On quantum advantage in the random access code protocols with two-qubit states

Som Kanjilal,1, * Chellassamy Jebarathinam,2, 3 Tomasz Paterek,4, 5, 6 and Dipankar Home7

1Harish-Chandra Research Institute Chhatnag Road, Jhunsi, Prayagraj (Allahabad) 211 019 India
2S. N. Bose National Centre for Basic Sciences, Block JD, Sector III, Salt Lake, Kolkata 700 106, India
3Department of Physics and Center for Quantum Frontiers of Research and Technology (QFort), National Cheng Kung University, Tainan 701, Taiwan
4School of Physical and Mathematical Sciences, Nanyang Technological University, 637371 Singapore, Singapore
5Majulab, International Joint Research Unit UMI 3654, CNRS, Universite Cote d’Azur, Sorbonne Universite, National University of Singapore, Nanyang Technological University, Singapore
6Institute of Theoretical Physics and Astrophysics, Faculty of Mathematics, Physics and Informatics, University of Gda´nsk, 80-308 Gda´nsk, Poland
7Center for Astroparticle Physics and Space Science (CAPSS), Bose Institute, Kolkata-700 091, India

Random access code (RAC) is an important communication task to conditionally access remote n-bit string even if one has limited information about it. Here we consider the version of this task assisted with shared randomness (quantum/classical) with fixed local dimension of two and the communicated information of a single classical bit. Quantum advantage is obtained in terms of worst-case success probability, p. We demonstrate that, there exist quantum strategies utilizing bipartite qubit state with invertible correlation matrix that outperform the corresponding dimensionally equivalent shared classical randomness source for RAC protocols when n = 2, 3. In case of n ≥ 4 such quantum strategies do not exist for the RAC protocols considered here.

I. INTRODUCTION

Quantum entanglement has long been recognized as a powerful resource demonstrating quantum nonlocality [1] as well as for implementing various information processing tasks [2]. In particular, in the area of quantum communication, the efficacy of quantum entanglement in implementing communication protocols with better-than-classical results has been extensively demonstrated [3]. However, since the creation, manipulation and protection of entanglement against decohering effects are quite daunting, it becomes important to ask whether quantum correlations inherent in the separable states can be harnessed as resource for quantum advantage in certain quantum information processing (QIP) tasks? It is this question that motivates the present paper which focuses, in particular, on the specific communication protocol known as finite shared randomness assisted Random Access Code (RAC) [4].

A n \overset{p}{\rightarrow} m m RAC is a two party information theoretic task where a sender/encoder (Alice) is in possession of a bit string of length n. It is a two step process, involving a communication step and a guessing step. In communication step, Alice sends to a receiver/decoder (Bob) another bit string of length m (m < n), encoding the information about n bit string [5]. In the guessing step, Bob guesses any of the n bits correctly with probability at least p [5, 6]. In other words, p is the worst case success probability corresponding to the RAC task. This task has been adapted for multifaceted applications ranging from random number generation [7], network coding theory [8], quantum key distribution [9] to dimension witnessing [10] and self-testing [11]. From the foundational perspective, we note that a version of RAC in the context of generalized probability theory [12] studied with respect to PR box [13] facilitates characterization of quantum theory from information theoretic principles [14].

Restricting ourselves to the n \overset{p}{\rightarrow} 1 1 RAC task, in the quantum regime, this can be implemented using either quantum bit communication (Quantum Random Access Code, QRAC) or a classical bit communication [6] with shared quantum state [15] (Entanglement Assisted Random Access Code, EARAC). Both the quantum versions of the RAC protocols have been experimentally demonstrated [16, 17]. In case of QRAC it was shown for n ≥ 4 and m = 1 there is no quantum strategy that yields p > 1/2 [18]. Nonetheless, QRAC with additional classical shared randomness can provide p > 1/2 for n ≥ 4 [6]. In case ofEARAC, a process known as concatenation (which involves multiple quantum states shared between Alice and Bob) is required to obtain quantum advantage for n ≥ 4 [15]. On this backdrop, a comparison between the classical shared randomness [6] and bipartite quantum state (without concatenation) in the context of RAC task was started in [4], in which; performance of most primitive classical shared randomness assisted RAC was described in detail. Here we describe the corresponding quantum protocol and a comparison with its classical counterpart is provided.

