arXiv:2405.07231v3 [quant-ph] 11 Feb 2025

Information capacity of quantum communication under natural physical assumptions

Jef Pauwels[1,2], Stefano Pironio[3], and Armin Tavakoli[4]

[1]Department of Applied Physics, University of Geneva, 1211 Geneva, Switzerland
[2]Constructor Institute of Technology (CIT), Geneva, Switzerland
[3]Laboratoire d'Information Quantique, Université libre de Bruxelles (ULB), Belgium
[4]Department of Physics and NanoLund, Lund University, Box 118, 22100 Lund, Sweden

The quantum prepare-and-measure scenario has been studied under various physical assumptions on the emitted states. Here, we first discuss how different assumptions are conceptually and formally related. We then identify one that can serve as a relaxation of all others, corresponding to a limitation on the one-shot accessible information of the state ensemble. This motivates us to study the optimal state discrimination probability of a source subject to these various physical assumptions. We derive general and tight bounds for states restricted by their quantum dimension, their vacuum component, an arbitrary uniform overlap, the magnitude of higher-dimensional signals and the experimenter's trust in their device. Our results constitute a first step towards a more unified picture of semi-device-independent quantum information processing.

1 Introduction

The prepare-and-measure (PM) scenario, Fig. 1, formalizes the simplest instance of a quantum communication experiment. A sender, Alice, encodes classical data into quantum systems which are sent to a receiver, Bob, who performs measurements to extract information. Protocols like BB84 and its many descendants [1] are archetypal examples of PM protocols, featuring fully characterized preparation and measurement devices. The advent of quantum technologies, and cryptographic applications in particular, has motivated the study of PM scenarios where devices are left uncharacterized up to some natural physical assumption on the preparation device. This is often referred to as semi-device-independent (SDI) quantum information.

The most common SDI assumption restricts the Hilbert space dimension of the states. Quantum systems can create correlations that cannot be simulated by classical systems of the same dimension [2–5]. This quantum-classical separation enables SDI quantum information protocols for quantum key distribution [6, 7], quantum random number generation [8, 9], self-testing and certification [10–14] and entanglement detection [15–17]. Dimension-restricted communication has also been studied when the parties can additionally share unbounded entanglement [18–20].

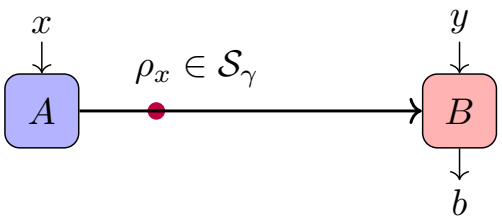

Figure 1: *Prepare-and-measure scenario.* Different SDI assumptions, γ, specify a restriction on the states that Alice can send to Bob. The set of allowed states under a given SDI assumption is denoted $\mathcal{S}_\gamma$.

The dimension represents the number of relevant degrees of freedom under the control of the experimenter. However, this is neither observable nor easy to precisely characterize. These shortcomings, which are especially salient for cryptographic applications, have partly motivated alternative communication assumptions. For example, the "almost dimension" approach assumes the states nearly, but not exactly, admit a d-dimensional representation [21]. Other proposals move away from the dimension entirely. An approach particularly well-suited to optical platforms supposes a limit on the photon excitations of the states, measured through the magnitude of the non-vacuum component [22]. This has e.g. been used for random number generation, in theory [23, 24] and practice [25–28]. Another approach is to bound the pairwise overlap between the states emitted by Alice [29, 30], which also has been used in various protocols [31–35]. Yet another communication assumption is a bound on the fidelity with which Alice prepares the specific states that she ideally intends to send to Bob [36]. This may be viewed as a relaxation of the perfect preparation assumption used in one-sided device-independent approaches [37]. For brevity, we shall refer to these different assumptions as (i) the dimension restriction, (ii) entanglement-assisted dimension

restriction, (iii) the vacuum component restriction, (iv) the overlap restriction, (v) almost dimension restriction, and (vi) the distrust restriction. Approaches (iii)-(vi) are primarily motivated by practical considerations, and (i)-(ii) partly also by the fundamental interest in comparing classical and quantum systems.

