + \frac{2}{\sqrt{5}}\sigma_y), \\ \{010, 011\} \mapsto \frac{1}{2}(\mathbf{I} + \frac{1}{\sqrt{5}}\sigma_x - \frac{2}{\sqrt{5}}\sigma_y), \\ \{101, 111\} \mapsto \frac{1}{2}(\mathbf{I} - \frac{1}{\sqrt{5}}\sigma_x + \frac{2}{\sqrt{5}}\sigma_y), \\ \{100, 110\} \mapsto \frac{1}{2}(\mathbf{I} - \frac{1}{\sqrt{5}}\sigma_x - \frac{2}{\sqrt{5}}\sigma_y), \end{cases}$$

Bob's decoding: $M_i \equiv \{\frac{1}{2}(\mathbf{I} + \mathbf{v}_i \cdot \sigma), \frac{1}{2}(\mathbf{I} - \mathbf{v}_i \cdot \sigma)\}$,

$$\text{e.g.} \begin{cases} x_1 \rightarrow \mathbf{v}_1 \equiv (1, 0, 0), \\ x_2 \rightarrow \mathbf{v}_2 \equiv (0, 1, 0), \\ x_3 \rightarrow \mathbf{v}_3 \equiv -\mathbf{v}_2, \\ x_1 \oplus x_2 \rightarrow \mathbf{v}_{12} \equiv \mathbf{v}_2, \\ x_1 \oplus x_3 \rightarrow \mathbf{v}_{13} \equiv \mathbf{v}_2. \end{cases}$$

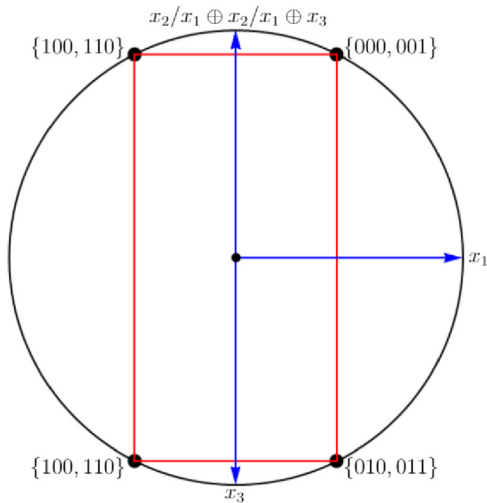


FIG. 8. ($|\mathcal{R}_i| = 5$) Optimal quantum protocol (planar) for a GRAC with $\mathcal{F}_{\mathcal{R}_i}^3 \equiv \{x_1, x_2, x_3, x_1 \oplus x_2, x_1 \oplus x_3\}$.

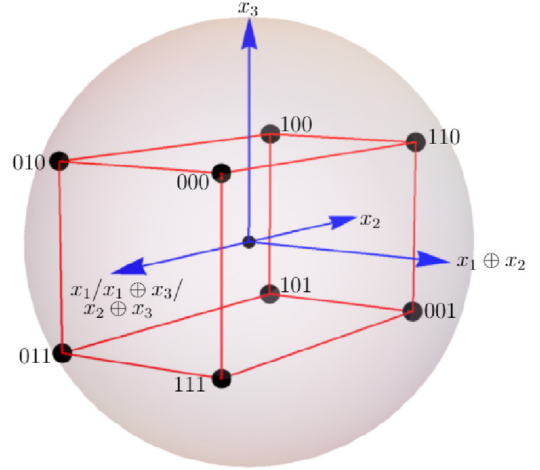


FIG. 9. ($|\mathcal{R}_i| = 6$) Encoded states and decoding measurements corresponding to the optimal quantum protocol for $\mathcal{F}_{\mathcal{R}_i}^3 \equiv \{x_1, x_2, x_3, x_1 \oplus x_2, x_1 \oplus x_3, x_2 \oplus x_3\}$.

(E) $\mathcal{F}_{\mathcal{R}_i}^3$ ($|\mathcal{R}_i| = 6$). Let us consider a particular case $\mathcal{F}_{\mathcal{R}_i}^3 \equiv \{x_1, x_2, x_3, x_1 \oplus x_2, x_1 \oplus x_3, x_2 \oplus x_3\}$. (See Fig. 9.)