We consider a version of RAC using a shared quantum state, not necessarily entangled [4]. To be more specific, we consider the scenario, where Alice and Bob try to perform the n \overset{p}{\rightarrow} 1 1 RAC task with the help of a single copy of any shared bipartite qubit state. We compare it with classical RAC protocol assisted with two bits of shared randomness, i.e., each party gets a bit from the shared source. Note that, the classical source is characterized in terms of a probability distribution over a four-bit string S1 × S2, where S2 is the binary-set {0, 1}. Quantum source is characterized in terms of a density matrix in C2 ⊗ C2, where C2 is two-dimensional Hilbert space. \( \otimes \) is cartesian product of sets and tensor product of Hilbert spaces respectively. Thus, we take both the resources to be dimensionally equivalent. The performance of such a classical n \overset{p}{\rightarrow} 1 1 RAC protocol has been studied in [4] and upper bounds on p (\( \frac{3}{7} \) and \( \frac{1}{2} \)) for n = 2 and n ≥ 3 respectively have been found. In this paper we study the corresponding quantum protocol. We show that for n = 2, 3 a bipartite qubit state can outperform the best dimensionally equivalent classical protocol. The resource empowering the quantum advantage is identified as invertibility of correlation matrix. Furthermore, we show that for n ≥ 4 there is no quantum advantage using a broad class of protocols.

Previous studies on the non-classical features required to outperform the classical variant of RAC protocol have taken

* som.kanjilal1011991@gmail.com
average success probability as the measure of efficiency [19] and demonstrated that preparation contextuality [20] is the resource for quantum advantage [16, 21]. In contrast, we have taken worst case probability as measure of efficiency which enables demonstrating the use of a separable state as a resource in the RAC protocol.

In the context of the shared randomness assisted RAC protocols, it was shown earlier that geometric discord helps to achieve quantum advantage in the 2 \( \xrightarrow{x} y \) and 3 \( \xrightarrow{1} \) 1 cases if we use Bell diagonal states as resource [4]. However, for these two RACs, if we confine ourselves to the separable state space, the optimal quantum advantage is provided by a non-maximal discordant Bell-diagonal state. Thus, in the context of 2 \( \xrightarrow{x} y \) 1 and 3 \( \xrightarrow{1} \) 1 cases, the amount of geometric discord does not specify the state yielding optimal efficiency. Consequently, a way out is to construct a suitable measure of non-classicality whose maximum value (within the separable state space) yields the quantum states with optimal efficiency. It was shown earlier that geometric discord helps to achieve quantum advantage corresponding for any encoding strategy. We will see for certain classes of bipartite qubit states with invertible correlation matrix is non-classical feature of a quantum state.

The paper is organized as follows. In Sec. II, we introduce the RAC protocol relevant for our purpose and show that there is no suitable encoding/decoding strategy leading to quantum advantage for these protocols with \( n \geq 4 \). In Sec III we show that, in the 2 \( \xrightarrow{x} y \) 1 case, for certain classes of bipartite qubit states with invertible correlation matrix, there exist suitable encoding strategies demonstrating quantum advantage corresponding for any encoding strategy. We will see that invertibility of correlation matrix is not sufficient to demonstrate quantum advantage for 2 \( \xrightarrow{x} y \) 1 RAC as the classical bound is greater than half. On the other hand, in the case of 3 \( \xrightarrow{x} y \) 1 RAC protocol, since the classical bound is half, invertibility of correlation matrix of any shared bipartite qubit states is sufficient to demonstrate quantum advantage.

II. QUANTUM ADVANTAGE IN FINITE SHARED RANDOMNESS ASSISTED RANDOM ACCESS CODES

The scenario we study is depicted in Fig. 1. Alice and Bob share a source of classical bits or quantum bits (qubits), \( S_R \), which delivers them systems \( r_a \) and \( r_b \), respectively. Alice’s dataset is a string of \( n \) classical bits \( x = \{ x_1, x_2, \ldots, x_n \} \) where \( x_i \) is either 0 or 1. She encodes the information about \( x \) in a bit \( a \) with the help of a (q)ubit from the shared source and communicates \( a \) to Bob. Using the communicated bit and the (q)ubit from the shared source Bob guesses a randomly chosen bit of Alice’s dataset. The classical version where single bit \( r_a \) and \( r_b \) is communicated to both parties and \( m = 1 \) has been studied and the upper bounds on the classical success probabilities have been obtained as follows

\[ p = \min_{x,y} \sum_{a,b} \frac{1}{2} \left( 1 + (\delta(x,a)\delta(y,b) - \delta(x,a)\delta(y,b)) \right) \]  

\[ = \min_{A_{x,y}} \sum_{a,b} \delta(x,a)\delta(y,b) \]  

\[ = \min_{A_{x,y}} \sum_{a,b} \delta(x,a)\delta(y,b) \]  

\[ = \min_{A_{x,y}} \sum_{a,b} \delta(x,a)\delta(y,b) \]  

Here \( \hat{B}_b \) is the projector pertaining to outcome \( b \) of measurement setting \( B \). The minimization is taken over both 2\( n \) Bloch vectors of \( A \) and \( n \) Bloch vectors of \( B \).

