Quantum resources and protocols are known to outperform their classical counterparts in 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 (MUBS), 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 Random Access Codes (GRACs). Finally, we detail the case of GRACs with three input bits, 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.

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 super-dense 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 pre-shared entanglement [2]. Similarly, the counter-intuitive feature of quantum entanglement is known to empower several seemingly impossible tasks. However, in 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 & Weiner, namely, it has been established that classical information storage capacity of a \( d \)-level quantum system is same as that of a classical \( d \)-state system [4].

These no-go results seem to point towards the conclusion that in absence of entanglement, quantum resources and protocols might not be better than their classical counterparts for transmission of classical information. However, in actuality, even without entanglement, finite dimensional quantum systems can outperform their classical counterparts in a large variety of stochastic communication tasks. \((n \to 1)\) 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 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 a number of foundational implications \([15–22]\), in particular, pre-shared Entanglement Assisted Random Access Codes (EARACs) are closely related to non-local games \([23, 24]\), and form the basis for the principle of Information Causality \([25, 26]\).

---

\(^1\) This problem was first studied by Stephen Wiesner under the name conjugate coding \([5]\)
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 an exclusive decoding reveals no non-trivial 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 \(n\) \((QKD)\) schemes wherein, in each round the receiver intends to decode a bit string \(x\), which take as input an \(n\) bit Boolean function \(f\). To this end, we introduce sets of \(n\) 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 0s as 1s over its input set.

In this work, we consider \(n \rightarrow 1\) bit Boolean functions which take as input an \(n\) bit string \(x \equiv \{x_1, x_2 \cdots x_n\} \in \{0, 1\}^n\) 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, \(\mathcal{X}_f(x)=0\) \(\equiv \{x \in \{0, 1\}^n \mid f(x) = 0\}\), must be the same as the cardinality of the set of inputs mapped to 1, \(\mathcal{X}_f(x)=1\) \(\equiv \{x \in \{0, 1\}^n \mid f(x) = 1\}\), i.e., \(|\mathcal{X}_f(x)=0| = |\mathcal{X}_f(x)=1| = 2^{n-1}\). 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., \(\forall x \in \{0, 1\}^n\) : \(p(x) = \frac{1}{2^n}\), \(p(f(x) = 0) = p(f(x) = 1) = \frac{1}{2}\). 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 \(\mathcal{X}_{f_1}(x)=0, \mathcal{X}_{f_2}(x)=1\) have equal overlaps with the sets \(\mathcal{X}_{f_1}(x)=0, \mathcal{X}_{f_2}(x)=1\), i.e., \(\forall i, j \in \{0, 1\}\) : \(|\mathcal{X}_{f_1}(x)=0 \cap \mathcal{X}_{f_2}(x)=1| = 2^{n-2}\). This further implies for a uniformly distributed string of inputs \(\forall i, j, k, l \in \{0, 1\}\) : \(p(f_1(x) = i | f_1(x) = j) = p(f_1(x) = k | f_2(x) = l) = \frac{1}{2}\). Next, we define sets of mutually unbiased balanced functions.

Definition 3 (MUBS). A set of functions \(\mathcal{F} = \{f_i\}_{i=1}^{\vert \mathcal{F} \vert}\) 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 \(\mathcal{F}_R^n \equiv \{f_r(x) = \bigoplus_{r_i=1}^n r_i x_i | r \equiv \{r_1, \ldots, r_n\} \in \mathcal{R} \}\) where \(\mathcal{R} \equiv \{r \in \{0, 1\}^n | \sum_i r_i \geq 1\}\) Notice that all functions in the set are balanced, i.e., \(\forall f \in \mathcal{F}_R^n : \mathcal{X}_{f(x)}=0 = |\mathcal{X}_{f(x)}=1| = 2^{n-1}\). Now any two distinct functions \(f_i, f_j \in \mathcal{F}_R^n\) differ by XOR of at least one completely independent bit, and XOR with a random bit obscures all information (one-time pad), 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 \(\mathcal{F}_R^2 = \{x_1, x_2, x_1 \oplus x_2\}\) forms a MUBS. Similarly, for the case of three bit input functions the set \(\mathcal{F}_R^3 = \{x_1, x_2, x_3, x_1 \oplus x_2, x_2 \oplus x_3, x_1 \oplus x_3, x_1 \oplus x_2 \oplus x_3\}\) forms a MUBS. In general, it is easy to see that any non-trivial subset of \(\mathcal{F}_R^n\) forms a MUBS, i.e., the sets \(\mathcal{F}_{R_j}^n \equiv \{f_r(x) = \bigoplus_{r_i=1}^n r_i x_i | r \equiv \{r_1, \ldots, r_n\} \in \mathcal{R}_j \}\) where \(\mathcal{R}_j \subseteq \mathcal{R}\).

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.

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, R_i)-GRAC). An (n, 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 x ∈ {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 their uniformly distributed input y ∈ R_i where R_i ⊆ R ≡ {r ∈ {0, 1}^n | ∑ r_i ≥ 1} and produces an output bit z ∈ {0, 1}. They win a round if z = f_y(x) = ∐_{i=1}^n x_i y_i. They gauge their performance on the basis of their average success probability

s^{(n, R_i)} = \frac{1}{2^n |R_i|} ∑_{x,y} p(z = f_y(x)|x,y).

We note here that the standard (n → 1) random access codes (RACs) form restricted cases of GRACs, specifically when Bob’s input y is uniformly sampled from R_{RAC} ≡ {r ∈ {0, 1}^n | ∑ r_i = 1}. We denote the success probability of (n → 1) RACs by s^{(n→1)}.

In this work, we study three distinct classes of communication protocols for (n, R_i) GRAC,

(i.) A classical communication C protocol for (n, R_i) GRAC is one wherein Alice encodes her input string x onto a bit ω ∈ {0, 1}, based on an encoding scheme E ω of the form {p_E(ω|x)}. Bob decodes the message based on their input to produce the output z employing a decoding scheme D ω of the form {p_D(z|ω,y)}. The average success probability for such a protocol is s^{(n, R_i)}_C = \frac{1}{2^n |R_i|} ∑_{x,y,ω} p_E(ω|x)p_D(z = f_y(x)|ω,y). The maximal classical success probability of (n, R_i) GRAC, s^{(n, R_i)}_C has the expression,

s^{(n, R_i)}_C = \max_{E,D} \left\{ \frac{1}{2^n |R_i|} ∑_{x,y,ω} p_E(ω|x)p_D(z = f_y(x)|ω,y) \right\}.

We note here that, as we are considering average success probability, the parties gain no advantage even 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, R_i) GRAC, without loss of generality, comprise of a deterministic encoding schemes such that ω = f_E(x), and deterministic decoding schemes such that z = f_D(y, ω).

