Quantum Information Processing (2019) 18:111
https://doi.org/10.1007/s11128-019-2228-3

Parity oblivious d-level random access codes and class of noncontextuality inequalities

Andris Ambainis[1] · Manik Banik[2] · Anubhav Chaturvedi[3] · Dmitry Kravchenko[1] · Ashutosh Rai[1]

Received: 19 July 2018 / Accepted: 21 February 2019 / Published online: 2 March 2019

Abstract

The quantum ontological feature of contextuality apart from being central to foundations of quantum theory forms the basis of quantum advantage in a multitude of information processing tasks. In particular, the contextuality of preparation procedures was shown to power a particular two-party information processing task "parity oblivious multiplexing" (Spekkens et al. Phys Rev Lett 102:010401 (2009). Specifically, it was shown that there exists a limit to how well any preparation noncontextual theory can perform in this task. This limit constitutes a noncontextuality inequality. Moreover, the authors demonstrated quantum violation of this inequality along with *preparation contextuality* associated with the ontic description underlying two-level completely mixed quantum state. In this work, we extend these arguments to apply to arbitrary dimensions by introducing a class of two-party information processing tasks, namely *d-level parity oblivious random access codes*. We analytically obtain classical (or equivalently preparation noncontextual) bounds on the success probability for these tasks for arbitrary d. For each value of d, this bound constitutes a unique noncontextuality inequality. Remarkably, these bounds are independent of the amount of communication. Furthermore, we find a classical protocol utilizing a $d_c = d$-dimensional classical message which saturates this bound. In order to establish nontriviality of these inequalities, we provide evidence of significant quantum violations. Specifically, by numerical techniques, we show that for $d = 3, \ldots, 10$, the noncontextuality bound is violated by quantum theory. (1) We provide explicit quantum protocols which violate the associated noncontextuality inequality for $d = 3, 4, 5$ employing $d_q = d$-leveled quantum systems. (2) Using see-saw semi-definite programming (SDP) technique, we find evidence (lower bounds) of significant quantum violation of these inequalities for $d = 3, \ldots, 10$. (3) With the help of *state-of-the-art* (NPA-hierarchy like) SDP technique, we provide upper bounds (independent of the dimension of the involved quantum systems) on quantum violation for $d = 3, \ldots, 10$.

✉ Anubhav Chaturvedi
anubhav.chaturvedi@research.iiit.ac.in

Extended author information available on the last page of the article

The introduced class of information tasks, thus, provides for operational depiction of preparation contextuality of the ontic description underlying mixed higher dimensional quantum systems.

Keywords Preparation contextuality · Parity oblivious random access codes · See-saw SDP

1 Introduction

Kochen–Specker (KS) contextuality theorem and Bell's nonlocality theorem are quintessential to foundations of quantum mechanics (QM). These theorems establish the impossibility of certain classes of ontic (hidden variable) explanations of QM. The derivation of Bell's theorem assumes the fundamental premises of *reality* and *locality* [1], while in the derivation of KS theorem, the *locality* assumption is replaced by that of *noncontextuality* [2–4]. Apart from their foundational importance, Bell nonlocality and KS contextuality form the key ingredients for a wide range of emerging quantum technologies such as device-independent quantum key distribution [5,6], device-independent quantum random number generation [7–11], quantum computation [12], and other applications in quantum information processing [13–17].

The notion of contextuality was generalized recently, by Spekkens, to arbitrary operational theories, and for different experimental schemes, viz. preparation procedure, measurement procedure, and transformation procedure [18,19]. The conventional notion of contextuality, i.e., KS contextuality, addresses only measurement contexts and has been extensively studied [20–24]. Recently, a number of interesting results have been uncovered with aid of the generalized framework [19,25–40]. In particular, preparation contextuality has been shown to be intimately linked with KS contextuality and Bell nonlocality [25–27,36]; moreover, preparation contextuality has demonstrated usefulness as a resource for an operational task called parity-oblivious multiplexing [28]. In this paper, we introduce a family of information processing tasks and derive corresponding noncontextuality inequalities which enables an operational depiction of preparation contextuality of ontic distributions associated with mixed states in higher dimensions.

Preparation contextuality is defined as the impossibility of representing two operationally equivalent preparations by identical ontological distributions. Suppose two operational preparations are equivalent in the sense that for all measurements, the outcome probability distributions for both of these preparations are identical, i.e., the two preparations are empirically indistinguishable. Then, a hidden variable model (ontic model) which reproduces the operational statistics is preparation noncontextual, if any two equivalent preparations impose equivalent probabilistic descriptions of the system at the ontological level (ontic distributions) [18]. The ontic distributions underlying any mixed quantum state are known to be preparation contextual [18,25].

In this work, we address the question whether preparation contextuality of higher dimensional mixed quantum states can be useful in some operational tasks. Interestingly, we get an affirmative answer to this question. We define a class of information tasks, namely *parity oblivious d-level random access codes*, henceforth abbreviated

as d-PORAC. These tasks are derivatives of the traditional random access code, which forms an important cryptographic primitive. We find the optimal success probabilities (bounds) for these tasks in any preparation noncontextual theory. For any d, such a bound constitutes a noncontextuality inequality, and a violation of the corresponding inequality by an operational theory implies that the theory and parity state must have a preparation contextual ontic description. Remarkably, these inequalities are independent of the dimension of the physical system under consideration and therefore are to be attributed similar status as the Bell inequalities. Then, for a three-level quantum system ($d_{\mathrm{q}} = 3$), we employ an exotic measurement bases, namely mutually asymmetrically biased bases (MABB), to construct a quantum protocol which exhibits the preparation contextuality of completely mixed state of three-level quantum system. We give two more explicit protocols showing quantum violation of respective inequalities for $d = 4$ and $d = 5$ employing $d_{\mathrm{q}} = 4$-dimensional and $d_{\mathrm{q}} = 5$-dimensional quantum systems, respectively. For $d = 3, \ldots, 10$, we provide evidence of significant quantum violation of the respective inequalities by finding lower bounds to quantum violation using see-saw semi-definite programming (SDP) algorithm [41–44]. Just like NPA-hierarchy [45] yields upper bounds on the violation of Bell inequalities and NV-hierarchy [46] upper bounds on the violation of dimension witnesses, we provide dimension-independent upper bounds on maximal quantum violation of the inequalities (defined in this work) using a *state-of-the- art* SDP technique tailored to preparation contextuality-related scenarios. Since the family of information processing tasks that we consider here provides for preparation noncontextuality inequalities in any finite dimension, it opens the possibility for operational depiction of preparation contextuality of ontic distributions underlying mixed sates of arbitrary dimension.

The paper is organized as follows: In Sect. 2, we introduce the tasks called d-level parity oblivious random access codes (d-PORAC) and analytically derive the optimal average classical success probabilities for these tasks for any d which is saturated by a $d_{\mathrm{c}} = d$-dimensional classical message; in Sect. 3, we derive upper bounds on the success probabilities of d-PORAC tasks in any preparation noncontextual theory which consequently provides for a class of noncontextual inequalities; in Sect. 4, we provide explicit quantum protocols which demonstrates quantum violation of these inequalities for $d = 3, 4, 5$ utilizing $d_{\mathrm{q}} = 3, 4, 5$-dimensional quantum systems. Furthermore, we provide numerical evidence for quantum violations of these noncontextual inequalities by providing lower bounds on the success probability and simultaneously, capping the quantum maximal violation using SDP for $d = 3, \ldots, 10$. The final Sect. 5 contains our concluding remarks.

2 Parity oblivious d-level random access codes

Consider the following two-party communication task. Alice receives uniformly at random some length-2 string $x = x_1x_2$, where x_n, for $n \in \{1, 2\}$, takes values from a d-level alphabet set $\{0, 1, \ldots, d-1\}$. Bob receives, uniformly at random, an index $y \in \{1, 2\}$. Bob's task is to recover the yth dit (i.e., x_y) in Alice's string. Alice can send some information about her string to help Bob; however, there is a restriction on Alice's communication to Bob which can be stated as follows; *Restriction* (**R**):

no information about the *parity* $x_1 \oplus_d x_2$ of Alice's string can be transferred to Bob, where $\oplus_d$ denotes addition modulo d. Let us denote Bob's guess about x_y by b and then the average success probability in this game can be expressed as $p(b = x_y)$.