For a bipartite qubit state given by

\[ \rho_{AB} = \frac{1}{4} [\hat{I} \otimes \hat{I} + \hat{M} \otimes \hat{N} + \hat{N} \otimes \hat{N} + \hat{I} \otimes \hat{I} + \hat{M} \otimes \hat{N} + \hat{N} \otimes \hat{I} + \hat{I} \otimes \hat{N} + \hat{M} \otimes \hat{M}], \]  

where \( \hat{M} \) and \( \hat{N} \) are Bloch vectors, with \( ||\hat{M}|| \leq 1, ||\hat{N}|| \leq 1 \) and \( T_{ij} = \text{Tr}(\hat{\sigma}_i \otimes \hat{\sigma}_j \rho_{AB}) \) is the 3 \( \times \) 3 correlation matrix, we can rewrite

FIG. 1. Shared randomness assisted 1 \( \xrightarrow{m} \) RAC. Bob is asked to give the value of randomly selected bit of Alice’s dataset. Alice communicates \( m \) bit string and they both share correlated classical or quantum bits from the source \( S_R \).

(i) \( p_{cl} \leq \frac{1}{2} \) if \( n \geq 3 \);

(ii) \( p_{cl} \leq \frac{1}{2} \) if \( n = 2 \);

(iii) \( p_{cl} \leq \frac{1}{2} \) for \( n \geq 2 \) if the bits have maximally mixed marginals, i.e. probability of getting bit 0 = probability of getting bit 1 = \( \frac{1}{2} \) for each party.
eq. (3) as

\[ p = \min_{\hat{A}, \hat{B}, \hat{M}} \left\{ \frac{1}{2} \sum_{a,b} \delta_{g_0(a,b), x_0} \left[ 1 + (-1)^a \hat{A}^\dagger \hat{M} + (-1)^b \hat{N}^\dagger \hat{B} + (-1)^{a+b} \hat{A}^\dagger T \hat{B} \right] \right\} \]  

(5)

here \( \hat{A}, \hat{B}, \hat{M} \) and \( \hat{N} \) are represented by \( 3 \times 1 \) column vectors (the first two being the Bloch vectors representing the measurements with the corresponding outcome being 0), \( \hat{A}^\dagger \) is the transpose of \( \hat{A} \), and \( T \) is the correlation matrix. Taking

\[ \sum_{a,b} \delta_{g_0(a,b), x_0} (-1)^a = 2\alpha(x,y), \]  

(6)

\[ \sum_{a,b} \delta_{g_0(a,b), x_0} (-1)^b = 2\beta(x,y), \]  

(7)

\[ \sum_{a,b} \delta_{g_0(a,b), x_0} (-1)^{a+b} = 2\gamma(x,y), \]  

(8)

we can re-write eq. (5) as

\[ p = \min_{\hat{A}, \hat{B}, \hat{M}} \left\{ \frac{1}{2} \left[ \alpha(x,y) + \beta(x,y)\hat{A}^\dagger \hat{M} + \gamma(x,y)\hat{N}^\dagger \hat{B} + \phi(x,y)\hat{A}^\dagger T \hat{B} \right] \right\} \]  

(10)

Note that, the term within the curly bracket in eq. (10) is actually the probability of success \( \sum_{a,b} p(g_0(a,b) = x_0|x,y) \) for the pair \( (x,y) \) as defined in eq. (1). From (i), the condition to demonstrate the advantage of bipartite qubit state over dimensionally equivalent shared randomness source in the \( n \rightarrow 1 \) RAC with \( n \geq 3 \) is to ensure that

\[ \sum_{a,b} p(g_0(a,b) = x_0|x,y) > 1 \]  

for each pair \( (x,y) \). In other words, given a pair \( (x,y) \), if the success probability exceeds the classical bound then quantum advantage is obtained for that pair. If such an advantage is obtained for all the pairs \( (x,y) \) then the shared quantum state leads to quantum advantage for the corresponding RAC protocol.