(ii.) A quantum prepare and measure protocol Q for (n, R_i) GRAC entertains Alice encoding her input onto a qubit ρ_x, which is transmitted to Bob. Bob upon receiving the qubit, performs the measurement \{M_i^y : ∑ M_i^y = I\} based on his input y to produce the outcome z. The average success probability for such a protocol has the expression s^{(n, R_i)}_Q = \frac{1}{2^n |R_i|} ∑_{x,y} Tr(ρ_x M_z^y = f_y(x)). The maximal quantum success probability of (n, R_i) GRAC S^{(n, R_i)}_Q has the expression,

S^{(n, R_i)}_Q = \max_{\{ρ_x, \{M_i^y\}\}} \left\{ \frac{1}{2^n |R_i|} ∑_{x,y} Tr(ρ_x M_z^y = f_y(x)) \right\},

where the maximization is over all two dimensional states \{ρ_x\} and two dimensional binary outcome measurements \{M_i^y\}. For maximal average success probability it is enough to consider pure states, i.e., ∀x : ρ_x ≡ |ψ_x⟩⟨ψ_x|, and measurement operators to be projectors, i.e., \{M_i^y \equiv \Pi_i^y ∈ \mathbb{I}\}. This allows us to re-express (2) as,

S^{(n, R_i)}_Q = \max_{\{r_x, \{y\}\}} \left\{ \frac{1}{2^n |R_i|} ∑_{x,y} \frac{1}{2} \left( 1 + (-1) f_y(x) r_x y_i \right) \right\},

where we have used Bloch vector notation for states ρ_x = I + r_x σ_z, and for measurements M_i^y = \frac{1 + (-1) y_i σ_y}{2}, where r_x ∈ R_3, y_i ∈ R_3 are unit vectors, such that ∀x : \|r_x\| = 1, ∀y : \|y\| = 1, and σ_z is the vector of Pauli matrices.

(iii.) An entangled assisted classical communication protocol EACC entails Alice and Bob pre-sharing 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_{i}^y : |ψ_{i}⟩ = \frac{1}{\sqrt{2}} (|0⟩ + (-1)^{y_i} |1⟩)\}, and transmits the outcome ω to Bob. Bob upon receiving the message ω, and his input y performs the binary outcome measurements \{M_i^{ω_y} : ∀ω_i : M_i^{ω_y} = I\} to produce the outcome z. The average success probability for such a protocol has the expression s_{EACC} = \frac{1}{2^n |R_i|} ∑_{x,y,ω} Tr(ρ_{AB} M_i^{ω_y} ⊗ M_z^{ω_y} = f_y(x)). The maximal success probability of EACC protocols in (n, R_i) GRAC, S^{(n, R_i)}_{EACC}, has the expression,

S^{(n, R_i)}_{EACC} = \max_{\{ρ_{AB}, \{M_i^{ω_y}\}\}} \left\{ \frac{1}{2^n |R_i|} ∑_{x,y,ω} Tr(ρ_{AB} M_i^{ω_y} ⊗ M_z^{ω_y} = f_y(x)) \right\}.

A. Bounding success of GRACs

Now we are prepared to present our results for bounding the average success probability of (n, R_i) GRACs.

Theorem 1. The maximal success probability of (n, R_i) GRACs, S^{(n, R_i)}_O, is lower bounded by that of (R_i | 1) RAC, S^{(|R_i| → 1)}_O, i.e.,

S^{(n, R_i)}_O ≥ S^{(|R_i| → 1)}_O,

where O ∈ {C, Q, EACC}.

Proof. To prove the desired thesis we provide a viable strategy for (n, R_i) GRAC which utilizes an optimal (|R_i| → 1) RAC as a subroutine, and achieves success s^{(n, R_i)}_O ≥ S^{(|R_i| → 1)}_O.
Given a \((n, R_i)\) GRAC with the input string \(x = \{x_1, \ldots, x_n\} \in \{0, 1\}^n\), consider the bit string \((f_i(x))_{i \in R_i}\). Notice that, \((f_i(x))_{i \in R_i}\) may not be uniformly distributed. Now, consider a \(|R_i| \rightarrow 1\) RAC with the input string \(\tilde{x} = \{\tilde{x}_1, \ldots, \tilde{x}_{|R_i|}\} \in \{0, 1\}^{|R_i|}\) with maximal success probability \(S_{O}^{(n, R_i)} = \frac{1}{2^{|R_i|}} \sum_{\tilde{z} \in \{0, 1\}^{|R_i|}} \text{Pr}(\tilde{z} = \tilde{x} | \tilde{x}, \tilde{y})\), where \(O \in \{C, Q, EACC\}\) specifies the particular type of the protocol. We use the string \((f_i(x))_{i \in R_i}\) as the input string for the \(|R_i| \rightarrow 1\) RAC, up to optimal reordering, i.e., \(\tilde{x} = \text{Perm}(f_i(x))_{i \in R_i}\). It is easy to see that, this protocol achieves success probability \(S_{O}^{(n, R_i)} \geq S_{O}^{(|R_i| \rightarrow 1)}\), where the inequality is saturated when the optimal strategy of \(|R_i| \rightarrow 1\) RAC has equal success for all inputs, \(\forall \tilde{x} \in \{0, 1\}^{|R_i|}, \frac{1}{2^{|R_i|}} \sum_{\tilde{z} \in \{0, 1\}^{|R_i|}} \text{Pr}(\tilde{z} = \tilde{x} | \tilde{x}, \tilde{y})\) is equal to \(\frac{1}{2^{|R_i|}} \sum_{\tilde{z} \in \{0, 1\}^{|R_i|}} \text{Pr}(\tilde{z} = \tilde{x} | \tilde{x}, \tilde{y})\).

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

\[
S_{Q}^{(n, R_i)} \leq \frac{1}{2} \left( 1 + \frac{1}{\sqrt{|R_i|}} \right),
\]

(6)

**Proof.** We start by recalling that the maximal success probability of prepare and measure protocol for an \((n, R_i)\) GRAC has the expression (3),

\[
S_{Q}^{(n, R_i)} = \max_{\{r_i, \{v_{y}\}\}} \left\{ \frac{1}{2^{|R_i|}} \sum_{xy} \frac{1}{2} \left( 1 + (-1)^{f_i(x)} r_x v_y \right) \right\},
\]

\[
= \frac{1}{2} \left( 1 + \frac{1}{2^{|R_i|}} \right) \max_{\{r_i, \{v_{y}\}\}} \left\{ \sum_{xy} \frac{1}{2} \left( 1 + (-1)^{f_i(x)} r_x v_y \right) \right\}.
\]

(7)

Consequently, finding maximal success probability of prepare and measure protocols in \((n, R_i)\) GRACs effectively boils down to solving the following optimization problem,

\[
\Phi(n, |R_i|) = \max_{\{r_i, \{v_{y}\}\}} \left\{ \Phi_{n, |R_i|}(\{r_i, \{v_{y}\}\}) \right\},
\]

\[
= \max_{\{v_{y}\}} \left\{ \sum_{r_i} \max_{y} \left\{ (-1)^{f_i(x)} r_x v_y \right\} \right\}.
\]

(8)

