Almost Qudits in the Prepare-and-Measure Scenario

Jef Pauwels,[1] Stefano Pironio,[1] Erik Woodhead,[1] and Armin Tavakoli[2,3]
[1]Laboratoire d'Information Quantique, CP 225, Université libre de Bruxelles (ULB), Avenue F. D. Roosevelt 50, 1050 Bruxelles, Belgium
[2]Institute for Quantum Optics and Quantum Information—IQOQI Vienna, Austrian Academy of Sciences, Boltzmanngasse 3, 1090 Vienna, Austria
[3]Atominstitut, Technische Universität Wien, Stadionallee 2, 1020 Vienna, Austria

(Received 18 August 2022; accepted 22 November 2022; published 16 December 2022)

Quantum communication is often investigated in scenarios where only the dimension of Hilbert space is known. However, assigning a precise dimension is often an approximation of what is actually a higher-dimensional process. Here, we introduce and investigate quantum information encoded in carriers that nearly, but not entirely, correspond to standard qudits. We demonstrate the relevance of this concept for semi-device-independent quantum information by showing how small higher-dimensional components can significantly compromise the conclusions of established protocols. Then we provide a general method, based on semidefinite relaxations, for bounding the set of almost qudit correlations, and apply it to remedy the demonstrated issues. This method also offers a novel systematic approach to the well-known task of device-independent tests of classical and quantum dimensions with unentangled devices. Finally, we also consider viewing almost qubit systems as a physical resource available to the experimenter and determine the optimal quantum protocol for the well-known random access code.

DOI: 10.1103/PhysRevLett.129.250504

Introduction.—The Hilbert space dimension of a system is a key property in quantum theory. Most experiments assume knowledge of it because it reflects the number of relevant independent degrees of freedom. Indeed, even the fundamental unit of quantum information, namely, the qubit, is expressed in terms of the (minimal meaningful) quantum dimension. It is natural that much research has been devoted to the quantum dimension: the device-independent certification of it [1–5], investigating the cost of classically simulating qubits [6–8], the advantage of using d-dimensional quantum systems (qudits) over classical systems (dits) in useful tasks [9–11], and performing quantum protocols in experiments where nothing but the dimension is assumed [12–15]. A large number of experiments have followed (see, e.g., [16–23]). Typically, these studies have focussed on prepare-and-measure scenarios, i.e., experiments in which a sender communicates quantum systems and a receiver measures them.

However, assigning a fixed dimension to a real-world quantum system is often an idealization. It is typically an approximation of what is actually an infinite-dimensional system. Common platforms for qubit communication, such as weak coherent pulses or polarization photons obtained by spontaneous parametric down-conversion constitute relevant examples. Indeed both very nearly correspond to harmonic oscillator qubits and polarization qubits, respectively, but the former still features higher-order oscillations and the latter still features multiphoton emissions. Whereas such dimensional deviations may often be viewed as negligible noise in device-dependent settings, it is much less clear whether the same is true in semi-device-independent quantum information protocols, namely, when experimental devices are mostly uncharacterized and we must assume that these deviations conspire against the experimenters. In fact, the practical challenges associated with assuming fixed quantum dimension have in recent times partly motivated semi-device-independent frameworks based assumptions entirely different from the dimension [24–29]. These approaches are based on limiting the distinguishability of quantum states in other ways, sometimes by specialization to a specific platform [25].

Here, we aim to remedy the shortcomings of dimension-based semi-device-independent quantum information protocols while maintaining basic interest in the quantum dimension. To this end, we introduce and investigate systems that only nearly admit a faithful description in terms of qudits. These "almost qudits" are formulated operationally, i.e., in a platform-independent way, and can thus be readily adapted to various quantum systems commonly modeled with a fixed dimension. We formalize the concept in the ubiquitous prepare-and-measure scenario and demonstrate its relevance by revisiting two established dimension-based quantum information protocols, for random number generation [30,31] and for certification of multioutcome measurements [22], and showcase how tiny higher-dimensional contributions can significantly compromise their conclusions. Small deviations from the assumed quantum dimension can cause compromised security for random number generation and false positives for measurement certification. These observations motivate us to develop general tools for analyzing almost qudit correlations. We introduce a hierarchy of semidefinite programming relaxations for bounding the set of almost qudit quantum correlations. We demonstrate its usefulness by fully resolving the issues observed for the two dimension-based protocols. Then, we change perspective and consider almost qudits as a resource for the experimenter; we show how to control the higher-dimensional components in order to optimally boost the performance of the QRAC [32]. Lastly, we discuss how our semidefinite programming hierarchy constitutes a general and useful tool for the well-researched task device-independent dimension certification.