The restriction on information transfer, i.e., **R**, induces a partition over the set of all strings $\{x_1x_2 : x_1, x_2 \in \{0, 1, \ldots, d-1\}\}$, into d equal parts which is defined as $\mathbb{P}_l := \{x_1x_2 \mid x_1 \oplus_d x_2 = l\}$, where $l \in \{0, \ldots, d-1\}$. Then, **R** implies that no information about to which partition $\mathbb{P}_l$ Alice's string x_1x_2 belongs can be transferred.

It is of crucial importance to differentiate the symbol d used to denote the levels of the classical inputs of Alice in the PORAC task from the symbols d_c which denotes the dimension of the classical message and d_q which denotes the dimension of the quantum message. Notice that while d is the parameter of task, there is no restriction on the amount of communication and hence d_c and d_q may be arbitrarily large.

2.1 Classical success of d-PORAC

Here, we derive the optimal classical average success probability for this game. First, we prove a lemma which is crucial to obtain the classical bound for d-PORAC task.

Lemma 1 *More than* 1*-dit information from Alice to Bob always carries some information about the parity* $x_1 \oplus_d x_2$.

Proof A classical encoding–decoding strategy could be either randomized or deterministic. Let us first consider the deterministic case.

In a deterministic strategy, for sending more than 1-dit information, it is necessary for Alice to encode her strings into more than d number of symbols. Then, let Alice have some encoding *onto* map,

$$\mathcal{E} : \{0, \ldots, d-1\}^2 \longrightarrow \{0, \ldots, d_\mathrm{c}\}, \tag{1}$$

where $d \leq d_\mathrm{c} \leq d^2 - 1$ and d_c is dimension of the classical message. Any such encoding map partitions the set of all strings (total d^2 in number) into $d_\mathrm{c} + 1$ parts $\mathbb{E}_j$, with $0 \leq j \leq d_\mathrm{c}$. On receiving the symbol j from Alice, Bob gets the information that Alice's string belongs to the partition $\mathbb{E}_j$, and then, Bob will not get any information about the parity of Alice's string if and only if $\mathcal{C}(\mathbb{E}_j \cap \mathbb{P}_l) = \mathcal{C}(\mathbb{E}_j \cap \mathbb{P}_{l'})$ for all $l, l' \in \{0, \ldots, d-1\}$, where $\mathcal{C}(\cdot)$ denotes cardinality of a set. Now, whenever $d_\mathrm{c} \geq d$, there exists at least one partition, say $\mathbb{E}_{j^*}$, in which the number of strings is strictly less than d. This further implies that there exists at least one partition $\mathbb{P}_{l^*}$ such that $\mathcal{C}(\mathbb{E}_{j^*} \cap \mathbb{P}_{l^*}) = 0$. Therefore, obtaining the symbol j^* from Alice, Bob will conclude that parity of the Alice's string is not l^*, and as a result, Bob can guess some other parity (except l^*) with a probability greater than $\frac{1}{d}$.

A randomized strategy is a probabilistic mixture of deterministic strategies. Therefore, playing with some randomized strategies, say $\mathcal{R}$, means playing a finite number of deterministic strategies $\mathcal{D}_s : s \in \{1, 2, \ldots, m\}$ according to some probability distributions $(p_1, p_2, \ldots, p_m)$. More than 1-dit (average) information transfer implies that at least one deterministic strategy $\mathcal{D}_\alpha$ for which $d_\mathrm{c} \geq d$ is played with some nonzero probabilities. Now from our proof for deterministic case, we know that whenever this happens some information about parity is transferred. □

According to Lemma 1, no more than 1-dit of *effective* information is allowed from Alice to Bob, which seems to be a similar restriction as in the d-level RAC task recently studied in [47]. However, this is a remarkable coincidence, as in a d-PORAC task there is no a priori restriction on the amount of communication, Alice may employ arbitrary large classical system with dimension d_c as long as it does not reveal any information about the parity but $d_c = d$ suffices, whereas in d-RAC, the restriction is amount of communication, i.e., no more than 1-dit information transfer is allowed. It is important to note that, the class of tasks we consider here is different from the parity-oblivious multiplexing (POM) task in [28]. POM is a task between two parties where some n-bit strings are given to the one party and the task of the other party is to guess an arbitrarily chosen single bit of the string; additionally, a restriction is imposed on allowed communication which in turn determines the possible classical protocols. The only allowed classical protocols for POM are those that *effectively* encode only a single bit (chosen arbitrarily) but at a fixed position in n-bit input strings. In contrast to this, for our d-level PORAC task, the considered restriction *effectively* allows 1-dit communication in more general ways.

Theorem 1 *The optimal classical success probability of d-PORAC is* $1/2(1 + 1/d)$.

Proof From Lemma 1 and the discussion soon after, it is clear that the optimal classical success probability of d-PORAC cannot be more than that of d-RAC. Recently, it has been shown that for d-RAC of string length 2, the optimal classical success probability is $1/2(1 + 1/d)$ [48]. The remaining argument is to show that even in d-PORAC, this optimal value of d-RAC is achievable. If Alice always encodes her first (second) dit and sends it to Bob, then Bob can perfectly guess about the first (second) dit and he guesses the other dit randomly; this protocol gives the required optimal average success probability the same as in d-RAC. Note that these protocols require $d_c = d$-dimensional classical message and the message does not carry any information about the parity. □

3 d-PORAC in a generalized operational theory

Alice and Bob can try to play this game using resources from a generalized operational theory [49,50]. However, in the following, we prove a *no-go* result which states that for certain class of such theories, the success probability for the d-PORAC game is no more than the optimal classical success.

3.1 Generalized operational theory

A generalized operational theory, as discussed in [18,19], merely specifies the probabilities $p(k|M, P)$ of different outcomes $k \in \mathcal{K}_M$ that may result from a measurement procedure $M \in \mathcal{M}$ performed on a system following some preparation procedures $P \in \mathcal{P}$, where $\mathcal{M}$ and $\mathcal{P}$ denote the sets of measurement procedures and preparation procedures, respectively and $\mathcal{K}_M$ denotes the set of measurement results for the measurement M. As an example, in an operational formulation of quantum theory

(QT), preparation P is associated with a density operator ρ on some Hilbert space, and measurement M is associated with a positive operator-valued measure (POVM) $\{E_k \mid E_k \geq 0 \; \forall \; k \text{ and } \sum_k E_k = \mathbf{I}\}$. The probability of obtaining outcome k is given by the Born rule, $p(k|M, P) = \text{Tr}(\rho E_k)$.

For playing the d-PORAC game in a generalized operational theory, Alice encodes her strings x in some state (preparation) P_x and sends the encoded state to Bob. For decoding yth dit, Bob performs some d outcome measurements M_y and guesses the dit according to the measurement results. The average success probability can be expressed as:

$$p(b = x_y) = \frac{1}{2 \times d^2} \sum_{y \in \{1,2\}} \sum_{n \in \{0,\ldots d-1\}^2} p(b = x_y | P_x, M_y). \tag{2}$$

To satisfy the parity oblivious condition, Alice's encoding must satisfy the following relations:

$$\sum_{x \in \mathbb{P}_l} p(P_x|k, M) = \sum_{x \in \mathbb{P}_{l'}} p(P_x|k, M), \quad \forall \, k, M, \\ \text{and } \forall \, l, l' \in \{0, \ldots, d-1\}. \tag{3}$$

Interestingly, due to this restriction, the success probability of d-PORAC in any preparation noncontextual theory is restricted by the optimal classical value. Before we prove such result, for completeness we give a short discussion of the general framework for ontological model of an operational theory and briefly explain the notion of preparation contextuality in these theories.

3.2 Ontological model

In an ontological model of an operational theory, the primitives of description are the *real* properties of a system, called ontic state $\lambda \in \Lambda$, where Λ is the ontic state space. A preparation procedure P yields a probability distribution $p(\lambda|P)$ over the ontic states. Measurement M performed on a system described by ontic state λ yields outcome k with probability $p(k|\lambda, M)$. The ontological model to be compatible with the operational theory must satisfy the probability reproducibility condition, i.e., $p(k|P, M) = \int_{\lambda \in \Lambda} \mathrm{d}\lambda \, p(\lambda|P) p(k|\lambda, M)$. An ontological model is preparation noncontextual, if two operational preparations yielding the same statistics for all possible measurements also yield the same distribution over the ontic states, i.e.,

$$\forall M : p(k|P, M) = p(k|P', M) \Rightarrow p(\lambda|P) = p(\lambda|P). \tag{4}$$

We now derive the optimal success probabilities of the d-PORAC games in any preparation noncontextual theory as stated in the following theorem.