In contrast to the above assumptions that relate directly to the physical or quantum aspects of the preparation, a communication framework was introduced in [38–40], in which the only assumption has an information-theoretic interpretation. Roughly speaking, it quantifies how much knowledge could in principle be gained about Alice's input by measuring her states. This information restriction on Alice's preparations can, in general, neither be directly deduced from the setup nor accurately bounded by measuring a suitable observable. Operationally, it can be interpreted as the best quantum state discrimination possible on Alice's states [41]. In this way, it provides an avenue to quantify the information cost of creating correlations between Alice and Bob.

In this paper, we begin by structuring this landscape of quantum communication assumptions and then identifying connections between the different frameworks, but argue that they admit no generic hierarchy of relations in terms of the supported quantum correlations. However, we observe that all assumptions admit a one-way connection to information. To make this connection explicit, we address the independently interesting question of determining the information capacity of quantum communication subjected to any of the considered restrictions. This amounts to bounding the best success probability in quantum state discrimination compatible with states limited by the various communication assumptions. For all assumptions, this is achieved analytically, in complete generality and, in most cases, provably tightly.

2 Overview of common SDI assumptions

Consider the prepare-and-measure scenario in Fig. 1. Alice privately selects an input x and encodes it in a quantum message ρ_x, sent to Bob over a noiseless channel, who performs a decoding measurement $\{M_{b|y}\}_y$ depending on y, yielding an outcome b. The resulting correlations are given by Born's rule, $p(b|x,y) = \mathrm{tr}\left(\rho_x M_{b|y}\right)$. Naturally, if no restriction is imposed on the systems ρ_x, Alice may simply send x over the channel, and Bob can simulate any $p(b|x,y)$. An assumed restriction on the devices is thus needed to limit the set of achievable correlations. Many assumptions, usually on the preparation device or, equivalently, on the channel connecting Alice and Bob have been studied in the literature. We summarize the most common ones below.

(i) Dimension [2, 3]. The state ρ_x is assumed to live in a Hilbert of fixed dimension d, that is, $\rho_x \in \mathcal{L}(\mathbb{C}^d)$, where $\mathcal{L}(\mathbb{C}^d)$ denotes the set of linear operators on $\mathbb{C}^d$. W.l.g. one can also limit the measurement to be d-dimensional, but one can notably not assume them projective [42–44].

(ii) Entanglement-assisted dimension [18–20]. Alice and Bob share an entangled state ϕ_{AB}. Alice encodes x in her part of the entangled state using a quantum channel Λ_x with fixed output dimension d (the dimension of her message), and sends the output to Bob. Bob measures the total state $\rho_x = (\Lambda_x \otimes \mathbb{1})[\phi_{AB}]$. One can generally not restrict the local dimension of ϕ_{AB} to message dimension d [45] and no upper bound on it is known.

(iii) Vacuum component [22, 23]. Define the the Hamiltonian $H = \mathbb{1} - |0\rangle\langle 0|$ and associate the state $|0\rangle$ to vacuum (no photon). A restriction, ω, is assumed on photon exctitation of Alice's states as $\mathrm{tr}(H\rho_x) \leq \omega$.

(iv) Overlaps [29, 30]. The states ρ_x are assumed to have purifications, $|\psi_x\rangle$, whose pairwise overlaps are bounded as $|\langle\psi_x|\psi_{x'}\rangle| \geq a_{xx'}$ for some $a_{xx'} \in \mathbb{R}$.

(v) Almost-dimension [21]. Assume that there exists a d-dimensional space, with projector Π_d, in which nearly all of the support of Alice's states is contained,

$$\mathrm{tr}(\rho_x \Pi_d) \geq 1 - \varepsilon \,, \tag{1}$$

for some small dimension-deviation parameters $\varepsilon \geq 0$. The part of the state that is not supported on Π_d corresponds to a deviation from the ideal d-dimensional system.

(vi) Distrust [36]. Alice aims to prepare a state $|\psi_x\rangle$ but her preparation device realizes the lab state ρ_x. Her distrust in the device is limited through the fidelity between the target state and the lab state, $\langle\psi_x|\rho_x|\psi_x\rangle \geq 1-\epsilon$, where $\epsilon \geq 0$ is the distrust parameter. The lab states need not be of the same dimension as the target states.