Almost qudits in the prepare-and-measure scenario.—A qudit is a quantum state that can be represented by a density matrix in a Hilbert space of dimension d, i.e., $\rho \in \mathcal{D}(\mathbb{C}^d)$. We say that quantum states in an experiment can be described by *almost qudits* ρ, if the states in principle require a representation in a countably unbounded Hilbert space [$\rho \in \mathcal{D}(\mathbb{C}^D)$ for any $D \geq d$], but their support is almost entirely on a d-dimensional subspace. Formally, we require that one can choose a representation such that

$$\mathrm{Tr}(\rho \Pi_d) \geq 1 - \epsilon, \tag{1}$$

for all states ρ where $\Pi_d = \sum_{j=1}^{d} |j\rangle\langle j|$ is the projector onto the qudit subspace and $\epsilon \in [0,1]$ is a deviation parameter quantifying the failure to admit a qudit description. The limiting cases, $\epsilon = 0$ and $\epsilon = 1$, correspond to a standard qudit and to an arbitrary quantum state, respectively. Here, we are mainly interested in the regime $0 < \epsilon \ll 1$. As a simple example, the optical coherent state $|\alpha\rangle = e^{-(|\alpha|/2)} \sum_{n=0}^{\infty} (\alpha^n/\sqrt{n!})|n\rangle$ has $D = \infty$ in the Fock basis but for small average photon numbers (i.e., $|\alpha| \ll 1$) it corresponds to an almost qubit ($d = 2$) with $\epsilon = 1 - e^{-|\alpha|}(1 + |\alpha|^2) \approx |\alpha|$.

The condition Eq. (1) is equivalent to the trace-norm condition $\|\rho - \Pi_d \rho \Pi_d\|_1 \leq \epsilon$, with the operational interpretation that no experimental procedure can distinguish an almost qudit from its (unnormalized) qudit projection with accuracy greater than ϵ. More generally, consider a prepare-and-measure experiment featuring a sender, Alice and a receiver, Bob. Alice selects an input $x \in \{1, \ldots, n_X\}$ and prepares a qudit state ρ_x that is sent to Bob, who in turn selects an input $y \in \{1, \ldots, n_Y\}$ and performs a corresponding quantum measurement $\{M_{b|y}\}_b$ with outcome b. The correlations are

$$p(b|x,y) = \mathrm{Tr}(\rho_x M_{b|y}). \tag{2}$$

If the states ρ_x in the experiment are not exactly qudits, but only almost qudits (1) associated with the deviation parameters ϵ_x, the probabilities can change by at most $|p^{(\epsilon_x)}(b|x,y) - p^{(0)}(b|x,y)| \leq 2\epsilon_x$. In the Supplemental Material (SM) Sec. I [33] we also show that for any linear functional $W = \sum_{bxy} c_{bxy} p^{(\epsilon_x)}(b|x,y)$, for real coefficients c_{bxy}, the maximal value based on Alice preparing almost qudits ($W^{(\epsilon_x)}$) can be bounded by a perturbation of the maximal value associated to standard qudits ($W^{(0)}$), namely,

$$W^{(\epsilon_x)} \leq W^{(0)} + 2\sum_{xy} \epsilon_x \max_b |c_{bxy}|. \tag{3}$$

Since the correction is of order $\max_x \epsilon_x$, one might believe that the practical impact of almost qudits on dimension-based quantum information protocols is accordingly small, and that such a perturbative approach would suffice. However, as we will show explicitly, such intuition is often misguided. A more sophisticated analysis is needed to remedy the limitations of dimension-based protocols without rendering their success rates considerably sub-optimal or even vanishing.

Finally, as with dimension-based correlations but unlike some other prepare-and-measure frameworks [26,29], almost qudit correlations have a natural classical analog. The classical case corresponds to assuming that all states are diagonal in the same basis, i.e., $\rho_x = \sum_m p(m|x)|m\rangle\langle m|$. The assumption (1) simplifies to $\forall\ x\colon \sum_{m=1}^{d} p(m|x) \geq 1 - \epsilon_x$. It follows that the set of classical correlations is a polytope. Without loss of generality, it can be characterised using a finite alphabet for m by following the methods of [28].