Theorem 2 *In any preparation noncontextual theory, the success probability of d-PORAC cannot be more than the optimal classical success probability, i.e.,* $1/2(1 + 1/d)$.

Proof The steps in the proof of this theorem resemble the proof of a similar theorem in [28], and here, we give a suitably modified proof for our theorem.

In an operational theory, the collection of all preparations $\mathcal{P}$ is a convex set, and this enables any probabilistic mixture of preparation procedures corresponding to different states of the theory to be again a valid preparation. Consider a mixed preparation P_l produced by choosing uniformly at random some preparations P_x corresponding to the string x belonging to the partition $\mathbb{P}_l$, i.e, $P_l = \frac{1}{d}\sum_{x\in\mathbb{P}_l} P_x$. Given the preparation P_l, the probability of obtaining outcome k for the measurement M is

$$p(k|P_l, M) = \frac{1}{d}\sum_{x\in\mathbb{P}_l} p(k|P_x, M). \tag{5}$$

Also the preparation P_l yields the distribution on the ontic state λ,

$$p(\lambda|P_l) = \frac{1}{d}\sum_{x\in\mathbb{P}_l} p(\lambda|P_x). \tag{6}$$

In any operational theory, the parity obliviousness puts the restriction described in Eq. (3). Using Bayes' theorem and the fact that Alice's strings come from an uniform distribution, we can write

$$\sum_{x\in\mathbb{P}_l} p(k|P_x, M) = \sum_{x\in\mathbb{P}_{l'}} p(k|P_x, M), \quad \forall\, k, M, \quad \text{and } \forall\, l, l' \in \{0, \ldots, d-1\}. \tag{7}$$

The above expression along with Eq. (5) implies $p(k|P_l, M) = p(k|P_{l'}, M)$ for all $l, l' \in \{0, \ldots, d-1\}$ and for all k, M. In other words, different preparations P_l corresponding to different partitions $\mathbb{P}_l$ are operationally equivalent. If we assume that an operational theory is preparation noncontextual, then according to Eq. (4), we have

$$p(\lambda|P_l) = p(\lambda|P_{l'}), \quad \forall\ l, l' \in \{0, \ldots, d-1\}, \tag{8}$$

or equivalently by using Eq. (6), we can say, for all l, l',

$$\sum_{x\in\mathbb{P}_l} p(\lambda|P_x) = \sum_{x\in\mathbb{P}_{l'}} p(\lambda|P_x). \tag{9}$$

Applying Bayes theorem in Eq. (9), we have, for all l, l',

$$\sum_{x\in\mathbb{P}_l} p(P_x|\lambda) = \sum_{x\in\mathbb{P}_{l'}} p(P_x|\lambda). \tag{10}$$

Thus we can say that, for preparation noncontextual models, parity obliviousness at the operational level implies similar consequence at the level of the hidden variables, i.e, parity obliviousness should be satisfied at the hidden variable level too.

Hidden state λ provides a classical encoding of x. But as just shown, for preparation noncontextual theories, λ cannot contain information about parity. Now the proof of this theorem follows from the result obtained in Lemma 1 and Theorem 1. □

Theorem 2 constitutes a class of preparation noncontextual inequalities, i.e., if in some operational theories, the success probability for d-PORAC game is more than the optimal classical success, then the operational theory must be preparation contextual.

4 Quantum violation of noncontextual inequalities

We first consider the 3-PORAC game and showcase the violation of the corresponding noncontextual inequality which in turn establishes preparation contextuality of ontic distribution associated with completely mixed state of a three-dimensional quantum system (qutrit).

Quantum protocol for 3*-PORAC*: In 3-PORAC task, the three parity partitions of Alice's strings are $\mathbb{P}_0 = \{00, 12, 21\}$, $\mathbb{P}_1 = \{01, 10, 22\}$, and $\mathbb{P}_2 = \{02, 20, 11\}$. For playing this game in quantum theory, Alice encodes her string x_1x_2 into some quantum states $\rho_{x_1x_2}$ and sends the state to Bob. The parity obliviousness requirement demands that

$$\rho_{00} + \rho_{12} + \rho_{21} = \rho_{01} + \rho_{10} + \rho_{22} = \rho_{02} + \rho_{20} + \rho_{11}, \tag{11}$$

If Alice encodes her strings into three orthogonal sets of states (each forming a basis) $\mathcal{A}_0 = \{|\psi_{00}\rangle, |\psi_{12}\rangle, |\psi_{21}\rangle\}$, $\mathcal{A}_1 = \{|\psi_{01}\rangle, |\psi_{10}\rangle, |\psi_{22}\rangle\}$, and $\mathcal{A}_2 = \{|\psi_{02}\rangle, |\psi_{20}\rangle, |\psi_{11}\rangle\}$ then the above requirement is always fulfilled.

Now consider the following pure state qutrit encoding. Denoting the computational basis of qutrit as $\{|0\rangle, |1\rangle, |2\rangle\}$, any vector $|\psi\rangle \in \mathbb{C}^3$ ($d_{\mathrm{q}} = 3$) can be represented as $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle + \gamma|2\rangle$. Alice encodes her strings as follows:

$$\begin{aligned}
|\psi_{21}\rangle &= |0\rangle, |\psi_{12}\rangle = |1\rangle, |\psi_{00}\rangle = |2\rangle;\\
|\psi_{01}\rangle &= \frac{1}{3}(2|0\rangle + |1\rangle - 2|2\rangle),\\
|\psi_{10}\rangle &= \frac{1}{3}(|0\rangle + 2|1\rangle + 2|2\rangle),\\
|\psi_{22}\rangle &= \frac{1}{3}(2|0\rangle - 2|1\rangle + |2\rangle);\\
|\psi_{02}\rangle &= \frac{1}{3}(\omega^2|0\rangle + 2\omega|1\rangle + 2|2\rangle),\\
|\psi_{20}\rangle &= \frac{1}{3}(2\omega^2|0\rangle + \omega|1\rangle - 2|2\rangle),\\
|\psi_{11}\rangle &= \frac{1}{3}(2\omega^2|0\rangle - 2\omega|1\rangle + |2\rangle);
\end{aligned}$$

where ω is cube root of unity. These three sets of orthonormal vectors $\mathcal{A}_0$, $\mathcal{A}_1$, and $\mathcal{A}_2$ have the following property; each vector from any of the set has similar overlap with vectors from the remaining two sets. More precisely, for example, $|\psi_{21}\rangle$ from the set $\mathcal{A}_0$ has similar overlaps (in absolute value) with vectors from set $\mathcal{A}_1$ and the set

$\mathcal{A}_2$. With set $\mathcal{A}_1$, the overlaps are $2/3$ with $|\psi_{01}\rangle$, $|\psi_{22}\rangle$, and $1/3$ with $|\psi_{10}\rangle$, and with $\mathcal{A}_2$, the overlaps are $1/3$ with $|\psi_{02}\rangle$, and $2/3$ with $|\psi_{20}\rangle$ and $|\psi_{11}\rangle$. This feature has a resemblance to a set of mutually unbiased basis (MUB) [51,52], except that in a MUB all overlaps are equal; therefore, we call the set of bases a *mutually asymmetrically biased basis* (MABB).

