Separable states improve protocols with restricted randomness

Tan Kok Chuan Bobby¹ and Tomasz Paterek¹,²

¹Centre for Quantum Technologies, National University of Singapore, 117543 Singapore
²School of Physical and Mathematical Sciences, Nanyang Technological University, 639798 Singapore

We give general arguments that separable states constitute a useful resource whenever randomness is not free. In particular, it is shown that they improve correlation assisted random access codes where correlated classical bits are replaced with correlated qubits. We show how the bias of classical bits can be used to avoid wrong answers and how advantage of quantum protocols is linked to quantum discord.

PACS numbers: 03.65.Ud,03.67.Ac,03.67.Hk

Introduction.—Quantum communication studies efficiency of various tasks in which quantum bits are transmitted between communicating parties or states with quantum correlations are assisting exchange of classical bits. Certain problems can be efficiently solved in this setting and examples include cryptography [1], communication complexity [2], or computation [3]. Instances of these problems draw their superiority from violation of Bell inequalities and accordingly require entanglement but outperform all solutions using (unlimited) classical randomness as characterised by local hidden variable models. Here we point out that new classes of states, correlated in a quantum way but not necessarily entangled, are likely to improve the quantum protocols if we make a fair counting of randomness in the classical and quantum cases, i.e. every bit is replaced by a qubit. We prove this rigorously for the task called random access code [4,6] assisted with two bits of randomness and expect that similar reasoning applies to all the problems mentioned above. Since not only all our computing machines but even the universe as a whole contain and process finite number of bits [7], the program of deriving limits on classical computation and communication that take restricted randomness into account is not only of practical interest but might also shed light on fundamental questions.

Many quantum states that are not entangled, so called separable states, still posses non-classical features such as those characterised by quantum discord [8,11]. The role of quantum discord in communication problems was quite extensively studied and connections were established with entanglement transformations [11,17], coherence of protocols [18], as well as with performance of solutions to certain problems that can be directly compared to their classical counterparts [19,21]. However, the latter link with the discord is established only for classical-quantum states [19] or for problems with additional constraints such as lack of certain reference frames [20,21]. It is therefore desirable to identify a well-known communication problem with many applications that can gain efficiencies from discarded states.

In this context, studying the random access codes assisted with restricted randomness is a natural choice. Indeed, a quantum version of this problem is as old as quantum information [4,6], the quantum codes were studied in general probabilistic theories [22], in relation with Popescu-Rohrlich boxes [23], led to information causality [24], find applications in quantum finite automata [6], quantum communication complexity [25], network coding [26], security of quantum-key distribution [27] and have been recently demonstrated experimentally [28]. Assuming restrictions on shared randomness, we will show that not only do separable discorded states allow better performance than the best classical solutions, they also outperform some entangled states.

Random access codes.—Imagine Bob would like to know (better than just by sheer guess) a random number from Alice’s telephone book. Is it necessary for her to send him the whole book or maybe she can transmit a fewer number of “encoded” pages such that Bob is reasonably confident of getting the correct number? Random access codes are strategies to solve this problem. In a classical $n \rightarrow 1$ random access code (RAC) Alice receives a random $n$-bit input $x$, communicates a single bit $c$ to Bob, who given this piece of information tries to guess the $i$th bit of Alice, $x_i$, by outputting his guess $b_i$ (in every run $i$ is chosen at random). In the quantum version one either communicates a quantum bit or in place of quantum communication Alice and Bob share a quantum state and are allowed to communicate one classical bit [29]. We study here the latter version of the problem and note that the role of quantum discord in the former version was considered in Ref. [30]. Our choice makes the relevance of shared randomness more transparent as by restricting the communication to classical the only additional resources are the assisting (qu)bits.