Defining, \(V_x = \sum_y (-1)^{f_i(x)} v_y\), we notice that the scalar product \(r_x V_x\) is maximized when \(r_x\) has the same direction as \(V_x\), i.e., when \(r_x = V_x / \|V_x\|\), which implies \(r_x V_x = \|V_x\|\). This observation allows us to re-express (8) as,

\[
\Phi(n, |R_i|) = \max_{\{v_{y}\}} \left\{ \sum_{x} \left\| \sum_{y} (-1)^{f_i(x)} v_y \right\| \right\}.
\]

(9)

We now further rewrite the equation (9) as,

\[
\Phi(n, |R_i|) = \max_{\{v_{y}\}} \left\{ \sum_{x} \left\| \sum_{y} \tilde{g}_y(x) v_y \right\| \right\};
\]

\[
\Phi_{n, |R_i|}(\{v_{y}\}) \equiv \sum_{x} \left\| \sum_{y} \tilde{g}_y(x) v_y \right\|,
\]

(10)

where \(\tilde{g}_y(x) = (-1)^{f_i(x)}\). Now, \(\Phi_{n, |R_i|}(\{v_{y}\})\) can be thought as the dot product between \(z = (1, 1, \ldots, 1) \in \mathbb{R}^n\) and \(w = (\left\| \sum_y \tilde{g}_y(x_1) v_y \right\|, \ldots, \left\| \sum_y \tilde{g}_y(x_2^n) v_y \right\|) \in \mathbb{R}^n\), where \(x_1 = (0, 0, \ldots, 0), \ldots, x_2^n = (1, 1, \ldots, 1)\). Now recall that Cauchy-Schwarz inequality implies,

\[
\Phi_{n, |R_i|}(\{v_{y}\}) = z \cdot w \leq \|z\| \|w\|.
\]

(11)

Now observe that,

\[
\|w\|^2 = \sum_x \left\| \sum_y \tilde{g}_y(x) v_y \right\|^2 = \sum_x \left( \sum_y \tilde{g}_y(x) v_y \cdot \tilde{g}_y(x) v_y' \right).
\]

(12)

There are two types of terms that appear in the sum in (12), (i) whenever \(y = y'\), in this case \(\forall y \in R_i, \tilde{g}_y(x) v_y \cdot \tilde{g}_y(x) v_y' = \|v_y\|^2\), (ii) whenever \(y \neq y'\), we have terms of the form \(\tilde{g}_y(x) \tilde{g}_y(x) v_y \cdot v_{y'}^*\). Now as all functions in our MUBs are balanced and pairwise mutually unbiased, there exits \(2^n-1\) strings \(x \in (X_{f_y=0} \cap X_{f_y'=0}) \cup (X_{f_y=1} \cap X_{f_y'=1})\) for which the coefficients \(\tilde{g}_y(x) \tilde{g}_y(x) v_y = 1\), and there exists \(2^n-1\) strings \(x \in (X_{f_y=0} \cap X_{f_y'=1}) \cup (X_{f_y=1} \cap X_{f_y'=0})\) for which the coefficients \(\tilde{g}_y(x) \tilde{g}_y(x) v_y = -1\). Consequently, all terms of the form (ii) cancel out, and we are left with,

\[
\|w\|^2 = \sum_{x \in \{0, 1\}^n, y \in R_i} \|v_y\|^2 = 2^n \|\tilde{r}\|,
\]

\[
\implies \|w\| = \sqrt{2^n \|\tilde{r}\|}.
\]

(13)

Since \(\|z\| = \sqrt{2^n}\), we have \(\Phi_{n, |R_i|}(\{v_{y}\}) \leq 2^n \sqrt{|R_i|}\), which when plugged back in (10) and (7) yields the desired thesis,

\[
S_{Q}^{(n, R_i)} \leq \frac{1}{2} \left( 1 + \frac{2^n \sqrt{|R_i|}}{2^n \|\tilde{r}\|} \right) = \frac{1}{2} \left( 1 + \frac{1}{\sqrt{|R_i|}} \right).
\]

(14)

**Theorem 3.** The maximal success probability of an EACC protocol in an \((n, R_i)\) GRAC, \(S_{EACC}^{(n, R_i)}\), is upper bounded by the maximum quantum value of the following Bell expression \(\Phi_{EACC}^{(n, R_i)}\), i.e., \(S_{EACC}^{(n, R_i)} \leq \Phi_{EACC}^{(n, R_i)}\)

\[
\Phi_{EACC}^{(n, R_i)} \equiv \frac{1}{2^n |R_i|} \sum_{x, y, y' \in \{0, 1\}} p(u = y, v = f_i(x)|x, y, y'),
\]

(15)
where \( x \in \{0, 1\}^n \) is Alice’s input, \((y_0 \in \{0, 1\}, y \in |R_i|)\) 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 \((n, R_i)\) GRAC achieving success probability \( S_{EACC}^{(n, R_i)} = \frac{1}{2^n|R_i|} \sum_{x,y,u} \text{Tr}(\rho_{AB} M^x_i \otimes M^u_j f(x)) \), 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 \((n, R_i)\) GRAC entails a pre-shared entangled state \( \rho_{AB} \), local measurements for Alice \( \{ M^x \} \), and local measurements for Bob \( \{ M^u \} \), where Alice’s output \( w \) 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 \( M^u_j \) he performs on his part of the entangled state. Finally, Bob relabels his output as \( v = \omega \). As a result, they obtain the correlation \( p(u, v|x, y_0, y) = \text{Tr}(\rho_{AB} M^x_i \otimes M^u_j f(x)) \). Clearly, this correlation because of the construction achieves the Bell value

\[
B_Q^{(n, R_i)} = \frac{1}{2^n|R_i|} \sum_{x,y,u} \text{Tr}(\rho_{AB} M^x_i \otimes M^u_j f(x)) = \frac{1}{2^n|R_i|} \sum_{x,y,u} \text{Tr}(\rho_{AB} M^x_i \otimes M^u_j f(x)) = \frac{1}{2^n|R_i|} \sum_{x,y,u} \text{Tr}(\rho_{AB} M^x_i \otimes M^u_j f(x)) = S_{EACC}^{(n, R_i)}
\]

Therefore, the maximum Bell value of the Bell expression (15), \( B_Q^{(n, R_i)} \) caps the success probability of EACC protocols in \((n, R_i)\) GRAC, \( S_{EACC}^{(n, R_i)} \).