For decoding each of the alphabet, Bob performs a three-outcome quantum measurement and guesses the alphabet based on the measurement result. Given the above encoding, Bob performs measurement $\sum_{i=0}^{2} |E_i\rangle\langle E_i| = \mathbf{I}_3$ to guess the first trit x_1, where

$$
\begin{aligned}
|E_0\rangle &= \frac{1}{\sqrt{7}} \left(|\psi_{00}\rangle - |\psi_{01}\rangle + |\psi_{02}\rangle\right), \\
|E_1\rangle &= \frac{1}{\sqrt{7}} \left(|\psi_{12}\rangle + |\psi_{10}\rangle + e^{\frac{\pi \mathbf{i}}{3}} |\psi_{11}\rangle\right), \\
|E_2\rangle &= \frac{1}{\sqrt{7}} \left(|\psi_{21}\rangle + |\psi_{22}\rangle + e^{\frac{2\pi \mathbf{i}}{3}} |\psi_{20}\rangle\right);
\end{aligned}
$$

and for the second trit x_2, he performs measurement $\sum_{i=0}^{2} |F_j\rangle\langle F_j| = \mathbf{I}_3$, where

$$
\begin{aligned}
|F_0\rangle &= \frac{1}{\sqrt{7}} \left(|\psi_{00}\rangle + |\psi_{10}\rangle - |\psi_{20}\rangle\right), \\
|F_1\rangle &= \frac{1}{\sqrt{7}} \left(|\psi_{21}\rangle + |\psi_{01}\rangle + e^{\frac{2\pi \mathbf{i}}{3}} |\psi_{11}\rangle\right), \\
|F_2\rangle &= \frac{1}{\sqrt{7}} \left(-|\psi_{12}\rangle + |\psi_{22}\rangle + e^{\frac{\pi \mathbf{i}}{3}} |\psi_{02}\rangle\right).
\end{aligned}
$$

For this quantum protocol, it turns out that $|\langle E_i|\psi_{ij}\rangle|^2 = |\langle F_j|\psi_{ij}\rangle|^2 = 7/9$ for $i, j = 0, 1, 2$. Therefore, the average success probability is $P = 1/18 \sum_{i,j=0,1,2} (|\langle E_i|\psi_{ij}\rangle|^2 + |\langle F_j|\psi_{ij}\rangle|^2) = 7/9$ which is strictly greater than the corresponding classical (noncontextual) bound, i.e., $1/2(1 + 1/3) = 2/3$.

In order to establish that in general, the inequalities presented in this work are nontrivial and provide for significant quantum violations, we used the following numerical methods to compute quantum violation and find the optimal protocol.

4.1 Nonlinear gradient descent

We find quantum protocols for $d = 4$ and $d = 5$ employing $d_q = 4$ and $d_q = 5$ dimensional quantum systems for communication, respectively, which violate the corresponding noncontextual bounds (see Appendix-A, B). These results were obtained numerically by optimizing over all possible pure state encoding, respectively, in $\mathbb{C}^4$ ($d_q = 4$) and $\mathbb{C}^5$ ($d_q = 5$) and all possible projective measurements for decoding. For $d = 4$ and $d = 5$, the obtained quantum protocol gives average success probabilities 0.7405 and 0.7177, respectively, which clearly beat the respective optimal classical (as well as noncontextual) bounds of 0.625 and 0.6. Specifically, for $d = 3, 4, 5$, we

parameterized pure states as preparations for Alice $\rho_{x_1x_2} = |\psi_{x_1x_2}\rangle\langle\psi_{x_1x_2}|$ (where $|\psi_{x_1x_2}\rangle \in \mathbb{C}^d$) that sum up to a completely mixed state $\frac{\mathbb{I}}{d}$ for each distinct value of the parity. For Bob, we parameterized projective measurements $|E_i\rangle\langle E_i|$ and $|F_i\rangle\langle F_i$ (where $|E_i\rangle, |F_i\rangle \in \mathbb{C}^d$). Based on these parameterizations, we used a straightforward gradient descent algorithm (a first-order iterative optimization algorithm for finding the maximum of a function) to find the optimal quantum protocol. Apart from the possibility of ending up in a local maximum, this method is exceedingly inefficient. In particular, the size of the Hilbert space we could handle was limited up to dimension 8.

4.2 See-saw iterative algorithm

We use see-saw SDP technique to obtain lower bounds on $d = 3, \ldots, 10$, demonstrating violation of the associated preparation noncontextual inequalities. The see-saw SDP iteration is an efficient algorithm for maximizing an affine functional with respect to Hermitian operators. The technique was first introduced to quantum information in [41] to find the maximal quantum violation of Bell inequalities. A variant of the see-saw SDP algorithm for Bell inequalities with multiple outcomes has also been described in [42–44]. The optimization problem relevant to this work consists of maximizing the success probability of the PORAC task with respect to d' dimensional states ρ_{x_0,x_1} and d' dimensional d outcome POVMs $\{M_b^y\}$:

$$\begin{aligned} \max \quad & p(b = x_y) = \frac{1}{2d^2}\mathrm{Tr}\{\rho_{x_0x_1} M^y_{b=x_y}\} \\ \text{subject to} \quad & \forall\, x_0, x_1 : \rho_{x_0x_1} \succeq 0; \\ & \forall\, x_0, x_1 : \mathrm{Tr}\{\rho_{x_0x_1}\} = 1; \\ & \forall\, y, b : M_b^y \succeq 0; \\ & \forall\, y : \sum_b M_b^y = \mathbb{I} \succeq 0; \end{aligned}$$

Notice that the objective function comprises of a product of semi-definite matrices. This keeps us from deploying this optimization problem as a SDP directly. This necessitates the see-saw iterative algorithm. Heuristically, the see-saw algorithm consists of fixing one of the two semi-definite variables and optimizing the other iteratively. In the first step of the algorithm, we choose and fix appropriate random matrices for Bob's POVMs (bold) and find optimum preparations for Alice which maximize the objective function:

$$\begin{aligned} \max \quad & p(b = x_y) = \frac{1}{2d^2}\mathrm{Tr}\{\rho_{x_0x_1} \mathbf{M^y_{b=x_y}}\} \\ \text{subject to} \quad & \forall\, x_0, x_1 : \rho_{x_0x_1} \succeq 0; \\ & \forall\, x_0, x_1 : \mathrm{Tr}\{\rho_{x_0x_1}\} = 1; \end{aligned}$$

Notice as now the objective function is linear on the semi-definite variables (Alice's preparations), this problem can easily be cast as a SDP. In the second step, we choose and fix the optimal preparations found in the previous step as Alice's preparations

(bold) for this round and optimize Bob's POVM so as to maximize the objective function:

$$\begin{aligned} \max \quad & p(b = x_y) = \frac{1}{2d^2}\mathrm{Tr}\{\boldsymbol{\rho}_{\mathbf{x_0 x_1}} M^y_{b=x_y}\} \\ \text{subject to} \quad & \forall\, y, b : M^y_b \succeq 0; \\ & \forall\, y : \sum_b M^y_b = \mathbb{I} \succeq 0; \end{aligned}$$

Again as the objective function is a linear function of the semi-definite variables (Bob's POVM), this problem can easily be cast as a SDP. Next, we fix Bob's POVM for the first step of the next iteration to be the optimal Bob's POVM found in the last step of the previous iteration. The algorithm then proceeds to repeat these steps for several iterations until the success probability reaches convergence. What is not guaranteed is that the algorithm will converge onto a global maximum. In order to better the chances for finding a global maximum, the entire procedure is repeated several times with different initial values. The results and the increasing trend of the ratio of quantum bias to classical bias are presented in Table 1 and Fig. 1, respectively.

4.3 *State-of-the-art* SDP hierarchy for upper bounds

Furthermore, we employ *state-of-the-art* NPA-hierarchy like SDP technique to obtain upper bounds on the quantum success probability of $d = 3, \ldots, 10$-level PORAC task. NPA- hierarchy [45] of Bell correlations and NV-hierarchy for finite dimensional correlations [46] use semi-definiteness of cleverly constructed series moment matrices to bound quantum correlations. Our method is an amalgamation of the methods presented in [45] and [46]. The resemblance of our method to the one in [45] is based on the fact that just like Bell inequalities, quantum bound for d-level PORAC is independent of the dimension of the physical (communicated) system. Our method relies on semi-definiteness of several distinct moment matrices, and in this sense, it resembles the method in [46]. The method, its detailed description, and the nuances thereof will be detailed in an upcoming article [53]. While level $= 1$ of this hierarchy is relatively computationally inexpensive, our machines can only perform level $= 2$ of this hierarchy for $d = 3, 4$. The results and the almost linearly increasing trend of the ratio of quantum bias to classical bias are presented in Table 1 and Fig. 1, respectively.