The existing quantum codes use a finite number of qubits and are compared with classical protocols with unlimited shared randomness [29]. Under such comparison, the quantum code can outperform the classical ones only if it is assisted by quantum states violating some Bell inequality, as all the states that admit a local hidden variable model (all separable states and some entangled ones, e.g. [31,32]) can be simulated with sufficient amount of
shared randomness, bringing no gain to the quantum protocol. However, if the size of the assisting resources is the same, states that do not violate any Bell inequality may possibly help improve the efficiency of the quantum protocol over the best classical ones. We stress that this holds not only for random access codes but generally for any task assisted with correlated resources, and suggests that other correlation-assisted communication protocols find a similar advantage using separable states.

We therefore restrict the amount of shared classical bits to be the same as the amount of shared quantum bits and study in detail the case of two assisting (qu)bits. We show how classical codes can gain additional efficiencies by utilising the bias of the assisting bits to avoid wrong guesses. Next, we provide quantum protocols assisted by separable states that outperform the best classical protocols, and show that in some cases they outperform even protocols assisted with quantum entanglement.

**Restricted classical randomness.**—A standard figure of merit characterising the efficiency of the RAC is the probability \( P_{\text{min}} \) of Bob’s correct guess in the worst case scenario (minimised over \( x \) and \( i \)). If no randomness is allowed \( P_{\text{min}} = 0 \), as there is always a bit that Bob guesses wrongly. \(^{23}\) In the presence of shared randomness, the efficiency \( P_{\text{min}} \) is additionally averaged over the assisting random bits. The following theorem characterises the maximal \( P_{\text{min}} \) in the presence of two bits of shared randomness.

**Theorem 1.** A classical \( n \to 1 \) RAC assisted with two bits from a common source has \( P_{\text{min}} \leq \frac{2}{3} \) if \( n = 2 \), and \( P_{\text{min}} \leq \frac{1}{2} \) if \( n > 2 \). For assisting bits having maximally mixed marginal for Bob one has \( P_{\text{min}} \leq \frac{1}{2} \) for all \( n > 1 \).

**Proof.** Let us denote the random bits of Alice and Bob by \( r_a \) and \( r_b \), respectively. Alice’s encoding is a binary function \( c = c(x, r_a) \), and Bob’s guess of \( x \) is a binary function \( b_i = b_i(c, r_b) \). Observe that for every given \( x \) Alice can choose from the following four possible encoding functions: 1) \( c = 0 \) independently of \( r_a \); 2) \( c = 1 \) independently of \( r_a \); 3) \( c = r_a \); 4) \( c = 1 \oplus r_a \), where \( \oplus \) denotes the binary sum. We prove that for two different inputs \( x \) and \( x’ \) Alice should not use the same encoding function as the probability of correct guess is then no greater than \( \frac{1}{2} \). Suppose for \( x \) and \( x’ \), Alice chooses the same encoding function from the options above, i.e., Alice’s message \( c \) is the same for both \( x \) and \( x’ \). Then Bob’s guesses of individual bits of \( x \) and \( x’ \), for a given \( r_b \), are the same and imply that the probabilities of correct guesses (averaged over the shared randomness) are also the same. Therefore, if they are correct for the bits of \( x \) with probability more than \( \frac{1}{2} \), the guess of the differing bit of \( x’ \) must be incorrect with the same probability. Hence, \( P_{\text{min}} \leq \frac{1}{2} \). Any sound strategy must therefore employ different encoding functions of Alice. Since there are only four different such functions, for all \( n \geq 3 \) the efficiency is at most \( \frac{1}{2} \). There is simply not enough shared randomness for Alice and Bob to do more.

