Connections between Mutually Unbiased Bases and Quantum Random Access Codes

Edgar A. Aguilar,[1,*] Jakub J. Borkała,[1] Piotr Mironowicz,[1,2,†] and Marcin Pawłowski[1]
[1]Institute of Theoretical Physics and Astrophysics, National Quantum Information Center, Faculty of Mathematics, Physics and Informatics, 80-308, Gdansk, Poland
[2]Department of Algorithms and System Modeling, Faculty of Electronics, Telecommunications and Informatics, Gdańsk University of Technology, Gdańsk 80-233, Poland

(Received 26 September 2017; revised manuscript received 14 May 2018; published 30 July 2018)

We present a new quantum communication complexity protocol, the promise-quantum random access code, which allows us to introduce a new measure of unbiasedness for bases of Hilbert spaces. The proposed measure possesses a clear operational meaning and can be used to investigate whether a specific number of mutually unbiased bases exist in a given dimension by employing semidefinite programming techniques.

DOI: 10.1103/PhysRevLett.121.050501

Introduction.—Mutually unbiased bases (MUBs) play a special role in the formalism of quantum mechanics. In particular they serve as complementary quantum tests, and find wide applicability in many fields of quantum information science such as quantum state tomography [1,2], quantum key distribution [3], quantum teleportation, and dense coding [4]. Hence, a general understanding of MUBs is well motivated and of general interest, see Ref. [5] for an extensive review and further references.

Explicitly, two orthonormal bases $\{|\psi_i^1\rangle\}_i$ and $\{|\psi_j^2\rangle\}_j$ of $\mathbb{C}^d$ are said to be mutually unbiased if

$$|\langle\psi_i^1|\psi_j^2\rangle|^2 = \frac{1}{d}, \quad \forall\ i,j \in [d], \tag{1}$$

where $[d] \equiv \{1,2,\ldots,d\}$. The term unbiased is used because if we pick any basis vector $|\psi_i^1\rangle$, then performing a measurement in the $\{|\psi_j^2\rangle\}_j$ basis will yield a completely random result (i.e., each outcome $|\psi_j^2\rangle$ will have equal detection probability $1/d$).

A set of MUBs in dimension d is said to be *maximal*, if there are $d+1$ bases which are all pairwise mutually unbiased. The construction of maximal sets when $d = p$, a prime number, was described by Ivonovic [1], and later by Wootters and Fields when $d = p^k$, a prime power [2]. The general problem of whether $d+1$ bases exist for arbitrary dimensions has remained open for at least the past 29 years.

In particular it is an open question whether a complete set of MUBs exists even in the simplest case, namely, in dimension 6. Zauner's conjecture states that *no more than three MUBs exist in dimension 6* [6]. The task of proving the conjecture is a research field on its own, see, e.g., Refs. [7,8] for partial analytical results supporting the conjecture. Numerical approaches have also failed to be conclusive [9].

In this Letter we introduce a novel protocol named promise-quantum random access code (PQRAC). The main idea of this protocol is to use the so-called $n^d \to 1$ quantum random access codes (QRACs) with certain constraints. Our main technical result shows that a specific average success probability of the protocol can be achieved if and only if n MUBs exist in dimension d.

The protocol allows us to create a new measure of unbiasedness, which quantifies the amount by which two (or more) bases are mutually unbiased. Other measures currently exist and are in use [4], yet the presented one possesses a direct operational interpretation as the success probability of a well-defined communication task.

Furthermore, the PQRAC game is suitable for numerical optimization techniques like semidefinite programming (SDP) [10]. In particular, one may use the see-saw method [11] to search for n MUBs in dimension d. What is more, PQRACs may be used together with the Navascues and Vertesi method [12] to discard the existence of n MUBs in a particular dimension. This exclusion is a rigorous statement, in contrast to drawing the conclusion out of the failure of trying to find them. We have been unable to rule out the existence of 4 MUBs in dimension 6, but argue that the problem is now at arm's length for future researchers.