Alice's encoding (planar):

$$\text{e.g.} \begin{cases} 000 \mapsto \frac{1}{2}(\mathbf{I} + \sqrt{\frac{2}{3}}\sigma_x + \frac{1}{\sqrt{6}}\sigma_y + \frac{1}{\sqrt{6}}\sigma_z), \\ 001 \mapsto \frac{1}{2}(\mathbf{I} - \sqrt{\frac{2}{3}}\sigma_x + \frac{1}{\sqrt{6}}\sigma_y - \frac{1}{\sqrt{6}}\sigma_z), \\ 010 \mapsto \frac{1}{2}(\mathbf{I} + \sqrt{\frac{2}{3}}\sigma_x - \frac{1}{\sqrt{6}}\sigma_y + \frac{1}{\sqrt{6}}\sigma_z), \\ 011 \mapsto \frac{1}{2}(\mathbf{I} + \sqrt{\frac{2}{3}}\sigma_x - \frac{1}{\sqrt{6}}\sigma_y - \frac{1}{\sqrt{6}}\sigma_z), \\ 100 \mapsto \frac{1}{2}(\mathbf{I} - \sqrt{\frac{2}{3}}\sigma_x - \frac{1}{\sqrt{6}}\sigma_y + \frac{1}{\sqrt{6}}\sigma_z), \\ 101 \mapsto \frac{1}{2}(\mathbf{I} - \sqrt{\frac{2}{3}}\sigma_x - \frac{1}{\sqrt{6}}\sigma_y - \frac{1}{\sqrt{6}}\sigma_z), \\ 110 \mapsto \frac{1}{2}(\mathbf{I} - \sqrt{\frac{2}{3}}\sigma_x + \frac{1}{\sqrt{6}}\sigma_y + \frac{1}{\sqrt{6}}\sigma_z), \\ 111 \mapsto \frac{1}{2}(\mathbf{I} + \sqrt{\frac{2}{3}}\sigma_x + \frac{1}{\sqrt{6}}\sigma_y - \frac{1}{\sqrt{6}}\sigma_z), \end{cases}$$

Bob's decoding: $M_i \equiv \{\frac{1}{2}(\mathbf{I} + \mathbf{v}_i \cdot \sigma), \frac{1}{2}(\mathbf{I} - \mathbf{v}_i \cdot \sigma)\}$,

$$\text{e.g.} \begin{cases} x_1 \rightarrow \mathbf{v}_1 \equiv (1, 0, 0), \\ x_3 \rightarrow \mathbf{v}_3 \equiv (0, 0, 1), \\ x_1 \oplus x_2 \rightarrow \mathbf{v}_{12} \equiv (0, 1, 0), \\ x_2 \rightarrow \mathbf{v}_2 \equiv -\mathbf{v}_1, \\ x_1 \oplus x_3 \rightarrow \mathbf{v}_{13} \equiv \mathbf{v}_1, \\ x_2 \oplus x_3 \rightarrow \mathbf{v}_{23} \equiv \mathbf{v}_1. \end{cases}$$

For this encoding decoding the average success probability turns out to be $P = \frac{1}{2}(1 + \frac{1}{\sqrt{6}})$, which is the optimal possible quantum success.