Impact of almost qubits on random number generation.—We investigate the impact of tiny higher-dimensional contributions on a well-known qubit-based protocol for random number generation [30,31]. The protocol relies on the quantum random access code (QRAC) in the scenario $(n_X, n_Y, n_B) = (4,2,2)$, where Alice's input is represented as two bits x_1 and x_2: Bob randomly selects one, which he aims to recover. On average, the probability of success reads $p_{\mathrm{RAC}} = \frac{1}{8} \sum_{x_1,x_2=0,1} \sum_{y=1,2} p(b = x_y|x,y)$. When Alice sends qubits, the optimal quantum protocol achieves $p_{\mathrm{RAC}}^{Q} = [(2+\sqrt{2})/4]$. The protocol uses p_{RAC} as a security parameter to certify that b is random [e.g., when $(x,y) = (1,1)$] also for an adversary who controls the devices via classical side information λ. The randomness can be quantified by the conditional min-entropy $R = -\log_2(P_g)$, where P_g is the largest probability of guessing b, i.e., $P_g = \max\{p(1|1,1), p(2|1,1)\}$, compatible with the observed value of p_{RAC}.

Consider for simplicity a perfect value $p_{\mathrm{RAC}} = p_{\mathrm{RAC}}^{Q}$, which certifies $R = -\log_2(p_{\mathrm{RAC}}^{Q}) \approx 0.228$ bits of randomness [30] under a qubit assumption. The randomness reduces considerably if the physical implementation uses almost qubits. Choosing only $\epsilon_x = 10^{-3}$, we found via seesaw a much less random quantum model, implying the upper bound $R \lesssim 0.152$ bits. Thus, a 0.1% deviation dimension deviation leads to a standard qubit-based analysis overestimating the randomness by at least about 50%. Playing the

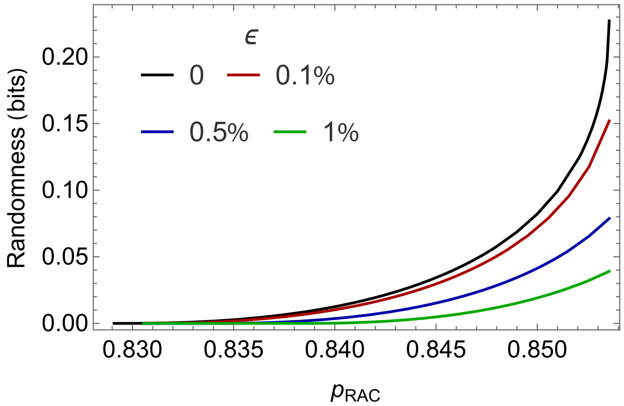

FIG. 1. Randomness certified by the observed parameter p_{RAC} for different deviation parameters ϵ. The black curve corresponds to the standard qubit-based protocol. These curves match, up to numerical precision, the lower bounds from the SDP hierarchy introduced around (5).

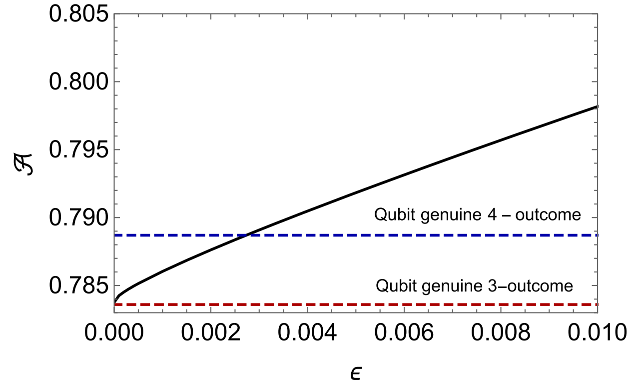

FIG. 2. Correlation function $\mathcal{A}$ versus the deviation parameter ϵ for almost qubits with ternary-outcome measurements (full black line). Dashed lines are ternary (red) and quaternary (blue) bounds on $\mathcal{A}$ assuming perfect qubits. These curves match, up to numerical precision, the upper bounds from the SDP hierarchy introduced around (5).

role of the adversary, we systematically searched numerically for quantum models for some small choices of ϵ with the aim of maximally compromising the amount of certified randomness. The results are illustrated in Fig. 1. We see that the amount of certified randomness drops rapidly with ϵ and that the detrimental impact is largest for well-performing experiments that approach the optimal value p_{RAC}^{Q}.

Impact of almost qubits on measurement certification.—As a second example, we consider the impact of almost qubits on a qubit-based protocol for certifying genuine four-outcome measurements. In Ref. [22], such a scheme is reported in the scenario $(n_X, n_Y) = (4, 4)$ where the first three measurement settings have binary outcomes ($b \in \{1, 2\}$) but the fourth setting has four possible outcomes ($b \in \{1, 2, 3, 4\}$). The task corresponds to the following objective:

$$\mathcal{A} \equiv \frac{1}{12}\sum_{x=1}^{4}\sum_{y=1}^{3} p(t_{x,y}|x, y) - \frac{1}{5}\sum_{x=1}^{4} p(x|x, y = 4), \quad (4)$$

where $t = [1, 1, 1; 1, 2, 2; 2, 1, 2; 2, 2, 1]$. The optimal value for qubits is $\mathcal{A}^{Q} = [(3 + \sqrt{3})/6] \approx 0.7887$. To achieve this, the setting $y = 4$ must correspond to a qubit symmetric informationally-complete positive operator-valued measurement. It was proven that $\mathcal{A} \gtrsim 0.78367$ implies that $y = 4$ corresponds to a genuine four-outcome measurement, i.e., a measurement that cannot be reduced to a classical mixture of measurements with at most three outcomes. This was experimentally certified by observing $\mathcal{A} \approx 0.785\,14$ [22].