Methods.—We begin by introducing *random access codes* (RACs) [13]. An $n^d \to 1$ RAC is a protocol in which Alice tries to compress an n-dit string into 1 dit, such that Bob can recover any of the n dits with high probability. More precisely, Alice receives a uniformly distributed random input string $\mathbf{x} = x_1 x_2 \cdots x_n$, $x_i \in [d]$. She then uses an encoding function $\mathcal{E}_c : [d]^n \to [d]$ (possibly classically probabilistic), and is allowed to send one dit $a = \mathcal{E}_c(\mathbf{x})$ to Bob. On the other side, Bob receives an input $y \in [n]$ (uniformly distributed), and together with Alice's message a uses one of n (possibly classically probabilistic) decoding functions $\mathcal{D}_c^y : [d] \to [d]$, to output $b = \mathcal{D}_c^y(a)$ as a guess for x_y. If Bob's guess is correct (i.e., $b = x_y$) then we

say that they are *successful*, otherwise we say that they are *unsuccessful* or *fail*.

Similarly, we define $n^d \to 1$ QRACs where Alice encodes her input n-dit string into a d-dimensional quantum system (qudit) via $\mathcal{E}_q : [d]^n \to \mathbb{C}^d$, and sends the qudit $\rho_{\mathbf{x}} = \mathcal{E}_q(\mathbf{x})$ to Bob. He then performs one of his decoding functions $\mathcal{D}_q^y : \mathbb{C}^d \to [d]$ to output his guess b for x_y. The decoding function is simply a quantum measurement; i.e., he outputs his guess b with probability $\mathbb{P}(b = x_y) = \mathrm{tr}[\rho_{\mathbf{x}} M_b^y]$, where the operators M_b^y are POVMs (i.e., positive and $\forall\, y \sum_b M_b^y = \mathbb{1}$). As a figure of merit, we employ the optimal average success probability for both RACs and QRACs:

$$\bar{P}_{c,q}(n,d) = \max_{\{\mathcal{E},\mathcal{D}\}} \frac{1}{n d^n} \sum_{\mathbf{x}} \sum_{y} \mathbb{P}(b = x_y). \tag{2}$$

The maximization is over encoding-decoding strategies $\{\mathcal{E}_{c,q}, \mathcal{D}_{c,q}\}$ (classical or quantum, respectively) [14], and the average is taken over all possible inputs $(\mathbf{x}, y)$ of Alice and Bob. In the quantum case, the optimal average success probability $\bar{P}_q$, can be achieved with pure states, $\rho_{\mathbf{x}} = |\mathbf{x}\rangle\langle\mathbf{x}|$ [13], where $|\mathbf{x}\rangle$ is the eigenvector of $\sum_y M_{x_y}^y$ with largest eigenvalue. In Ref. [15], it was shown that for $2^d \to 1$ QRACs this maximum is achieved when the operators M_b^y are (rank 1) projective measurements. Therefore, throughout the rest of this Letter we will be considering only pure-state encoding and von-Neumann measurements.

RACs and QRACs have increasingly become an experimental tool to test the "quantumness" or nonclassical behavior of a system [16,17]. For fixed n and d, we have $\bar{P}_c < \bar{P}_q$, and a gap is exploited to show that a system is behaving nonclassically. For example a $2^2 \to 1$ RAC has $\bar{P}_c = 0.75$, while the corresponding QRAC has an optimal average success probability of $\bar{P}_q = (2 + \sqrt{2})/4 \approx 0.8536$ [18]. Thus for a system of dimension 2, observing an average success probability greater than 0.75 indicates nonclassical behavior.

The quantum advantage comes from encoding Alice's state as a superposition of the bases $\{|\psi_i^1\rangle\}_i$ and $\{|\psi_j^2\rangle\}_j$, namely, $|\mathbf{x}\rangle = \alpha|\psi_{x_1}^1\rangle + \beta|\psi_{x_2}^2\rangle$, while Bob measures in the $\{|\psi_i^y\rangle\}_i$ basis. We have the following:

Lemma 1. For a $2^d \to 1$ QRAC, the optimal average success probability

$$\bar{P}_q(2,d) = \frac{1}{2}\left(1 + \frac{1}{\sqrt{d}}\right) \tag{3}$$

is obtained if and only if Bob's measurement bases $\{|\psi_i^1\rangle\}_i$, $\{|\psi_j^2\rangle\}_j$ are mutually unbiased.