Now we can restate the condition of quantum advantage in light of eq. (10) as follows: for each pair \( (x,y) \) if there exists a constant \( \epsilon(x,y) > 0 \) such that

\[ \hat{A}^\dagger T \hat{B} = \frac{1 + \epsilon(x,y) - \alpha(x,y) - \beta(x,y)\hat{A}^\dagger \hat{M} - \gamma(x,y)\hat{N}^\dagger \hat{B} + \phi(x,y)}{\phi(x,y)} \]  

(11)

then quantum advantage is obtained.

Note that, writing eq. (11) we assumed \( \phi(x,y) \neq 0 \) for all the pairs \( (x,y) \). This does not rule out the strategies corresponding to \( \phi(x,y) = 0 \) for quantum advantage. However if \( \phi(x,y) = 0 \) then the success probability for the pair \( (x,y) \) does not depend on the correlation matrix \( T \). In this case, the same success probability is obtained if we use the product state \( \text{Tr}_B[\rho_{AB}] \otimes \text{Tr}_A[\rho_{AB}] \) instead of \( \rho_{AB} \). Since, the product state does not admit any correlations one is not able to obtain any advantage for the pair \( (x,y) \). Thus, the protocols with \( \phi(x,y) \neq 0 \) for all the pairs \( (x,y) \), exhaust those that may lead to quantum advantage.

Within this class of protocols we show that for \( n \geq 4 \) there does not exist any strategy leading to quantum advantage i.e. there is no \( (\mathcal{A}, \mathcal{B}) \) such that quantum advantage is obtained using bipartite qubit state. In particular, similar to [18], we show there does not exist \( 2^n \) distinct encoding strategies such that eq. (11) is satisfied for each \( x \) and \( y \).

For \( n = 2, 3 \) cases, there exists a classical decoding strategy \( g_0(a,b) = (a + b) \mod 2 \) and we construct protocols demonstrating quantum advantage when the correlation matrix is invertible.

In what follows, we start with the proof of impossibility of quantum advantage for \( n \geq 4 \). This was proven in [8] for QRAC protocol whereas, our proof is for shared quantum state assisted RAC protocol from the described class.

**Result 1.** For \( n \geq 4 \) 1 RAC protocol with bipartite qubit state as resource, given a set of classical decoding strategies \( g_0(a,b) \) and a set of \( n \) decoding operations \( \mathcal{B} = \{ \hat{B}_j \} \) there does not exist \( 2^n \) encoding operations \( \mathcal{A} \) such that quantum advantage is obtained, in other words, there does not exist \( 2^n \) encoding operations \( \mathcal{A} \) such that eq. (11) is satisfied for each \( \hat{A}_x \in \mathcal{A} \) and \( \hat{B}_j \in \mathcal{B} \).

**Proof.** Let us assume

\[ \chi(x,y) = \frac{1 + \epsilon(x,y) - \alpha(x,y) - \beta(x,y)\hat{A}^\dagger \hat{M} - \gamma(x,y)\hat{N}^\dagger \hat{B} + \phi(x,y)}{\phi(x,y)} \]  

(12)

with this notation we can re-write eq. (11) as

\[ \hat{A}^\dagger T \hat{B} = \chi(x,y) \]  

(13)

Now, taking \( B = [\hat{B}_1, \hat{B}_2, \hat{B}_3, \ldots, \hat{B}_n] \) as the \( 3 \times n \) matrix and \( \chi(x) = [\chi(x,1), \chi(x,2), \chi(x,3), \ldots, \chi(x,n)] \) as a \( 1 \times n \) row vector we have the following system of \( n \) linear equations for three components of \( \hat{A}_x \) as the unknown variables:

\[ \hat{A}^\dagger T B = \chi(x) \]  

(14)

The solution for \( T^\dagger \hat{A}_x \) is then given by

\[ T^\dagger \hat{A}_x = (BB^\dagger)^{-1} B \chi(x) \]  

(15)

In Appendix A we show that \( (BB^\dagger)^{-1} B = B(B^\dagger B)^{-1} \) and hence

\[ T^\dagger \hat{A}_x = B(B^\dagger B)^{-1} \chi(x). \]  

(16)