5 Concluding remarks

The information processing tasks d-PORAC defined in our work lead to a class of noncontextual inequalities for all finite values of d. These inequalities are independent of dimension of the classical systems and therefore are similar to Bell inequalities. In order to establish nontriviality of these inequalities, we provide evidence of significant quantum violation of these inequalities for $d \in \{3, \ldots, 10\}$. Remarkably, the ratio of

Table 1 List of bounds on the quantum success probability of $d = 2, \ldots,$ 10-PORAC

d	See-saw lower bound	Level = 1 upper bound	Level = 2 upper bound
2	0.85355	0.85355	0.85355
3	0.77778	0.80473	0.78049
4	0.74050	0.78033	0.74827
5	0.71773	0.76568	0.72274
6	0.69312	0.75592	–
7	0.67386	0.74894	–
8	0.66381	0.74371	–
9	0.65000	0.73965	–
10	0.64876	0.73639	–

First column contains lower bounds obtained from within quantum mechanics employing see-saw SDP technique. The second column contains upper bounds obtained with the aid of level = 1 NPA-hierarchy like SDP technique. Third column contains upper bounds obtained with the aid of level = 2 NPA-hierarchy like SDP technique. For level = 2, $d = 6$ was already too expensive for our machines. Note that the bound for $d = 2$ was analytically proved in [28] and serves as a Sanity Test for our numerical methods

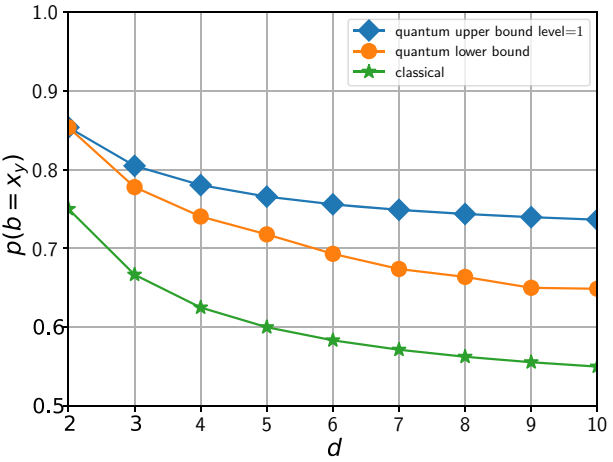

Fig. 1 Trend of success probability in d-PORAC tasks **a** achievable while using classical or equivalently preparation noncontextual resources (these form our noncontextual inequalities), **b** lower bounds on quantum success probabilities obtained via see-saw SDP (these serve as demonstration of violation of our noncontextual inequalities), and **c** upper bounds on quantum success probabilities obtained via NPA-hierarchy like SDP techniques [53] (these bounds are independent of the dimension d_q of the system)

quantum bias to classical bias $\Phi = \frac{p_q(b=x_y)-\frac{1}{2}}{p_c(b=x_y)-\frac{1}{2}}$ increases with d (the task parameter) (see Fig. 2).

The PORAC tasks introduced in this work are based on random access codes, which form an important cryptographic and computational primitive, and therefore, the d-PORAC has a potential of spawning novel cryptographic and computational applications like oblivious transfer protocols or privacy preserving computation.

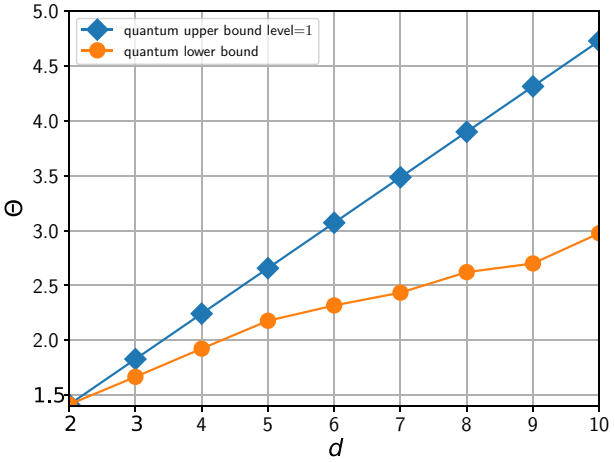

Fig. 2 Increasing trend of the ratio of quantum bias to classical bias for the d-PORAC task $\Theta = \frac{p_q(b=x_y)-\frac{1}{2}}{p_c(b=x_y)-\frac{1}{2}}$ using **a** lower bounds on quantum success probability obtained with aid of see-saw SDP techniques and **b** upper bounds on quantum success probability obtained via NPA-hierarchy like SDP techniques [53]

In contrast to our work, the quantum protocols for the $d = 2$ case in [28] are the same as the $2 \mapsto 1$ and $3 \mapsto 1$ quantum random access code (QRAC) protocols [54,55]. This fails for higher d: The d-level QRAC protocols in [47] for string length 2 fail to satisfy the requirement of parity obliviousness condition (as defined in our information task) for $d = 3$. As a result, our encoding–decoding scheme is quite different from the quantum RAC protocol given in [47]. Furthermore, mutually unbiased basis has found substantial applications in information processing tasks such as self-testing, quantum randomness amplification, compressed sensing and has been studied thoroughly, and here, we introduced *mutually asymmetrically biased basis* which may have similar potential for applications and deserves further research.

Our work leads to some open problems. The authors in [26,36] have found the optimal quantum violation of the noncontextual inequality given in [28]. Though we report on lower and upper bounds on the noncontextual inequality using SDP techniques, finding the optimal quantum violations of contextuality inequalities derived in this work can be an interesting problem for future works. Furthermore, just like information causality bounds the quantum success probability of entanglement-assisted random access codes, it might be worthwhile to look for information theoretic principles that bound the quantum success probability of the d-PORAC tasks. More importantly, we believe that the operational task defined in this work suffices to reveal preparation contextuality of ontic distributions associated with mixed states of any finite dimensional quantum system. For this, construction of generic quantum protocols for arbitrary values of d is required and which we leave here as an interesting open problem.

Acknowledgements MB acknowledges his visit at the University of Latvia, AR acknowledges his visit at the Institute of Mathematical Sciences, India, and AC acknowledges KCIK, Poland, where this work has been done. MB, AC, and AR would like to thank G. Kar and S. Ghosh for fruitful discussions. MB acknowledges

support through an INSPIRE-faculty position at S. N. Bose National Centre for Basic Sciences, by the Department of Science and Technology, Government of India. AA, DK, and AR acknowledge support by the European Union Seventh Framework Programme (FP7/2007-2013) under the RAQUEL (Grant Agreement No. 323970) Project, QALGO (Grant Agreement No. 600700) project, and the ERC Advanced Grant MQC. AC would like to acknowledge the grant FirstTEAM (Grant No. FirstTEAM/2016-1/5) from FNP, ERC AdG QOLAPS. .

A Quantum protocol for 4-PORAC game

Here, parity partitions of Alice's strings are $\mathbb{P}_0 = \{00, 13, 31, 22\}$, $\mathbb{P}_1 = \{01, 10, 23, 32\}$, $\mathbb{P}_2 = \{02, 20, 11, 33\}$, and $\mathbb{P}_3 = \{03, 30, 12, 21\}$. Let Alice encode her string x_1x_2 into some quantum states $\rho_{x_1x_2}$ and send the state to Bob. The parity obliviousness requirement demands that

$$\begin{aligned}\rho_{00} + \rho_{13} + \rho_{31} + \rho_{22} = \rho_{01} + \rho_{10} + \rho_{23} + \rho_{32} = \rho_{02} + \rho_{20} + \rho_{11} + \rho_{33} \\ = \rho_{03} + \rho_{30} + \rho_{12} + \rho_{21}.\end{aligned} \tag{12}$$

If Alice encodes her strings into four orthonormal sets of states

$$\begin{aligned}\mathcal{A}_0 = \{|\psi_{00}\rangle, |\psi_{13}\rangle, |\psi_{31}, |\psi_{22}\rangle\}, \quad \mathcal{A}_1 = \{|\psi_{01}\rangle, |\psi_{10}\rangle, |\psi_{23}, |\psi_{32}\rangle\}, \\ \mathcal{A}_2 = \{|\psi_{02}\rangle, |\psi_{20}\rangle, |\psi_{11}, |\psi_{33}\rangle\}, \quad \mathcal{A}_3 = \{|\psi_{03}\rangle, |\psi_{30}\rangle, |\psi_{12}, |\psi_{21}\rangle\},\end{aligned}$$

then the above requirement is always fulfilled.