We now focus on the \( 2 \to 1 \) RAC. In every protocol run, i.e., for a fixed \( x \), Bob needs to prepare a guesses \( b_1 \) and \( b_2 \) for the individual bits of Alice’s input which we order as \( b_{c,r_b} = (b_1, b_2) \), with indices \( c, r_b \) describing the variables accessible to Bob. Employing a method similar to Ref. \( [6] \), we define points \( P(x) = (P(b_1 = 1), P(b_2 = 1)) \) that represent the probabilities of Bob’s guesses being equal to 1. Writing explicitly the points corresponding to the four Alice’s encoding functions gives:

\[
\begin{align*}
P_1(x^1) &= p_{b_0,0,0} + p_{b_0,1,0} + p_{b_0,0,1} + p_{b_1,1,0}, \quad (1a) \\
P_2(x^2) &= p_{b_1,0,1} + p_{b_1,1,1} + p_{b_0,1,0} + p_{b_1,1,1}, \quad (1b) \\
P_3(x^3) &= p_{b_0,0,0} + p_{b_0,1,0} + p_{b_1,0,1} + p_{b_1,1,1}, \quad (1c) \\
P_4(x^4) &= p_{b_0,0,1} + p_{b_0,1,1} + p_{b_1,0,0} + p_{b_1,1,0}, \quad (1d)
\end{align*}
\]

where \( p_{kl} = \Pr(r_a = k, r_b = l) \) is the distribution of the common source of randomness, \( x^j \) denote the four different values of \( x \) with index \( j \) denoting the different encodings employed, and we used the fact that \( \Pr(b_1 = 1 | r_a, r_b, x) = b_i \). To prove \( P_{\text{min}} \leq \frac{2}{3} \), first note that Bob’s guesses \( b_{c,r_b} \) for different values of \( c \) and \( r_b \) must be different. This is because in the above expressions for every point \( P_j(x^j) \), we must have \( b_{c,r_b} \) corresponding to Bob correctly giving the answer to both bits of \( x \). Otherwise, the probability of correctly giving the first bit is solely given by \( p_{kl} \) corresponding to the correct guess of this bit and similarly for the second bit. As a consequence, the probability of guessing the second bit correctly is not greater than \( 1 - p_{kl} \), implying \( P_{\text{min}} \leq \frac{1}{2} \).

Since there are only four possible guesses \( b_{c,r_b} \) and only four points \( P_j(x^j) \), Bob’s guesses \( b_{c,r_b} \) cannot be the same for different \( c \) and \( r_b \).

We will now find the optimal strategy maximising \( P_{\text{min}} \) only for inputs \( x^3 \) and \( x^4 \) in Eqs. (1c) and (1d). Since only two inputs are considered and the definition of \( P_{\text{min}} \) includes minimisation over all four inputs, in this way we obtain an upper bound on \( P_{\text{min}} \). It will turn out that this upper bound is actually achieved. In the best case, Bob never outputs a guess with both bits guessed wrongly. Assume they are \( b_{1,1} \) and \( b_{0,1} \) in Eqs. (1c) and (1d), respectively. Therefore, the best case corresponds to \( p_{11} = 0 \). Since a guess giving the two bits of \( x^3 \) correctly must be different from the guess giving the two bits of \( x^4 \) correctly, and the probability of guessing any single bit is a sum of \( p_{kl} \) corresponding to both bits and one bit guessed correctly, one may verify that

\[
P_{\text{min}} = \min(p_{00} + p_{01}, p_{00} + p_{10}, p_{01} + p_{10}).
\] (2)

This is maximised for the biased distribution \( p_{00} = p_{01} = p_{10} = \frac{1}{2} \), which implies that the optimal value is \( P_{\text{min}} = \frac{2}{3} \). The optimal code achieving this value is presented in the Supplementary Online Material \(^{24}\).

For the second part of the proof we again utilize the fact that Bob’s guesses \( b_{c,r_b} \) must be different for different values of \( c \) and \( r_b \). Since \(^{13}\) involves the marginal...
distribution of Bob, the assumption of maximal mixedness gives \( P_1(x^1) = \frac{1}{2} b_{0,0} + \frac{1}{2} b_{0,1} \), and there is always an individual bit of \( x^1 \) that is guessed with probability \( \frac{1}{2} \), thus \( P_{\min} \leq \frac{1}{2} \).

We would like to note that studies of randomness usually employ so-called “common randomness”, i.e. pairs of perfectly correlated and locally completely random bits, whereas our proof shows that one can utilise the bias of randomness to gain efficiency, in this case to avoid giving wrong answers.