**IV. \( n = 3 \): A CASE STUDY**

In this section, we study and characterize \((n = 3, R_i)\) 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 \((n = 3, R_i)\) GRACs, Alice encodes her input string \( x \in \{0, 1\}^3 \) onto a classical bit message \( \omega \in \{0, 1\} \), based on a deterministic encoding scheme \( E \), \( \omega = f_E(x) \). On the other end, Bob upon receiving \( \omega \) from Alice, decodes it to produce his output \( z = f_D(y, \omega) \) based on a deterministic decoding scheme \( D \). The optimal classical strategy for \((n \to 1)\) RACs, without loss of generality, turns out to be majority encoding, i.e., \( \omega = \text{maj}(x_1, \ldots, x_3) \), and identity decoding, i.e., \( \omega = \omega \) \([30, 31]\). However, as we demonstrate below, this strategy may not be optimal for \((n = 3, R_i)\) GRACs.

| \( x \) | \( \omega = \text{maj}(x_1, x_2, x_3) \) | \( \omega = x_1 \land \neg(x_2 \land x_3) \) | \( |x_1| \) | \( |x_2| \) | \( |x_3| \) | \( |x_1 \oplus x_2| \) | \( |x_1 \oplus x_3| \) | \( |x_2 \oplus x_3| \) |
|---|---|---|---|---|---|---|---|---|
| (000) | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| (001) | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 |
| (010) | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 1 |
| (011) | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 0 |
| (100) | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 0 |
| (101) | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 1 |
| (110) | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 0 |
| (111) | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 1 |

Table I. (Color online) Explicit comparison of classical strategies, (i.) majority-encoding and identity-decoding (green), and (ii.) An encoding strategy entailing \( \omega = x_1 \land \neg(x_2 \land x_3) \), along with the decoding scheme entailing producing \( z = \omega \oplus 1 \) whenever Bob is asked to guess \( x_2, x_3 \), or \( x_1 \oplus x_2 \oplus x_3 \), and \( z = \omega \) otherwise, for \((n = 3, R_i)\) GRAC. We also enlist the guess probability for the functions \( f_j \in \mathcal{F}^R_i \) in the bottom row, for the ease of access. The asterisk (*) indicates the use of inverse identity decoding, i.e., \( z = \omega \oplus 1 \) for the particular function.

**Observation 1.** Unlike \((n \to 1)\) RAC, majority encoding and identity decoding is not optimal for all \((n = 3, R_i)\) GRACs,

**Proof.** To prove this thesis, we shall consider the \((n = 3, R_i)\) GRAC which entails the entire MUBS \( \mathcal{F}^R_i \). For this task, the majority encoding, i.e., \( \omega = \text{maj}(x_1, x_2, x_3) \),
Table II. The maximal classical success probability of \((n = 3, R)\) GRACs, \(S^{(n, R)}_C\), listed along with the number of MUBFs Bob’s required to guess. These values are contrasted against the maximal success probability of standard \((n = |R| \rightarrow 1)\) RACs, \(S^{(|R| \rightarrow 1)}_C\), 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 the surprising feature of GRACs termed harder the task, greater the payoff (see Observation 3).

| | \(S^{(|R| \rightarrow 1)}_C\) | \(S^{(n, R)}_C\) |
|---|---|---|
| 2 | \(\frac{3}{4} = 0.75\) | \(\frac{3}{4} = 0.75\) |
| 3 | \(\frac{3}{4} = 0.75\) | \(\frac{3}{4} = 0.75\) |
| 4 | \(\frac{11}{16} = 0.6875\) | \(\frac{3}{4} = 0.75\) |
| 5 | \(\frac{11}{16} = 0.6875\) | \(\frac{11}{16} = 0.6875\) |
| 6 | \(\frac{21}{32} = 0.65625\) | \(\frac{2}{3} \approx 0.67\) |
| 7 | \(\frac{21}{32} = 0.65625\) | \(\frac{37}{56} \approx 0.66\) |

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

**Observation 3.** [Harder the task, greater the payoff] In the case of four questions, \(|R| = 4\), and \(\exists x \in \{0, 1\}^3 : f_1(x) \oplus f_j(x) \neq f_k(x) \oplus f_l(x)\), 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 \((n = 3, R)\) GRACs. We employed standard see-saw semi-definite programming technique to obtain lower bounds on maximal success probability of such protocols. Additionally, we employed the
Table III. The maximal quantum success probability of prepare and measure qubit protocols for \((n=|\mathcal{R}_i|\to 1)\) RACs, \(S^{|\mathcal{R}_i|\to 1}_Q\), listed along with the number of MUBFs Bob is required to guess. These values are contrasted against the maximal quantum success probability of standard \((n=|\mathcal{R}_i|\to 1)\) RACs, \(S^{(3,|\mathcal{R}_i|)}_Q\), which form lower bounds for the former according to Theorem 1. All values were obtained upon coincidence (upto numerical precision) of lower bounds obtained from see-saw semi-definite programming method, and upper bounds obtained via Navascues-Vertesi hierarchy of semidefinite programming relaxations, along with retrieval of explicit quantum protocols. In all cases expect when \(|\mathcal{R}_i|=4\), notice that the maximal quantum success probabilities saturate the upper-bounds, \(\frac{1}{2} \left(1 + \frac{1}{\sqrt{|\mathcal{R}_i|}}\right)\), 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 general qubit protocols go beyond the classical bound, \(\frac{11}{16} = 0.6875\), but saturate the maximal success probability of qubits for \((4 \to 1)\) RAC, \(\frac{1}{2} \left(1 + \frac{\sqrt{2} + \sqrt{5}}{8}\right)\approx 0.74\).

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 Appendix Section V).

1. 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 \(\Lambda : L(\mathcal{H}_{in}) \to L(\mathcal{H}_{out})\), where \(L(\mathcal{X})\) be the set of linear operators acting on the Hilbert space \(\mathcal{X}\); \(\mathcal{H}_{in} & \mathcal{H}_{out}\) respectively denote input and output Hilbert space of the map \(\Lambda\) [32–34]. Since we are considering qubit communication therefore we have \(\mathcal{H}_{in} = \mathcal{H}_{out} = \mathbb{C}^2\). Furthermore, a channel is known to be unital if completely mixed state remains invariant under it. In the following we analyze effect of the following two unital qubit channels [33, 34] on the performance of qubit prepare and measure protocols.

(a.) Depolarising channel: The effect of a depolarizing channel \(\Phi_{Depol}^\lambda\) is to keep the input state intact with probability \((1-\lambda)\), while with probability \(\lambda\) an ‘error’ occurs entirely replacing the input state by white noise, i.e., a generic initial state \(\rho_{in} = \frac{1}{2} \mathbb{1}\) is distorted to,

\[
\rho_{out} = \Phi_{Depol}^\lambda(\rho_{in}) = \lambda \mathbb{1} + (1-\lambda)\rho_{in},
\]

where \(\lambda \in [0,1]\) is the noise parameter. Now, for qubits, increasing the noise parameter \(\lambda\) shrinks the Bloch sphere uniformly, so it is enough to consider

![Figure 1](image1.png)

Figure 1. The maximal quantum success probability of \((n=3,|\mathcal{R}_i|)\) GRAC with \(|\mathcal{R}_i| = \{4,5\}\) in presence of dephasing channel with noise parameter \(\lambda\). 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 exceeds that of \((n=3,|\mathcal{R}_i|)\) GRAC with five MUBFs, which is yet another instance of harder the task, greater the payoff.

