Identifying the value of a random variable unambiguously: Quantum versus classical approaches

Saronath Halder,[1] Alexander Streltsov,[1,2] and Manik Banik[3]
[1]Centre for Quantum Optical Technologies, Centre of New Technologies, University of Warsaw, Banacha 2c, 02-097 Warsaw, Poland
[2]Institute of Fundamental Technological Research, Polish Academy of Sciences, Pawińskiego 5B, 02-106 Warsaw, Poland
[3]Department of Physics of Complex Systems, S.N. Bose National Center for Basic Sciences, Block JD, Sector III, Salt Lake, Kolkata 700106, India

(Received 14 December 2022; accepted 16 April 2024; published 6 May 2024)

Quantum resources may provide an advantage over their classical counterparts. Theoretically, in certain tasks, this advantage can be very high. In this work, we construct such a task based on a game, mediated by the Referee and played between Alice and Bob. The Referee sends Alice a value of a random variable. At the same time, the Referee also sends Bob some partial information regarding that value. Here partial information can be defined in the following way. Bob gets the information of a random set that must contain the value of the variable, which is sent to Alice by the Referee, along with other value(s). Alice is not allowed to know what information is sent to Bob by the Referee. Again, Bob does not know which value of the random variable is sent to Alice. Now, the game can be won if and only if Bob can unambiguously identify the value of the variable that is sent to Alice, with some nonzero probability, no matter what information Bob receives or which value is sent to Alice. However, to help Bob, Alice sends some limited amount of information to him, based on any strategy that is fixed by Alice and Bob before the game begins. We show that if Alice sends a limited amount of classical information, then the game cannot be won, while the quantum analog of the "limited amount of classical information" is sufficient for winning the game. Thus, it establishes a quantum advantage. We further analyze several variants of the game and provide certain bounds on the success probabilities. Moreover, we establish connections between the trine ensemble, mutually unbiased bases, and the encoding-decoding strategies of those variants. We also discuss the role of quantum coherence in the present context.

DOI: 10.1103/PhysRevA.109.052608

I. INTRODUCTION

Efficient utilization of nonclassical features of elementary quantum systems, such as coherent superposition, quantum entanglement, measurement incompatibility, and indefinite causal order, leads to advantageous information and communication protocols that otherwise are not possible with classical resources [1,2]. A few such innovative protocols are quantum cryptography [3], quantum superdense coding [4], and quantum teleportation [5], which establish quantum advantages in a communication scenario by invoking quantum entanglement between the sender and the receiver. Quantum advantages, however, are hard to find and sometimes constrained by fundamental no-go theorems. For instance, Holevo's no-go theorem [6] limits the capacity of a quantum channel as that of its classical counterpart when no preshared entanglement between the sender and the receiver is allowed. More recently, a stronger version of this no-go theorem was obtained that establishes that the classical information storage in an n-level quantum system is not better than the corresponding classical n-state system [7].

In this work, we report a communication advantage of an elementary quantum system without invoking any preshared entanglement between the sender (Alice) and the receiver (Bob). At this point, the task of random access codes (RACs), which also depicts communication advantages of quantum systems between an unentangled sender and receiver, is worth mentioning. In an RAC, a long message is encoded into fewer bits with the ability to recover (decode) any one of the initial bits with a high degree of success probability. Historically, quantum random access codes (QRACs) were first studied by Wiesner, and they were termed "conjugate coding" [8]. Later QRACs were reanalyzed by Ambainis *et al.* [9,10], and subsequently they attracted a huge amount of research interest [11–21]. The task we consider, however, is different from the RAC task, and it can best be described in terms of a game, mediated by the Referee and played between Alice and Bob. The Referee sends Alice a value of a random variable. At the same time, the Referee also sends Bob some partial information regarding that value. Here partial information can be defined in the following way. Bob gets the information of a random set that must contain the value of the variable, which is sent to Alice by the Referee, along with other value(s). Alice is not allowed to know what information is sent to Bob by the Referee. Again, Bob does not know which value of the random variable is sent to Alice. Now, the game can be won if and only if Bob can unambiguously identify the value of the variable that is sent to Alice, with some nonzero probability, no matter what information Bob receives or which value is sent to Alice. However, to help Bob, Alice sends some limited information to him. This is based on any strategy that is fixed by Alice and Bob before the game begins. We mention here that only deterministic strategies are considered in this work, i.e., the parties do not use any randomness. For example, when Alice sends a cbit, she sends either "0" or "1." On the other

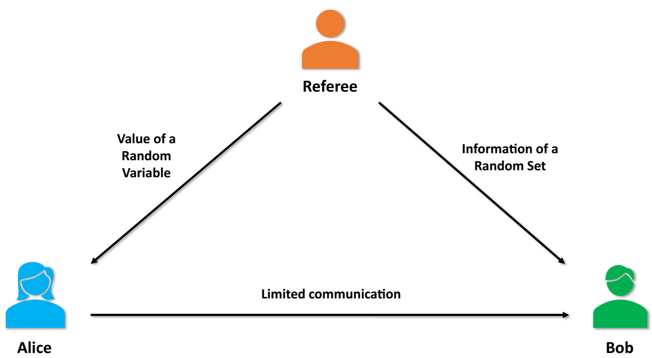

FIG. 1. There are three spatially separated parties: the Referee, Alice, and Bob. The Referee sends a value of a random variable to Alice. At the same time, the Referee sends the information of a random set to Bob. The set contains the value of the random variable, sent to Alice, along with some other value(s). Remember that Alice does not know about the information of the random set that is sent to Bob, but she knows the size of the set. Similarly, Bob does not know which value of the random variable is sent to Alice. The task of Bob is to unambiguously identify the value of the random variable sent to Alice, with some nonzero probability all the time, i.e., no matter what information he receives from the Referee or which value of the random variable is sent to Alice by the Referee. However, Alice is allowed to send a limited amount of information to Bob based on any predecided strategy. This is to help Bob in identifying the value of the variable unambiguously. Note that both Alice and Bob know about all possible values of the random variable.

hand, when she sends a qubit, she actually sends a pure qubit state. No additional correlation (local or global) is used by Alice and Bob. See also Fig. 1 for the description of the present game.

Note that the game can be won perfectly if there is no restriction imposed on the available communication from Alice to Bob. Interesting situations arise only when the allowed communication is limited. In that situation, Bob is not able to identify the value of the random variable perfectly all the time. Then, it can be explored how well Bob can identify the value of the random variable no matter what information he receives. In particular, this becomes a probabilistic case that helps us to explore the advantages and limitations of resources. In this direction (the direction of the probabilistic study), there are two popular settings that researchers usually adopt. One is the minimum error strategy: Bob can try to identify the value of the random variable minimizing the error. The other is the unambiguous strategy: Bob can try to identify the value of the random variable without committing any error, but in this case there will be a nonzero probability of inconclusive outcome. In other words, the unambiguous strategy can be explained as either answering the right result without any error, or answering "inconclusive." But the former answer has to occur with nonzero probability. In this work we consider the second strategy, i.e., the unambiguous strategy, and we explore corresponding bounds on the success probabilities considering different cases. We also explore the role of several mathematical concepts in these cases.

We are now ready to define Bob's task more accurately. This is done by following the definition of an unambiguously distinguishable set of quantum states. Suppose a set of quantum states is given and we want to distinguish these states unambiguously. If a particular state of the given set can be identified error-free with some nonzero probability, then we say that the state is unambiguously identifiable. Moreover, if all the states of a given set are unambiguously identifiable, then the set is unambiguously distinguishable [22,23] and the task of the state distinguishability can be accomplished unambiguously with some nonzero probability. Similarly, here we are interested in those situations in which all values of a random variable are unambiguously identifiable no matter what information Bob receives. Such a situation implies that the task of determining the value of the random variable unambiguously with some nonzero probability can be accomplished. So, we set the condition of winning the game as follows: the game can be won if and only if Bob is able to identify the value of the random variable error-free with some nonzero probability all the time (no matter which value is sent to Alice by the Referee or what information Bob receives).

Previously, a few communication tasks were designed in which a huge separation between classical and quantum resources was reported [24–28]. In our game also, we report a huge advantage of qubit communication over classical communication, and theoretically this advantage might be increased up to an arbitrary height if the dimension of the random variable increases. In Sec. II, we first present an elementary version of the game. We also present several variants of this game in that section. We find the connection of trine ensemble with the encoding-decoding strategy of a variant. Then, we provide several generalizations of this game for higher-dimensional random variables. These generalizations are given in Secs. III and IV. Eventually, we present several bounds on the success probabilities, and we find a connection with mutually unbiased bases and the encoding-decoding strategy of a variant of the game. In a few cases, we derive the optimal success probabilities and discuss their achievability. In Sec. V, another generalization is given. We also discuss the role of coherence in this game. Finally, a conclusion is drawn in Sec. VI, and we mention some open problems that warrant further research.

II. AN ELEMENTARY VERSION OF THE GAME

We assume that there are three parties: the Referee, Alice, and Bob. The Referee sends the value of a three-dimensional random variable to Alice. We denote the variable by X and its dimension by d. In this section, we assume $d = 3$. Here X is a discrete variable, so one may formulate our communication task without defining the dimension of X. However, for the convenience of equations that will appear later in the paper, we define the dimension of the variable X as the number of available values. In fact, in some cases this quantity also helps us to understand the quality or quantity of the communication required (from Alice to Bob) to accomplish our task.