Restricted quantum randomness.—Having established the classical bounds we proceed to demonstrate quantum protocols that exceed them. We present explicit \( 2 \to 1 \) and \( 3 \to 1 \) quantum random access codes assisted with two correlated qubits. These special cases are of particular interest because they may be concatenated to generate more general \( n \to 1 \) quantum codes (see Ref. [29] for a detailed discussion of this procedure). After introducing the notation and essential concepts, we present detailed protocols and study their efficiency when assisted with Bell diagonal states.

Throughout the rest of the paper we employ the Bloch representation of qubit states and measurements, i.e. the three dimensional vector \( \vec{s} \) represents the qubit state \( \rho(\vec{s}) = (\mathbb{I} + \vec{s} \cdot \vec{\sigma})/2 \), where \( \vec{\sigma} = (\sigma_1, \sigma_2, \sigma_3) \) is the vector of Pauli matrices \( \sigma_x, \sigma_y, \sigma_z \). A unit vector \( \vec{\alpha} \) represents an ideal measurement with the probability of obtaining a measurement outcome \( \alpha = 0, 1 \), when measured on the state \( \rho \), being \( \text{Tr} \left( \frac{1 + (-1)\alpha \vec{\sigma} \cdot \vec{\alpha}}{2} \rho \right) \).

A general two-qubit state is of the form \( \rho_{ab} = \frac{1}{2}(\mathbb{I} \otimes \mathbb{I} + \vec{a}_0 \cdot \vec{\sigma} \otimes \mathbb{I} + \mathbb{I} \otimes \vec{b}_0 \cdot \vec{\sigma} + \sum_{l,m=1}^{3} E_{lm} \sigma_l \otimes \sigma_m) \), where \( \vec{a}_0 \) and \( \vec{b}_0 \) are the local Bloch vectors of Alice and Bob, respectively. The matrix \( E \) is the correlation matrix, and can always be made diagonal by an appropriate choice of local bases [35]. We therefore assume, without loss of generality, that the reference frames are appropriately chosen such that \( E = \text{diag}(E_1, E_2, E_3) \). If \( E_i \neq 0 \) we say that the state is correlated along that axis. We also make use of the fact that if Alice performs a measurement \( \vec{\alpha} \) with outcome \( \alpha \) on her half of the system, then Bob’s post-measurement Bloch vector is:

\[
\vec{b}(\alpha) = \frac{\vec{b}_0 + (-1)^\alpha E \vec{\alpha}}{1 + (-1)^\alpha \vec{\sigma} \cdot \vec{a}_0},
\]

where \( E \) is assumed to be the diagonal correlation matrix.

We shall explore the relationship between our protocols and a class of quantum correlations referred to as quantum discord [8–11]. Specifically, we employ the normalized geometric measure of quantum discord [20]. A general zero-discord state has the form \( \sigma_{ab} = p_0 \rho_0 \otimes |0\rangle \langle 0| + p_1 \rho_1 \otimes |1\rangle \langle 1| \), and the normalized geometric discord of \( \rho_{ab} \) is defined to be [20]:

\[
D_{ab}^2(\rho_{ab}) \equiv 2 \min_{E} \text{Tr}(\rho_{ab} - \sigma_{ab})^2.
\]

For Bell diagonal states we have \( D_{ab}^2 = \frac{1}{2}(E_2^2 + E_3^2) \), where it is assumed that \( E_1^2 \) is the biggest among squared diagonal elements of \( E \).