(*) Information [38–40]. Given the classical-quantum state $\rho_{XB} = \frac{1}{n}\sum_{x=1}^{n} |x\rangle\langle x| \otimes \rho_x$, the conditional min-entropy is $H_{\min}(X|B) = -\log_2(P_g)$ with

$$P_g\left(\{\rho_x\}\right) \equiv \max_{\{N_x\}} \frac{1}{n} \sum_{x=1}^{n} \mathrm{tr}\left(\rho_x N_x\right), \tag{2}$$

where n is the number of states and $\{N_x\}_x$ is a measurement. Thus, P_g is the optimal probability of correctly guessing the classical value x given the quantum state ρ_x [41]. The accessible information, measuring how much information the states ρ_x convey about x, is then defined as the entropy difference $\mathcal{I} \equiv H_{\min}(X) - H_{\min}(X|B) = \log(n) + \log(P_g)$, where we assumed that X is uniform. The information restriction assumption introduced in [38–40] is then the limit $\mathcal{I} \leq \alpha$ for some $\alpha \geq 0$, or equivalently, a limitation $P_g \leq \frac{2^\alpha}{n}$.

3 Role of shared randomness

In general, a communication assumption can be written as $\{\rho_x\}_x \in \mathcal{S}_\gamma$, for some selected set $\mathcal{S}_\gamma$, where γ indexes the specific assumption parameters. Specifically, $\gamma = d$ for the (entanglement-assisted) dimension, $\gamma = \omega$ for the vacuum assumption, $\gamma = (a_{xx'})_{xx'}$ for the overlap assumption, $\gamma = (d, \epsilon)$ for the almost dimension, $\gamma = (\varepsilon, \psi_x)_x$ for the distrust and $\gamma = \alpha$ for the information. The corresponding PM scenario can always be extended by allowing for shared randomness (SR) between Alice and Bob, leading to the correlations $p(b|x,y) = \sum_\lambda q_\lambda \operatorname{tr}\left(\rho_x^\lambda M_{b|y}^\lambda\right)$, where λ denotes the shared randomness and q is a distribution. Now, the assumption can be formulated in two different ways; either as *peak-γ* or *average-γ*. Average-γ means that the parameter assumption, γ, holds when averaging out λ,

$$\{\rho_x^\lambda\}_x \in \mathcal{S}_{\gamma_\lambda} \quad \text{with} \sum_\lambda q_\lambda \gamma_\lambda = \gamma. \tag{3}$$

For instance, in the vacuum component framework, the states can sometimes have larger or smaller vacuum components $\omega^\lambda = \operatorname{tr}\left(\rho_x^\lambda H\right)$ but on average it respects the vacuum limit $\sum_\lambda q_\lambda \omega^\lambda \leq \omega$. Peak-$\gamma$ means that the assumption holds also when conditioning on λ,

$$\{\rho_x^\lambda\}_x \in \mathcal{S}_\gamma\,, \quad \forall \lambda\,. \tag{4}$$

Continuing the example, the states may be different for each λ but their vacuum component always respects the limit $\operatorname{tr}\left(\rho_x^\lambda H\right) \leq \omega$ for all λ.

The peak-γ assumption is natural for all cases considered above. At the level of the correlations, it corresponds simply to taking the convex-hull of the set of correlations without SR. The average-γ restriction has been studied explicitly for the vacuum [22], almost qudit [21] and distrust [36] assumptions. It has also been studied for Bell scenarios with dimension assumptions [46]; see also Appendix C in Ref. [21].

It is also relevant to distinguish between whether the states ρ_x^λ are assumed pure or mixed. Depending on the assumption, this can change the set of correlations [39, 47]. While purity can be assumed w.l.g for (entanglement-assisted) dimension (by exploiting shared randomness, every mixed state admits a decomposition into pure states, each satisfying the assumption), there is neither a proof nor a counterexample of the same holding for the other assumptions.