The proof is given in the Supplemental Material [19]. We find it interesting to note here an observation that Lemma 1 cannot be generalized to the case of $n^d \to 1$ QRACs for $n \geq 3$, as stated below:

Observation 1. The MU condition on Bob's measurement bases is not sufficient for obtaining the optimal average success probability in $n^d \to 1$ QRACs when $n \geq 3$.

The proof of this result is by direct calculation (see Supplemental Material [19] for details). This occurs since there are inequivalent subsets of MUBs (i.e., not related by unitary transformations) in higher dimensions. As an example, let us consider the case $n = 3$, $d = 5$. Bob must choose 3 different measurement bases, and he can do so in $\binom{6}{3} = 20$ ways. Half of those selections lead to an average success probability of 0.610 855, while the other half give 0.596 449. Hence, the choice of the subset of MUBs matters. This feature occurs also for other choices of n and d. However, we conjecture that the optimal average success probability for $n^d \to 1$ QRACs is indeed achieved with a suitable choice of MUBs.

Next we define a $(n,m)^d \to 1$ PQRAC, $m \leq n$, as an $n^d \to 1$ QRAC with an extra promise. Let S_m^n be the set of all possible subsets of $[n]$ of size m. Then in a PQRAC, Alice receives an additional input $z \in S_m^n$, with the promise that $y \in z$. That is, Alice knows that Bob will not be questioned over some of Alice's inputs, see Fig. 1 for an illustration of a PQRAC.

Hence, the optimal average success probability [Eq. (2)], is modified in the case of $(n,m)^d \to 1$ PQRACs to

$$\tilde{P}_q(n,m,d) = \max_{\{\rho,\{M\}\}} \frac{1}{\binom{n}{m} m d^m} \sum_{z \in S_m^n} \sum_{\mathbf{x}_z} \sum_{y \in z} \mathrm{tr}[\rho_{\mathbf{x},z} M_{x_y}^y], \tag{4}$$

where the summation over $\mathbf{x}_z$ indicates a summation over $x_{i_1}, x_{i_2}, \ldots, x_{i_m}$ such that $\{i_1, i_2, \ldots, i_m\} = z$, and the maximization is taken over all quantum encoding and decoding strategies $\{\rho, \{M\}\}$. Now, we are able to prove our main technical result:

Lemma 2. For a $(n,2)^d \to 1$ PQRAC, the following holds:

$$\tilde{P}_q(n,2,d) \leq \frac{1}{2}\left(1 + \frac{1}{\sqrt{d}}\right) \tag{5}$$

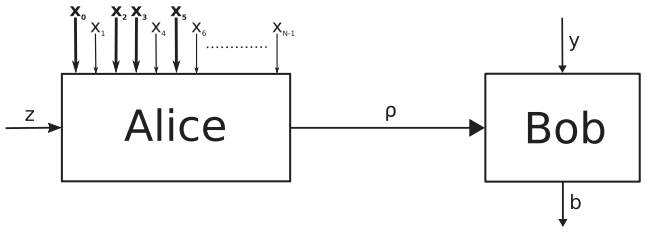

FIG. 1. Schematic representation of a $(n,m)^d \to 1$ promise–quantum random access code. Here $x_i \in [d]$, $y \in [n]$, and z is a subset of $[n]$ with m elements. The bold inputs x_k depict $k \in z$. ρ is the quantum state that Alice sends to Bob.

with equality if and only if at least n MUBs exist in dimension d.

Proof.—We begin by writing the optimal average success probability of the $(n,2)^d \to 1$ PQRAC.

$$\tilde{P}_q(n,2,d) = \max_{\{\rho,\{M\}\}} \frac{1}{\binom{n}{2}2d^2} \sum_{z\in S_2^n} \sum_{\mathbf{x}_z} \sum_{y\in z} \mathrm{tr}[\rho_{\mathbf{x},z} M^y_{x_y}]$$
$$\leq \frac{1}{\binom{n}{2}} \sum_{z\in S_2^n} \left(\max_{\{\rho,\{M\}\}} \frac{1}{2d^2} \sum_{\mathbf{x}_z} \sum_{y\in z} \mathrm{tr}[\rho_{\mathbf{x},z} M^y_{x_y}] \right).$$