3 \to 1 code.—The codes presented here are similar to the codes assisted with quantum entanglement [29], with the key difference in the choice of Alice’s measurements. We focus first on the class of Bell diagonal states \( \rho_{ab} \) correlated along all three axes \( x, y \) and \( z \):

\[
\rho_{ab} = \frac{1}{4} \left( \mathbb{I} \otimes \mathbb{I} + \sum_{i=1}^{3} E_i \sigma_i \otimes \sigma_i \right),
\]

though the presented protocols can give better than classical results for more general assisting states (e.g. it will be easy to verify that \( a_0 \) can be arbitrary). The protocol is as follows:

(i) For input \( x \), Alice performs the measurement \( \vec{\alpha}(x) = \vec{\alpha}(x)/|\vec{\alpha}(x)| \), where \( \vec{\alpha}(x) = (-1)^{x_1} \vec{E}_1, (-1)^{x_2} \vec{E}_2, (-1)^{x_3} \vec{E}_3) \).

(ii) Alice sends her measurement outcome \( c = \alpha \) to Bob.

(iii) To guess the \( i \)th bit of Alice, Bob measures along \( \sigma_i \), obtains the outcome \( \beta_i \), and puts \( \beta_i \oplus c \) as the guess.

To grasp the mechanism of this protocol, note that depending on the measurement result of Alice, \( \alpha \), the post-measurement vectors of Bob, \( \vec{b}(\alpha) \), point towards the opposite vertices of a cube that encode either input \( x \) or \( \bar{x} \), having all individual bits of \( x \) flipped. After receiving the communication from Alice, Bob can correct for this by flipping his outcome if \( \vec{b}(\alpha) \) points towards the vertex \( \bar{x} \).

The probability of correct guess of every individual bit is therefore the same, giving \( P_{\min} \), and for Bell diagonal states it is equal to

\[
P_{\min} = \frac{1}{2} \left( 1 + \frac{1}{\sqrt{E_1^2 + E_2^2 + E_3^2}} \right),
\]

where the second term in the bracket is the overlap between \( \vec{b}(\alpha) \) and the \( x, y, \) or \( z \) axis (see Supplementary Online Material [34] for illustration). Since \( P_{\min} > \frac{1}{2} \), this quantum code is thus more efficient than the best classical code (see Theorem 1).

2 \to 1 code.—This code can operate on a slightly broader class of states as we now allow \( E_3 \) to vanish. The protocol follows the same procedures as in the 3 \to 1 case, with the exception that Alice’s measurements are given by \( \vec{\alpha}(x) = (-1)^{x_1} \vec{E}_1, (-1)^{x_2} \vec{E}_2, 0 \), the efficiency of this quantum code can then be verified to be

\[
P_{\min} = \frac{1}{2} \left( 1 + \frac{1}{\sqrt{E_1^2 + E_2^2}} \right).
\]
According to Theorem 1, $P_{\min} \leq \frac{1}{2}$ for classical protocols using bits with maximally mixed marginals, which we note is satisfied by the quantum state considered above. This shows that the presented code outperforms the best classical protocols when utilising similar resources. Even if Alice and Bob were allowed to share more generally correlated classical bits, for which $P_{\min}$ may be as high as $\frac{2}{3}$ for the $2 \rightarrow 1$ case, the above code may nonetheless still outperform the best possible classical RACs so long as the assisting qubits are sufficiently strongly correlated. Interestingly, it turns out that entanglement is not a necessary prerequisite to present such a quantum advantage. We demonstrate this with concrete examples in the following section.

**Examples.**—Consider Werner states, belonging to the class of Bell diagonal states and given by the mixture of white noise and maximally entangled state \[ \rho_{ab} = (1 - q) \frac{I \otimes I}{4} + q |\psi\rangle \langle \psi|, \quad q \in [0,1]. \] (7)
The state is entangled for $q > \frac{1}{3}$ and is separable otherwise. Its geometric discord can easily be verified to be $D_{a \mid b} = q$ \[ \text{ref} \]. Since for the Werner states all $E_i = \pm q$, Eqs. (5) and (6) reveal that the geometric discord directly measures the efficiency of the quantum codes assisted with this class of states. Moreover, it is the presence of quantum discord in the assisting states that empowers the quantum advantage.