So, the Referee sends Alice x_i (value of X), while x_i belongs to the set $\{x_1, x_2, x_3\}$. This set is known to both Alice and Bob. On the other hand, the Referee sends Bob "j," where this "j" is associated with a random set S_j. We denote by $n := |S_j|$ the size of S_j. In this section, we consider $n = 2$. This value is known to both Alice and Bob. Depending on the values of d

and n, three random sets can be defined: $S_1 \equiv \{x_1, x_2\}$, $S_2 \equiv \{x_2, x_3\}$, $S_3 \equiv \{x_3, x_1\}$. These definitions are also known to both Alice and Bob. Note that two things—(i) sending x_i to Alice and (ii) sending "j" to Bob—are simultaneously done by the Referee. Again, information on which set is sent to Bob is not known to Alice, and similarly, Bob does not know which value of the random variable is sent to Alice. But j will be chosen (randomly) in such a way that S_j must contain the particular value of X that is sent to Alice by the Referee, along with some other value of X. For example, if x_1 is sent to Alice, then either 1 or 3 is sent to Bob. If 1 is sent, then it means Bob is instructed that the value of the variable that is sent to Alice belongs to S_1. Similarly, if 3 is sent, then it means Bob is instructed that the value of the variable that is sent to Alice belongs to S_3. Clearly, before Alice receives the value of the random variable, Alice and Bob know that the information regarding any set can be sent to Bob, and these sets are equally probable. When we say that the sets are equally probable, one may point out that this applies only to the sets containing the value of X that is sent to Alice by the Referee because the probability of the other set is null. While this is correct, in the overall process all sets are equally probable. Therefore, Alice and Bob have to fix an encoding-decoding strategy accordingly. To help Bob in identifying the value of the variable, Alice is allowed to send a classical bit (cbit) or a quantum bit (qubit). The game can be won if and only if Bob is able to identify x_i unambiguously with some nonzero probability $\forall j = 1, 2, 3$. Remember that Alice does not know the information on which set is sent to Bob, but she knows that the set must contain the value of the random variable that she has received, along with some other value.

In this context, the first thing we want to prove is the following. If Alice sends only a cbit to Bob, then it is not always possible for Bob to unambiguously identify the value of the random variable that Alice receives with some nonzero probability. This can be illustrated through a simple example. Suppose Alice tries to fix an encoding strategy, and for this purpose she thinks about computing a function:

$$\mathcal{F} = 0 \;\text{ if }\; x_i = x_1, \quad \mathcal{F} = 1 \;\text{ if }\; x_i \neq x_1.$$

This is one of the simplest forms that can be computed by Alice, and before the game starts, Alice can inform Bob about computing this function. Similarly, there can be many other strategies that can be adopted by both Alice and Bob. However, the key point is that $\mathcal{F}$ cannot have more than two values because Alice is allowed to send a cbit only to Bob. But through those two values of $\mathcal{F}$ it is not possible for Bob to extract three different values of X, which is necessary for unambiguous identification. More precisely, in this example, if x_2 or x_3 is sent to Alice, then she sends "1" to Bob. In such a situation, if Bob receives a $j = 2$ value from the Referee, he is not be able to identify the value of the random variable unambiguously with some nonzero probability.

We are now ready to present the above observation in a proposition form, and we also provide a general proof of the proposition.

Proposition 1. There exists no strategy through which the game can be won when Alice is allowed to send only a cbit to Bob.

Proof. The encoding-decoding strategy should be fixed before the value of the random variable is sent to Alice. The values of the variable are equally probable. Thus, the information on which value set is sent to Bob is also completely random. Furthermore, this information is not known to Alice. Thus, "the information regarding the random set" does not help Alice to fix an encoding strategy. But this information may help Bob to choose the right decoding strategy.

However, to fix an encoding-decoding strategy through which the game can be won, Alice has to compute a function, and before the game starts Alice can inform Bob about this function. This is like the example given above, but the function can be any function.

Because the random variable is three-dimensional, the function must output three different values corresponding to the values of the random variable. But when Alice is allowed to send only a cbit, Alice cannot encode three different values of a function within that cbit.

Next, we assume that the function does not output different values corresponding to the values of the random variable. In that case, there must be at least one situation when the value of the variable cannot be identified unambiguously. More precisely, this means that there exists at least one value of j (where j is associated with S_j) for which an unambiguous identification is not possible. These complete the proof. ■

Proposition 2. There exists a strategy through which the game can be won when Alice sends a qubit to Bob, i.e., Bob is able to identify x_i $\forall j$ unambiguously with some nonzero probability.

Proof. To prove the above proposition, if an explicit strategy is provided through which the game can be won, then it is sufficient. For example, Alice can avail herself of the following encoding strategy:

$$x_1 \rightarrow |0\rangle, \;\; x_2 \rightarrow |1\rangle, \;\; x_3 \rightarrow \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle,$$

where the states $|0\rangle$ and $|1\rangle$ are orthogonal to each other.

Now, if any two values of X are chosen, then the corresponding states are linearly independent states that can be unambiguously distinguished with some nonzero probability [29]. In this way, for any value of j (where j is associated with S_j), Bob is able to identify the value of the variable unambiguously with at least some nonzero probability, and thus the game can be won. These complete the proof. ■

From Propositions 1 and 2, it is clear that in the context of the present game, a qubit can provide an advantage over a cbit. Again, the advantage is coming from superposition. Also notice that we compare between deterministic strategies only, since we do not allow the parties to use any type of randomness here. More precisely, in our case when Alice sends a cbit, she sends either "0" or "1," and when Alice sends a qubit, she actually sends a pure qubit state. No additional correlation (local or global) is used by Alice and Bob. However, in the following, we explore the advantage of qubit communication in detail.

A. Bounds on the success probabilities

Before we proceed, we mention that we are going to talk about two types of success probabilities: *individual probability* and *average probability*. But before we provide these definitions, it is important to say the following. Here we consider a random variable that has different values. Now a value of the variable is sent to Alice, while at the same time the Referee also sends some partial information regarding that value to Bob. This partial information is defined by different j values, where j is associated with S_j. Corresponding to each j value, we define "*an event*." Based on these events, we now provide the definitions of two types of success probabilities.

Definition 1 (Individual probability of success). This is the probability of successfully identifying the value of the random variable that is sent to Alice in each event.

According to the winning condition of the game, the individual probabilities of success must be nonzero.

Definition 2 (Average probability of success). We first take the sum of all individual probabilities. Then, we divide that sum by the total number of events. Thus, we get the average probability of success.

As mentioned, an event is defined by a "j" value. If p_j is the probability of success corresponding to a "j" value, then p_j's are individual probabilities of success. Furthermore, the average probability of success $\mathcal{P}_{\text{avg}}^{(d)}$, when $\dim X = d$, is defined as

$$\mathcal{P}_{\text{avg}}^{(d)} = \frac{1}{|j|} \sum_j p_j,$$

where $|j|$ is the total number of events, given by $\binom{d}{n}$.

Proposition 3. The average probability of success can be maximized by sending only a cbit from Alice to Bob, but in this scenario the goal of the present game cannot be achieved.

Proof. The values of the random variable are equally probable. Thus, the information regarding any set can be sent to Bob. These sets are also equally probable. To achieve the present goal, the values of the random variables of a particular set must be associated with linearly independent states in order to ensure unambiguous discrimination [29]. In an unambiguous discrimination of two pure states, the probability of an inconclusive outcome depends on the overlap of the states [30–32]. So, the average probability of success, denoted by $\mathcal{P}_{\text{avg}}^{(3)}$, is given as follows:

$$\mathcal{P}_{\text{avg}}^{(3)} = 1 - \tfrac{1}{3}[|\langle\phi_1|\phi_2\rangle| + |\langle\phi_2|\phi_3\rangle| + |\langle\phi_3|\phi_1\rangle|]. \tag{1}$$

Here, the superscript "(3)" indicates that the dimension of X is 3. The states $|\phi_i\rangle$, $\forall i = 1, 2, 3$, are the states that are used for the encoding strategy by Alice. They are defined as follows: We assume that the values of the random variables are mapped against these states: $x_1 \to |\phi_1\rangle$, $x_2 \to |\phi_2\rangle$, $x_3 \to |\phi_3\rangle$, where $|\phi_3\rangle = a_1 |\phi_1^\perp\rangle + a_2 |\phi_2^\perp\rangle$. The states $|\phi_1\rangle$ and $|\phi_2\rangle$ must be linearly independent. The coefficients a_1 and a_2 are some complex numbers such that $|\phi_3\rangle$ is a valid quantum state. Again, we take the values of $|a_1|, |a_2|$ as nonzero. It is quite clear now that the average probability of an inconclusive outcome in the present case is dependent on $[|\langle\phi_1|\phi_2\rangle| + |\langle\phi_2|\phi_3\rangle| + |\langle\phi_3|\phi_1\rangle|]$. So, to increase $\mathcal{P}_{\text{avg}}^{(3)}$, we have to decrease the average probability of an inconclusive outcome. For this purpose, we consider the following:

$$\begin{aligned} &|\phi_1\rangle = |\phi\rangle\,, \ \ |\phi_2\rangle = a\,|\phi\rangle + b\,|\phi^\perp\rangle\,, \\ &|\phi_3\rangle = a_1\,|\phi^\perp\rangle + a_2(b^*\,|\phi\rangle - a^*\,|\phi^\perp\rangle). \end{aligned} \tag{2}$$