Note that, existence of \( 2^n \) distinct encoding operations \( \{\hat{A}_x\} \) is equivalent to the existence of \( 2^n \) distinct operations \( \{T^\dagger \hat{A}_x\} \). From eq. (16) it is evident that existence of \( 2^n \) distinct operations \( \{T^\dagger \hat{A}_x\} \) depends upon invertibility of \( n \times n \) matrix \( B^\dagger B \). Note that the columns of \( B \) are the unit norm vectors \( \{\hat{B}_1, \hat{B}_2, \hat{B}_3, \ldots, \hat{B}_n\} \) on the Bloch sphere, therefore the \( B^\dagger B \) is a Gram matrix with diagonal entries equal to 1 and off-diagonal entries being cosines of the angles between the decoding operations \( \hat{B}_i \) and \( \hat{B}_j \). It is known that a Gram matrix
with \( n \) \( m \)-dimensional vectors is invertible if and only if the set of vectors \( \{ \hat{B}_1, \hat{B}_2, \hat{B}_3, \ldots, \hat{B}_n \} \) is linearly independent \([26]\). However, in case of a qubit system \( n \geq 4 \) linearly independent vectors on Bloch sphere do not exist. Thus \( 2^n \) distinct operations of the form of eq. (16) do not exist for \( n \geq 4 \). We can also use eigenvalue decomposition of \( B^\dagger B \) to argue for the non-existence. Note that matrix \( B^\dagger B \) is invertible if and only if all its eigenvalues are non-zero, however in case of \( B^\dagger B \) with \( B \) being a \( 3 \times n \) matrix, maximum number of non-zero eigenvalues is 3, thus \( B^\dagger B \) is non-invertible for \( n \geq 4 \).

As \( 2^n \) distinct \( \{ T^\dagger \hat{A}_i \} \) do not exist it follows that \( 2^n \) distinct encoding operations \( \{ \hat{A}_i \} \) do not exist. \( \square \)

### III. QUANTUM ADVANTAGE FOR \( 2 \overset{\theta}{\rightarrow} 1 \) AND \( 3 \overset{\theta}{\rightarrow} 1 \) RANDOM ACCESS CODES

In this section we construct RAC protocols demonstrating quantum advantage for \( n = 2, 3 \). To achieve this, we consider the classical decoding strategy \( g_{s}(a, b) = (a + b) \mod 2 \). It follows that, we have \( \alpha(x, y) = 1, \beta(x, y) = \gamma(x, y) = 0 \) and \( \phi(x, y) = (-1)^{xy} \). We start with \( 2 \overset{\theta}{\rightarrow} 1 \) RAC then move to \( 3 \overset{\theta}{\rightarrow} 1 \) case.

#### A. Quantum Advantage for \( 2 \overset{\theta}{\rightarrow} 1 \) Random Access Codes

The condition for quantum advantage for \( 2 \overset{\theta}{\rightarrow} 1 \) RAC is now given by

\[
\min_{\hat{A}_s, e \in [A, B]} \left\{ \frac{1}{2} \left( 1 + (-1)^{sy} \hat{A}_s^\dagger T \hat{B}_s \right) \right\} > \frac{2}{3}
\]

(17)

In what follows, we will assume that the decoding operations are orthogonal i.e. \( \hat{B}_s = (\hat{B}_1, \hat{B}_2)|\hat{B}_1^\dagger \hat{B}_2 = 0 \) and choose encoding operations of the form

\[
\hat{A}_s = \frac{(T^{-1})^\dagger((-1)^{sy} \hat{B}_1 + (-1)^{sz} \hat{B}_2)}{||(T^{-1})^\dagger((-1)^{sy} \hat{B}_1 + (-1)^{sz} \hat{B}_2)||}.
\]

(18)

Given this choice of quantum strategy \( \{A, B\} \) we find out the lower and upper bounds on the worst case success probability \( p \) and find suitable condition on the state-parameters such that the lower bound of \( p \) exceeds the classical upper bound of \( \frac{2}{3} \). In particular, the following result is to be proved

**Result 2.** Corresponding to any set of orthogonal decoding strategies there exists a suitable set of encoding strategies demonstrating quantum advantage over dimensionally equivalent finite shared randomness assisted \( 2 \overset{\theta}{\rightarrow} 1 \) RAC protocol (\( p > \frac{2}{3} \)), if the correlation matrix is invertible and square of the smallest correlation is greater than \( \frac{2}{3} \).