![Figure 2](image2.png)

Figure 2. The ratio of maximal quantum success probability to maximal classical success probability, \(R_{0/C} = \frac{S^{(3,|\mathcal{R}_i|)}_Q}{S^{(3,|\mathcal{R}_i|)}_C}\), for \((n=3,|\mathcal{R}_i|)\) GRACs with \(|\mathcal{R}_i| = \{2,7\}\) plotted against \(1-\lambda\) where \(\lambda\) is the noise parameter of the dephasing channel.
Table IV. Threshold value of the noise parameter $\lambda_{\text{crit}}$ for depolarizing channel, such that we can retrieve the quantum advantage in $n = 3, R_i$ GRACs. Note that for $|R_i| = 4$ we considered only the cases for which $f_i \oplus f_j \neq f_k \oplus f_l$. Consequently, we observe that for $|R_i| = 3$ the noise threshold is lower than that of $|R_i| = 5, 6, 7$, which forms yet another instance of harder the task, greater the payoff.

| $|R_i|$ | $S_{\text{EACC}}^{(|R_i|-1)}$ | $S_{\text{EACC}}^{(3, R_i)}$ |
|-------|-----------------|-----------------|
| 2     | $\frac{1}{2} (1 + \frac{1}{\sqrt{2}})$ $\approx$ 0.85 | $\frac{1}{2} (1 + \frac{1}{\sqrt{2}})$ $\approx$ 0.85 |
| 3     | $\frac{1}{2} (1 + \frac{1}{\sqrt{3}})$ $\approx$ 0.78 | $\frac{1}{2} (1 + \frac{1}{\sqrt{3}})$ $\approx$ 0.78 |
| 4     | $\frac{1}{2} (1 + \frac{\sqrt{2} + \sqrt{5}}{4})$ $\approx$ 0.74 | $\frac{1}{2} (1 + \frac{1}{\sqrt{4}}) = $ 0.75 |
| 5     | $\approx$ 0.7135 | $\frac{1}{2} (1 + \frac{1}{\sqrt{5}})$ $\approx$ 0.72 |
| 6     | $\approx$ 0.6940 | $\frac{1}{2} (1 + \frac{1}{\sqrt{6}})$ $\approx$ 0.70 |
| 7     | $\approx$ 0.6786 | $\frac{1}{2} (1 + \frac{1}{\sqrt{7}})$ $\approx$ 0.69 |

Table V. The maximal quantum success probability of entanglement assisted one bit communication protocols for $(3, R_i)$ GRACs, $S_{\text{EACC}}^{(3, R_i)}$, listed along with the number of MUBFs $x$ required to guess. These values are contrasted against the maximal quantum success probability of standard $(n = |R_i| \rightarrow 1)$ RACs, $S_{\text{EACC}}^{(|R_i|-1)}$, which form lower bounds for the former according to Theorem 1. All values were obtained upon coincidence of lower bounds obtained from see-saw semi-definite programming method, and upper bounds obtained 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 $\frac{1}{2} \left( 1 + \frac{1}{\sqrt{|R_i|}} \right)$.

the noisy versions of the optimal preparations we recovered above. In the Table IV we list the threshold value of the noise parameter $\lambda$ such that we can retrieve a quantum advantage in $(n = 3, R_i)$ GRACs. Yet again, we witness the reappearance of the characteristic phenomenon of GRACs, namely, harder the task, greater the payoff, as the noise threshold $\lambda_{\text{crit}}$ in the cases with $|R_i| = 5, 6, 7$ MUBFs exceeds that of $|R_i| = 3$.

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

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

where $\lambda \in [0, 1]$ is the noise parameter. Unlike the depolarising channel, here, the optimal quantum strategy, always performs as well as the optimal classical strategy. Therefore, in Fig. 2 we plot the ratio optimal quantum success probability to that of maximal classical success probability, $R_{Q/C} = \frac{S_{Q}^{(n=3, R_i)}}{S_{C}^{(n=3, R_i)}}$, for different numbers of MUBFs, wherein we employed a bit-flip channel, i.e. $n \equiv [1,0,0]^T$, 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 $(n = 3, R_i)$ GRAC with four MUBFs exceeds that of $(n = 3, R_i)$ GRAC with five MUBFs (see Fig. 1).

### C. Entanglement assisted classical communication

Finally, we investigate the performance of shared entanglement and cbit communication protocols. Again, we employ standard see-saw semi-definite 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 super-dense coding protocol [2] (see also [35]). Moreover, it has also been shown that entanglement, more generally nonlocal correlations, can increase the zero-error capacity [36, 37] of a noisy classical channel [38, 39]. More strikingly, as established recently, entanglement can empower even a noiseless classical channel [40]. 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 $\exists x : f_i(x) \oplus f_j(x) \neq f_k(x) \oplus f_l(x)$, entanglement assisted classical communication protocols can outperform the prepare and measure qubit protocols.

### V. DISCUSSIONS AND OUTLOOK

We introduce 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 [41], wherein the authors also consider a generaliz-
ation 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 fixed size of the sender’s input bits. Manifestly, the generalization considered in this work differs from that considered in [41]. 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 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 sender’s input data comprising of three independently distributed bits.

This work motivated 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 the for axiomatic derivation of Hilbert space quantum mechanics research have initiated the study of generalized probability theories (GPT) [42–46]. The seminal two-party-two-input-two-output $(2 \rightarrow 2 \rightarrow 2)$ Popescu-Rohrlich (PR) correlation [47] 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 as the marginal state space of the set of all $2 \rightarrow 2 \rightarrow 2$ no-signaling correlations. A particular generalization of this Box world is the polygon model where state spaces are described by symmetric polygons [48] which has been studied extensively in the recent past [49–56]. 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 $x \equiv x_1 \cdots x_n \in \{0, 1, \ldots, d - 1\}^n$ [21, 31, 57]. 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

MB acknowledges research grant of INSPIRE-faculty fellowship from the Department of Science and Technology, Government of India. AC acknowledges financial support by NCN grant SHENG 2018/30/Q/ST2/00625. The numerical optimization was carried out using Ncpol2sdpa [58], YALMIP [59] and SDPT3 [60].
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 \(\mathcal{R}_i \subset \mathcal{R}_r\), \(|\mathcal{R}_i| = 2\) are equivalent up to a reordering of the input strings. We give an explicit example using \(\mathcal{F}^3_{\mathcal{R}_i} = \{x_1, x_2\}\). 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 \((2 \rightarrow 1)\) RAC. Recall that, optimal quantum protocol for \((2 \rightarrow 1)\) is given by,

\[
\begin{align*}
\text{Alice’s encoding: } & \{0,1\}^2 \ni x_1x_2 \mapsto \rho_{x_1x_2} \\
& \begin{cases} 00 \mapsto \frac{1}{2} \left( I + \frac{1}{\sqrt{2}} \sigma_x + \frac{1}{\sqrt{2}} \sigma_y \right) \\
01 \mapsto \frac{1}{2} \left( I + \frac{1}{\sqrt{2}} \sigma_x - \frac{1}{\sqrt{2}} \sigma_y \right) \\
10 \mapsto \frac{1}{2} \left( I - \frac{1}{\sqrt{2}} \sigma_x + \frac{1}{\sqrt{2}} \sigma_y \right) \\
11 \mapsto \frac{1}{2} \left( I - \frac{1}{\sqrt{2}} \sigma_x - \frac{1}{\sqrt{2}} \sigma_y \right)
\end{cases}
\end{align*}
\]
e.g., \(\{10\} \mapsto v_1 = \frac{1}{2} (I + \sigma_y)\), \(\{01\} \mapsto v_2 = \frac{1}{2} (I - \sigma_y)\).