$|\phi_1\rangle$ and $|\phi_2\rangle$ are linearly independent, $\langle\phi|\phi^\perp\rangle = 0$, and $|a|^2 + |b|^2 = 1$. a^* and b^* are complex conjugates of the complex numbers a and b. We can rewrite $|\phi_3\rangle$ as $a_2 b^*\,|\phi\rangle + (a_1 - a_2 a^*)\,|\phi^\perp\rangle$, where $|a_2 b^*|^2 + |(a_1 - a_2 a^*)|^2 = 1$. We next want to calculate the lower bound of the quantity, $[|\langle\phi_1|\phi_2\rangle| + |\langle\phi_2|\phi_3\rangle| + |\langle\phi_3|\phi_1\rangle|]$, which can be rewritten as follows:

$$|\langle\phi_1|\phi_2\rangle| + |\langle\phi_2|\phi_3\rangle| + |\langle\phi_3|\phi_1\rangle| = |a| + |b|(|a_1| + |a_2|). \tag{3}$$

Since $|a_1| + |a_2|$ cannot be zero, by setting $|b| = 0$ we minimize the quantity $|b|(|a_1| + |a_2|)$. This implies that $[|\langle\phi_1|\phi_2\rangle| + |\langle\phi_2|\phi_3\rangle| + |\langle\phi_3|\phi_1\rangle|] = 1$ and $\mathcal{P}_{\text{avg}}^{(3)} = \frac{2}{3}$. In the following, we prove that this is the maximum value of $\mathcal{P}_{\text{avg}}^{(3)}$. But if $|b| = 0$, then $|\phi_1\rangle$ and $|\phi_2\rangle$ become linearly dependent, and this is not good when one wants to achieve the goal of the present game. Therefore, when $|b| \neq 0$ we want to determine how to reduce the value of the quantity of (3), i.e., we want to check if there is any way of maximizing the quantity of (1) along with winning the game.

If $|b| \neq 0$, then to reduce the value of the quantity of (3), we have to reduce the quantity $|a_1| + |a_2|$. It is easy to show that $(|a_1| + |a_2|) \geqslant 1$. For this purpose, we derive the following:

$$\begin{aligned} &|a_2 b^*|^2 + |(a_1 - a_2 a^*)|^2 = 1 \\ &\quad\Rightarrow |a_2|^2|b|^2 + (a_1^* - a_2^* a)(a_1 - a_2 a^*) = 1 \\ &\quad\Rightarrow |a_1|^2 + |a_2|^2 - (a_1^* a_2 a^* + a_1 a_2^* a) = 1 \\ &\quad\Rightarrow |a_1| + |a_2| = \sqrt{[1 + 2|a_1||a_2| + (a_1^* a_2 a^* + a_1 a_2^* a)]} \\ &\quad= \sqrt{[1 + 2|a_1||a_2|\{1 + |a| \cos{(\theta_1 + \theta - \theta_2)}\}]}, \end{aligned} \tag{4}$$

where $a = |a|e^{\mathbf{i}\theta}$ and $a_i = |a_i|e^{\mathbf{i}\theta_i}$, $\forall i = 1, 2$, $\mathbf{i} = \sqrt{-1}$. From the above, it is clear that $(|a_1| + |a_2|) \geqslant 1$ and $(|a_1| + |a_2|) = 1$ if and only if one of the following conditions is satisfied: $|a_1| = 0$, $|a_2| = 0$, or $|a| = 1$ along with $\cos{(\theta_1 + \theta - \theta_2)} = -1$. By setting $(|a_1| + |a_2|) \geqslant 1$, we get the following lower bound:

$$[|\langle\phi_1|\phi_2\rangle| + |\langle\phi_2|\phi_3\rangle| + |\langle\phi_3|\phi_1\rangle|] \geqslant (|a| + |b|). \tag{5}$$

We can also think about minimizing the quantity $|a| + |b|$, which is 1, if and only if either of the following conditions is satisfied: $|a| = 0$ or $|b| = 0$. Finally, we consider all the possibilities together for increasing the value of $\mathcal{P}_{\text{avg}}^{(3)}$. But we see that the maximum value of this quantity is $\frac{2}{3}$. This is achievable if and only if one of the following conditions is satisfied:

$$\begin{aligned} &\text{(i)} \quad |a| = 1,\ |b| = 0,\ |(a_1 - a_2 a^*)|^2 = 1; \\ &\text{(ii)} \quad |b| = 1,\ |a| = 0,\ |a_1| = 1,\ |a_2| = 0; \\ &\text{(iii)} \quad |b| = 1,\ |a| = 0,\ |a_1| = 0,\ |a_2| = 1. \end{aligned} \tag{6}$$

It is easy to check that for each of the above conditions, two of the states of (2) are going to be the same state, and the other state is orthogonal to that state. Such an encoding can be communicated, for sure, from Alice's side to Bob's side by sending a cbit only. The same states can correspond to 0 while the orthogonal state can correspond to 1, or vice versa. However, for such an encoding, for at least one value of j (j is associated with S_j), Bob will not be able to identify the value of X unambiguously with some nonzero probability. Thus, the goal of the present game cannot be achieved. These complete the proof. ■

Notice that to win the game, it is quite justifiable to start with the states of (2) because if we choose any two states from these three states, then the two states are going to be linearly independent for sure when we take the coefficients $|a|, |b|, |a_1|, |a_2|$ as nonzero. In particular, here we have taken the states $|\phi_1\rangle$ and $|\phi_2\rangle$ as linearly independent. So, like $\{|\phi_1\rangle, |\phi_2\rangle\}$, $\{|\phi_1^\perp\rangle, |\phi_2^\perp\rangle\}$ are also linearly independent and they form a basis for two-dimensional Hilbert space. Thus, $|\phi_3\rangle$ can be written as a linear combination of $|\phi_1^\perp\rangle$ and $|\phi_2^\perp\rangle$. This is what we have considered. However, we end up with the fact that if we want to achieve the maximum value of the average probability of success, then the game cannot be won. Again, there is no quantum advantage in maximizing the average probability of success as this maximum value can be achieved when Alice is sending a classical bit to Bob. In fact, from the proof of Proposition 3, it is clear that the maximum value of $\mathcal{P}_{\text{avg}}^{(3)}$ cannot be achieved when states of a quantum encoding strategy are pairwise linearly independent. Nevertheless, we are interested in the following: Bob unambiguously identifies the value of X all the time (for all "j" values, where j is associated with S_j), i.e., in every event with some nonzero probability. Furthermore, we search for the maximum value of $\mathcal{P}_{\text{avg}}^{(3)}$ when Alice and Bob win the game. From the preceding proposition, we can conclude that to win the game, $|b|$ must be nonzero. In that case, we can start with the lower bound given in (5). In fact, we argue that this lower bound is achievable *if and only if* $(|a_1| + |a_2|) = 1$. We now put this condition in a proposition form.

Proposition 4. The lower bound of (5) is achievable if and only if $|a_1| + |a_2| = 1$, provided $|b| \neq 0$.

Proof. The "if" part is already shown in the proof of the preceding proposition; in particular, see (3). Thus, for the "only if" part, we consider the following:

$$|a| + |b|(|a_1| + |a_2|) = |a| + |b| \Rightarrow |b|(|a_1| + |a_2| - 1) = 0. \tag{7}$$

We have already mentioned that $|b| \neq 0$, so the only possibility is $(|a_1| + |a_2| - 1) = 0$, i.e., $|a_1| + |a_2| = 1$, to satisfy the bound. These complete the proof. ■

We now want two things together: (a) winning the game and (b) achieving the lower bound of (5). We set (a) here because it is the main goal. On the other hand, (b) helps to reduce the probability of an inconclusive outcome. Together these can be expressed in the following manner:

$$\begin{aligned}
&\text{We want: } \epsilon > 0,\\
&\text{Such that } (1 - |\langle\phi_i|\phi_{i'}\rangle|) \geqslant \epsilon,\\
&\forall i, i' = 1, 2, 3,\ i \neq i'\\
&\text{and}\\
&|\langle\phi_1|\phi_2\rangle| + |\langle\phi_2|\phi_3\rangle| + |\langle\phi_3|\phi_1\rangle| = |a| + |b|. \qquad (8)
\end{aligned}$$

To solve the above, we can start with $|a_1| + |a_2| = 1$, so that $|\langle\phi_1|\phi_2\rangle| + |\langle\phi_2|\phi_3\rangle| + |\langle\phi_3|\phi_1\rangle| = |a| + |b|$. Now, $|a_1| + |a_2| = 1$ only when $a_1 = 0$ or $a_2 = 0$ because $|a|$ cannot be 1; see (4) for details. Either of the conditions $a_1 = 0$ or $a_2 = 0$ provides a similar type of solution, so without loss of generality we can take $a_2 = 0$. Therefore, the states of (2) become

$$|\phi_1\rangle = |\phi\rangle,\ |\phi_2\rangle = a|\phi\rangle + b|\phi^\perp\rangle,\ |\phi_3\rangle = |\phi^\perp\rangle. \tag{9}$$

We take $|a| \geqslant |b|$. So, for each value of "j" (j is associated with S_j), the individual probabilities of success are 1, $1 - |a|$, and $1 - |b|$. Among these three probabilities, the minimum value is $1 - |a|$. Thus, we take $1 - |a| = \epsilon$. In this way, we get a solution of (8) given by

$$\begin{aligned}
&|\phi_1\rangle = |\phi\rangle,\ |\phi_2\rangle = (1-\epsilon)|\phi\rangle + \sqrt{2\epsilon - \epsilon^2}\,|\phi^\perp\rangle,\\
&|\phi_3\rangle = |\phi^\perp\rangle.
\end{aligned}$$

In this case,

$$|\langle\phi_1|\phi_2\rangle| + |\langle\phi_2|\phi_3\rangle| + |\langle\phi_3|\phi_1\rangle| = 1 - \epsilon + \sqrt{2\epsilon - \epsilon^2}$$

and

$$\mathcal{P}_{\text{avg}}^{(3)} = \tfrac{1}{3}(2 + \epsilon - \sqrt{2\epsilon - \epsilon^2}).$$

Let us understand the meaning of this solution with one example.