The same statement also holds for more general codes. For example, concatenating $2 \rightarrow 1$ code assisted by the Werner state as in Ref. \[ \text{ref} \], one finds that the efficiency of $2^n \rightarrow 1$ code is given by

\[ P_{\min} = \frac{1}{2} \left( 1 + \frac{D_{a \mid b}}{\sqrt{2}} \right)^m. \] (8)
The concatenation of the quantum codes requires $2^m - 1$ pairs of qubits in the Werner state and a fair comparison with the classical case is then made by replacing the qubit pairs with correlated bits that have maximally mixed marginals. Numerical simulations indicate that $4 \rightarrow 1$ classical RACs formed through the concatenation procedure cannot achieve $P_{\min} > \frac{1}{2}$. We conjecture in general that the concatenation of $2 \rightarrow 1$ classical RACs assisted with bits having maximally mixed marginals cannot give $P_{\min} > \frac{1}{2}$, and therefore that the quantum advantage is present for any $m$, as indicated in Eq. (5).

We now show that a separable state may be used to outperform the best classical code assisted with two correlated random bits. The example once again utilises Bell diagonal states. Recall that the classical bound is $P_{\min}^{2 \rightarrow 1} = \frac{2}{3} \approx 0.667$ for all classical $2 \rightarrow 1$ RACs, and $P_{\min}^{3 \rightarrow 1} = \frac{2}{3}$ for all classical $3 \rightarrow 1$ RACs. By optimising the efficiency of the $2 \rightarrow 1$ quantum code, see Eq. (6), over the separable Bell diagonal states one finds that the optimal state has $E_1 = E_2 = \frac{1}{2}$, which gives the efficiency $P_{\min} = \frac{1}{2} (1 + \frac{1}{2\sqrt{2}}) \approx 0.677$, slightly above the classical bound. Better results are obtained for the $3 \rightarrow 1$ quantum code. By optimising Eq. (5) over separable Bell diagonal states, the best state has $E_1 = E_2 = E_3 = \frac{1}{3}$ and the efficiency is $P_{\min} = \frac{1}{2} (1 + \frac{1}{3\sqrt{2}}) \approx 0.596$, considerably above the classical bound. Note that there may exist a quantum code achieving better efficiencies, utilising some other class of separable state or following a different procedure.

In the last example we show that separable states can even outperform some entangled states. We have already demonstrated that using a separable state the $2 \rightarrow 1$ quantum code may achieve efficiencies of at least $P_{\min} = \frac{1}{2} (1 + \frac{1}{2\sqrt{2}})$. Comparing this with Eq. (5), one can see that it outperforms the protocol assisted with the entangled Werner states for $\frac{1}{3} < q < \frac{1}{2}$. It remains to show that there is no better quantum protocol for $2 \rightarrow 1$ quantum code assisted with the Werner states. This follows from the optimality of the protocol for the maximally entangled state $|\psi\rangle$ shown in Refs. \[ \text{ref} \], the fact that the completely mixed state encodes local randomness giving at most $P_{\min} = \frac{1}{2}$, and that the Werner state is a mixture of these two states.

**Conclusions.**—We demonstrated that separable states are a useful resource in random access codes as soon as finite shared randomness in the quantum and classical protocols is counted in the same way, i.e. bits are replaced with qubits. This is in particular relevant if randomness is not a freely available resource. We hope the example given here opens a research avenue on efficiency of solutions to various problems in the presence of restricted randomness. This is of both practical and fundamental interest. On the practical side, computers can use only a finite and restricted set of random bits for computations and therefore separable states are likely to enlarge the class of states that allows quantum advantages once these restrictions are taken into account. On the fundamental side, it would be interesting to know if entanglement is necessary to demonstrate in a Bell-like scenario deviations from predictions of local hidden variable models that involve only a finite number of bits.

This work is supported by the National Research Foundation, the Ministry of Education of Singapore, and start-up grant of the Nanyang Technological University. We thank Kavan Modi for discussions.