Using a seesaw routine, we found an almost qubit model with deviation parameter $\epsilon_x \approx 5 \times 10^{-4}$ that reproduces the observed certificate using only a ternary-outcome measurement. This would constitute a false positive when the lab states are not exactly qubits. Moreover, using only $\epsilon_x \approx 3 \times 10^{-3}$, ternary-outcome measurements can even exceed the qubit quantum limit $\mathcal{A}^{Q}$. These results are part of the systematic numerical search, see Fig. 2, for the trade-off between $\mathcal{A}$ and ϵ for ternary-outcome measurements.

Finally, in SM Sec. II [33], we also investigate the impact of almost qubits on self-testing protocols based on the QRAC [14,34–36]. It quantitatively benchmarks a preparation device that aims to emit the four states used in the BB84 quantum key distribution protocol.

Semidefinite relaxations.—The considerable impact of small dimension deviations on protocols naturally motivates the development of methods for characterizing the set of almost qudit correlations. We introduce a hierarchy of semidefinite programming relaxations for bounding this set in arbitrary prepare-and-measure scenarios. This consists of a sequence of computable necessary conditions for the existence of an almost qudit model for a given distribution $p(b|x, y)$.

Define $S = \{\mathbb{1}, V, \rho_1, \ldots, \rho_{n_X}, M_{1|1}, \ldots, M_{n_B|n_Y}\}$ where $\mathbb{1}$ is the identity on $\mathbb{C}^D$ and V is an auxiliary operator whose properties are to be specified. While in general ρ_x can be mixed, we can without loss of generality assume that it is pure ($\rho_x = \rho_x^2$) for the purposes of the semidefinite relaxation; see SM Sec. III [33]. Also, we can w.l.g. assume that the measurements are projective ($M_{b|y}M_{b'|y} = \delta_{b,b'}M_{b|y}$) because of the possibility of Neumark dilations. We then build a monomial list $\mathcal{S}$ which consists of products of the elements of S. Which products to include is a degree of freedom and corresponds to the level of the relaxation. Then, associate a $|\mathcal{S}| \times |\mathcal{S}|$ moment matrix $\Gamma_{u,v} = \mathrm{Tr}(uv^\dagger)$, for $u, v \in \mathcal{S}$. Importantly, the quantum probabilities (2) appear as elements in Γ and are therefore fixed to the values $p(b|x, y)$. Because of rules such as normalization of states, cyclicity of trace, and projectivity of measurements, many elements in Γ are equivalent. The remaining entries are viewed as free variables. By construction Γ is positive semidefinite.

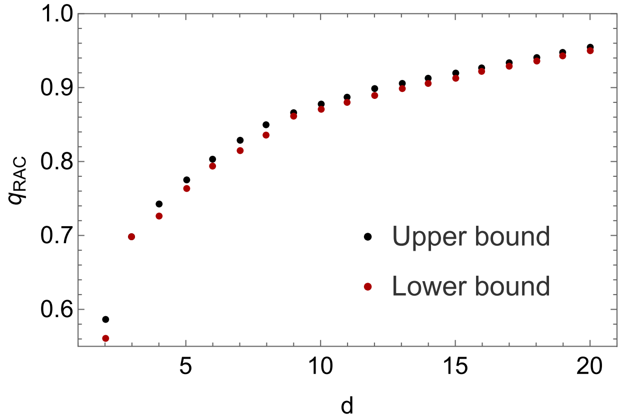

FIG. 3. Upper and lower bounds on the success probability of the three-trit QRAC for qudits of dimensions $d = 2, \ldots, 20$. Upper bounds were computed using partially symmetrized semidefinite relaxations (variable elimination methods but no block diagonalization) at level 2 of the hierarchy. Lower bounds were computed by seesaw.