Example 1. We assume that $\epsilon = 0.1$. So, if we consider the encoding through the states $|\phi_1\rangle = |\phi\rangle$, $|\phi_2\rangle = 0.9|\phi\rangle + \sqrt{0.19}\,|\phi^\perp\rangle$, $|\phi_3\rangle = |\phi^\perp\rangle$, then $(1 - |\langle\phi_i|\phi_{i'}\rangle|) \geqslant 0.1$ and $\mathcal{P}_{\text{avg}}^{(3)} = 0.5547$ (approx.). In fact, there is no solution for which $(1 - |\langle\phi_i|\phi_{i'}\rangle|) \geqslant 0.1$ while at the same time $\mathcal{P}_{\text{avg}}^{(3)} > 0.5547$.

Example 2. If we think about maximizing ϵ within the problem of (8), then the only possibility is that we take $|a| = |b| = 1/\sqrt{2}$. This is a special case of the problem of (8). The maximum value of ϵ is given by $1 - (1/\sqrt{2})$, achievable through the states $|\phi_1\rangle = |\phi\rangle$, $|\phi_2\rangle = (|\phi\rangle + |\phi^\perp\rangle)/\sqrt{2}$, $|\phi_3\rangle = |\phi^\perp\rangle$, $|\langle\phi_1|\phi_2\rangle| + |\langle\phi_2|\phi_3\rangle| + |\langle\phi_3|\phi_1\rangle| = \sqrt{2}$, and $\mathcal{P}_{\text{avg}}^{(3)} = 1 - (\sqrt{2}/3)$. Notice that $|\langle\phi_1|\phi_2\rangle| + |\langle\phi_2|\phi_3\rangle| + |\langle\phi_3|\phi_1\rangle| = \sqrt{2}$ is the *greatest lower bound*, and $|\phi_2\rangle$ is now a maximally coherent state[1] with respect to the $\{|\phi\rangle, |\phi^\perp\rangle\}$ basis.

B. Role of the trine ensemble

Having optimized the average probability of success, we now consider optimizing the individual probabilities of success. In the case of the problem of (8), this means that we drop the constraint $|\langle\phi_1|\phi_2\rangle| + |\langle\phi_2|\phi_3\rangle| + |\langle\phi_3|\phi_1\rangle| = |a| + |b|$. Then, some of the individual probabilities of success might be improved. Alice and Bob can fix the following encoding process:

$$\begin{aligned}
&x_1 \rightarrow |\phi_1\rangle = |0\rangle,\ x_2 \rightarrow |\phi_2\rangle = \tfrac{1}{2}(|0\rangle + \sqrt{3}\,|1\rangle),\\
&x_3 \rightarrow |\phi_3\rangle = \tfrac{1}{2}(|0\rangle - \sqrt{3}\,|1\rangle). \qquad (10)
\end{aligned}$$

[1]For details regarding quantum coherence, one can refer to [33] and references therein. However, all states of the form $\mu_0|\mu_0'\rangle + \mu_1|\mu_1'\rangle$ are coherent states with respect to the basis $\{|\mu_0'\rangle, |\mu_1'\rangle\}$, $|\mu_0|, |\mu_1| > 0$. Now, if this basis is an orthonormal basis and $\mu_0 = \mu_1 = 1/\sqrt{2}$, then the superposed states, just mentioned, are maximally coherent states with respect to the basis $\{|\mu_0'\rangle, |\mu_1'\rangle\}$.

Accordingly, the measurement that is performed by Bob to decode the information is given by the positive operator valued measure (POVM) elements $\Pi_i = \frac{2}{3}|\tilde{\phi}_i\rangle\langle\tilde{\phi}_i|$, where $|\tilde{\phi}_i\rangle$ is orthogonal to $|\phi_i\rangle$, defined in the above equation $\forall i = 1, 2, 3$. In this case, unambiguous discrimination is accomplished by the elimination of a state. Here the individual probability of success is 0.5 and the average probability of success is also 0.5. Clearly, in this case some of the individual probabilities of success are improved, but the average probability of success is decreased. Then, the question of interest is as follows: What is the optimal strategy to ensure that the success probability in any individual case cannot be less than a maximal value?

$$\begin{aligned}&\text{We want: } \epsilon_{\max} > 0,\\ &\text{Such that } (1 - |\langle\phi_i|\phi_{i'}\rangle|) \geqslant \epsilon_{\max},\\ &\forall i, i' = 1, 2, 3,\ i \neq i',\end{aligned}$$

where $\epsilon_{\max}$ is the maximum probability at least achievable in the individual cases. To figure this out, we consider a specific encoding $x_i \to |\phi_i\rangle$, $i = 1, 2, 3$,

$$|\phi_1\rangle = |0\rangle\,, |\phi_2\rangle = a\,|0\rangle + b\,|1\rangle\,, |\phi_3\rangle = a\,|0\rangle - b\,|1\rangle\,,$$

where a, b are complex numbers such that $|a|^2 + |b|^2 = 1$. Notice that if we pick any two states from these three states, then the picked states are linearly independent and thus they can be distinguished unambiguously. One may wonder why we consider the same coefficients a, b for both states $|\phi_2\rangle$ and $|\phi_3\rangle$. The reason is as follows. Suppose we take different coefficients for $|\phi_3\rangle$. It may then be possible to reduce the overlap between $|\phi_1\rangle$ and $|\phi_3\rangle$ in comparison with the overlap between $|\phi_1\rangle$ and $|\phi_2\rangle$. But in that case, the overlap between $|\phi_2\rangle$ and $|\phi_3\rangle$ may increase. On the other hand, if we take the same coefficients, then keeping the overlaps between the pairs $\{|\phi_1\rangle\,, |\phi_2\rangle\}$ and $\{|\phi_1\rangle\,, |\phi_3\rangle\}$ the same, one can reduce the overlap between $|\phi_2\rangle$ and $|\phi_3\rangle$. This is extremely important to solve the above problem (finding the value of $\epsilon_{\max}$). However, we do not consider $|\phi_2\rangle$ and $|\phi_3\rangle$ orthogonal to each other, as this case was already discussed (see Example 2 of the previous subsection). Let us now calculate the probabilities of success for each pair of states,

$$\begin{aligned}j = 1 &\Rightarrow p_{\{|\phi_1\rangle,|\phi_2\rangle\}} \Rightarrow 1 - |\langle\phi_1|\phi_2\rangle| = 1 - |a|,\\ j = 2 &\Rightarrow p_{\{|\phi_2\rangle,|\phi_3\rangle\}} \Rightarrow 1 - |\langle\phi_2|\phi_3\rangle| = 1 - |(|a|^2 - |b|^2)|,\\ j = 3 &\Rightarrow p_{\{|\phi_3\rangle,|\phi_1\rangle\}} \Rightarrow 1 - |\langle\phi_3|\phi_1\rangle| = 1 - |a|.\end{aligned}$$

In this case, we assume $|a| < |b|$. So, $0 < |a|^2 < 1/2$ and $1/2 < |b|^2 < 1$. If $|a|^2 = |b|^2 = 1/2$, then it is similar to Example 2. We now consider a small positive number $0 < \delta < 1/2$, such that $|a|^2 = 1/2 - \delta$ and $|b|^2 = 1/2 + \delta$. So, the success probabilities, corresponding to $j = 1, 2, 3$, become $1 - \sqrt{1/2 - \delta}$, $1 - 2\delta$, and $1 - \sqrt{1/2 - \delta}$. We then assume $2\delta \geqslant \sqrt{1/2 - \delta} \;\Rightarrow\; \delta \geqslant 1/4$. Clearly, $\epsilon_{\max} = 0.5$ when $\delta = 1/4$. Similarly, if we take $2\delta \leqslant \sqrt{1/2 - \delta}$, then we get $\delta \leqslant 1/4$. In this case, also $\epsilon_{\max} = 0.5$ when $\delta = 1/4$. These suggest that the maximum achievable value of ϵ, i.e., $\epsilon_{\max}$, is 0.5 and this is happening when $\delta = 1/4$, thereby the values of $|a|^2$ and $|b|^2$ are 1/4 and 3/4. Thus, we get the trine ensemble as the optimal solution when we only focus on improving the individual probabilities. One can also check this by considering $|a| > |b|$, but no better value of ϵ can be obtained with this consideration.