Bob will guess the bit value as ‘0’ whenever he obtains \(’+1’\) outcome, otherwise he guess the value as ‘1’. To make this protocol work for an arbitrary \(\mathcal{F}^n_{\mathcal{R}_i} = \{f_q, f_r\}\), Alice follows the encoding \(f_q^i \cap f_r^j \mapsto |\psi\rangle_{x_1x_2}\) and Bob performs the measurement \(M_i\) 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 \(\frac{1}{2} \left( 1 + \frac{1}{\sqrt{2}} \right)\).

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

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

Alice’s encoding:

\[
\begin{align*}
\{x_1x_2x_3\} \mapsto \rho_{x_1x_2x_3} \\
e.g. & \frac{1}{2} \left( I + \frac{1}{\sqrt{3}} \sigma_x + \frac{1}{\sqrt{3}} \sigma_y + \frac{1}{\sqrt{3}} \sigma_z \right) \\
& \frac{1}{2} \left( I - \frac{1}{\sqrt{3}} \sigma_x - \frac{1}{\sqrt{3}} \sigma_y - \frac{1}{\sqrt{3}} \sigma_z \right).
\end{align*}
\]
Bob’s decoding: $M_i \equiv \begin{cases} \frac{1}{2}(I + v_i,\sigma), & \frac{1}{2}(I - v_i,\sigma) \end{cases}$

e.g. $x_1 \rightarrow v_1 \equiv (1,0,0)$
$x_2 \rightarrow v_2 \equiv (0,1,0)$
$x_3 \rightarrow v_3 \equiv (0,0,1)$.

Case-(ii): If $f_i \oplus f_i = f_i$, then every such set is equivalent to the set $F_{R_i}^3 = \{x_1, x_2, x_1 \oplus x_2\}$.

Alice’s encoding:

$\begin{cases} 
\{000,001\} \rightarrow \frac{1}{2} \left( I + \frac{1}{\sqrt{3}} \sigma_x + \frac{1}{\sqrt{6}} \sigma_y + \frac{1}{\sqrt{6}} \sigma_z \right) \\
\{010,011\} \rightarrow \frac{1}{2} \left( I + \frac{1}{\sqrt{3}} \sigma_x + \frac{1}{\sqrt{6}} \sigma_y - \frac{1}{\sqrt{6}} \sigma_z \right) \\
\{001,010\} \rightarrow \frac{1}{2} \left( I - \frac{1}{\sqrt{3}} \sigma_x + \frac{1}{\sqrt{6}} \sigma_y - \frac{1}{\sqrt{6}} \sigma_z \right) \\
\{100,101\} \rightarrow \frac{1}{2} \left( I - \frac{1}{\sqrt{3}} \sigma_x - \frac{1}{\sqrt{6}} \sigma_y + \frac{1}{\sqrt{6}} \sigma_z \right).
\end{cases}$

Bob’s decoding: $M_i \equiv \begin{cases} \frac{1}{2}(I + v_i,\sigma), & \frac{1}{2}(I - v_i,\sigma) \end{cases}$

e.g. $x_1 \rightarrow v_1 \equiv (1,0,0)$
$x_2 \rightarrow v_2 \equiv (0,1,0)$
$x_1 \oplus x_2 \rightarrow v_{12} \equiv (0,0,1)$.

Figure 5. ($|\mathcal{R}_i| = 3$) Optimal Encoding protocol for $F_{R_i}^3 = \{f_i, f_i, f_i\}$ with $f_i \oplus f_i = f_i$. Black dots denote the encoded states of Eq.(18). They form the vertices of a regular tetrahedron. For evaluating the function $x_a \in \{x_1, x_2, x_3, x_1 \oplus x_2\}$, Bob performs the measurement $M_a \equiv \begin{cases} \frac{1}{2}(I + v_a,\sigma), & \frac{1}{2}(I - v_a,\sigma) \end{cases}$ on the received state and guess the function value as ‘0’ if he obtains outcome ‘+1’, otherwise guess the value as ‘1’. He chooses $v_1 = (1,0,0) = v_2$, $v_3 = (0,1,0)$, and $v_{12} = (0,0,1)$.

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

Alice’s encoding:

$\begin{cases} 
000 \rightarrow \frac{1}{2} \left( I + \sqrt{\frac{2}{3}} \sigma_x + \frac{1}{\sqrt{6}} \sigma_y + \frac{1}{\sqrt{6}} \sigma_z \right) \\
001 \rightarrow \frac{1}{2} \left( I + \sqrt{\frac{2}{3}} \sigma_x - \frac{1}{\sqrt{6}} \sigma_y + \frac{1}{\sqrt{6}} \sigma_z \right) \\
010 \rightarrow \frac{1}{2} \left( I + \frac{1}{\sqrt{6}} \sigma_y - \frac{1}{\sqrt{6}} \sigma_z \right) \\
011 \rightarrow \frac{1}{2} \left( I + \frac{1}{\sqrt{6}} \sigma_y + \frac{1}{\sqrt{6}} \sigma_z \right) \\
100 \rightarrow \frac{1}{2} \left( I - \frac{1}{\sqrt{3}} \sigma_x + \frac{1}{\sqrt{6}} \sigma_y + \frac{1}{\sqrt{6}} \sigma_z \right) \\
101 \rightarrow \frac{1}{2} \left( I - \frac{1}{\sqrt{3}} \sigma_x - \frac{1}{\sqrt{6}} \sigma_y + \frac{1}{\sqrt{6}} \sigma_z \right) \\
110 \rightarrow \frac{1}{2} \left( I - \frac{1}{\sqrt{3}} \sigma_x + \frac{1}{\sqrt{6}} \sigma_y + \frac{1}{\sqrt{6}} \sigma_z \right) \\
111 \rightarrow \frac{1}{2} \left( I - \frac{1}{\sqrt{3}} \sigma_x - \frac{1}{\sqrt{6}} \sigma_y + \frac{1}{\sqrt{6}} \sigma_z \right). \\
\end{cases}$

Bob’s decoding: $M_i \equiv \begin{cases} \frac{1}{2}(I + v_i,\sigma), & \frac{1}{2}(I - v_i,\sigma) \end{cases}$

e.g. $x_1 \rightarrow v_1 \equiv (1,0,0)$
$x_2 \rightarrow v_2 \equiv v_1$
$x_3 \rightarrow v_3 \equiv (0,1,0)$
$x_1 \oplus x_2 \rightarrow v_{12} \equiv (0,0,1)$.