The inequality follows, since the strategies to maximize the summands might not be compatible with each other globally. In fact, we recognize the term in parentheses as $\bar{P}_q(2,d)$, the optimal success probability for a $2^d \to 1$ QRAC [Eq. (2)]. From Lemma 1, this maximization occurs if and only if the measurement bases corresponding to the set z are mutually unbiased. It follows that it is possible to simultaneously satisfy all of these maximization constraints if and only if there exists n MUBs in dimension d. □

The intuition behind Lemma 2, is that Bob must be ready to measure in all n bases. If there exist n bases which are all pairwise mutually unbiased, then essentially they are just playing a more complicated version of the usual $2^d \to 1$ QRAC. If these bases do not exist, then for some $z \in S_2^n$, the protocol will not be able to achieve the optimal value [Eq. (3)], dropping the entire average.

Results.—In the context of MUBs, Ref. [4] has introduced a distance measure between two bases $\{|\psi_i^1\rangle\}_i$ and $\{|\psi_j^2\rangle\}_j$ which quantifies unbiasedness:

$$D^2_{\psi^1\psi^2} = 1 - \frac{1}{d-1} \sum_{i,j\in[d]} \left(|\langle\psi_i^1|\psi_j^2\rangle|^2 - \frac{1}{d} \right)^2. \quad (6)$$

The measure is symmetric ($D^2_{\psi^1\psi^2} = D^2_{\psi^2\psi^1}$). If the bases are the same, then $D^2_{\psi^1\psi^1} = 0$. The maximum $D^2_{\psi^1\psi^2} = 1$ is obtained if and only if the bases are mutually unbiased. For a set of n bases in $\mathbb{C}^d$ ($\{\psi^j\} = \{|\psi_i^j\rangle\}_i$, $j \in [n]$), one can analyze the average square distance between all possible pairs of bases [4]:

$$\bar{D}^2(\{\psi^i\}_i) = \frac{1}{\binom{n}{2}} \sum_{\{a,b\}\in S_2^n} D^2_{\psi^a\psi^b}. \quad (7)$$

Likewise, $\bar{D}^2 = 1$ if and only if all bases are pairwise mutually unbiased. However, Eq. (7) is an abstract distance measure, lacking an operational interpretation.

Lemma 2 immediately leads us to our first result. Given a set of n bases in dimension d we define as their unbiasedness measure the average success probability in a $(n,2)^d \to 1$ PQRAC if the bases are used as Bob's measurement bases. This measure is thus defined operationally and has the following properties: (1) The maximum of $\bar{P}_q(2,d) = \frac{1}{2}(1+d^{-1/2})$ is attainable if and only if all bases are pairwise unbiased. (2) It is symmetric under permutation of bases. (3) The minimal value of $\bar{P}_c(2,d) = \frac{1}{2}(1+d^{-1})$ is achieved if and only if all bases are the same. The optimal classical success probability of $n^d \to 1$ RACs is shown in Ref. [27].

Explicitly, given n bases of $\mathbb{C}^d$, $\{\psi^i\}_i$, the maximum attainable average success probability of the PQRAC, $\bar{p}$, is

$$\bar{p}(\{\psi^i\}_i) = \frac{1}{\binom{n}{2}} \sum_{\{a,b\}\in S_2^n} \left(\frac{1}{2} + \frac{1}{2d^2} \sum_{i,j\in[d]} |\langle\psi_i^a|\psi_j^b\rangle| \right), \quad (8)$$

which comes as a direct conclusion of Lemma 1. We may normalize Eq. (8) such that the minimum value is 0 (obtained if and only if all bases are the same), and the maximum value is 1 (obtained if and only if all bases are pairwise MU) and get the expression

$$\bar{Q}(\{\psi^i\}_i) = \frac{\bar{p}(\{\psi^i\}_i) - \bar{P}_c(2,d)}{\bar{P}_q(2,d) - \bar{P}_c(2,d)}. \quad (9)$$

See the Supplemental Material [19] for a direct comparison between Eqs. (9) and (7).