From the above discussion, it is clear that finding the value of $\epsilon_{\max}$ is connected with finding the point where all of the individual probabilities are equal. In other words, if we set the overlap of $|\phi_1\rangle$ and $|\phi_2\rangle$ as $|a|$, then clearly the overlap of $|\phi_1\rangle$ and $|\phi_3\rangle$ also needs to be $|a|$. This gives the construction of the encoding presented here, and all that is left is to find the point where $1 - |a| = 1 - |(|a|^2 - |b|^2)|$, which occurs when $|a| = 1/2$ and $|b| = \sqrt{3}/2$. This solution gives the states of the trine ensemble (for details regarding the trine ensemble, see Ref. [34] and the references therein).

Furthermore, notice that in the case of a quantum strategy like Proposition 2, for which the game can be won, Bob can change his measurement according to the information of the set that he receives from Referee. For example, if Bob receives "1," then Bob distinguishes between $|\phi_1\rangle$ and $|\phi_2\rangle$. Again, if Bob is given "2," then Bob distinguishes between $|\phi_2\rangle$ and $|\phi_3\rangle$. In each case, Bob can choose a measurement defined by suitable POVM elements to achieve the optimal probability. Clearly, if the constraint is put on Bob that "he cannot change his measurement," i.e., if he is allowed to perform only one measurement, then the situation is more complex. Here the motivation of fixing this constraint can be described as follows. Actually, in our case a measurement corresponds to a specific setup. So, with increasing the number of required measurements, the number of required setups also increases. This is certainly a costly affair. Therefore, it is reasonable to consider the constraint that "Bob is not able to change his measurement." In fact, it demonstrates less resource requirement in a practical situation as Bob is allowed to use only one measurement setup. However, for the simplest case (i.e., $d = 3$) described above, we can have a solution through the so-called "trine" ensemble.

III. FOUR-DIMENSIONAL RANDOM VARIABLE

In this section, we consider that the dimension of the random variable is four, i.e., $d = 4$, but still we consider that $n = 2$. So, in this case there could be six random sets, given by $S_1 = \{x_1, x_2\}$, $S_2 = \{x_1, x_3\}$, $S_3 = \{x_1, x_4\}$, $S_4 = \{x_2, x_3\}$, $S_5 = \{x_2, x_4\}$, $S_6 = \{x_3, x_4\}$. Ultimately, Bob receives a "j" value ("j" can be $1, 2, \dots, 6$) from the Referee and tries to distinguish between two states, where the encoding of the quantum scenario is like $x_i \to |\phi_i\rangle\,, \forall i = 1, 2, 3, 4$. Overall, here our communication task proceeds in the same way as described in the previous section.

In this case also if Alice sends only a cbit, then the game cannot be won. This is obvious because when $d = 3$ by sending a cbit, the game cannot be won, and when d is increased but n is the same, the complexity of the game is also increased. Therefore, it is obvious that the game cannot be won. However, we will show that by sending a qubit, the game can be won. We define $\mathcal{P}^{(4)}_{\text{avg}}$ as the average probability of success when $d = 4$. $\mathcal{P}^{(4)}_{\text{avg}}$ is given by

$$\begin{aligned}\mathcal{P}^{(4)}_{\text{avg}} = 1 - \tfrac{1}{6}[&|\langle\phi_1|\phi_2\rangle| + |\langle\phi_1|\phi_3\rangle| + |\langle\phi_1|\phi_4\rangle|\\ &+ |\langle\phi_2|\phi_3\rangle| + |\langle\phi_2|\phi_4\rangle| + |\langle\phi_3|\phi_4\rangle|].\end{aligned} \quad (11)$$

We rewrite this equation as follows:

$$\begin{aligned}\mathcal{P}^{(4)}_{\text{avg}} &= 1 - \tfrac{1}{12}[(|\langle\phi_1|\phi_2\rangle| + |\langle\phi_2|\phi_3\rangle| + |\langle\phi_1|\phi_3\rangle|) \\ &\quad + (|\langle\phi_2|\phi_3\rangle| + |\langle\phi_2|\phi_4\rangle| + |\langle\phi_3|\phi_4\rangle|) \\ &\quad + (|\langle\phi_1|\phi_2\rangle| + |\langle\phi_1|\phi_4\rangle| + |\langle\phi_2|\phi_4\rangle|) \\ &\quad + (|\langle\phi_1|\phi_3\rangle| + |\langle\phi_1|\phi_4\rangle| + |\langle\phi_3|\phi_4\rangle|)] \\ \Rightarrow \mathcal{P}^{(4)}_{\text{avg}} &= \frac{1}{4}\big[\big(\mathcal{P}^{(3)}_{\text{avg}}\big)_{123} + \big(\mathcal{P}^{(3)}_{\text{avg}}\big)_{234} + \big(\mathcal{P}^{(3)}_{\text{avg}}\big)_{124} \\ &\quad + \big(\mathcal{P}^{(3)}_{\text{avg}}\big)_{134}\big],\end{aligned} \tag{12}$$

where $(\mathcal{P}^{(3)}_{\text{avg}})_{klm}$ stands for the average probability of success, provided there are three values of the random variable available: x_k, x_l, and x_m, $k \neq l \neq m$. Clearly, $\mathcal{P}^{(4)}_{\text{avg}}$ is maximum when individual $(\mathcal{P}^{(3)}_{\text{avg}})_{klm}$ are maximum. From the previous section, it is known that $(\mathcal{P}^{(3)}_{\text{avg}})_{klm} \leqslant \frac{2}{3}$, and the equality holds when we apply an encoding like $x_k \to 0$, $x_l \to 0$, and $x_m \to 1$. Therefore, it must be the case that $\mathcal{P}^{(4)}_{\text{avg}} \leqslant \frac{2}{3}$, but the question is if an encoding exists for which $\mathcal{P}^{(4)}_{\text{avg}} = \frac{2}{3}$. Such an encoding is given by $x_1 \to 0$, $x_2 \to 0$, $x_3 \to 1$, and $x_4 \to 1$. Notice that if we choose any three values from $\{x_i | i = 1, 2, 3, 4\}$, the encoding is always like $x_k \to 0$, $x_l \to 0$, and $x_m \to 1$, or like $x_k \to 1$, $x_l \to 1$, and $x_m \to 0$, $k \neq l \neq m$.

However, for this type of encoding, if Bob receives "1" or "6," he fails to identify the value of the random variable unambiguously with some nonzero probability. This is not allowed if Alice and Bob want to win the game. At the same time, it is also important to maximize $\mathcal{P}^{(4)}_{\text{avg}}$. As we have seen, to maximize $\mathcal{P}^{(4)}_{\text{avg}}$, we have to maximize the individual quantities $(\mathcal{P}^{(3)}_{\text{avg}})_{klm}$. Ultimately, it is required to minimize the quantity $|\langle\phi_k|\phi_l\rangle| + |\langle\phi_l|\phi_m\rangle| + |\langle\phi_m|\phi_k\rangle|$ for $k, l, m \in \{1, 2, 3, 4\}$ and $k \neq l \neq m$, and thus we can think about the lower bound of (5). We are now ready to present a similar problem to that given in (8) but for $d = 4$,

$$\begin{aligned}&\text{We want: } \epsilon > 0,\ \text{Such that: } (1 - |\langle\phi_i|\phi_{i'}\rangle|) \geqslant \epsilon, \\ &\forall i, i' = 1, 2, 3, 4,\ i \neq i' \text{ and} \\ &|\langle\phi_k|\phi_l\rangle| + |\langle\phi_l|\phi_m\rangle| + |\langle\phi_m|\phi_k\rangle| = |a| + |b|, \\ &\forall k, l, m = 1, 2, 3, 4, k \neq l \neq m.\end{aligned} \tag{13}$$

One may think that for different sets of $\{k, l, m\}$ there should be different sets of $\{a, b\}$. But that is not the case. In particular, we will fix ϵ first and then we will fix the condition following the previous section, i.e., $|\langle\phi_k|\phi_l\rangle| + |\langle\phi_l|\phi_m\rangle| + |\langle\phi_m|\phi_k\rangle| = 1 - \epsilon + \sqrt{2\epsilon - \epsilon^2}$. Remember that we want to achieve the lower bound of (5) as it helps to maximize the individual $(\mathcal{P}^{(3)}_{\text{avg}})_{klm}$ and thereby $\mathcal{P}^{(4)}_{\text{avg}}$. Now, for achieving the lower bound of (5), the if and only if condition is $|a_1| + |a_2| = 1$. Ultimately, the solution of the problem (13) turns out to be the following:

$$\begin{aligned}&|\phi_1\rangle = |\phi\rangle\,,\ |\phi_2\rangle = (1 - \epsilon)\,|\phi\rangle + \sqrt{2\epsilon - \epsilon^2}\,|\phi^{\perp}\rangle\,, \\ &|\phi_3\rangle = |\phi^{\perp}\rangle\,, |\phi_4\rangle = \sqrt{2\epsilon - \epsilon^2}\,|\phi\rangle - (1 - \epsilon)\,|\phi^{\perp}\rangle\,.\end{aligned} \tag{14}$$

Now, if we choose any three states from the above, then the condition $|\langle\phi_k|\phi_l\rangle| + |\langle\phi_l|\phi_m\rangle| + |\langle\phi_m|\phi_k\rangle| = 1 - \epsilon + \sqrt{2\epsilon - \epsilon^2}$ is satisfied. It is also easily verifiable that $(1 - |\langle\phi_i|\phi_{i'}\rangle|) \geqslant \epsilon$, $\forall\, i, i' = 1, 2, 3, 4$, $i \neq i'$. In this regard, note that we have assumed $|a| \geqslant |b|$, so $(1 - \epsilon) \geqslant \sqrt{2\epsilon - \epsilon^2}$, resulting in the fact that $1 - |\langle\phi_2|\phi_3\rangle| = 1 - |\langle\phi_1|\phi_4\rangle| = 1 - \sqrt{2\epsilon - \epsilon^2} \geqslant \epsilon$. Notice that $\forall i = 1, 2, 3, 4$, $|\phi_i\rangle$'s of (15) belong to two-dimensional Hilbert space, and thus by sending a qubit from Alice's side to Bob, the problem of (13) can be solved and thereby the game can be won for $d = 4$ and $n = 2$.