Next, we impose the almost qudit property. To this end, we use the operator V to emulate the projection operator Π_d. Thus, we insist that V is projective ($V = V^2$) and its trace is d ($\mathrm{Tr}V = d$). The former impacts the equivalences among the entries of Γ while the latter implies the additional constraint $\Gamma_{\mathbb{1},V} = d$. The almost qudit constraint (1) can then be imposed through explicit constraints on $\Gamma_{\rho_x,V}$. A necessary condition for the existence of a quantum model is the feasibility of the following semidefinite program:

$$\text{find}\,\Gamma \quad \text{such that} \quad \forall\ x\colon \Gamma_{\mathbb{1},\rho_x} = 1, \qquad \Gamma_{\mathbb{1},V} = d$$
$$\Gamma_{\rho_x,V} \geq 1 - \epsilon_x, \quad \text{and} \quad \Gamma \succeq 0. \tag{5}$$

Furthermore, this tool can be immediately adapted to bounding the maximal quantum value of a generic linear objective function: simply substitute the feasibility problem (5) for a maximization problem in which $\Gamma_{\rho_x,M_{b|y}}$ are now free variables appearing in the objective function.

Almost qudit protocols.—We showcase the utility of the semidefinite relaxation hierarchy by applying it to the previously considered protocols. In Fig. 1, we reported upper bounds on the randomness under the almost qubit assumption. In order to be able to certify randomness, we require lower bounds. Upper bounds on the guessing probability P_g (lower bounds on R) under quantum correlation constraints are typically compatible with semidefinite relaxations [37]. Using our method with a moment matrix of size 115 we reproduced the curves in Fig. 1 up to solver precision. Thus, these curves certify the optimal randomness extraction for almost qubits. It is instructive to compare to a naive perturbation analysis of the standard qubit scenario, following Eq. (3). This approach is considerably suboptimal (see SM, Sec. I [33]). For instance, for $\epsilon = 0.1\%$, the amount of certified randomness is underestimated by 46%, and already for $\epsilon = 1\%$ randomness cannot be certified at all.

Similarly, using a moment matrix of size 235 we can prove that the previously reported value of ϵ for a falsely positive genuine four-outcome measurement is optimal. More generally, we obtain tight upper bounds on $\mathcal{A}$ for any ϵ under ternary-outcome measurements. These accurately coincide with the lower bounds reported in Fig. 2. Thus, the certification can be performed under the almost qubit assumption. Again, performing the same analysis using the perturbative approach (3) leads to significantly suboptimal bounds (see SM, Sec. I [33]). For example, under ternary-outcome measurements, a perturbative analysis deduces a deviation parameter $\epsilon \approx 5 \times 10^{-4}$ from the experimental value of $\mathcal{A}$ in [22], five times smaller than the optimal deviation parameter.

Bounding standard qudit correlations.—An important special case of our method is $\epsilon_x = 0$, corresponding to standard qudits. Naturally, bounding qudit correlations has been the subject of prior research [10,38–40]. The leading established method is also based on semidefinite relaxations [10] but differs significantly from ours. While [10] requires numerical sampling to construct the moment matrix, ours is fully deterministic. Also, although not strictly necessary, it typically favors separate semidefinite programs for all rank combinations of the measurement operators [39]. This scales very quickly in all three parameters (n_Y, n_B, d). In contrast, our method requires only a single semidefinite program. A key distinguishing feature of our method is that the complexity of the program is independent of d. Furthermore, it also applies to the classical case, relevant when linear programming becomes too expensive, simply by imposing commutation constraints $[\rho_x, \rho_{x'}] = 0$ and $[M_{b|y}, M_{b'|y'}] = 0$ in the moment matrix. The main drawback is that our method does not converge (see SM, Sec. III [33], for an example). The basic reason is that our method actually characterizes a superset of qudit systems, namely, correlations obtained from systems whose dimension, when averaged over a hidden variable, is d [39,41]. Although convergence is also not known for the established method [39], it performs better in some cases.

We exemplify the usefulness of our method by addressing intermediate-scale dimensions in the simplest variant of a QRAC for which no analytical solution is presently known. Alice has three trits $x_1x_2x_3 \in \{1,2,3\}$ and communicates a d-dimensional system. Bob receives $y \in \{1,2,3\}$ and aims to output $b = x_y$. The success probability is $q_{\mathrm{RAC}} = (1/81)\sum_{x_1x_2x_3y} p(b = x_y|x,y)$. Invoking the symmetries of the RAC (see Ref. [40]) to reduce the number of independent variables, we used semidefinite relaxations of size 1128 to bound q_{RAC} for every $d = 2, \ldots, 20$. Crucially, because the complexity of the computation is independent of d, we can readily evaluate higher-dimensional cases. In Fig. 3 we plot the resulting upper bounds together with lower bounds on q_{RAC} obtained via seesaw. These bounds are not expected to be optimal, but we conclude from the narrow gap between the upper and lower bounds that our upper bounds are at worst only nearly optimal. Importantly, we see that the gap narrows with increasing dimension, which attests to the accuracy of the semidefinite relaxation method on the scale when it is most relevant, namely, for higher dimensional systems.