### A. Optimal classical protocol

We present an explicit classical protocol achieving $P_{\min} = \frac{2}{3}$. It uses two assisting correlated random bits distributed with probabilities $p_{00} = p_{01} = p_{10} = \frac{1}{3}$ and $p_{11} = 0$ (as in the proof of Theorem 1 of the main article). The protocol is detailed in Table \[ \text{ref} \] where Alice’s encoding and Bob’s output is completely specified. We also give there the resulting points $P(x) = (\Pr(b_1 = 1), \Pr(b_2 = 1))$ that represent the probabilities of Bob’s
guesses being equal to one. Fig. 1 shows these points in the space of all points $P$ and reveals that $P_{\text{min}} = \frac{2}{3}$.

**TABLE I: The optimal classical protocol.**

| $x$ | $(r_a, r_b)$ | $c(x, r_a)$ | $B(c, r_b)$ | $P(x)$ |
|----|--------------|-------------|-------------|--------|
| 00 | (0,0)        | 0           | (0,1)       | (1/3, 1/3) |
| 01 | (0,1)        | 0           | (0,0)       |
| 10 | (1,0)        | 1           | (1,0)       |
| 11 | (1,1)        | 1           | (1,1)       |

**FIG. 1:** The points within the square represent the probabilities (Pr($b_1 = 1$), Pr($b_2 = 1$)) of Bob’s guesses being equal to 1. The quadrant $Q_x$ contains all the points giving rise to Bob’s correct guess of Alice’s individual inputs $x_1$ and $x_2$ being more than $\frac{1}{2}$ (excluding the lines bisecting the square). The points connected with dashed lines represent the best classical RAC assisted with two bits from a common source and show that at best $P_{\text{min}} = \frac{2}{3}$.

**B. Quantum $3 \to 1$ Random Access Code assisted with two qubits in Bell diagonal state**

The protocol begins when Alice receives an input $x = x_1x_2x_3$. Based on the input, she performs a measurement

$$\hat{\alpha}(x) = \frac{\vec{\alpha}(x)}{||\vec{\alpha}||}, \quad \text{with} \quad \vec{\alpha}(x) = \begin{pmatrix} (-1)^{x_1}/E_1 \\ (-1)^{x_2}/E_2 \\ (-1)^{x_3}/E_3 \end{pmatrix},$$

where $E_i$ are the diagonal elements of the correlation matrix of the shared assisting state. Depending on the input, her measurement vectors point towards the vertices of a cuboid embedded in the Bloch sphere (see Fig. (2)). As a result of her measurement (with outcome $\alpha$) and the correlations in the shared state, the postmeasurement local Bloch vector on Bob’s side, $\vec{b}(\alpha) = (-1)^\alpha((-1)^{x_1}, (-1)^{x_2}, (-1)^{x_3})/||\vec{\alpha}||$, points towards one of the vertices of an inner cube within the Bloch sphere (see Fig. (2)).

**FIG. 2:** The quantum $3 \to 1$ random access code assisted with two qubits. (a) Alice’s measurement vectors point towards the vertices of a cuboid embedded within the Bloch sphere. (b) Bob’s post-measurement Bloch vectors point towards the vertices of an inner cube centered at the origin. See text for explanation how the code works.