A. Role of mutually unbiased bases

Example 3. If we think about maximizing ϵ within the problem of (13), then the only possibility is that we take $|a| = |b| = 1/\sqrt{2}$, i.e., $(1 - \epsilon) = \sqrt{2\epsilon - \epsilon^2} = 1/\sqrt{2}$. This is a special case of the problem of (13). The maximum value of ϵ is given by $1 - (1/\sqrt{2})$, achievable through the encoding $x_i \to |\phi_i\rangle$, $\forall i = 1, 2, 3, 4$, where the states $|\phi_1\rangle = |\phi\rangle$, $|\phi_2\rangle = (|\phi\rangle + |\phi^{\perp}\rangle)/\sqrt{2}$, $|\phi_3\rangle = |\phi^{\perp}\rangle$, $|\phi_4\rangle = (|\phi\rangle - |\phi^{\perp}\rangle)/\sqrt{2}$, $|\langle\phi_k|\phi_l\rangle| + |\langle\phi_l|\phi_m\rangle| + |\langle\phi_m|\phi_k\rangle| = \sqrt{2}$, and $\mathcal{P}^{(3)}_{\text{avg}} = \mathcal{P}^{(4)}_{\text{avg}} = 1 - (\sqrt{2}/3)$. Notice that $|\phi_i\rangle$'s are from mutually unbiased bases of two-dimensional Hilbert space. We now put this observation in a proposition form.

Proposition 5. To maximize ϵ in the problem of (13), it is necessary and also sufficient to encode the values of a four-dimensional random variable, within the states of mutually unbiased bases.[2]

The proof of the above proposition follows from *Example 2* and *Example 3*.

IV. HIGHER-DIMENSIONAL RANDOM VARIABLE

In this section, we consider that the dimension of the random variable is $d \geqslant 5$. But still we consider that $n = 2$. Ultimately, Bob receives a "j" value from the Referee and then tries to distinguish between two states, where the encoding in the quantum scenario is given by $x_i \to |\phi_i\rangle$, $\forall i \in \{1, 2, \dots, d\}$. Following a similar argument to that given in the previous section, it can be argued that by sending only a cbit, the game cannot be won when $d \geqslant 5$, too. We can define $\mathcal{P}^{(d)}_{\text{avg}}$ in a similar way as we did for $\mathcal{P}^{(4)}_{\text{avg}}$ and $\mathcal{P}^{(3)}_{\text{avg}}$. $\mathcal{P}^{(d)}_{\text{avg}}$ is given by

$$\begin{aligned}\mathcal{P}^{(d)}_{\text{avg}} &= 1 - \frac{2}{d(d-1)}\bigg(\sum_{i,i'} |\langle\phi_i|\phi_{i'}\rangle|\bigg) \\ &= \frac{6}{d(d-1)(d-2)}\bigg[\sum_{k,l,m} \big(\mathcal{P}^{(3)}_{\text{avg}}\big)_{klm}\bigg],\end{aligned} \tag{15}$$

where $i, i', k, l, m \in \{1, 2, \dots, d\}$, $i \neq i'$, and $k \neq l \neq m$. $(\mathcal{P}^{(3)}_{\text{avg}})_{klm}$ are similar quantities as defined in the previous section. The second line of the above equation tells us that if the quantities $(\mathcal{P}^{(3)}_{\text{avg}})_{klm}$ are maximized, then the quantity $\mathcal{P}^{(d)}_{\text{avg}}$ will be maximized. We know that $(\mathcal{P}^{(3)}_{\text{avg}})_{klm}$ can be maximized when we use the following (classical) encoding: $x_k \to 0$, $x_l \to 0$, and $x_m \to 1$ (or, in other words, any two

[2] We consider two bases $\mathcal{B}_1 = \{|\nu_1\rangle, |\nu_2\rangle, \dots, |\nu_{\mathcal{D}}\rangle\}$ and $\mathcal{B}_2 = \{|\nu'_1\rangle, |\nu'_2\rangle, \dots, |\nu'_{\mathcal{D}}\rangle\}$ in a $\mathcal{D}$-dimensional Hilbert space. We say that these bases are mutually unbiased if and only if $|\langle\nu_i|\nu'_{i'}\rangle| = 1/\sqrt{\mathcal{D}}$ for every i, i'. For details regarding mutually unbiased bases, one can refer to [35–37].

of the three randomly chosen values of a random variable are encoded against the same bit value, and the third value of the random variable is encoded against the orthogonal bit value). It is easy to check that when $d \geqslant 5$, it is not possible to have an encoding strategy such that among d values of a random variable if we randomly choose three values x_k, x_l, and x_m, then the corresponding quantity $(\mathcal{P}^{(3)}_{\text{avg}})_{klm}$ is maximum. Nevertheless, what could be a sensible choice here is that we can fix a number $N < \frac{d!}{3!(d-3)!}$ for $d \geqslant 5$ and we can maximize this number N. The significance of this number is that we can get at least N ensembles of randomly chosen $\{x_k, x_l, x_m\}$ such that the quantity $(\mathcal{P}^{(3)}_{\text{avg}})_{klm}$ is maximum. So, the question is as follows: What is the encoding strategy corresponding to maximum N? We first adopt an encoding strategy for even d, where half of the values of the random variable are encoded against 0 and the other half are against 1. Here, $N = \frac{d!}{3!(d-3)!} - 2 \times \frac{(d/2)!}{3!(d/2-3)!}$. If we encode $(d/2 + d')$ values of the random variable against a particular bit value and the remaining values of the random variable against the orthogonal bit value, then the value of N becomes strictly less than $\frac{d!}{3!(d-3)!} - 2 \times \frac{(d/2)!}{3!(d/2-3)!}$ for any nonzero d' (d' is an integer). In this way, we argue that the strategy in which half of the values of the random variable are encoded against a particular bit value and the other half against the orthogonal bit value is the best strategy, i.e., $\mathcal{P}^{(d)}_{\text{avg}}$ is maximized here when d is even. In the same way (as argued for even d), it is possible to show that for odd d one can adopt a strategy in which $(d-1)/2 + 1$ values of the random variable can be encoded against a particular bit value while $(d-1)/2$ values of the random variable can be encoded against the orthogonal bit value. In fact, this is the best strategy for odd d in a sense that for this strategy, N is going to be maximum and thereby the quantity $\mathcal{P}^{(d)}_{\text{avg}}$ will be maximum. However, we have to remember that these strategies do not help to win the game.

We can also define a similar problem to that given in (13) for $d \geqslant 5$. But the relation $|\langle\phi_k|\phi_l\rangle| + |\langle\phi_l|\phi_m\rangle| + |\langle\phi_m|\phi_k\rangle| = |a| + |b|$ cannot be true for all randomly chosen x_k, x_l, x_m. This can be easily checked. So, again we have to consider the number N and we have to maximize N, such that at least we can get N ensembles of randomly chosen x_k, x_l, x_m for which the relation $|\langle\phi_k|\phi_l\rangle| + |\langle\phi_l|\phi_m\rangle| + |\langle\phi_m|\phi_k\rangle| = |a| + |b|$ can be true. This modified version of the problem is particularly important if we try to maximize ϵ when $d = 5$ or 6, because in these cases, one can consider encoding the values x_5 and x_6 against the eigenvectors of the Pauli matrix σ_y to solve the problem. In higher dimensions ($d > 6$), it is not known how to solve this problem with maximum ϵ. However, if we just think about winning the game dropping the condition of satisfying the relation $|\langle\phi_k|\phi_l\rangle| + |\langle\phi_l|\phi_m\rangle| + |\langle\phi_m|\phi_k\rangle| = |a| + |b|$, then it is possible by sending only a qubit even if $d > 6$. The reason is described in the following.