For illustrative purposes, we have optimized the value of the $(4,2)^6 \to 1$ PQRAC game expression using the see-saw method [11]. This allows us to show how the optimization of Eq. (9) may be used to construct MUBs in a particular dimension, as well as providing numerical examples of how $\bar{D}^2$ and $\bar{Q}$ compare. With this method, the maximal value of $\bar{D}^2$ of four MUBs in dimension 6 we obtained is 0.998 284 with $\bar{Q} = 0.998\,045$. On the other hand, the bases from [28,29] have $\bar{D}^2 = 0.998\,292$, and $\bar{Q} = 0.998\,036$. With this result one sees that the two measures, Eqs. (7) and (9), are not equivalent and induce different partial orderings on the sets of bases. See the Supplemental Material [19] for more details.

Our second result is another direct application of Lemma 2, and deals with ruling out if there are n mutually unbiased bases in dimension d. Explicitly, if it is possible to show that there are no sets of encoded states and measurement bases that would obtain a success probability of $\bar{P}_q(2,d)$, then one immediately concludes that there does not exist n MUBs in the given dimension. Thus one may use the SDP hierarchy of relaxations proposed by Navascues and Vertesi (NV) [12]. The method defines a sequence of SDP problems yielding upper bounds to optimization tasks over quantum probability distributions with dimensional constraints. One can show that the method converges to the accurate quantum values [30]. If at a given level of the hierarchy the upper bound falls below the threshold $\bar{Q} = 1$, then the conclusion follows. We emphasize that if n MUBs do not exist in a particular dimension, then applying the SDP hierarchy to the $(n,2)^d$

PQRAC gives an algorithmic way of proving their nonexistence. On the other hand, if n MUBs do exist, the proposed method will fail to draw a conclusion.

Implementing the hierarchy.—Let us try to directly apply the NV hierarchy to the $(n,2)^d \to 1$ PQRAC. To implement the kth level of the hierarchy, Q^k, the set $\mathbb{S}_d^k$ of all feasible moment matrices of order $2k$ arising from quantum systems of dimension d must be calculated. For this, moment matrices Γ_k^j are randomly generated from this set until $\mathrm{span}(\{\Gamma_k^j\}_j) = \mathbb{S}_d^k$. In practice, the algorithm keeps creating new moment matrices $j = \{1, 2, \ldots, v_k\}$ and stops when $\Gamma_k^{v_k+1} \in \mathrm{span}(\{\Gamma_k^j\}_{j=1}^{v_k})$. The method requires an assumption on the rank of the projectors $\{M_b^y\}$, but in our scenario Bob's optimal strategy is to implement d-dimensional von Neumann measurements; therefore, all operators are rank 1.

In order to generate Γ_k^j, we randomly choose $A = \binom{n}{2}d^2$ states for Alice to encode and $B = nd$ measurement operators for Bob (n bases of $\mathbb{C}^d$). Then, Γ_k^j contains the traces of all strings of size less than or equal to $2k$ constructed from Alice's states and Bob's operators. For example, typical matrix elements of Γ_1^j include $\mathrm{tr}[\rho_{\mathbf{x},z}^j \rho_{\mathbf{x}',z'}^j]$, $\mathrm{tr}[\rho_{\mathbf{x},z}^j M_b^{y,j}]$, and $\mathrm{tr}[M_b^{y,j} M_{b'}^{y',j}]$. While in Γ_3^j, we can find $\mathrm{tr}[\rho_{\mathbf{x},z}^j M_b^{y,j} M_{b'}^{y',j} M_{b''}^{y'',j} \rho_{\mathbf{x}',z'}^j M_{b'''}^{y''',j}]$, etc.

We write the kth order relaxation to our problem as the following semidefinite program [12]:

$$\begin{aligned} &\tilde{P}_q(n,2,d) = \max\ \mathrm{tr}[\hat{\mathcal{B}}\Gamma_k] \\ &\text{s.t.}\quad \Gamma_k \in \mathbb{S}_d^k, \qquad (\Gamma_k)_{1,1} = 1, \qquad \Gamma_k \geq 0, \end{aligned} \tag{10}$$

where we call $\hat{\mathcal{B}}$ the *PQRAC game matrix*, and construct it to "pick out" the values $\mathrm{tr}[\rho_{\mathbf{x},z} M_b^y]$ from Γ_k such that $b = x_y$ and $y \in z$.

Roughly $\frac{1}{2}(A+B)^{4k}$ real-valued numbers need to be stored in a computer's RAM in order to describe the set of all feasible moment matrices $\mathbb{S}_d^k$. Below, we describe a potentially quadratic reduction in the problem's memory requirements. See the Supplemental Material [19] for details.