Almost qubits as a resource.—So far, we considered situations in which the experimenter aims to prepare a qudit but fails to control the small higher-dimensional components of the lab state. Consider the complementary situation in which the experimenter has the ability to manipulate the entire almost qudit. Then, almost qudits become a resource for boosting quantum communication beyond standard qudits. An example of this is when Alice prepares the states

$$|\phi_{00}\rangle = \sqrt{1-\epsilon}|0\rangle + \sqrt{\epsilon}|2\rangle, \quad |\phi_{10}\rangle = \sqrt{1-\epsilon}s_{01}^{+} - \sqrt{\epsilon}s_{23}^{+},$$
$$|\phi_{11}\rangle = \sqrt{1-\epsilon}|1\rangle + \sqrt{\epsilon}|3\rangle, \quad |\phi_{01}\rangle = \sqrt{1-\epsilon}s_{01}^{-} - \sqrt{\epsilon}s_{23}^{-},$$

where $s_{ij}^{\pm} = [(|i\rangle \pm |j\rangle)/\sqrt{2}]$. These allow for boosting the success probability of the QRAC [32]. By optimally choosing the measurement operator $\{M_{0|y}\}$ as the projector onto the positive eigenspace of the operator $O_y = \sum_{x_1,x_2}(-1)^{x_y}|\phi_{x_1x_2}\rangle\langle\phi_{x_1x_2}|$, one finds the success probability $p_{\mathrm{RAC}}(\epsilon) = \frac{1}{2} + (1/2\sqrt{2})\sqrt{1+4\epsilon-4\epsilon^2}$. We have proven that this strategy is the best allowed by quantum theory by employing a moment matrix of size 107. For the most relevant case of small ϵ, there is an immediate connection to the standard qubit scenario: the first-order approximation is $p_{\mathrm{RAC}}(\epsilon) \approx [(2+\sqrt{2})/4] + (\epsilon/\sqrt{2})$, which is a linear correction to the success probability p_{RAC}^{Q} of the standard QRAC. Note that a perturbative approach (3) would overestimate the correction term, at 2ϵ.

Discussion.—We presented several examples demonstrating how tiny deviations from an assumed dimension can significantly compromise the conclusions of established protocols. We introduced almost qudits as an avenue to remedy these problems and developed general tools to characterize their correlations.

Our Letter leaves several natural questions. Which experimental platforms are most and least prone to dimensional deviations? What resources could an eavesdropper use to efficiently hack them? How do we wisely tailor protocols to perform well for almost qudit systems? These matters are particularly relevant in the context of the increasing interest in high-dimensional quantum information [42–46]. Moreover, what is the magnitude of quantum advantage possible from almost qudits, as compared to classical almost dits? Is it possible to add additional constraints that would lead to a convergent hierarchy? Can these ideas be leveraged to qubit-based quantum key distribution protocols [12,13]? Finally, the notion of almost qudits can be extended into entanglement-based scenarios. Do our methods also apply and how do they compare to established semi-definite program hierarchies for the dimension-bounded Bell scenario [10,47]?

A. T. is supported by the Wenner-Gren Foundations. S. P. and J. P. acknowledge funding from the QuantERA II Program that has received funding from the European Union’s Horizon 2020 research and innovation program under Grant Agreement No. 101017733 and the F.R.S-FNRS Pint-Multi program under Grant Agreement No. R.8014.21, from the F.R.S-FNRS through the PDR T.0171.22, from the FWO and F.R.S.-FNRS under the Excellence of Science (EOS) program Project No. 40007526 and from the FWO through the BeQuNet SBO Project No. S008323N. J. P. is a FRIA grantee and S. P. is a a Research Director of the Fonds de la Recherche Scientifique—FNRS.