For all assumptions, the set of correlations without SR under assumption γ is strictly contained in the set with peak-γ SR, which itself is strictly contained in the set for average-γ SR. In constrast, for the information assumption, the correlations without SR, with peak-γ SR, and with average-γ SR are all equivalent. Following eqs. (2), (3) and (4), these three sets are defined as those corresponding to a source sending, respectively, states ρ_x satisfying $P_g(\{\rho_x\}) \leq \gamma$, states ρ_x^λ satisfying $P_g(\{\rho_x^\lambda\}) \leq \gamma$ for all λ, and states ρ_x^λ satisfying $\sum_\lambda q(\lambda) P_g(\{\rho_x^\lambda\}) \leq \gamma$. But the SR can always be incorporated in the emitted states themselves without increasing their information content [39]. Indeed, simply define as emitted states the cq-states $\tilde{\rho}_x = \sum_\lambda q(\lambda)|\lambda\rangle\langle\lambda| \otimes \rho_x^\lambda$, whose guessing probability is $P_g(\{\tilde{\rho}_x\}) = \sum_\lambda q(\lambda) P_g(\{\rho_x^\lambda\}) \leq \gamma$. Any peak-$\gamma$ or average-γ strategy can thus be recast as an equivalent strategy that does not feature SR and which satifies the information restriction $P_g \leq \gamma$.

Note that starting from the information restriction $\mathcal{I} = \log(n) + \log(P_g(\{\rho_x\})) \leq \alpha \equiv \gamma$, rather than directly from the guessing probability, there are two ways to extend it from the no SR case to the average-γ SR. One possibility is to assume for each λ that $\mathcal{I}_\lambda \leq \alpha_\lambda$ with $\sum_\lambda q(\lambda)\alpha_\lambda = \alpha$, i.e., the average is taken at the level of the information quantity itself. The other possibility is to take the average at the level of the guessing probability and define the information bound as a bound $\log(n) + \log\left(\sum_\lambda q(\lambda) P_g(\{\rho_x^\lambda\})\right) \leq \alpha$, which is equivalent to the average guessing probability bound $\sum_\lambda q(\lambda) P_g(\{\rho_x^\lambda\}) \leq 2^\alpha/n$. This corresponds to the situation described above and to the choice made in [38, 39].

4 Connecting the assumptions

In Fig. 2, we summarize the relations between the various assumptions, as discussed below.

Dimension-based assumptions. The dimension is a special case of both the entanglement-assisted dimension and the almost dimension. In the former, we need only to restrict to sharing separable states, while in the latter we just set the dimensional deviation in Eq. (1) to $\varepsilon = 0$. However, these two are independent, and therefore incomparable, generalizations of the dimension restriction.

Vacuum restriction. The vacuum component restriction can be seen as a limiting case of an almost dimension restriction. The latter is motivated as a correction to exact dimension restrictions, which are meaningful only when $d \geq 2$. However, an almost dimension restriction can in principle also be defined for $d = 1$. The projector Π_d is then a pure state, which we call the vacuum $|0\rangle$. This reduces Eq. (1) to the vaccum component assumption. Consequently, the methodology developed in Ref. [21] for bounding correlations under almost d-dimensional systems can also be applied to analyze correlations under a vacuum component restriction [48]. This is also a useful observation because, in the absence of such methods, the SDI protocols based on vacuum component restrictions have so far been limited to using just two states (analytically solvable) [22, 23]. Interestingly, the vacuum component restriction can equally be viewed as

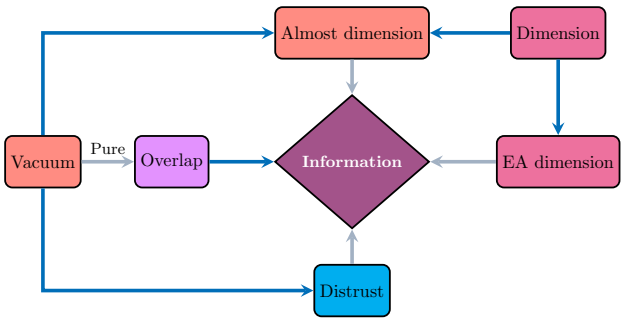

Figure 2: Relation between various SDI assumptions. Blue (grey) arrows indicate that one assumption is a special case (relaxation) of the other. The overlap relaxation of the vacuum only holds for pure states.

a limiting case of the distrust restriction. Indeed, the experimenter selects all target states to be vacuum, independently of x, i.e. $|\psi_x\rangle = |0\rangle$. This means that the numerical methods for distrust restricted correlations, developed in [36], also can be used to analyze the case of restricted vacuum components.