**Proof.** Without loss of generality we can take \( T \) to be diagonal i.e. \( T = \text{diag}[t_1, t_2, t_3] \), where \( 1 \geq |t_1| \geq |t_2| \geq |t_3| \) and \( \hat{e}_i \) is the Cartesian axis of Bob. Consequently, the inverse matrix, \( T^{-1} \)

can be written as \( T^{-1} = \text{diag}[\frac{1}{t_1}, \frac{1}{t_2}, \frac{1}{t_3}] \) with \( 1 \leq \frac{1}{t_1} \leq \frac{1}{t_2} \leq \frac{1}{t_3} \).

Taking \( \hat{B}_s = \frac{1}{\sqrt{t_2}}(\hat{B}_1 + \hat{B}_2) \) we obtain the minimum success probability as follows

\[
p = \frac{1}{2} \left[ 1 + \frac{1}{\sqrt{2} \max(||T^{-1} \hat{B}_1||, ||T^{-1} \hat{B}_2||)} \right].
\]

(19)

Note that, \( \{\hat{e}_1, \hat{e}_2, \hat{e}_3\} \) forms a complete basis. Consequently, we can write \( \hat{B}_s \) as follows

\[
\hat{B}_s = \cos \theta \hat{e}_1 + \sin \theta (\sin \phi \hat{e}_2 + \cos \phi \hat{e}_3),
\]

(20)

\[
\hat{B}_s = -\sin \theta \hat{e}_1 + \cos \theta (\sin \phi \hat{e}_2 + \cos \phi \hat{e}_3),
\]

(21)

Eq. (19) can then be rewritten as

\[
p = \frac{1}{2} \left[ 1 + \frac{1}{\sqrt{2} \max(K_+, K_-)} \right],
\]

(22)

where

\[
K_+ = \frac{\cos^2 \theta}{t_1^2} + \frac{\sin^2 \theta \cos^2 \phi}{t_2^2} + \frac{\sin^2 \theta \sin^2 \phi}{t_3^2},
\]

(23a)

\[
K_- = \frac{\sin^2 \theta}{t_1^2} + \frac{\cos^2 \theta \cos^2 \phi}{t_2^2} + \frac{\cos^2 \theta \sin^2 \phi}{t_3^2}.
\]

(23b)

Using eq. (22), condition \( p > \frac{2}{3} \) can be re-written as

\[
\max(K_+, K_-) < \frac{9}{2} = 4.5.
\]

(24)

Note that, \( K_+ \) and \( K_- \) are the convex combinations of \((\frac{1}{t_1^2}, \frac{1}{t_2^2}, \frac{1}{t_3^2})\). In other words, for any choice of \((\theta, \phi)\) in eqs. (20) and (21) we have \(^1\)

\[
\frac{1}{t_1^2} \leq K_+ \leq \frac{1}{t_3^2}.
\]

Accordingly

\[
\frac{1}{t_1^2} \leq \max(K_+, K_-) \leq \frac{1}{t_3^2}.
\]

Using the lower and upper bounds of \(\max(K_+, K_-)\) on eq. (22) we finally obtain

\[
\frac{1}{2} \left( 1 + \frac{|t_3|}{\sqrt{2}} \right) \leq p \leq \frac{1}{2} \left( 1 + \frac{|t_1|}{\sqrt{2}} \right)
\]

(25)

Note that, in the case of \( 2 \overset{\theta}{\rightarrow} 1 \) the condition of quantum advantage is \( p > \frac{2}{3} \), which is satisfied for any choice of \((\theta, \phi)\) in eqs. (20) and (21) when \( |t_3| \geq \frac{\sqrt{2}}{3} \). In other words, we achieve quantum advantage for any choice of orthogonal decoding operations if the correlation matrix is invertible and square of the smallest correlation is greater than \( \frac{2}{3} \). \( \square \)

---

\(^1\) If \( x \) is a convex combination of \([x_1, x_2, \ldots, x_n]\) then \( \min\{x_1, x_2, \ldots, x_n\} \leq x \leq \max\{x_1, x_2, \ldots, x_n\} \).
Note that, we have compared the quantum RAC with the corresponding classical RAC whose bound is $\frac{1}{2}$ i.e. the case (ii) of the classical RAC discussed at the beginning. If we compare it with the case (iii), then the invertibility of correlation matrix ensures existence of encoding-decoding strategies such that $p > \frac{1}{2}$. Additional requirement on the correlation matrix is required to achieve $p > \frac{3}{4}$.