A. Large quantum-classical separation

Suppose, the dimension of the random variable, the value of which is sent to Alice, is "$d > 6$." (Previously, we have discussed how to maximize $\mathcal{P}^{(d)}_{\text{avg}}$ for $d \geqslant 5$. But with that strategy, the game cannot be won. Here we want to discuss a strategy for $d > 6$, with which the game can be won.) But ultimately, the Referee sends the information of a random set of cardinality 2 to Bob. Here also, Alice is allowed to send Bob one (qu)bit of information. In this scenario, we can establish quite a high advantage of quantum communication over its classical counterpart. In brief, we term this "large quantum-classical separation." However, we mention that this advantage is demonstrated with respect to a specific goal, i.e., with some nonzero probability, Bob has to identify the value of the random variable sent to Alice by the Referee no matter which value she receives or what information Bob receives from the Referee. This "high advantage" is explained in a later portion. This is based on the fact that two quantum states $|0\rangle$ and $|1\rangle$ can be superposed in infinitely many ways. We suppose that the superposed states are $a_i|0\rangle + b_i|1\rangle$, where $|a_i|^2 + |b_i|^2 = 1$ and $|a_i|$, $|b_i|$ are nonzero. It is also possible to ensure that for any value of d, the encoding process can be done in such a way that if any two states are chosen, they must be linearly independent. The linear independence part is to confirm the unambiguous identification of the value of the random variable.

Here the parties apply the following encoding process: $x_i \to a_i|0\rangle + b_i|1\rangle$, $\forall i = 1, 2, \ldots, d$, and both a_i, b_i are nonzero. For simplicity, we can take them as positive. Next, we assume that between two arbitrary states $a_l|0\rangle + b_l|1\rangle$ and $a_{l'}|0\rangle + b_{l'}|1\rangle$, Bob has to distinguish unambiguously with some nonzero probability. So, we have to find out the condition for which these two states can be linearly independent. We take $c_1(a_l|0\rangle + b_l|1\rangle) + c_2(a_{l'}|0\rangle + b_{l'}|1\rangle) \equiv (0, 0)$ or $(c_1a_l + c_2a_{l'})|0\rangle + (c_1b_l + c_2b_{l'})|1\rangle \equiv (0, 0)$. Thus, $(c_1a_l + c_2a_{l'}) = 0 = (c_1b_l + c_2b_{l'})$. Clearly, for different positive values of $a_l, a_{l'}, b_l, b_{l'}$, both $(c_1a_l + c_2a_{l'})$ and $(c_1b_l + c_2b_{l'})$ are zero when $c_1 = c_2 = 0$ or $\frac{a_l}{b_l} = \frac{a_{l'}}{b_{l'}}$. But the second condition does not arise if a_l and $a_{l'}$ are different since $a_i^2 + b_i^2 = 1\ \forall i = l, l'$. Therefore, the only option that is left is $c_1 = c_2 = 0$. This implies that the states $a_l|0\rangle + b_l|1\rangle$ and $a_{l'}|0\rangle + b_{l'}|1\rangle$ are linearly independent and they can be distinguished unambiguously with some nonzero probability. In this way, we can construct a strategy of sending a qubit, via which it is always possible to identify the value of the random variable unambiguously with some nonzero probability under the present conditions.

On the other hand, by sending a cbit it is not possible to identify the value of the random variable unambiguously with some nonzero probability under the present conditions. The proof is due to the similar argument to that given in the proof of Proposition 1. Moreover, recall that "d" can be anything. Arguably, for a very large "d," to accomplish the present task Alice must send a large number of classical bits. Therefore, in the present scenario, a qubit is always effective but a large number of cbits may not be. In this way, one can realize a large quantum-classical separation. In fact, theoretically this separation can be arbitrarily large. However, if Alice sends only a qubit for winning the game, the success probability of unambiguously identifying the value of the random variable with increasing d must be decreasing. Clearly, for a large value of d, it may not be possible to quantify the small value of the success probability (individual or average) experimentally. Again, how far these success probabilities can be determined experimentally is a completely different problem, and we are leaving it for future studies.

V. GENERAL DESCRIPTION OF THE GAME

There are three spatially separated parties: the Referee, Alice, and Bob. The Referee sends a value $x_i \in \{x_1, x_2, \dots, x_d\}$ of a random variable X to Alice, where d is the dimension of X. At the same time, the Referee also sends the information j of a random set S_j to Bob such that S_j contains the particular x_i that is sent to Alice, along with some other value(s) $x_{i'} \in \{x_1, x_2, \dots, x_d\}$, but $i \neq i'$. Note that Alice does not know the information j that is sent to Bob by the Referee, and similarly, Bob does not know the information x_i that is sent to Alice by the Referee. The task of Bob is to identify the value of the random variable that is sent to Alice by the Referee. Clearly, the question of interest is if the task can be accomplished for any value of j. However, to help Bob, Alice sends n-level information to Bob regarding x_i. This communication is one-way, i.e., there is no communication from Bob's side to Alice's side. But before the game starts, they (Alice and Bob) can fix an encoding-decoding strategy. Notice that if $n = d$, then the scenario is trivial, i.e., Bob is able to identify the value of the random variable perfectly (with 100% certainty) for any value of j. When $n < d$ (i.e., n is limited), Bob is not able to identify the value of the random variable perfectly for all values of j. Then, it can be explored how well Bob can identify the value of the random variable for any value of j.

We mention that for unambiguous identification, we have to keep the size of the set S_j, i.e., $|S_j| = n$, $2 \leqslant n < d$, because if $|S_j| > n$, then unambiguous identification of the value of the random variable is clearly not possible. Now, when a value of the random variable is sent to Alice, information on a set is sent to Bob. This set must contain the value that is sent to Alice along with other $n - 1$ values. Here the question is how many such sets are possible? This is clearly equal to $\binom{d}{n} = \frac{d!}{n!(d-n)!}$. These numbers define different values of j. Remember that Alice does not know the information on which set is sent to Bob, but she knows that the set must contain the value of the random variable, which she has received, along with some other value(s). We mention that the set of values of the variable X, i.e., $\{x_1, x_2, \dots, x_d\}$, is known to both Alice and Bob. The value of n is also known to Alice and Bob. Based on the values of d and n, several random sets can be defined; these definitions are also known to them.

A. $n > 2$ case

We next consider that when the dimension of the random variable is "d," the Referee sends a random set of cardinality "n" to Bob. In this case, if $n > 2$, then sending a qubit from Alice's side to Bob will not help in accomplishing the task. In particular, it is possible to show that the above is solvable if Alice is allowed to send a qunit (n-level quantum system) to Bob. On the other hand, sending a cnit (n-level classical system) will not help in accomplishing the task of identifying the value of the random variable unambiguously with some nonzero probability for all j values. We mention that in the classical case, an n-level information is defined by cnit, which can have the values $0, 1, \dots, n - 1$. In the quantum case, an n-level information is defined by qunit, which can have the states $|0\rangle, |1\rangle, \dots, |n - 1\rangle$. The general case is quite straightforward. Here we only discuss the case when $d = 4$ and $n = 3$, that is, Alice is given $x_i \in \{x_1, x_2, x_3, x_4\}$ and Bob is given "j," where "j" is associated with S_j, $\forall j = 1, 2, 3, 4$. Here, $S_1 = \{x_1, x_2, x_3\}$, $S_2 = \{x_1, x_3, x_4\}$, $S_3 = \{x_1, x_2, x_4\}$, and $S_4 = \{x_2, x_3, x_4\}$.

We assume that Alice is allowed to send a ctrit (three-level classical system) to Bob. The values of the random variable are equally probable, and thus the sets S_j are also equally probable. So, here Alice has to compute a function that must output different values for different x_i, otherwise unambiguous identification of x_i is impossible for all values of j. Now, even if computation of such a function is possible, encoding the values of the function corresponding to different x_i within a three-level classical system is impossible. Thus, it is not possible for Alice and Bob to win that game when Alice is allowed to send only a ctrit to Bob.

However, it is possible to construct a quantum strategy through which Bob can identify the value of the random variable unambiguously with some nonzero probability for all values of j when Alice is sending only a qutrit to Bob. The encoding strategy is given as follows: $x_i \rightarrow |\phi_i\rangle$, $\forall i = 1, 2, 3, 4$. We can take $|\phi_i\rangle$ as linearly independent states $\forall i = 1, 2, 3$, and we can take $|\phi_4\rangle$ as $a_1 |\phi_1\rangle + a_2 |\phi_2\rangle + a_3 |\phi_3\rangle$, where $|a_i|$ are nonzero. a_i are chosen in such a way that $|\phi_4\rangle$ must be a valid state. For simplicity, one can simply take $|\phi_i\rangle$ as $|i\rangle$, $i = 1, 2, 3$. Here, $\{|i\rangle\}$ forms a basis for a qutrit system. Now, notice that for any value of "j," Bob is left with three linearly independent vectors that can be distinguished unambiguously with some nonzero probability. Therefore, the value of the random variable can be identified unambiguously with some nonzero probability for all values of j. We mention that if $\{|\phi_1\rangle, |\phi_2\rangle, |\phi_3\rangle\}$ is a basis, then we say that the state of the form $\mu_1 |\phi_1\rangle + \mu_2 |\phi_2\rangle + \mu_3 |\phi_3\rangle$ is a coherent state of coherence rank 3 with respect to the considered basis; here, $|\mu_i| > 0$ $\forall i$. We now provide the following proposition:

Proposition 6. For winning the game, it is necessary and also sufficient for the state $|\phi_4\rangle$ to have coherence rank 3 with respect to the basis $\{|\phi_1\rangle, |\phi_2\rangle, |\phi_3\rangle\}$.