Note that $\hat{\mathcal{B}} = \hat{\mathcal{B}}^T$, and is a sparse matrix with a lot of symmetries. In this case, we employ the symmetries corresponding to relabeling measurement device outputs, and the ones corresponding to permuting the labels of the measurement devices themselves. This approach has been followed on the Navascues-Pironio-Acin hierarchy in the Bell-test scenario [31].

Let $\hat{\mathcal{B}}$ be invariant under the group of transformations $\mathcal{G}$. In other words, for every representation G of an element $g \in \mathcal{G}$, $G\hat{\mathcal{B}}G^T = \hat{\mathcal{B}}$. Then, if we apply a group action on the game matrix inside the objective function [Eq. (10)], this would be equivalent to applying a group action on Γ_k. Namely, $\mathrm{tr}[\hat{\mathcal{B}}\Gamma_k] = \mathrm{tr}[\hat{\mathcal{B}}G^T\Gamma_k G]$. Therefore, it is unnecessary to consider the full space of feasible moment matrices $\mathbb{S}_d^k$ and we can simplify Eq. (10) into

$$\begin{aligned} &\tilde{P}_q(n,2,d) = \max \mathrm{tr}[\hat{\mathcal{B}}\hat{\Gamma}_k] \\ &\text{s.t.}\quad \hat{\Gamma}_k \in \mathcal{G}(\mathbb{S}_d^k), \qquad (\hat{\Gamma}_k)_{1,1} = 1, \qquad \hat{\Gamma}_k \geq 0, \end{aligned} \tag{11}$$

where we denote $\mathcal{G}(\mathbb{S}_d^k)$ as the set of feasible moment matrices which are $\mathcal{G}$ invariant. In order to implement this, we generate random invariant moment matrices $\hat{\Gamma}_k^j$ by first creating a moment matrix Γ_k^j and averaging it out over all of the group elements:

$$\hat{\Gamma}_k^j = \frac{1}{|\mathcal{G}|}\sum_{\mathcal{G}} G\Gamma_k^j G^T. \tag{12}$$

Clearly $\hat{\Gamma}_k^j \in \mathcal{G}(\mathbb{S}_d^k)$, and this is repeated until $\mathrm{span}(\{\hat{\Gamma}_k^j\}_j) = \mathcal{G}(\mathbb{S}_d^k)$. To illustrate the power of Eq. (11), we report that for a $(4,2)^5 \to 1$ PQRAC, $\dim(\mathbb{S}_5^1) = 13672$ and the SDP run-time was 22.5 h on a desktop computer, whereas $\dim(\mathcal{G}(\mathbb{S}_5^1)) = 7$ and had a run-time of 50 s.

Using this, we have implemented Q^1 and a subset of the "almost quantum" level [32] ($Q^{1+\mathrm{succ}}$) for some relevant PQRAC cases. The level $Q^{1+\mathrm{succ}}$ includes traces of strings of length ≤ 2 from the set of operators $\{\{\rho_{\mathbf{x},z}^j\}, \{M_b^{y,j}\}, \{\rho_{x_{z_1},x_{z_2},\{z_1,z_2\}}^j M_{x_{z_i}}^{z_i,j}\}\}$. That is, we also included pairs of states and measurements which lead to successful trials. The details of the implementation are found in the Supplemental Material [19].

For the $(4,2)^6$ PQRAC, we obtain a value of $\bar{Q} = 1.428\,825\,41$ for the first level of the hierarchy Q^1. This bound is greatly improved for $Q^{1+\mathrm{succ}}$, where $\bar{Q} = 0.999\,999\,96$. With our numerical precision and at this hierarchy level we have been unable to rigorously exclude the existence of 4 MUBs in dimension 6 [33]. We notice that the hierarchy level Q^2 was also unable to rule out the existence of 4 MUBs in $d = 2$ ($\bar{Q} = 0.999\,999\,99$). If these four bases existed, together with the $d = 3$ MUBs, one could create four MUBs in dimension 6. We conjecture that in order for a level of the hierarchy to be able to rule out the existence of 4 MUBs in dimension 6, it must first rule out the existence of 4 MUBs in $d = 2$. Future work requires more efficient ways of calculating Eq. (11), and higher levels of the hierarchy.