Almost dimension and distrust Does an almost dimension restriction admit any meaningful connection to a distrust restriction? The almost dimension too can be reformulated as a fidelity condition. The definition of fidelity for mixed states is $F(\sigma,\tau) = \left(\mathrm{tr}\sqrt{\sqrt{\sigma}\tau\sqrt{\sigma}}\right)^2$. For arbitrary positive operators A and B, it follows that $F(A, BAB) = \mathrm{tr}(AB)^2$. The almost dimension assumption can then be interpreted as the fidelity between ρ_x and its normalized projection onto the d-dimensional subspace Π_d. That is, $F\left(\rho_x, \frac{\Pi_d\rho_x\Pi_d}{\mathrm{tr}(\rho_x\Pi_d)}\right) = \mathrm{tr}(\rho_x\Pi_d) \geq 1-\varepsilon$ via Eq. (1). What decisively distinguishes it from the distrust assumption is that Π_d cannot depend on x, as this would defeat the notion of the ensemble $\{\rho_x\}$ approximating a d-dimensional system.

Overlaps. Finally, the overlap restriction can be viewed as a relaxation of a vacuum restriction in the special case where all states $|\psi_x\rangle$ are pure. The vacuum component restriction $\mathrm{tr}(|\psi_x\rangle\langle\psi_x|\,(\mathbb{1} - |0\rangle\langle 0|)) \leq \omega$ imposes a constraint on minimal overlap of the lab states, $|\langle\psi_x|0\rangle| \geq \sqrt{1-\omega}$. This restriction, on the minimal overlap between the lab states and the fixed reference state $|0\rangle$, in turn, implies a restriction on the minimal pairwise overlaps between the lab states. We will soon return to quantifying this.

Information. While the above assumptions in general are not comparable, they can all be linked to the notion of restricted accessible information (see Fig. 2). This is possible because the information restriction has no privileged state spaces but only concerns how operationally useful the states are for carrying the information. Specifically, there exist fundamental limits on the amount of information an n-state quantum ensemble can carry when restricted by any one of the assumptions under pure states. This leads directly to a bound under average-γ SR in all cases except entanglement-assisted dimension, for which the bound necessarily diverges unless one restricts to peak-γ SR.

5 Information cost

Determining the largest accessible information that can be carried by an ensemble of n pure states limited by any one of the trust assumptions amounts to evaluating an upper limitation on the ability to use such states for state discrimination, see Eq. (2). We express this as

$$P_g^* \equiv \max_{\{\psi_x\}\in\mathcal{S}_\gamma} P_g(\{\psi_x\}), \tag{5}$$

where $\psi_x = |\psi_x\rangle\langle\psi_x|$ is pure. We now address this problem for all considered settings. Then, we show how the results are valid also under SR.

Dimension. For completeness, we first rederive the known fact that any dimension-restricted ensemble, i.e. $\mathcal{S} = \mathcal{L}(\mathbb{C}^d)$, carries at most $\log d$ bits [49]. Taking $n \geq d$ and using the fact that for any measurement N_x the corresponding optimal states ψ_x are projectors on the eigenvector of N_x with the largest eigenvalue, we obtain $P_g^* = \max_{\{N_x\}} \frac{1}{n}\sum_x \lambda_{\max}(N_x) \leq \max_{\{N_x\}} \frac{1}{n}\sum_x \mathrm{tr}(N_x) = \frac{d}{n}$, where we have used that $\sum_x N_x = \mathbb{1}_d$. The information cost becomes $\mathcal{I} \leq \log(d)$, independently of n. This bound can be saturated trivially by d states forming a basis of $\mathbb{C}^d$. We note that this also follows directly from the fact that the signaling dimension [50] of quantum and classical systems of dimension d are equal [51].