Here, we consider four-dimensional pure state encoding. Denoting the computational basis of $\mathbb{C}^4$ as $\{|0\rangle, |1\rangle, |2\rangle, |3\rangle\}$, any vector $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle + \gamma|2\rangle + \delta|3\rangle$ can be represented as $|\psi\rangle \equiv [\alpha, \beta, \gamma, \delta]$. Alice's encoding is as follows:

$$|\psi_{00}\rangle = [0, 0, 0, 1],\ |\psi_{31}\rangle = [0, 0, 1, 0],\ |\psi_{13}\rangle = [0, 1, 0, 0],\ |\psi_{22}\rangle = [1, 0, 0, 0]; \tag{13}$$

$$\begin{aligned}|\psi_{01}\rangle &= [-0.1345 + 0.0225i, -0.2539 - 0.3035i, 0.5839 + 0.0576i, 0.6933], \\ |\psi_{10}\rangle &= [0.1283 - 0.0404i, 0.3662 + 0.4578i, -0.3931 - 0.0344i, 0.6947], \\ |\psi_{32}\rangle &= [-0.6624 + 0.2077i, -0.2564 - 0.3007i, -0.5853 - 0.0330i, 0.1349], \\ |\psi_{23}\rangle &= [-0.6843 + 0.1143i, 0.3204 + 0.4909i, 0.3862 + 0.0849i, -0.1366];\end{aligned} \tag{14}$$

$$\begin{aligned}|\psi_{20}\rangle &= [-0.6194 + 0.2157i, 0.2488 + 0.2796i, 0.0007 - 0.0001i, 0.6556], \\ |\psi_{02}\rangle &= [-0.6191 + 0.2154i, 0.0004 + 0.0002i, -0.3737 - 0.0291i, -0.6556], \\ |\psi_{11}\rangle &= [-0.3285 + 0.1796i, -0.5105 - 0.4114i, 0.6532 - 0.0575i, -0.0010], \\ |\psi_{33}\rangle &= [0.0005 + 0.0000i, 0.4360 + 0.4899i, 0.6534 + 0.0510i, -0.3747];\end{aligned} \tag{15}$$

$$|\psi_{30}\rangle = [0.3702 - 0.1379i, -0.0719 - 0.1161i, 0.6935 + 0.0054i, -0.5868],$$

$$
\begin{aligned}
|\psi_{03}\rangle &= [0.3780 - 0.1122i, -0.4163 - 0.5556i, 0.1361 - 0.0021i, 0.5865],\\
|\psi_{12}\rangle &= [0.5494 - 0.2050i, 0.4360 + 0.5393i, 0.1361 - 0.0159i, 0.3954],\\
|\psi_{21}\rangle &= [-0.5627 + 0.1673i, 0.0751 + 0.1129i, 0.6935 + 0.0271i, 0.3941]. \quad (16)
\end{aligned}
$$

Each of the four sets $\mathcal{A}_0, \mathcal{A}_1, \mathcal{A}_2$, and $\mathcal{A}_3$ forms an orthogonal basis and hence satisfies the parity obliviousness condition. For decoding the first alphabet, Bob performs a four-outcome measurement $\sum_{i=0}^{3} |E_i\rangle\langle E_i| = \mathbf{I}_4$ and guesses the alphabet according to the measurement result, where

$$
\begin{aligned}
|E_0\rangle &= [-0.2490 + 0.0899i, 0.1973 + 0.2519i, -0.3188 - 0.0254i, -0.8516],\\
|E_1\rangle &= [0.3019 - 0.1035i, 0.5355 + 0.6622i, -0.2626 - 0.0386i, 0.3202],\\
|E_2\rangle &= [-0.8013 + 0.2896i, 0.2154 + 0.2354i, 0.3198 + 0.0008i, 0.2646],\\
|E_4\rangle &= [-0.3024 + 0.1035i, -0.1890 - 0.1869i, -0.8509 - 0.0298i, 0.3197]; \quad (17)
\end{aligned}
$$

and for second alphabet, Bob performs measurement $\sum_{i=0}^{3} |F_i\rangle\langle F_i| = \mathbf{I}_4$, where

$$
\begin{aligned}
|F_o\rangle &= [0.2496 - 0.0892i, -0.2004 - 0.2484i, 0.3187 + 0.0114i, -0.8522],\\
|F_1\rangle &= [-0.3082 + 0.0849i, -0.1800 - 0.1951i, 0.8493 + 0.0679i, 0.3186],\\
|F_2\rangle &= [-0.8022 + 0.2868i, -0.2041 - 0.2454i, -0.3195 - 0.0067i, -0.2650],\\
|F_3\rangle &= [0.3076 - 0.0847i, -0.5244 - 0.6714i, -0.2618 - 0.0427i, 0.3195]. \quad (18)
\end{aligned}
$$

For this above encoding–decoding, we find that $P = \frac{1}{32}\sum_{i,j} Tr[\rho_{i,j}E_i + F_j] = 0.7405$ while the optimal classical average success probability is $1/2(1 + 1/4) = 0.625$.

B Quantum protocol for 5-PORAC game

Here, parity partitions are $\mathbb{P}_0 = \{00, 14, 41, 23, 32\}, \mathbb{P}_1 = \{01, 10, 24, 42, 33\}, \mathbb{P}_2 = \{02, 20, 11, 34, 43\}$, $\mathbb{P}_3 = \{03, 30, 12, 21, 44\}$, and $\mathbb{P}_4 = \{04, 40, 13, 31, 22\}$. The parity obliviousness conditions read

$$
\begin{aligned}
\rho_{00} + \rho_{14} + \rho_{41} + \rho_{23} + \rho_{32} &= \rho_{01} + \rho_{10} + \rho_{24} + \rho_{42} + \rho_{33} = \rho_{02}\\
&\quad + \rho_{20} + \rho_{11} + \rho_{34} + \rho_{43}\\
&= \rho_{03} + \rho_{30} + \rho_{12} + \rho_{21}\\
&\quad + \rho_{44} = \rho_{04} + \rho_{40} + \rho_{13} + \rho_{31} + \rho_{22} \quad (19)
\end{aligned}
$$

Alice encodes her strings into five orthonormal sets of states

$$
\mathcal{A}_0 = \{|\psi_{00}\rangle, |\psi_{14}\rangle, |\psi_{41}, |\psi_{23}\rangle, |\psi_{32}\rangle\}, \quad \mathcal{A}_1 = \{|\psi_{01}\rangle, |\psi_{10}\rangle, |\psi_{24}, |\psi_{42}\rangle, |\psi_{33}\rangle\},
$$

$\mathcal{A}_2 = \{|\psi_{02}\rangle, |\psi_{20}\rangle, |\psi_{11}, |\psi_{34}\rangle, |\psi_{43}\rangle\}$, $\mathcal{A}_3 = \{|\psi_{03}\rangle, |\psi_{30}\rangle, |\psi_{12}, |\psi_{21}, |\psi_{44}\rangle\rangle\}$, $\mathcal{A}_4 = \{|\psi_{04}\rangle, |\psi_{40}\rangle, |\psi_{13}, |\psi_{31}, |\psi_{22}\rangle\rangle\}$.