[1] N. Brunner, S. Pironio, A. Acin, N. Gisin, A. A. Méthot, and V. Scarani, Testing the Dimension of Hilbert Spaces, Phys. Rev. Lett. **100**, 210503 (2008).
[2] R. Gallego, N. Brunner, C. Hadley, and A. Acín, Device-Independent Tests of Classical and Quantum Dimensions, Phys. Rev. Lett. **105**, 230501 (2010).
[3] M. Hendrych, R. Gallego, M. Mičuda, N. Brunner, A. Acín, and J. P. Torres, Experimental estimation of the dimension of classical and quantum systems, Nat. Phys. **8**, 588 (2012).
[4] J. Ahrens, P. Badziag, A. Cabello, and M. Bourennane, Experimental device-independent tests of classical and quantum dimensions, Nat. Phys. **8**, 592 (2012).
[5] A. Tavakoli, J. Pauwels, E. Woodhead, and S. Pironio, Correlations in entanglement-assisted prepare-and-measure scenarios, PRX Quantum **2**, 040357 (2021).
[6] E. F. Galvão and L. Hardy, Substituting a Qubit for an Arbitrarily Large Number of Classical Bits, Phys. Rev. Lett. **90**, 087902 (2003).
[7] B. F. Toner and D. Bacon, Communication Cost of Simulating Bell Correlations, Phys. Rev. Lett. **91**, 187904 (2003).
[8] M. J. Renner, A. Tavakoli, and M. T. Quintino, The classical cost of transmitting a qubit, arXiv:2207.02244.
[9] A. Nayak, Optimal lower bounds for quantum automata and random access codes, in *Proceedings of the 40th Annual Symposium on Foundations of Computer Science (Cat. No.99CB37039)* (IEEE Computer Society, NW Washington, DC, 1999), pp. 369–376.
[10] M. Navascués and T. Vértesi, Bounding the Set of Finite Dimensional Quantum Correlations, Phys. Rev. Lett. **115**, 020501 (2015).
[11] A. Tavakoli, A. Hameedi, B. Marques, and M. Bourennane, Quantum Random Access Codes Using Single *d*-Level Systems, Phys. Rev. Lett. **114**, 170502 (2015).
[12] M. Pawłowski and N. Brunner, Semi-device-independent security of one-way quantum key distribution, Phys. Rev. A **84**, 010302(R) (2011).