Entanglement-assisted dimension. The set of states ψ_x generated via entanglement-assisted quantum communication obeys no-signaling, meaning that Bob's local state is independent of Alice's operation, i.e. $\psi^B \equiv \mathrm{tr}_A(\psi_x)$ for all x. We can thus restrict to bipartite states with a constant marginal on Bob. Then, for $n \geq d^2$ [18], $P_g^* \leq \max \frac{d}{n}\sum_x \mathrm{tr}\left(\psi_x^B N_x^B\right) = \max \frac{d}{n}\sum_x \mathrm{tr}\left(\psi_B N_x^B\right) = \frac{d^2}{n}$. Here, we used that the Schmidt number of ψ_x is at most d which implies $\mathrm{tr}(\psi_x N_x) \leq d\,\mathrm{tr}\left(\psi_x^B N_x^B\right)$, where $N_x^B = \mathrm{tr}_A(N_x)$. In the last step, we used that $\sum_x N_x^B = \mathrm{tr}_A \sum_x N_x = \mathrm{tr}_A(\mathbb{1}_d \otimes \mathbb{1}) = d\mathbb{1}$. The associated information cost is $\mathcal{I} \leq 2\log(d)$. This can be saturated using a d-dimensional dense coding protocol [52].

Overlaps. When $n = 2$, the overlap of two pure states is one-to-one with their accessible information. This follows from the derivation of the Helstom bound for two-state discrimination [53]. In this sense, the overlap is a special case of the information restriction (thus the connection in Fig. 2). For $n > 2$ and a uniform overlap constraint $\langle\psi_x|\psi_{x'}\rangle \geq a$, we can use the observation that for ensembles that are equiprobable and equiangular [54] the optimal measurement for

state discrimination is the so-called pretty good measurement [55], defined as $N_x = S^{-1/2}\psi_x S^{-1/2}$ where $S = \sum_x \psi_x$. This leads to

$$P_g \leq \frac{1}{n^2}\left((n-1)\sqrt{1-a} + \sqrt{(n-1)a+1}\right)^2 . \quad (6)$$

Vacuum component. W.l.g we can select the amplitude associated with the vacuum $|0\rangle$ to be real and then use the simulation technique of [56] to embed the non-vacuum components in a sufficiently high-dimensional real-valued Hilbert space. The reachable state space therefore forms a cone around the vacuum state with radius $\sqrt{1-\omega}$. We optimally choose all states on the boundary of this cone, i.e. $\sqrt{1-\omega} = \langle 0|\psi_x\rangle$. The value of P_g is invariant under permutations of the label x. From any optimal solution, we can then always form a solution where all the states have identical overlaps $\langle\psi_x|\psi_{x'}\rangle = a$ for all $x \neq x'$. Indeed, consider the direct sum states $|\Psi_x\rangle = \frac{1}{\sqrt{N}} \oplus_k \sigma_k|\psi_x\rangle$ where the sum k runs over the N permutations σ_k of the input labels x. Then the states $|\Psi_x\rangle$ have now equal overlaps, guessing probability P_g at least equal to the original one, and all have an overlap $\sqrt{1-\omega}$ with the vacuum state $\frac{1}{\sqrt{N}} \oplus_k |0\rangle$ (which can be unitarily mapped to the original vacuum state $|0\rangle \oplus 0 \ldots \oplus 0$ if desired).

Given our result for the overlap assumption above, to evaluate P_g, we only need to minimize the overlap a. The Gram matrix associated with the states $\{|\psi_1\rangle, \ldots, |\psi_n\rangle, |0\rangle\}$ is $G = \begin{pmatrix} A & B \\ B^T & 1 \end{pmatrix}$, where A is $n \times n$ with 1 on the diagonals and a on the off-diagonals, and B is $n \times 1$ with all entries $\sqrt{1-\omega}$.