- [1] C. E. Shannon, *Bell Syst. Tech. J.* **27**, 379 (1948).
- [2] C. H. Bennett and S. J. Wiesner, *Phys. Rev. Lett.* **69**, 2881 (1992).
- [3] A. S. Holevo, *Prob. Peredachi Inf.* **9**, 3 (1973).
- [4] P. E. Frenkel and M. Weiner, *Commun. Math. Phys.* **340**, 563 (2015).
- [5] S. Wiesner, *ACM Sigact News* **15**, 78 (1983).
- [6] A. Ambainis, A. Nayak, A. Ta-Shma, and U. Vazirani, in *Proceedings of the Thirty-First Annual ACM Symposium on Theory of Computing* (ACM, New York, 1999), pp. 376–383.
- [7] A. Ambainis, A. Nayak, A. Ta-Shma, and U. Vazirani, *J. ACM* **49**, 496 (2002).
- [8] H. Buhrman, R. Cleve, S. Massar, and R. de Wolf, *Rev. Mod. Phys.* **82**, 665 (2010).
- [9] H. Klauck, in *Proceedings of the 42nd IEEE Symposium on Foundations of Computer Science* (IEEE, New York, 2001), pp. 288–297.
- [10] I. Kerenidis and R. De Wolf, *J. Comput. Syst. Sci.* **69**, 395 (2004).
- [11] S. Aaronson, in *Proceedings of the 19th IEEE Annual Conference on Computational Complexity, 2004* (IEEE, New York, 2004), pp. 320–332.
- [12] S. Wehner and R. De Wolf, in *International Colloquium on Automata, Languages, and Programming* (Springer, New York, 2005), pp. 1424–1436.
- [13] D. Gavinsky, J. Kempe, O. Regev, and R. De Wolf, *SIAM J. Comput.* **39**, 1 (2009).
- [14] M. Hayashi, K. Iwama, H. Nishimura, R. Raymond, and S. Yamashita, in *Annual Symposium on Theoretical Aspects of Computer Science* (Springer, New York, 2007), pp. 610–621.
- [15] R. W. Spekkens, D. H. Buzacott, A. J. Keehn, B. Toner, and G. J. Pryde, *Phys. Rev. Lett.* **102**, 010401 (2009).
- [16] M. Banik, S. S. Bhattacharya, A. Mukherjee, A. Roy, A. Ambainis, and A. Rai, *Phys. Rev. A* **92**, 030103(R) (2015).
- [17] A. Chailloux, I. Kerenidis, S. Kundu, and J. Sikora, *New J. Phys.* **18**, 045003 (2016).
- [18] A. Hameedi, A. Tavakoli, B. Marques, and M. Bourennane, *Phys. Rev. Lett.* **119**, 220402 (2017).
- [19] S. Ghorai and A. K. Pan, *Phys. Rev. A* **98**, 032110 (2018).
- [20] D. Saha and A. Chaturvedi, *Phys. Rev. A* **100**, 022108 (2019).
- [21] A. Ambainis, M. Banik, A. Chaturvedi, D. Kravchenko, and A. Rai, *Quantum Inf. Process.* **18**, 111 (2019).
- [22] A. Chaturvedi and D. Saha, *Quantum* **4**, 345 (2020).
- [23] M. Pawłowski and M. Żukowski, *Phys. Rev. A* **81**, 042326 (2010).
- [24] A. Chaturvedi, M. Pawłowski, and K. Horodecki, *Phys. Rev. A* **96**, 022125 (2017).
- [25] M. Pawłowski, T. Paterek, D. Kaszlikowski, V. Scarani, A. Winter, and M. Żukowski, *Nature (London)* **461**, 1101 (2009).
- [26] S. W. Al-Safi and A. J. Short, *Phys. Rev. A* **84**, 042323 (2011).
- [27] M. Pawłowski and N. Brunner, *Phys. Rev. A* **84**, 010302(R) (2011).
- [28] A. Chaturvedi, M. Ray, R. Veynar, and M. Pawłowski, *Quantum Inf. Process.* **17**, 131 (2018).
- [29] A. Chaturvedi, M. Farkas, and V. J. Wright, *Quantum* **5**, 484 (2021).
- [30] A. Ambainis, D. Leung, L. Mancinska, and M. Ozols, [arXiv:0810.2937](https://arxiv.org/abs/0810.2937).
- [31] A. Tavakoli, J. Pauwels, E. Woodhead, and S. Pironio, [arXiv:2103.10748](https://arxiv.org/abs/2103.10748).