Conclusions.—In this Letter we give a new class of quantum games, PQRACs, which serve as an operational way of testing unbiasedness. It also enables one to reformulate the problem of searching for a given number of MUBs in a particular dimension as a problem of optimizing the strategy of the PQRAC game. In particular, if one is able to get a proper upper bound on the value of the game, then our formulation allows us to exclude the

existence of a given number of MUBs in the considered dimension. We have exploited the symmetries of the PQRAC game matrix in the Navascues and Vertesi hierarchy. We hope this will lead to rigorously proving Zauner's conjecture by considering higher levels.

This Letter was supported by EU grant RAQUEL, ERC AdG QOLAPS, National Science Centre (NCN) Grant No. 2014/14/E/ST2/00020, and DS Programs of the Faculty of Electronics, Telecommunications and Informatics, Gdańsk University of Technology. E. A. acknowledges support from CONACyT, and P. M. acknowledges support from K. Witalewska. The SDP optimizations have been performed using OCTAVE [34] with SDPT3 solver [35,36], SEDUMI [37], and YALMIP toolbox [38]. We thank D. Saha and M. Farkas for discussions about the theory, N. Miklin for discussions about the numerical implementation, and I. Bengtsson for guidance with the literature.

*ed.alex.aguilar@gmail.com
†piotr.mironowicz@gmail.com

[1] I. D. Ivonovic, Geometrical description of quantal state determination, J. Phys. A **14**, 3241 (1981).
[2] W. K. Wootters and B. D. Fields, Optimal state-determination by mutually unbiased measurements, Ann. Phys. (N.Y.) **191**, 363 (1989).
[3] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (1984), Vol. 175, p. 8, http://researcher.watson.ibm.com/researcher/files/us-bennetc/BB84highest.pdf.
[4] I. Bengtsson, W. Bruzda, A. Ericsson, J.-A. Larsson, W. Tadej, and K. Życzkowski, Mutually unbiased bases and hadamard matrices of order six, J. Math. Phys **48**, 052106 (2007).
[5] I. B. K. Z. Thomas Durt and B.-G. Englert, On mutually unbiased bases, Int. J. Quantum. Inform. **08**, 535 (2010).
[6] G. Zauner, Quantum designs: Foundations of a noncommutative design theory, Int. J. Quantum. Inform. **09**, 445 (2011).
[7] P. Jaming, M. Matolcsi, P. Mra, F. Szllsi, and M. Weiner, A generalized pauli problem and an infinite family of mub-triplets in dimension 6, J. Phys. A **42**, 245305 (2009).
[8] M. Grassl, On SIC-POVMs and MUBs in Dimension 6, arXiv:quant-ph/0406175.
[9] S. Brierley and S. Weigert, Mutually unbiased bases and semi-definite programming, J. Phys. Conf. Ser. **254**, 012008 (2010).
[10] L. Vandenberghe and S. Boyd, Semidefinite programming, SIAM Rev. **38**, 49 (1996).
[11] R. F. Werner and M. M. Wolf, Bell inequalities and entanglement, Quantum Inf. Comput. **1**, 1 (2001).
[12] M. Navascués and T. Vértesi, Bounding the Set of Finite Dimensional Quantum Correlations, Phys. Rev. Lett. **115**, 020501 (2015).
[13] A. Ambainis, D. Leung, L. Mancinska, and M. Ozols, Quantum Random Access Codes with Shared Randomness, arXiv:0810.2937.
[14] In fact, supremum should be taken in Eq. (2). However, the success probability is a continuous function of $\{\mathcal{E}, \mathcal{D}\}$, which are defined over the compact sets of states and measurements, hence, the sup is attainable.
[15] M. Farkas, Self-testing mutually unbiased bases in the prepare-and-measure scenario, arXiv:1803.00363.
[16] A. Tavakoli, A. Hameedi, B. Marques, and M. Bourennane, Quantum Random Access Codes using Single d-Level Systems, Phys. Rev. Lett. **114**, 170502 (2015).