where the encoded states written in the computational basis of $\mathbb{C}^5$ are as follows,

$$
\begin{aligned}
&|\psi_{00}\rangle = [0,0,0,0,1],\ |\psi_{41}\rangle = [0,0,0,1,0],\ |\psi_{14}\rangle = [0,0,1,0,0],\\
&|\psi_{32}\rangle = [0,1,0,0,0],\ |\psi_{23}\rangle = [1,0,0,0,0]; \qquad (20)\\
&|\psi_{10}\rangle = [0.23497 - 0.07340i, 0.16411 - 0.10914i, 0.42583 + 0.50168i,\\
&\quad -0.19303 + 0.15607i, -0.63712],\\
&|\psi_{01}\rangle = [-0.18462 + 0.06593i, -0.20731 + 0.12870i, -0.16285\\
&\quad -0.18055i, 0.51463 - 0.38890i, -0.65332],\\
&|\psi_{42}\rangle = [-0.24112 + 0.08538i, -0.56454 + 0.30980i, -0.12652 - 0.15098i,\\
&\quad -0.52601 + 0.37747i, -0.24885],\\
&|\psi_{24}\rangle = [-0.60757 + 0.21215i, -0.21817 + 0.12492i, 0.41531\\
&\quad +0.49038i, 0.16960 - 0.12466i, 0.25570],\\
&|\psi_{33}\rangle = [0.62265 - 0.18358i, -0.57837 + 0.29870i, 0.13628\\
&\quad +0.19373i, 0.19499 - 0.14425i, 0.19985]; \qquad (21)\\
&|\psi_{20}\rangle = [-0.37409 + 0.52632i, -0.24065 - 0.01880i, 0.09926 - 0.17359i,\\
&\quad -0.07590 - 0.25674i, 0.64274],\\
&|\psi_{02}\rangle = [0.13977 - 0.20058i, 0.64176 + 0.05606i, -0.12928\\
&\quad +0.21553i, 0.06055 + 0.19160i, 0.64938],\\
&|\psi_{42}\rangle = [-0.37619 + 0.53274i, 0.18936 + 0.01847i, -0.12115\\
&\quad +0.20752i, 0.19401 + 0.62175i, -0.23774],\\
&|\psi_{24}\rangle = [0.11346 - 0.15816i, -0.65018 - 0.05766i, -0.33344\\
&\quad +0.55217i, 0.07480 + 0.22713i, 0.25061],\\
&|\psi_{33}\rangle = [0.14855 - 0.19490i, -0.25265 - 0.02560i, 0.34980\\
&\quad -0.54834i, 0.17203 + 0.61397i, 0.21416]; \qquad (22)\\
&|\psi_{30}\rangle = [-0.00534 - 0.24987i, 0.47253 + 0.43074i, 0.24297 + 0.07217i,\\
&\quad -0.20191 + 0.01868i, -0.65066],\\
&|\psi_{03}\rangle = [0.02569 + 0.64638i, -0.18296 - 0.16861i, -0.19043\\
&\quad -0.04582i, 0.25060 + 0.00014i, -0.64689],\\
&|\psi_{12}\rangle = [-0.01010 - 0.19929i, -0.49199 - 0.42851i, 0.63332 + 0.13808i,\\
&\quad -0.24023 + 0.00154i, -0.23796],\\
&|\psi_{21}\rangle = [0.04174 + 0.64483i, 0.15569 + 0.12225i, 0.24257 + 0.04356i,\\
&\quad -0.65035 + 0.01444i, 0.24365],\\
&|\psi_{44}\rangle = [0.00276 + 0.24838i, 0.16596 + 0.19200i, 0.61595\\
&\quad +0.19261i, 0.64285 + 0.04428i, 0.20539]; \qquad (23)
\end{aligned}
$$

$$
\begin{aligned}
|\psi_{40}\rangle &= [0.12419 + 0.15209i, -0.04125 - 0.23659i, -0.02914 \\
&\quad - 0.24743i, 0.20620 - 0.62431i, 0.63986], \\
|\psi_{04}\rangle &= [-0.15096 - 0.18341i, 0.03763 + 0.20009i, 0.06565 + 0.64204i, \\
&\quad - 0.07449 + 0.23344i, 0.65234], \\
|\psi_{31}\rangle &= [-0.39083 - 0.51585i, 0.05268 + 0.25138i, -0.05547 - 0.64174i, \\
&\quad - 0.06555 + 0.18659i, 0.24731], \\
|\psi_{13}\rangle &= [-0.14877 - 0.19642i, 0.14476 + 0.63049i, 0.01710 \\
&\quad + 0.20906i, 0.19415 - 0.61023i, -0.25833], \\
|\psi_{22}\rangle &= [-0.40081 - 0.51459i, -0.13601 - 0.63082i, 0.03136 \\
&\quad + 0.24802i, 0.08812 - 0.22522i, -0.19270].
\end{aligned} \tag{24}
$$

Bob's first decoding measurement is $\sum_{i=0}^{4} |E_i\rangle\langle E_i| = \mathbf{I}_5$ where,

$$
\begin{aligned}
|E_0\rangle &= [-0.03309 + 0.25670i, -0.25437 - 0.07003i, -0.06867 \\
&\quad - 0.25502i, 0.18550 - 0.19008i, -0.85036], \\
|E_1\rangle &= [0.25000 + 0.08268i, 0.03584 - 0.27017i, 0.42688 \\
&\quad + 0.73497i, -0.24068 - 0.09143i, -0.26020], \\
|E_2\rangle &= [0.36296 - 0.76531i, 0.17253 - 0.20234i, -0.26009 \\
&\quad + 0.03026i, 0.21365 + 0.17299i, -0.26023], \\
|E_3\rangle &= [-0.22262 - 0.15015i, 0.71573 + 0.45450i, 0.25044 \\
&\quad - 0.09303i, -0.15832 - 0.19830i, -0.27073], \\
|E_4\rangle &= [-0.22262 - 0.15015i, 0.71573 + 0.45450i, 0.25044 \\
&\quad - 0.09303i, -0.15832 - 0.19830i, -0.27073];
\end{aligned} \tag{25}
$$

and the second decoding measurement is $\sum_{i=0}^{4} |F_i\rangle\langle F_i| = \mathbf{I}_5$ where,

$$
\begin{aligned}
|F_0\rangle &= [-0.11375 + 0.23729i, -0.21967 - 0.13607i, -0.14148 \\
&\quad - 0.23461i, 0.12307 - 0.24902i, 0.84366], \\
|F_1\rangle &= [0.22685 + 0.13877i, 0.09381 - 0.24781i, 0.26314 \\
&\quad - 0.04382i, -0.57053 + 0.62201i, 0.27479], \\
|F_2\rangle &= [0.26939 - 0.00519i, 0.81916 + 0.21292i, -0.24642 \\
&\quad + 0.11038i, 0.24692 + 0.08601i, 0.26415], \\
|F_3\rangle &= [0.11939 - 0.84029i, -0.03406 + 0.26824i, 0.19925 \\
&\quad - 0.16385i, -0.21871 - 0.15566i, 0.26064], \\
|F_4\rangle &= [-0.25062 - 0.06551i, -0.17506 + 0.20714i, 0.21985 \\
&\quad + 0.81608i, 0.16329 + 0.20819i, 0.27390].
\end{aligned} \tag{26}
$$

For this above encoding–decoding, it turns out that $P = \frac{1}{50} \sum_{i,j} Tr[\rho_{i,j} E_i + F_j] = 0.71773$ while the optimal classical average success probability is $1/2(1+1/5) = 0.6$.