Proof. The states $|\phi_1\rangle$, $|\phi_2\rangle$, and $|\phi_3\rangle$ are linearly independent. So, they form a basis for a qutrit (three-level quantum) system. The sufficient condition follows from the fact that there exists a strategy that is given above. The necessary condition follows from a couple of arguments. If the coherence rank is less than 3, then there is at least one value of "j" for which three states (to be distinguished by Bob) are not linearly independent, and thus the unambiguous discrimination of such states is not possible. Furthermore, the coherence rank cannot be greater than 3 when Alice is sending a qutrit to Bob. These complete the proof. ∎

From the above example, it is quite realizable that by using the same model, it is possible to show that a qunit is a more powerful resource than a cnit in the context of the present task. Again, if the dimension of the random variable "d" is very large, then it is also possible to show that a qunit can provide an advantage over a large number of cnits in the context of achieving a specific goal in our game.

VI. CONCLUSION

To develop quantum technologies, it is necessary to explore what advantages one can achieve using quantum resources over their classical counterparts. Furthermore, it is also important to identify the scenarios in which it is not possible to achieve such advantages.

In this work, we have designed a task that can be described in terms of a game, mediated by a Referee and played between Alice and Bob. The Referee sends Alice a value of a random variable. At the same time, the Referee also sends Bob some partial information regarding that value. Here partial information can be defined in the following way. Bob gets the information of a random set that must contain the value of the variable that is sent to Alice by the Referee, along with other value(s). Alice is not allowed to know what information is sent to Bob by the Referee. Again, Bob does not know which value of the random variable is sent to Alice. Now, the game can be won if and only if Bob can unambiguously identify the value of the variable with some nonzero probability, no matter what information Bob receives or which value is sent to Alice. However, to help Bob, Alice sends some limited information to him based on any predecided strategy.

For this game, we have shown an advantage of sending a qubit over cbit(s). However, whether there is any quantum advantage at all depends on the goal we set. In particular, we have proved that in some scenarios, it is never possible to achieve any quantum advantage. We also mention that to establish a quantum advantage, it is not necessary to share entanglement among the spatially separated parties in the present game. Actually, here quantum coherence plays the key role. We have also analyzed several variants of the game and provided certain bounds on the success probabilities. Moreover, we have established connections between the trine ensemble, mutually unbiased bases, and the encoding-decoding strategies of the variants. In fact, our games should be treated as applications of the trine ensemble, mutually unbiased bases, and quantum coherence.

To understand the application of the present game, it is required to explain its similarity with the quantum dense coding protocol [4]. Consider the simplest case of our game, i.e., the $d = 3$ case. In this case, Alice is given a random two-bit string that belongs to the set $\{00, 01, 10\}$. One can think that these are basically values of the random variable. There is a limited communication from Alice's side to Bob, which is one qubit or one cbit. Bob's task is to identify the bit string error-free. The only difference between the dense coding and our game is that in the former protocol there is entanglement present between Alice and Bob, while in our case there is no entanglement present between Alice and Bob. Instead, Bob is receiving additional information (which is from the Referee) in our case. Here, as with dense coding, when Alice communicates a qubit more information can be extracted by Bob regarding the bit string of Alice. The setting of dense coding is well established at present in quantum information theory. Therefore, exploiting its connection with our game, one can think about various applications in information processing protocols. However, further analysis is required to exhibit such applications explicitly.

Finally, we want to talk about the experimental realization of the game. As explained above, our game has a similarity with the setting of the dense coding protocol. In fact, the dense coding protocol was experimentally demonstrated several years back [38]. So, we believe that there is a possibility to demonstrate our game experimentally. However, we mention that here we have considered a probabilistic setting. In this regard, we mention Ref. [39], where the optimal unambiguous state elimination problem was demonstrated experimentally. In our case, when $n = 2$, state elimination and state discrimination are equivalent. So, there is a possibility of demonstrating some versions of our game experimentally. Nevertheless, with increasing dimension of the random variable, the situation will become more complex.

For further research, we present the following open question. What will happen in our communication tasks when extra resources, such as randomness, entanglement, etc., are provided between Alice and Bob?

ACKNOWLEDGMENTS

We acknowledge discussion with M. Parniak, M. Lipka, and M. Mazelanik. This work was supported by the National Science Centre, Poland (Grant No. 2022/46/E/ST2/00115) and the "Quantum Optical Technologies" project, carried out within the International Research Agendas programme of the Foundation for Polish Science co-financed by the European Union under the European Regional Development Fund. M.B. acknowledges funding from the National Mission in Interdisciplinary Cyber-Physical systems from the Department of Science and Technology through the I-HUB Quantum Technology Foundation (Grant No. I-HUB/PDF/2021-22/008), support through the research grant of INSPIRE Faculty fellowship from the Department of Science and Technology, Government of India, and the start-up research grant from SERB, Department of Science and Technology (Grant No. SRG/2021/000267).

[1] J. P. Dowling and G. J. Milburn, Philos. Trans. R. Soc. (London) Ser. A **361**, 1655 (2003).
[2] I. H. Deutsch, PRX Quantum **1**, 020101 (2020).
[3] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[4] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).
[5] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
[6] A. S. Holevo, Prob. Inf. Trans. **9**, 177 (1973).
[7] P. E. Frenkel and M. Weiner, Commun. Math. Phys. **340**, 563 (2015).
[8] S. Wiesner, ACM SIGACT News **15**, 78 (1983).
[9] A. Ambainis, A. Nayak, A. Ta-Shma, and U. Vazirani, *Proceedings of the 31st Annual ACM Symposium on Theory of Computing (STOC'99)* (ACM, New York, 1999), pp. 376–383.
[10] A. Ambainis, A. Nayak, A. Ta-Shma, and U. Vazirani, J. ACM **49**, 496 (2002).
[11] S. Aaronson, Theor. Comput. **1**, 1 (2005).
[12] D. Gavinsky, J. Kempe, O. Regev, and R. de Wolf, in *Proceedings of the 38th Annual ACM Symposium on Theory of Computing (STOC'06)* (ACM, New York, 2006), pp. 594–603.

[13] S. Aaronson, Proc. R. Soc. A **463**, 3089. (2007).

[14] R. W. Spekkens, D. H. Buzacott, A. J. Keehn, B. Toner, and G. J. Pryde, Phys. Rev. Lett. **102**, 010401 (2009).

[15] M. Pawłowski, T. Paterek, D. Kaszlikowski, V. Scarani, A. Winter, and M. Żukowski, Nature (London) **461**, 1101 (2009).

[16] H.-W. Li, M. Pawłowski, Z.-Q. Yin, G.-C. Guo, and Z.-F. Han, Phys. Rev. A **85**, 052308 (2012).

[17] M. Banik, S. S. Bhattacharya, A. Mukherjee, A. Roy, A. Ambainis, and A. Rai, Phys. Rev. A **92**, 030103(R) (2015).

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

[19] A. Ambainis, M. Banik, A. Chaturvedi, D. Kravchenko, and A. Rai, Quant. Inf. Proc. **18**, 111 (2019).

[20] M. Vaisakh, R. Patra, M. Janpandit, S. Sen, M. Banik, and A. Chaturvedi, Phys. Rev. A **104**, 012420 (2021).

[21] R. K. Patra, S. G. Naik, E. P. Lobo, S. Sen, G. L. Sidhardh, M. Alimuddin, and M. Banik, Phys. Rev. Lett. **130**, 110202 (2023).

[22] A. Chefles, Phys. Rev. A **69**, 050307(R) (2004).

[23] S. Halder and U. Sen, Phys. Rev. A **105**, L030401 (2022).

[24] S. Massar, D. Bacon, N. J. Cerf, and R. Cleve, Phys. Rev. A **63**, 052305 (2001).

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

[26] R. de Wolf, SIAM J. Comput. **32**, 681 (2003).

[27] E. F. Galvão and L. Hardy, Phys. Rev. Lett. **90**, 087902 (2003).

[28] C. Perry, R. Jain, and J. Oppenheim, Phys. Rev. Lett. **115**, 030504 (2015).

[29] A. Chefles, Phys. Lett. A **239**, 339 (1998).

[30] I. Ivanovic, Phys. Lett. A **123**, 257 (1987).

[31] D. Dieks, Phys. Lett. A **126**, 303 (1988).

[32] A. Peres, Phys. Lett. A **128**, 19 (1988).

[33] A. Streltsov, G. Adesso, and M. B. Plenio, Rev. Mod. Phys. **89**, 041003 (2017).

[34] S. M. Barnett and S. Croke, Adv. Opt. Photon. **1**, 238 (2009).

[35] I. D. Ivonovic, J. Phys. A **14**, 3241 (1981).

[36] I. Ivanovic, Phys. Lett. A **228**, 329 (1997).

[37] S. Bandyopadhyay, P. O. Boykin, V. Roychowdhury, and F. Vatan, Algorithmica **34**, 512 (2002).

[38] K. Mattle, H. Weinfurter, P. G. Kwiat, and A. Zeilinger, Phys. Rev. Lett. **76**, 4656 (1996).

[39] J. W. Webb, I. V. Puthoor, J. Ho, J. Crickmore, E. Blakely, A. Fedrizzi, and E. Andersson, Phys. Rev. Res. **5**, 023094 (2023).