[1] A. K. Ekert, Phys Rev. Lett. 67, 661 (1991).
[2] H. Buhrman, R. Cleve, S. Massar, and R. de Wolf, Rev. Mod. Phys. 82, 665 (2010).
[3] J. Anders and D. E. Browne, Phys Rev. Lett. **102**, 050502 (2009).
[4] S. Wiesner, ACM Sigact News **15**, 78 (1983).
[5] A. Ambainis, in *Proc. ACM Symp. on Theory of Computing* (1999).
[6] A. Ambainis, A. Nayak, A. Ta-Shma, and U. Vazirani, J. ACM **49**, 496 (2002).
[7] S. Lloyd, Phys Rev. Lett. **88**, 237901 (2002).
[8] L. Henderson and V. Vedral, J. Phys. A **34**, 6899 (2001).
[9] H. Ollivier and W. H. Zurek, Phys. Rev. Lett. **88**, 017901 (2002).
[10] L. C. Céleri, J. Maziero, and R. M. Serra, Int. J. Quant. Inf. **9**, 1837 (2011).
[11] K. Modi, A. Brodutch, H. Cable, T. Paterek, and V. Vedral, Rev. Mod. Phys. **84**, 1655 (2012).
[12] D. Cavalcanti, L. Aolita, S. Boixo, K. Modi, M. Piani, and A. Winter, Phys. Rev. A **83**, 032324 (2011).
[13] V. Madhok and A. Datta, Phys. Rev. A **83**, 032323 (2011).
[14] A. Streltsov, H. Kampermann, and D. Bruß, Phys Rev. Lett. **106**, 160401 (2011).
[15] M. Piani, S. Gharibian, G. Adesso, J. Calsamiglia, P. Horodecki, and A. Winter, Phys Rev. Lett. **106**, 220403 (2011).
[16] A. Streltsov, H. Kampermann, and D. Bruß, Phys. Rev. Lett. **108**, 250501 (2012).
[17] T. K. Chuan, J. Maillard, K. Modi, T. Paterek, M. Paternostro, and M. Piani, Phys. Rev. Lett. **109**, 070501 (2012).
[18] V. Madhok and A. Datta, arXiv:1107.0994 (2011).
[19] S. Boixo, L. Aolita, D. Cavalcanti, K. Modi, and A. Winter, Int. J. Quant. Inf. **9**, 1643 (2011).
[20] B. Dakić, Y. O. Lipp, X. Ma, M. Ringbauer, S. Kropatschek, S. Barz, T. Paterek, V. Vedral, A. Zeilinger, Č. Brukner, et al., Nat. Phys. **8**, 666 (2012).
[21] P. Horodecki, J. Tuziemski, P. Mazurek, and R. Horodecki, arXiv:1306.4938 (2013).
[22] G. V. Steeg and S. Wehner, Quantum Inf. Comput. **9**, 0801 (2009).
[23] A. Grudka, K. Horodecki, M. Horodecki, W. Klobus, and M. Pawłowski, arXiv:1307.7904 (2013).
[24] M. Pawłowski, T. Paterek, D. Kaszlikowski, V. Scarani, A. Winter, and M. Żukowski, Nature **461**, 1101 (2009).
[25] H. Klauck, in *Proc. IEEE Symp. on Foundations of Computer Science* (IEEE, 2001), pp. 288–297.
[26] M. Hayashi, K. Iwama, H. Nishimura, R. Raymond, and S. Yamashita, New J. Phys. **8**, 129 (2006).
[27] H.-W. Li, M. Pawłowski, Z.-Q. Yin, G.-C. Guo, and Z.-F. Han, Phys. Rev. A **85**, 052308 (2012).
[28] R. W. Spekkens, D. H. Buzacott, A. J. Keehn, B. Toner, and G. J. Pryde, Phys. Rev. Lett. **102**, 010401 (2009).
[29] M. Pawłowski and M. Żukowski, Phys. Rev. A **81**, 042326 (2010).
[30] Y. Yao, H.-W. Li, X.-B. Zou, J.-Z. Huang, C.-M. Zhang, Z.-Q. Yin, W. Chen, G.-C. Guo, and Z.-F. Han, Phys. Rev. A **86**, 062310 (2012).
[31] R. F. Werner, Phys. Rev. A **40**, 4277 (1989).
[32] M. L. Almeida, S. Pironio, J. Barrett, G. Toth, and A. Acin, Phys Rev. Lett. **99**, 040403 (2007).
[33] A. Ambainis, D. Leung, L. Mancinska, and M. Ozols, arXiv:0810.2937 (2008).
[34] Supplementary Online Material (2014).
[35] R. Horodecki and M. Horodecki, Phys. Rev. A **54**, 1838 (1996).
[36] B. Dakić, V. Vedral, and Č. Brukner, Phys Rev. Lett. **105**, 190502 (2010).