References

1. Bell, J.S.: On the Einstein podolsky rosen paradox. Physics **1**, 195–200 (1964)
2. Kochen, S., Specker, E.P.: The problem of hidden variables in quantum mechanics. J. Math. Mech. **17**, 59 (1967)
3. Mermin, N.D.: Hidden variables and the two theorems of John Bell. Rev. Mod. Phys. **65**, 803 (1993)
4. Brunner, N., Cavalcanti, D., Pironio, S., Scarani, V., Wehner, S.: Bell nonlocality. Rev. Mod. Phys. **86**, 419 (2014)
5. Barrett, J., Hardy, L., Kent, A.: No signaling and quantum key distribution. Phys. Rev. Lett. **95**, 010503 (2005)
6. Acín, A., Gisin, N., Masanes, L.: From Bells theorem to secure quantum key distribution. Phys. Rev. Lett. **97**, 120405 (2006)
7. Pironio, S., et al.: Random numbers certified by Bells theorem. Nature **464**, 1021 (2010)
8. Colbeck, R., Renner, R.: Free randomness can be amplified. Nat. Phys. **8**, 450 (2012)
9. Abbott, A.A., Calude, C.S., Conder, J., Svozil, K.: Strong Kochen-Specker theorem and incomputability of quantum randomness. Phys. Rev. A **86**, 062109 (2012)
10. Um, Mark, et al.: Experimental certification of random numbers via quantum contextuality. Sci. Rep. **3**, 1627 (2013)
11. Chaturvedi, A., Banik, M.: Measurement-device-independent randomness from local entangled states. EPL **112**, 30003 (2015)
12. Howard, M., Wallman, J.J., Veitch, V., Emerson, J.: Contextuality supplies the 'magic' for quantum computation. Nature **510**, 351 (2014)
13. Brunner, N., Pironio, S., Acín, A., Gisin, N., Methot, A.A., Scarani, V.: Testing the dimension of Hilbert space. Phys. Rev. Lett. **100**, 210503 (2008)
14. Das, S., Banik, M., Rai, A., Gazi, M.D.R., Kunkri, S.: Hardy's nonlocality argument as a witness for postquantum correlations. Phys. Rev. A **87**, 012112 (2013)
15. Mukherjee, A., Roy, A., Bhattacharya, S.S., Das, S., Gazi, MdR, Banik, M.: Hardy's test as a device-independent dimension witness. Phys. Rev. A **92**, 022302 (2015)
16. Roy, A., Mukherjee, A., Guha, T., Ghosh, S., Bhattacharya, S.S., Banik, M.: Nonlocal correlations: fair and unfair strategies in conflicting Bayesian game. arXiv:1601.02349 (Accepted in Phys. Rev. A)
17. Auletta, V., Ferraioli, D., Rai, A., Scarpa, G., Winter, A.: Belief-invariant equilibria in games with incomplete information. arXiv:1605.07896
18. Spekkens, R.W.: Contextuality for preparations, transformations, and unsharp measurements. Phys. Rev. A **71**, 052108 (2005)
19. Harrigan, N., Rudolph, T.: Ontological models and the interpretation of contextuality. arXiv:0709.4266
20. Peres, A.: Incompatible results of quantum measurements. Phys. Lett. A **151**, 107 (1990)
21. Mermin, N.D.: Simple unified form for the major no-hidden-variables theorems. Phys. Rev. Lett. **65**, 3373 (1990)
22. Grudka, A., et al.: Quantifying contextuality. Phys. Rev. Lett. **112**, 120401 (2014)
23. Yu, S., Oh, C.H.: State-independent proof of Kochen–Specker theorem with 13 rays. Phys. Rev. Lett. **108**, 030402 (2012)
24. Cabello, A.: Minimal proofs of state-independent contextuality. arXiv:1201.0374
25. Banik, M., Bhattacharya, S.S., Choudhary, S.K., Mukherjee, A., Roy, A.: Ontological models, preparation contextuality and nonlocality. Found. Phys. **44**, 1230 (2014)
26. Banik, M., Bhattacharya, S.S., Mukherjee, A., Roy, A., Ambainis, A., Rai, A.: Limited preparation contextuality in quantum theory and its relation to the Cirel'son bound. Phys. Rev. A **92**, 030103(R) (2015)
27. Leifer, M.S., Maroney, O.J.E.: Maximally epistemic interpretations of the quantum state and contextuality. Phys. Rev. Lett. **110**, 120401 (2013)
28. Spekkens, R.W., Buzacott, D.H., Keehn, A.J., Toner, B., Pryde, G.J.: Preparation contextuality powers parity-oblivious multiplexing. Phys. Rev. Lett. **102**, 010401 (2009)
29. Kunjwal, R., Spekkens, R.W.: From the Kochen–Specker theorem to noncontextuality inequalities without assuming determinism. Phys. Rev. Lett. **115**, 110403 (2015)
30. Kunjwal, R., Spekkens, R.W.: From statistical proofs of the Kochen–Specker theorem to noise-robust noncontextuality inequalities. Phys. Rev. A **97**, 052110 (2018)
31. Kunjwal, R.: Beyond the Cabello–Severini–Winter framework: making sense of contextuality without sharpness of measurements. arXiv:1709.01098

32. Kunjwal, R.: Hypergraph framework for irreducible noncontextuality inequalities from logical proofs of the Kochen–Specker theorem. arXiv:1805.02083
33. Kunjwal, R., Lostaglio, M., Pusey, M.F.: Anomalous weak values and contextuality: robustness, tightness, and imaginary parts. arXiv:1812.06940
34. Mazurek, M.D., Pusey, M.F., Kunjwal, R., Resch, K.J., Spekkens, R.W.: An experimental test of noncontextuality without unphysical idealizations. Nat. Commun. **7**, 11780 (2016)
35. Pusey, M.F.: The robust noncontextuality inequalities in the simplest scenario. arXiv:1506.04178
36. Chailloux, A., Kerenidis, I., Kundu, S., Sikora, J.: Optimal bounds for parity-oblivious random access codes. New J. Phys. **18**, 045003 (2016)
37. Krishna, A., Spekkens, R.W., Wolfe, E.: Deriving robust noncontextuality inequalities from algebraic proofs of the Kochen–Specker theorem: the Peres–Mermin square. New J. Phys. **19**, 123031 (2017)
38. Schmid, D., Spekkens, R.W.: Contextual advantage for state discrimination. Phys. Rev. X **8**, 011015 (2018)
39. Schmid, D., Spekkens, R.W., Wolfe, E.: All the noncontextuality inequalities for arbitrary prepare-and-measure experiments with respect to any fixed set of operational equivalences. Phys. Rev. A **97**, 062103 (2018)
40. Hameedi, A., Tavakoli, A., Marques, B., Bourennane, M.: Communication games reveal preparation contextuality. Phys. Rev. Lett. **119**, 220402 (2017)
41. Werner, R.F., Wolf, M.M.: Bell inequalities and entanglement. Quantum Inf. Comput. **1**, 1–25 (2001)
42. Liang, Y.C., Doherty, A.C.: Better Bell-inequality violation by collective measurements. Phys. Rev. A **73**, 052116 (2006)
43. Liang, Y.C., Doherty, A.C.: Bounds on quantum correlations in Bell-inequality experiments. Phys. Rev. A **75**, 042103 (2007)
44. Liang, Y.C., Lim, C.W., Deng, D.L.: Reexamination of a multisetting Bell inequality for qudits. Phys. Rev. A **80**, 052116 (2009)
45. Navascues, M., Pironio, S., Acín, A.: A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations. New J. Phys. **10**, 073013 (2008)
46. Navascues, M., Vertesi, T.: Bounding the set of finite dimensional quantum correlations. Phys. Rev. Lett. **115**, 020501 (2015)
47. Tavakoli, A., Hameedi, A., Marques, B., Bourennane, M.: Quantum random access codes using single *d*-level systems. Phys. Rev. Lett. **114**, 170502 (2015)
48. Ambainis, A., Kravchenko, D., Rai, A.: Optimal classical random access codes using single d-level systems. arXiv:1510.03045
49. Barrett, J.: Information processing in generalized probabilistic theories. Phys. Rev. A **75**, 032304 (2007)
50. Janotta, P., Gogolin, C., Barrett, J., Brunner, N.: Limits on nonlocal correlations from the structure of the local state space. New J. Phys. **13**, 063024 (2011)
51. Ivanovic, I.D.: Geometrical description of quantal state determination. J. Phys. A **14**, 3241 (1981)
52. Wootters, W.K., Fields, B.D.: Optimal state-determination by mutually unbiased measurements. Ann. Phys. **191**, 363 (1989)
53. Chaturvedi, A., Saha, D., Mironowicz, P, Pawłowski, M.: Unified framework for communication and correlations (up-coming)
54. Ambainis, A., Nayak, A., Ta-Shma, A., Vazirani, U.: Dense quantum coding and a lower bound for 1-way quantum automata. In: Proceedings of 31st ACM Symposium on Theory of Computing, pp. 376–383 (1999)
55. Ambainis, A., Nayak, A., Ta-Shma, A., Vazirani, U.: Dense quantum coding and quantum finite automata. J. ACM **49**, 496 (2002)

Affiliations

Andris Ambainis[1] · Manik Banik[2] · Anubhav Chaturvedi[3] · Dmitry Kravchenko[1] · Ashutosh Rai[1]

Andris Ambainis
andris.ambainis@lu.lv

Manik Banik
manik11ju@gmail.com

Dmitry Kravchenko
kravchenko@gmail.com

Ashutosh Rai
arai.qis@gmail.com

1 Faculty of Computing, University of Latvia, Raina bulv. 19, Riga 1586, Latvia

2 S.N. Bose National Center for Basic Sciences, Block JD, Sector III, Salt Lake, Kolkata 700098, India

3 Institute of Theoretical Physics and Astrophysics, National Quantum Information Centre, Faculty of Mathematics, Physics and Informatics, University of Gdańsk, Wita Stwosza 57, 80-308 Gdańsk, Poland