This protocol yields the average success probability $\frac{1}{2} \left( 1 + \sqrt{\frac{2}{3}} + \sqrt{\frac{2}{3}} \right)$. Note that the average success is still less than $3/4$. However, up to numerical precision, the lower
bound obtained from see-saw semi-definite programming method, and upper bounds obtained via Navascues-Vertesi hierarchy of semidefinite relaxations is same as the value obtained with the present explicit protocol (see Table III).

(D) \(|\mathcal{R}_i| = 5\): Let us consider a particular case \(\mathcal{F}_3^{\mathcal{R}_i} \equiv \{x_1, x_2, x_3, x_1 \oplus x_2, x_1 \oplus x_3\}\).

Alice’s encoding (non-planar):

| Encoding | Encoding (non-planar) |
|----------|-----------------------|
| 000      | \(\frac{1}{2}(I + \frac{1}{\sqrt{3}}\sigma_x + \frac{2}{\sqrt{3}}\sigma_z)\) |
| 001      | \(\frac{1}{2}(I + \frac{1}{\sqrt{3}}\sigma_x + \frac{2}{\sqrt{3}}\sigma_y)\) |
| 010      | \(\frac{1}{2}(I + \frac{1}{\sqrt{3}}\sigma_x - \frac{2}{\sqrt{3}}\sigma_y)\) |
| 011      | \(\frac{1}{2}(I + \frac{1}{\sqrt{3}}\sigma_x - \frac{2}{\sqrt{3}}\sigma_z)\) |
| 100      | \(\frac{1}{2}(I - \frac{1}{\sqrt{3}}\sigma_x + \frac{2}{\sqrt{3}}\sigma_y)\) |
| 101      | \(\frac{1}{2}(I - \frac{1}{\sqrt{3}}\sigma_x - \frac{2}{\sqrt{3}}\sigma_z)\) |
| 110      | \(\frac{1}{2}(I - \frac{1}{\sqrt{3}}\sigma_x + \frac{2}{\sqrt{3}}\sigma_z)\) |
| 111      | \(\frac{1}{2}(I - \frac{1}{\sqrt{3}}\sigma_x - \frac{2}{\sqrt{3}}\sigma_z)\) |

e.g. \(x_1 \rightarrow v_1 \equiv (1, 0, 0)\) 

Bob’s decoding: \(M_i \equiv \left\{\frac{1}{2}(I + v_i, \sigma), \frac{1}{2}(I - v_i, \sigma)\right\}\)

A straightforward calculation yields the average success probability \(\frac{1}{2} \left(1 + \frac{\sqrt{3}}{2}\right)\) 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. 8). We, however, find that a different strategy where the encoded states lie on a great circle (Fig. 8) but yields the maximum success.

Alice’s encoding (planar):

| Encoding | Encoding (planar) |
|----------|-------------------|
| 000      | \(\frac{1}{2}(I + \frac{1}{\sqrt{3}}\sigma_x + \frac{2}{\sqrt{3}}\sigma_y)\) |
| 010      | \(\frac{1}{2}(I + \frac{1}{\sqrt{3}}\sigma_x - \frac{2}{\sqrt{3}}\sigma_y)\) |
| 011      | \(\frac{1}{2}(I + \frac{1}{\sqrt{3}}\sigma_x - \frac{2}{\sqrt{3}}\sigma_z)\) |
| 100      | \(\frac{1}{2}(I - \frac{1}{\sqrt{3}}\sigma_x + \frac{2}{\sqrt{3}}\sigma_y)\) |
| 101      | \(\frac{1}{2}(I - \frac{1}{\sqrt{3}}\sigma_x + \frac{2}{\sqrt{3}}\sigma_z)\) |
| 110      | \(\frac{1}{2}(I - \frac{1}{\sqrt{3}}\sigma_x - \frac{2}{\sqrt{3}}\sigma_z)\) |
| 111      | \(\frac{1}{2}(I - \frac{1}{\sqrt{3}}\sigma_x - \frac{2}{\sqrt{3}}\sigma_y)\) |

e.g. \(x_1 \rightarrow v_1 \equiv (1, 0, 0)\) 

Bob’s decoding: \(M_i \equiv \left\{\frac{1}{2}(I + v_i, \sigma), \frac{1}{2}(I - v_i, \sigma)\right\}\)

(e) \(\mathcal{F}_3^{\mathcal{R}_i} (|\mathcal{R}_i| = 6)\): Let us consider a particular case \(\mathcal{F}_3^{\mathcal{R}_i} \equiv \{x_1, x_2, x_3, x_1 \oplus x_2, x_1 \oplus x_3, x_2 \oplus x_3\}\).
Figure 9. \(|R_i| = 6\) Encoded states and decoding measurements corresponding the optimal quantum protocol for \(F_2^3 \equiv \{x_1, x_2, x_3, x_1 \oplus x_2, x_1 \oplus x_3, x_2 \oplus x_3\}\).

Alice’s encoding (planar):

\[
\begin{align*}
000 \mapsto & \frac{1}{2} \left( I + \frac{\sqrt{3}}{2} \sigma_x + \frac{1}{\sqrt{6}} \sigma_y + \frac{1}{\sqrt{6}} \sigma_z \right) \\
001 \mapsto & \frac{1}{2} \left( I - \frac{\sqrt{3}}{2} \sigma_x + \frac{1}{\sqrt{6}} \sigma_y - \frac{1}{\sqrt{6}} \sigma_z \right) \\
010 \mapsto & \frac{1}{2} \left( I + \frac{\sqrt{3}}{2} \sigma_x - \frac{1}{\sqrt{6}} \sigma_y + \frac{1}{\sqrt{6}} \sigma_z \right) \\
011 \mapsto & \frac{1}{2} \left( I + \frac{\sqrt{3}}{2} \sigma_x - \frac{1}{\sqrt{6}} \sigma_y - \frac{1}{\sqrt{6}} \sigma_z \right) \\
100 \mapsto & \frac{1}{2} \left( I - \frac{\sqrt{3}}{2} \sigma_x - \frac{1}{\sqrt{6}} \sigma_y + \frac{1}{\sqrt{6}} \sigma_z \right) \\
101 \mapsto & \frac{1}{2} \left( I - \frac{\sqrt{3}}{2} \sigma_x - \frac{1}{\sqrt{6}} \sigma_y - \frac{1}{\sqrt{6}} \sigma_z \right) \\
110 \mapsto & \frac{1}{2} \left( I - \frac{\sqrt{3}}{2} \sigma_x + \frac{1}{\sqrt{6}} \sigma_y + \frac{1}{\sqrt{6}} \sigma_z \right) \\
111 \mapsto & \frac{1}{2} \left( I + \frac{\sqrt{3}}{2} \sigma_x + \frac{1}{\sqrt{6}} \sigma_y - \frac{1}{\sqrt{6}} \sigma_z \right)
\end{align*}
\]

e.g.