It is positive semidefinite by construction. We therefore compute $a^* = \min_{G \succeq 0} a$. Using Schur complements, the eigenvalues of G can be evaluated analytically. From the smallest one, we obtain the result $a^* = 1 - \frac{n}{n-1}\omega$. Combining this with the pretty good measurement leads to the bound

$$P_g \leq \frac{1}{n}\left(\sqrt{\omega(n-1)} + \sqrt{1-\omega}\right)^2 , \quad (7)$$

valid when $0 \leq \omega \leq \frac{n-1}{n}$, while $P_g = 1$ otherwise. It can be saturated by construction. The corresponding accessible information increases monotonically in n. The reason is that even if ω is very small, since there is no dimension restriction, we can always choose the small non-vacuum component of each state orthogonal to that of all the other states, thus increasing the information.

Almost dimension and distrust. For bounding the information capacity associated with almost dimension-restricted or distrust-restricted states, we rely on a useful operator inequality. Specifically, we observe that the method in Ref. [57] for proving Lemma 1 can be recycled to prove the following more general statement. Let $|\phi\rangle$ be any state such that $\langle\phi|\Pi_d|\phi\rangle \geq 1-\varepsilon$. Then, $|\phi\rangle\langle\phi| \preceq (1+\mu)\tilde{\sigma} + h(\varepsilon,\mu)\mathbb{1}_D$ for every $\mu \geq -1$, where $\tilde{\sigma} = \frac{\Pi_d|\phi\rangle\langle\phi|\Pi_d}{\langle\phi|\Pi_d|\phi\rangle}$ and $h(\varepsilon,\mu) = (\sqrt{\mu^2 + 4\varepsilon(1+\mu)} - \mu)/2$. We apply this independently to each pure ψ_x in Eq. (2) and optimally choose each associated μ to be identical. Using that n states span an n-dimensional subspace, we can restrict to n-dimensional POVMs and obtain $P_g^* \leq (1+\mu)\left[\max_{\{N_x\}} \frac{1}{n}\sum_x \mathrm{tr}\left(\tilde{\psi}_x N_x\right)\right] + h(\mu,\varepsilon)$. In the case of the almost dimension assumption, $\tilde{\psi}_x$ are d-dimensional and hence the maximization is bounded by d/n. In the case of distrust assumption, Π_d is simply replaced by $|\psi_x\rangle\langle\psi_x|$ and we have $\tilde{\psi}_x = |\psi_x\rangle\langle\psi_x|$. Therefore, the maximisation becomes just $P_g(\{\psi_x\})$ for the target ensemble. Let P_g^0 denote the value of the maximization for either the almost dimension case or the distrust case. Minimising the RHS over μ, we find

$$P_g^\varepsilon \leq P_g^0 + (1-2P_g^0)\varepsilon + 2\sqrt{P_g^0(1-P_g^0)}\sqrt{\varepsilon(1-\varepsilon)}. \quad (8)$$

Note that in the special case of $d = 1$, for the almost dimension, for which $P_g^0 = \frac{1}{n}$, this bound reduces to that obtained for vacuum component restrictions in Eq. (7). We have not been able to prove that the bound is tight in general, but for every numerical case study conducted, we find that the bound is indeed tight for the almost dimension assumption [58]. For the distrust assumption, the bound is generally not tight unless the target states are optimal for state discrimination [58].

It can be straightforwardly shown that the above information capacity bounds hold also when SR is included. First, from the linearity of P_g, our results also hold for the peak-γ SR assumption. Second, we note that the bound on P_g for every assumption except entanglement-assisted dimension is concave in each of the respective assumption parameters (the dimension d, the energy ω, the overlap a, distrust parameter ϵ, almost qudits (ϵ, d)[1]). This implies that our results also hold for the average-γ assumption, for all but the entanglement-assisted dimension[2].

An independently interesting consequence of this result is to bound the information capacity of n optical coherent states with a limited average photon number but arbitrary phase. Recall the coherent state $|\alpha\rangle = e^{-\frac{|\alpha|}{2}} \sum_{k=0}^{\infty} \frac{|\alpha|^k e^{i\theta k}}{\sqrt{k!}} |k\rangle$. For small average photon numbers, $N = |\alpha|^2$, this can be seen as an almost qubit with $\varepsilon = 1 - e^{-|\alpha|}(1+|\alpha|^2) \approx \sqrt{N}$. Inserting this in (8) and then computing $\mathcal{I}$ yields the desired bound.