**B. Quantum Advantage for $3 \rightarrow 1$ Random Access Codes**

In case of $3 \rightarrow 1$ RAC protocol we only need $p > \frac{1}{2}$ for quantum advantage. In other words, we have

$$p = \min_{\hat{A}, \hat{B}, t \in \mathbb{R}} \left\{ \frac{1}{2} (1 + (-1)^{\frac{3}{2}} \hat{A}^T \hat{B} t) \right\} > \frac{1}{2} \quad (26)$$

Using the arguments of Sec. II we observe that in case of $3 \rightarrow 1$ RAC protocol quantum advantage is obtained if

$$(-1)^{\frac{3}{2}} \hat{A}^T \hat{B} t > 0 \quad (27)$$

for each $x \in [1, 2, \ldots, 8]$ and $y \in [1, 2, 3]$. In what follows, we prove the following:

**Result 3.** For $3 \rightarrow 1$ RAC protocol assisted with a bipartite qubit state with invertible correlation matrix, corresponding to any triad of non-coplanar vectors describing a set of decoding strategies, there exists a suitable set of encoding strategies such that $p > \frac{1}{2}$, thereby demonstrating quantum advantage.

**Proof.** Given a set of decoding strategies $B_3 = \{\hat{B}_1, \hat{B}_2, \hat{B}_3\}$, for each $x$ we consider

$$\hat{A}_x = \frac{(T^{-1}) (\frac{1}{2} \hat{B}_x \times \hat{B}_1 + (-1)^{\frac{1}{2}} \hat{B}_x \times \hat{B}_1 + (-1)^{\frac{1}{2}} \hat{B}_1 \times \hat{B}_2)}{\|T^{-1}((\frac{1}{2} \hat{B}_x \times \hat{B}_x + (-1)^{\frac{1}{2}} \hat{B}_x \times \hat{B}_x + (-1)^{\frac{1}{2}} \hat{B}_1 \times \hat{B}_2))\|}. \quad (28)$$

For such encoding operations, taking $V$ as the volume of the Parallelepiped formed using $\{\hat{B}_1, \hat{B}_2, \hat{B}_3\}$, we have

$$(-1)^{\frac{3}{2}} \hat{A}_x^T \hat{B}_t = \frac{V}{\|T^{-1}((\frac{1}{2} \hat{B}_x \times \hat{B}_x + (-1)^{\frac{1}{2}} \hat{B}_x \times \hat{B}_x + (-1)^{\frac{1}{2}} \hat{B}_1 \times \hat{B}_2))\|}$$

satisfying eq. $(27)$ for each $(x, y)$ and consequently, $p > \frac{1}{2}$.

Note that; $p > \frac{1}{2}$ if the decoding operations are non-coplanar vectors. □

As an illustration of the above result we consider bipartite qubit state given by eq. (4) along with diagonal correlation matrix $T = \text{diag}[t_1, t_2, t_3]$. If Bob’s decoding operations are taken to be along the Cartesian axes that diagonalize $T$ then we obtain the encoding operations from eq. $(28)$ as follows:

$$\hat{A}_x = \frac{1}{\sqrt{t_1^2 + t_2^2 + t_3^2}} \left[\begin{matrix} (-1)^{\frac{3}{2}} t_1 \hat{e}_1 + (-1)^{\frac{3}{2}} t_2 \hat{e}_2 + (-1)^{\frac{3}{2}} t_3 \hat{e}_3 \end{matrix}\right]. \quad (29)$$

where $\{\hat{e}_1, \hat{e}_2, \hat{e}_3\}$ are the corresponding orthogonal axes of Bob. In this case the minimum success probability is given by

$$p = \frac{1}{2} \left( 1 + \frac{1}{\sqrt{t_1^2 + t_2^2 + t_3^2}} \right). \quad (30)$$

**IV. CONCLUSIONS**

In summary, we have obtained quantum strategies assisted with bipartite qubit states that outperform in the $n \rightarrow 1$ RAC task the best dimensionally-equivalent classical protocol. In the case of $n = 2, 3$ a bipartite qubit state with invertible correlation matrix can be used as a resource behind quantum advantage. These results provide the first step towards the possibility of using invertibility of correlation matrix as resource for a quantum information theoretic task. Detailed study regarding resource theory [27] of invertibility of correlation matrix is an interesting problem for the future. For $n \geq 4$ we have provided an alternative proof of the result of [18] for a class of RAC protocols. It would be worthwhile to study whether one can generalize the proof to $n \rightarrow m$ RAC protocol.