- [32] A. Ambainis, D. Kravchenko, and A. Rai, [arXiv:1510.03045](https://arxiv.org/abs/1510.03045).
- [33] A. Hameedi, D. Saha, P. Mironowicz, M. Pawłowski, and M. Bourennane, *Phys. Rev. A* **95**, 052345 (2017).
- [34] D. Saha and J. J. Borkala, *Europhys. Lett.* **128**, 30005 (2020).
- [35] *States, Effects, and Operations Fundamental Notions of Quantum Theory*, edited by K. Kraus, A. Böhm, J. D. Dollard, and W. Wootters, Lecture Notes in Physics Vol. 190 (Springer, New York, 1983).
- [36] C. H. Bennett, P. W. Shor, J. A. Smolin, and A. V. Thapliyal, *Phys. Rev. Lett.* **83**, 3081 (1999).
- [37] C. Shannon, *IRE Trans. Inf. Theory* **2**, 8 (1956).
- [38] J. Korner and A. Orlitsky, *IEEE Trans. Inf. Theory* **44**, 2207 (1998).
- [39] T. S. Cubitt, D. Leung, W. Matthews, and A. Winter, *Phys. Rev. Lett.* **104**, 230503 (2010).
- [40] T. S. Cubitt, D. Leung, W. Matthews, and A. Winter, *IEEE Trans. Inf. Theory* **57**, 5509 (2011).
- [41] P. E. Frenkel and M. Weiner, [arXiv:2103.08567](https://arxiv.org/abs/2103.08567).
- [42] J. F. Doriguello and A. Montanaro, *Quantum* **5**, 402 (2021).
- [43] L. Hardy, [arXiv:quant-ph/0101012](https://arxiv.org/abs/quant-ph/0101012).
- [44] J. Barrett, *Phys. Rev. A* **75**, 032304 (2007).
- [45] G. Chiribella, G. M. D’Ariano, and P. Perinotti, *Phys. Rev. A* **81**, 062348 (2010).
- [46] H. Barnum and A. Wilce, *Electron. Notes Theor. Comput. Sci.* **270**, 3 (2011), Proceedings of the Joint 5th International Workshop on Quantum Physics and Logic and 4th Workshop on Developments in Computational Models (QPL/DCM 2008).
- [47] L. Masanes and M. P. Müller, *New J. Phys.* **13**, 063001 (2011).
- [48] S. Popescu and D. Rohrlich, *Found. Phys.* **24**, 379 (1994).
- [49] P. Janotta, C. Gogolin, J. Barrett, and N. Brunner, *New J. Phys.* **13**, 063024 (2011).
- [50] D. A. Yopp and R. D. Hill, *Lin. Multilin. Alg.* **53**, 167 (2005).
- [51] S. Weis, *J. Convex. Anal.* **19**, 815 (2012).
- [52] S. Massar and M. K. Patra, *Phys. Rev. A* **89**, 052124 (2014).
- [53] S. W. Al-Safi and J. Richens, *New J. Phys.* **17**, 123001 (2015).
- [54] M. Banik, S. Saha, T. Guha, S. Agrawal, S. S. Bhattacharya, A. Roy, and A. S. Majumdar, *Phys. Rev. A* **100**, 060101(R) (2019).
- [55] S. S. Bhattacharya, S. Saha, T. Guha, and M. Banik, *Phys. Rev. Research* **2**, 012068(R) (2020).
- [56] S. Saha, S. S. Bhattacharya, T. Guha, S. Halder, and M. Banik, *Ann. Phys. (Leipzig)* **532**, 2000334 (2020).
- [57] S. Saha, T. Guha, S. S. Bhattacharya, and M. Banik, [arXiv:2012.05781](https://arxiv.org/abs/2012.05781).
- [58] A. Tavakoli, A. Hameedi, B. Marques, and M. Bourennane, *Phys. Rev. Lett.* **114**, 170502 (2015).
- [59] P. Wittek, *ACM Trans. Math. Softw.* **41**, 1 (2015); <https://ncpol2sdpa.readthedocs.io/en/stable/index.html>.
- [60] J. Löfberg, in *Proceedings of the CACSD Conference* (Taipei, Taiwan, 2004); <https://yalmip.github.io/>.
- [61] K.-C. Toh, M. J. Todd, and R. H. Tütüncü, *Optim. Methods Softw.* **11**, 545 (1999); <https://www.mosek.com/documentation/>.