[17] G. Cañas, J. Cariñe, E. S. Gómez, J. F. Barra, P. Mironowicz, A. Cabello, G. B. Xavier, G. Lima, and M. Pawłowski, Experimental quantum randomness generation invulnerable to the detection loophole, arXiv:1410.3443.
[18] A. Ambainis, A. Nayak, A. Ta-Shma, and U. Vazirani, Dense quantum coding and a lower bound for 1-way quantum automata, in *Proceedings of the Thirty-first Annual ACM Symposium on Theory of Computing, STOC '99* (ACM, New York, NY, USA 1999), pp. 376–383.
[19] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.121.050501, for the proof of Lemma 1 and Observation 1, an analysis of the measure $\bar{Q}$, and details of the SDP symmetrization method, which includes Refs [21–27].
[20] A. Marshall, I. Olkin, and B. Arnold, *Inequalities: Theory of Majorization and Its Applications*, Springer Series in Statistics (Springer, New York, 2010).
[21] K. F. Pál and T. Vértesi, Maximal violation of a bipartite three-setting, two-outcome bell inequality using infinite-dimensional quantum systems, Phys. Rev. A **82**, 022116 (2010).
[22] C. Spearman, The proof and measurement of association between two things, Am. J. Psychology **100**, 441 (1987).
[23] S. Lieberson, Limitations in the application of non-parametric coefficients of correlation, Am. Sociological Rev. **29**, 774 (1964).
[24] D. Reinsel, J. Gantz, and J. Rydning, Data Age 2025: The Evolution of Data to Life-Critical, An IDC White Paper, 2017, https://www.seagate.com/files/www-content/our-story/trends/files/Seagate-WP-DataAge2025-March-2017.pdf.
[25] Titan supercomputer, https://www.olcf.ornl.gov/for-users/system-user-guides/titan/, Accessed: 2018-03-30.
[26] E. Aguilar and P. Mironowicz, Symmetric reductions for sdp hierarchies in finite dimensions (to be published).
[27] M. Czechlewski, D. Saha, A. Tavakoli, and M. Pawłowski, Efficient device independent dimension witness of arbitrary quantum systems employing binary outcome measurements, arXiv:1803.05245.
[28] P. Butterley and W. Hall, Numerical evidence for the maximum number of mutually unbiased bases in dimension six, Phys. Lett. A **369**, 5 (2007).
[29] P. Raynal, X. Lü, and B.-G. Englert, Mutually unbiased bases in six dimensions: The four most distant bases, Phys. Rev. A **83**, 062303 (2011).
[30] M. Navascués, A. Feix, M. Araújo, and T. Vértesi, Characterizing finite-dimensional quantum behavior, Phys. Rev. A **92**, 042117 (2015).
[31] D. Rosset, Characterization of Correlations in Quantum Networks, 2015, https://archive-ouverte.unige.ch/unige:77401.
[32] M. Navascués, Y. Guryanova, M. J. Hoban, and A. Acín, Almost quantum correlations, Nat. Commun. **6**, 6288 (2015).

[33] Pushing our limitations to the extreme, we further implemented another subset of the almost quantum level, $Q^{1+\mathrm{succ}+BB}$, yielding $\bar{Q} = \mathbf{0.999\,999}\,89$, which we consider inconclusive.

[34] J. W. Eaton, D. Bateman, and R. Wehbring, *The GNU Octave 3.8 Reference Manual - Part 2/2: Free Your Numbers*, ISBN-13: 978-9881327741, https://www.amazon.com/GNU-Octave-3-8-Reference-Manual/dp/9881327741.

[35] K. C. Toh, M. Todd, and R. H. Tütüncü, SDPT3—A MATLAB software package for semidefinite programming, Optim. Methods Software **11**, 545 (1999).

[36] R. H. Tütüncü, K. C. Toh, and M. J. Todd, Solving semidefinite-quadratic-linear programs using SDPT3, Math. Program. **95**, 189 (2003).

[37] J. F. Sturm, Using SEDUMI 1.02, a matlab toolbox for optimization over symmetric cones, Optim. Methods Software **11**, 625 (1999).

[38] J. Löfberg, YALMIP: a toolbox for modeling and optimization in MATLAB, in *2004 IEEE International Conference on Robotics and Automation (IEEE Cat. No. 04CH37508), Taipei*, 2004, pp. 284–289, DOI: 10.1109/CACSD.2004.1393890.