**ACKNOWLEDGMENTS**

SK thanks NASI Research Associate fellowship. CJ acknowledges S. N. Bose Centre, Kolkata for the post-doctoral fellowship and support from Ministry of Science and Technology of Taiwan (MOST 108-2811-M-006-516). TP acknowledges support from the Polish National Agency for Academic Exchange NAWA Project No. PPN/PPO/2018/1/00007/U/00001. The research of DH is supported by NASI Senior Scientist Fellowship and the QUEST-DST project Q-98 of the Govt. of India.

[1] John S. Bell, “On the einstein podolsky rosen paradox,” *Physics Physique Fizika* **1**, 195–200 (1964).

[2] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters, “Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels,” *Phys. Rev. Lett.* **70**, 1895–1899 (1993).

[3] Charles H. Bennett and Stephen J. Wiesner, “Communication via one- and two-particle operators on einstein-podolsky-rosen states,” *Phys. Rev. Lett.* **69**, 2881–2884 (1992).
Appendix A: Proof of $(BB^\dagger)\cdot B = B(B^\dagger B)^{-1}$

**Theorem 1.** Any $m \times n$ matrix $B$ satisfies

$$(BB^\dagger)\cdot B = B(B^\dagger B)^{-1} \quad (A1)$$

**Proof.** Without loss of generality we assume $m \leq n$.

First consider $B$ to be a $m \times n$ diagonal matrix i.e. $B = \text{diag}[b_{ij}]$, where $1 \leq i \leq m$. As $B$ is a diagonal matrix its transpose $B^\dagger$ is $n \times m$ matrix with the same elements i.e. $B^\dagger = \text{diag}[b_{ij}]$, where $1 \leq i \leq m$. Then $BB^\dagger$ is a $m \times m$ diagonal matrix with the entries $b_{ii}^2$ i.e. $BB^\dagger = \text{diag}[b_{ii}^2]$, where $1 \leq i \leq m$. The inverse of $BB^\dagger$ is a $m \times m$ matrix with the entries $\frac{1}{b_{ii}^2}$, i.e. $(BB^\dagger)^{-1} = \text{diag}[\frac{1}{b_{ii}^2}]$, where $1 \leq i \leq m$. $(BB^\dagger)^{-1}B$ is a $m \times n$ diagonal matrix with the entries $\frac{1}{b_{ii}}$, i.e. $(BB^\dagger)^{-1}B = \text{diag}[\frac{1}{b_{ii}}]$, where $1 \leq i \leq m$. Following the same process it can be shown that $(B^\dagger B)^{-1}$ is $n \times n$ diagonal matrix with non-zero diagonal elements for the first $m$ rows, i.e. $(B^\dagger B)^{-1} = \text{diag}[\frac{1}{b_{ii}}]$, where $1 \leq i \leq m$. Then it can be seen that $B(B^\dagger B)^{-1}$ is $n \times m$ diagonal matrix with entries $\frac{1}{b_{ii}}$, i.e. $B(B^\dagger B)^{-1} = \text{diag}[\frac{1}{b_{ii}}]$, where $1 \leq i \leq m$. Therefore, $(BB^\dagger)^{-1}B = B(B^\dagger B)^{-1}$ when $B$ is a diagonal matrix.

For a general $m \times n$ matrix $B$ we use the singular value decomposition (SVD) of $B$ i.e. $B = U\Sigma B^\dagger$ where $\Sigma$ is the $m \times n$ diagonal matrix, $U$ and $V$ are $m \times m$ and $n \times n$ unitary matrices respectively. The LHS of eq. (A1) can now be written as

$$(BB^\dagger)^{-1}B = (U\Sigma B^\dagger)^{-1}U\Sigma B^\dagger V^\dagger = U(\Sigma B)^{-1}\Sigma B^\dagger V^\dagger \quad (A2)$$

Similarly, the RHS of eq. (A1) can be written as

$$B(B^\dagger B)^{-1} = U\Sigma B^\dagger (V\Sigma^{-1} B V^\dagger)^{-1} = U\Sigma B^\dagger V^\dagger \quad (A3)$$

Since $\Sigma$ is a diagonal matrix we have already seen that $(\Sigma B)^{-1}\Sigma B = \Sigma_B(\Sigma_B^\dagger \Sigma_B)^{-1}$, thus eqs. (A2) and (A3) are equal. □