Bob’s decoding: \(M_i \equiv \left\{ \frac{1}{2}(I + v_i \sigma), \frac{1}{2}(I - v_i \sigma) \right\}\)

\[
\begin{align*}
\begin{cases}
  x_1 \rightarrow v_1 \equiv (1, 0, 0) \\
  x_3 \rightarrow v_3 \equiv (0, 0, 1) \\
  x_1 \oplus x_2 \rightarrow v_{12} \equiv (0, 1, 0) \\
  x_2 \rightarrow v_2 \equiv -v_1 \\
  x_1 \oplus x_3 \rightarrow v_{13} \equiv v_1 \\
  x_2 \oplus x_3 \rightarrow v_{23} \equiv v_1.
\end{cases}
\end{align*}
\]

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

\[\text{References}\]

[1] C. E. Shannon, The Bell System Technical Journal 27, 379 (1948).
[2] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. 69, 2881 (1992).
[3] A. S. Holevo, Problemy Peredachi Informatsii 9, 3 (1973).
[4] P. E. Frenkel and M. Weiner, Communications in Mathematical Physics 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 (1999) pp. 376–383.
[7] A. Ambainis, A. Nayak, A. Ta-Shma, and U. Vazirani, J. ACM 49, 496–511 (2002).
[8] H. Buhrman, R. Cleve, S. Massar, and R. de Wolf, Rev. Mod. Phys. 82, 665 (2010).
[9] H. Klauck, in Proceedings 42nd IEEE Symposium on Foundations of Computer Science (IEEE, 2001) pp. 288–297.
[10] I. Kerenidis and R. De Wolf, Journal of Computer and System Sciences 69, 395 (2004).
[11] S. Aaronson, in Proceedings. 19th IEEE Annual Conference on Computational Complexity, 2004. (IEEE, 2004) pp. 320–332.
[12] S. Wehner and R. De Wolf, in International Colloquium on Automata, Languages, and Programming (Springer, 2005) pp.
1424–1436.

[13] D. Gavinsky, J. Kempe, O. Regev, and R. De Wolf, SIAM Journal on Computing 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, 2007) pp. 610–621.

[15] R. W. Spekkens, D. H. Buzacott, A. J. Kehnh, B. Toner, and G. J. Pryde, Physical review letters 102, 010401 (2009).

[16] M. Banik, S. S. Bhattacharya, A. Mukherjee, A. Roy, A. Ambainis, and A. Rai, Physical Review A 92, 030103 (2015).

[17] A. Chailloux, I. Kerenidis, S. Kundu, and J. Sikora, New Journal of Physics 18, 045003 (2016).

[18] A. Hameedi, A. Tavakoli, B. Marques, and M. Bourennane, Physical review letters 119, 220402 (2017).

[19] S. Ghora and A. Pan, Physical Review A 98, 032110 (2018).

[20] D. Saha and A. Chaturvedi, Physical Review A 100, 022108 (2019).

[21] A. Ambainis, M. Banik, A. Chaturvedi, D. Kravchenko, and A. Rai, Quantum Information Processing 18, 1 (2019).

[22] A. Chaturvedi and D. Saha, Quantum 4, 345 (2020).

[23] M. Pawłowski and M. Zukowski, Physical Review 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. Zukowski, Nature 461, 1101 (2009).

[26] S. W. Al-Safi and A. J. Short, Physical Review A 84, 042323 (2011).

[27] M. Pawłowski and N. Brunner, Phys. Rev. A 84, 010302 (2011).

[28] A. Chaturvedi, M. Ray, R. Veynar, and M. Pawłowski, Quantum information processing 17, 1 (2018).

[29] A. Chaturvedi, M. Farkas, and V. J. Wright, arXiv:2010.05853 (2020).

[30] A. Ambainis, D. Leung, L. Mancinska, and M. Ozols, arXiv preprint arXiv:0810.2937 (2008).

[31] A. Ambainis, D. Kravchenko, and A. Rai, arXiv preprint arXiv:1510.03045 (2015).

[32] K. Kraus, A. Böhm, J. D. Dollard, and W. Wootters, Lecture notes in physics 190 (1983).

[33] M. A. Nielsen and I. Chuang, “Quantum computation and quantum information,” (2002).

[34] M. M. Wilde, Quantum information theory (Cambridge University Press, 2013).

[35] C. H. Bennett, P. W. Shor, J. A. Smolin, and A. V. Thapliyal, Phys. Rev. Lett. 83, 3081 (1999).

[36] C. Shannon, IRE Transactions on Information Theory 2, 8 (1956).

[37] J. Korner and A. Orlitsky, IEEE Transactions on Information Theory 44, 2207 (1998).

[38] T. S. Cubitt, D. Leung, W. Matthews, and A. Winter, Phys. Rev. Lett. 104, 230503 (2010).

[39] T. S. Cubitt, D. Leung, W. Matthews, and A. Winter, IEEE Transactions on Information Theory 57, 5509 (2011).

[40] P. E. Frenkel and M. Weiner, arXiv:2103.08567 (2021).

[41] J. F. Doriguello and A. Montanaro, Quantum 5, 402 (2021).

[42] L. Hardy, arXiv preprint quant-ph/0101012 (2001).

[43] J. Barrett, Phys. Rev. A 75, 032304 (2007).

[44] G. Chiribella, G. M. D’Ariano, and P. Perinotti, Phys. Rev. A 81, 062348 (2010).

[45] H. Barnum and A. Wilce, Electronic Notes in Theoretical Computer Science 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).

[46] L. Masanes and M. P. Müller, New Journal of Physics 13, 063001 (2011).

[47] S. Popescu and D. Rohrlich, Foundations of Physics 24, 379 (1994).

[48] P. Janotta, C. Gogolin, J. Barrett, and N. Brunner, New Journal of Physics 13, 063024 (2011).

[49] D. A. Yopp and R. D. Hill §, Linear and Multilinear Algebra 53, 167 (2005).

[50] S. Weis, arXiv preprint arXiv:1107.2319 (2011).

[51] S. Massar and M. K. Patra, Physical Review A 89, 052124 (2014).

[52] S. W. Al-Safi and J. Richens, New Journal of Physics 17, 123001 (2015).

[53] M. Banik, S. Saha, T. Guha, S. Agrawal, S. S. Bhattacharya, A. Roy, and A. Majumdar, Physical Review A 100, 060101 (2019).

[54] S. S. Bhattacharya, S. Saha, T. Guha, and M. Banik, Physical Review Research 2, 012068 (2020).

[55] S. Saha, S. S. Bhattacharya, T. Guha, S. Halder, and M. Banik, Annalen der Physik 532, 2000334 (2020).

[56] S. Saha, T. Guha, S. S. Bhattacharya, and M. Banik, arXiv preprint arXiv:2012.05781 (2020).

[57] A. Tavakoli, A. Hameedi, B. Marques, and M. Bourennane, Phys. Rev. Lett. 114, 170502 (2015).

[58] P. Wittek, ACM Trans. Math. Softw. 41, 1 (2015).

[59] J. Löff, in In Proceedings of the CACSD Conference (Taipei, Taiwan, 2004).

[60] K.-C. Toh, M. J. Todd, and R. H. Tütüncü, Optim. Methods Softw. 11, 545 (1999).