[13] E. Woodhead and S. Pironio, Secrecy in Prepare-and-Measure Clauser-Horne-Shimony-Holt Tests with a Qubit Bound, Phys. Rev. Lett. **115**, 150501 (2015).
[14] A. Tavakoli, J. Kaniewski, T. Vértesi, D. Rosset, and N. Brunner, Self-testing quantum states and measurements in the prepare-and-measure scenario, Phys. Rev. A **98**, 062307 (2018).
[15] A. Tavakoli, Semi-Device-Independent Certification of Independent Quantum State and Measurement Devices, Phys. Rev. Lett. **125**, 150503 (2020).
[16] A. Bennet, T. Vértesi, D. J. Saunders, N. Brunner, and G. J. Pryde, Experimental Semi-Device-Independent Certification of Entangled Measurements, Phys. Rev. Lett. **113**, 080405 (2014).
[17] P. Mironowicz, A. Tavakoli, A. Hameedi, B. Marques, M. Pawłowski, and M. Bourennane, Increased certification of semi-device independent random numbers using many inputs and more post-processing, New J. Phys. **18**, 065004 (2016).
[18] D. Martínez, A. Tavakoli, M. Casanova, G. Cañas, B. Marques, and G. Lima, High-Dimensional Quantum Communication Complexity Beyond Strategies Based on Bell's Theorem, Phys. Rev. Lett. **121**, 150504 (2018).
[19] G. Foletto, L. Calderaro, G. Vallone, and P. Villoresi, Experimental demonstration of sequential quantum random access codes, Phys. Rev. Res. **2**, 033205 (2020).
[20] T. Lunghi, J. B. Brask, C. C. W. Lim, Q. Lavigne, J. Bowles, A. Martin, H. Zbinden, and N. Brunner, Self-Testing Quantum Random Number Generator, Phys. Rev. Lett. **114**, 150501 (2015).
[21] H. Anwer, S. Muhammad, W. Cherifi, N. Miklin, A. Tavakoli, and M. Bourennane, Experimental Characterization of Unsharp Qubit Observables and Sequential Measurement Incompatibility via Quantum Random Access Codes, Phys. Rev. Lett. **125**, 080403 (2020).
[22] A. Tavakoli, M. Smania, T. Vértesi, N. Brunner, and M. Bourennane, Self-testing nonprojective quantum measurements in prepare-and-measure experiments, Sci. Adv. **6**, eaaw6664 (2020).
[23] M. Farkas, N. Guerrero, J. Cariñe, G. Cañas, and G. Lima, Self-Testing Mutually Unbiased Bases in Higher Dimensions with Space-Division Multiplexing Optical Fiber Technology, Phys. Rev. Appl. **15**, 014028 (2021).
[24] R. Chaves, J. B. Brask, and N. Brunner, Device-Independent Tests of Entropy, Phys. Rev. Lett. **115**, 110501 (2015).
[25] T. Van Himbeeck, E. Woodhead, N. J. Cerf, R. García-Patrón, and S. Pironio, Semi-device-independent framework based on natural physical assumptions, Quantum **1**, 33 (2017).
[26] Y. Wang, I. W. Primaatmaja, E. Lavie, A. Varvitsiotis, and C. C. W. Lim, Characterising the correlations of prepare-and-measure quantum networks, npj Quantum Inf. **5**, 17 (2019).
[27] A. Tavakoli, E. Zambrini Cruzeiro, J. Bohr Brask, N. Gisin, and N. Brunner, Informationally restricted quantum correlations, Quantum **4**, 332 (2020).
[28] A. Tavakoli, E. Zambrini Cruzeiro, E. Woodhead, and S. Pironio, Informationally restricted correlations: A general framework for classical and quantum systems, Quantum **6**, 620 (2022).
[29] A. Tavakoli, Semi-Device-Independent Framework Based on Restricted Distrust in Prepare-and-Measure Experiments, Phys. Rev. Lett. **126**, 210503 (2021).
[30] H.-W. Li, Z.-Q. Yin, Y.-C. Wu, X.-B. Zou, S. Wang, W. Chen, G.-C. Guo, and Z.-F. Han, Semi-device-independent random-number expansion without entanglement, Phys. Rev. A **84**, 034301 (2011).
[31] H.-W. Li, M. Pawłowski, Z.-Q. Yin, G.-C. Guo, and Z.-F. Han, Semi-device-independent randomness certification using $n \to 1$ quantum random access codes, Phys. Rev. A **85**, 052308 (2012).
[32] A. Ambainis, A. Nayak, A. Ta-Shma, and U. Vazirani, Dense quantum coding and quantum finite automata, J. Assoc. Comput. Mach. **49**, 496 (2002).
[33] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.129.250504 for a proof of the perturbative bound for linear functionals of the probabilities, an analysis of a self-testing protocol for almost qudits, technical details about the SDP hierarchy for almost qudits and a perturbative analysis of the randomness generation protocol studied in this Letter.
[34] M. Farkas and J. Kaniewski, Self-testing mutually unbiased bases in the prepare-and-measure scenario, Phys. Rev. A **99**, 032316 (2019).
[35] K. Mohan, A. Tavakoli, and N. Brunner, Sequential random access codes and self-testing of quantum measurement instruments, New J. Phys. **21**, 083034 (2019).
[36] N. Miklin, J. J. Borkała, and M. Pawłowski, Semi-device-independent self-testing of unsharp measurements, Phys. Rev. Res. **2**, 033014 (2020).
[37] L. Masanes, S. Pironio, and A. Acín, Secure device-independent quantum key distribution with causally independent measurement devices, Nat. Commun. **2**, 238 (2011).
[38] P. Mironowicz, H.-W. Li, and M. Pawłowski, Properties of dimension witnesses and their semidefinite programming relaxations, Phys. Rev. A **90**, 022322 (2014).
[39] M. Navascués, A. Feix, M. Araújo, and T. Vértesi, Characterizing finite-dimensional quantum behavior, Phys. Rev. A **92**, 042117 (2015).
[40] A. Tavakoli, D. Rosset, and M.-O. Renou, Enabling Computation of Correlation Bounds for Finite-Dimensional Quantum Systems via Symmetrization, Phys. Rev. Lett. **122**, 070501 (2019).
[41] S. Gribling, D. de Laat, and M. Laurent, Bounds on entanglement dimensions and quantum graph parameters via noncommutative polynomial optimization, Math. Program. **170**, 5 (2018).
[42] F. Bouchard, R. Fickler, R. W. Boyd, and E. Karimi, High-dimensional quantum cloning and applications to quantum hacking, Sci. Adv. **3**, e1601915 (2017).
[43] M. Erhard, R. Fickler, M. Krenn, and A. Zeilinger, Twisted photons: New quantum perspectives in high dimensions, Light Sci. Appl. **7**, 17146 (2018).
[44] M. Erhard, M. Krenn, and A. Zeilinger, Advances in high-dimensional quantum entanglement, Nat. Rev. Phys. **2**, 365 (2020).
[45] Y. Chi, J. Huang, Z. Zhang, J. Mao, Z. Zhou, X. Chen, C. Zhai, J. Bao, T. Dai, H. Yuan, M. Zhang, D. Dai, B. Tang,

Y. Yang, Z. Li, Y. Ding, L. K. Oxenløwe, M. G. Thompson, J. L. O'Brien, Y. Li, Q. Gong, and J. Wang, A programmable qudit-based quantum processor, Nat. Commun. **13**, 1166 (2022).

[46] M. Ringbauer, M. Meth, L. Postler, R. Stricker, R. Blatt, P. Schindler, and T. Monz, A universal qudit quantum processor with trapped ions, Nat. Phys. **18**, 1053 (2022).

[47] M. Navascués, G. de la Torre, and T. Vértesi, Characterization of Quantum Correlations with Local Dimension Constraints and its Device-Independent Applications, Phys. Rev. X **4**, 011011 (2014).