[1] It is straightforward to verify the concavity of the bivariate function (8) from the negativity of the Hessian.

[2] For example, setting $N = 30$, with an entanglement-assisted qutrit, a dense coding strategy achieves $P_g = 9/30$. However, one can send an *average* qutrit by mixing a qubit with probability 2/3 and a 5-dimensional system with probability 1/3. Using dense coding strategies, one can achieve a guessing probability of $P_g = 11/30$.

6 Final remarks

Quantum communication assumptions in the prepare-and-measure scenario can be divided into two classes. The first class limits the weight of the state on various subspaces. These can correspond to the available degrees of freedom (dimension, almost dimension and entanglement-assisted dimension), the vacuum subspace, the subspace spanned by each of the other states of Alice (overlap assumption), the subspace corresponding to her target states (distrust assumption) etc. The second class does not favor any particular subspaces but is instead concerned with limiting the capacity of the states w.r.t. a specific operational task. This task can for instance be state discrimination, as in the considered information restriction setting, but can in principle be arbitrary. Developing a formalism and methodology for correlations obtained under assumptions on bounded subspace weights and capacity restrictions are natural next steps towards a unified picture of SDI. This is important because although we have established several tight information capacity relations, this does not imply that the set of correlations under a given communication assumption can w.l.g. be substituted with that obtained from the associated informationally restricted communication. In this context, we also note that while the set of correlations without SR, with average-γ SR, and with peak-γ SR can be distinct depending on the assumption, they all relax to the same set of information-constrained correlations if in the latter the SR is taken at the level of P_g, i.e., $P_g = \sum_\lambda q_\lambda P_g(\{\rho_x^\lambda\}_x) \leq \gamma$, as considered here and in [38, 39]. This would not be the case for an alternative definition, where the information itself is averaged over the SR, i.e., $I = \log(n) + \sum_\lambda q_\lambda \log P_g(\{\rho_x^\lambda\}_x) \leq \gamma$. Developing a formalism for the latter case is an interesting open question.

Acknowledgments

A.T. is supported by the Wenner-Gren Foundation, by the Knut and Alice Wallenberg Foundation through the Wallenberg Center for Quantum Technology (WACQT) and the Swedish Research Council under Contract No. 2023-03498. J.P. acknowledges support from the Swiss National Science Foundation via the NCCR-SwissMap. S.P. acknowledges funding from the VERIqTAS project within the QuantERA II Programme 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 R.8014.21, from the European Union's Horizon Europe research and innovation program under the project "Quantum Security Networks Partnership" (QSNP, grant agreement No 101114043), 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 40007526, from the FWO through the BeQuNet SBO project S008323N, from the Belgian Federal Science Policy through the contract RT/22/BE-QCI and the EU "BE-QCI" program. S.P. is a Research Director of the Fonds de la Recherche Scientifique – FNRS.

References

[1] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. "Quantum cryptography". Rev. Mod. Phys. **74**, 145–195 (2002).

[2] Stephanie Wehner, Matthias Christandl, and Andrew C Doherty. "Lower bound on the dimension of a quantum system given measured data". Phys. Rev. A**78**, 062112 (2008).

[3] Rodrigo Gallego, Nicolas Brunner, Christopher Hadley, and Antonio Acín. "Device-independent tests of classical and quantum dimensions". Phys. Rev. Lett. **105**, 230501 (2010).

[4] Nicolas Brunner, Miguel Navascués, and Tamás Vértesi. "Dimension witnesses and quantum state discrimination". Phys. Rev. Lett. **110**, 150501 (2013).

[5] Armin Tavakoli, Alley Hameedi, Breno Marques, and Mohamed Bourennane. "Quantum random access codes using single d-level systems". Phys. Rev. Lett. **114**, 170502 (2015).

[6] Marcin Pawłowski and Nicolas Brunner. "Semi-device-independent security of one-way quantum key distribution". Phys. Rev. A **84**, 010302 (2011).

[7] Erik Woodhead and Stefano Pironio. "Secrecy in prepare-and-measure clauser-horne-shimony-holt tests with a qubit bound". Phys. Rev. Lett. **115**, 150501 (2015).

[8] Hong-Wei Li, Marcin Pawłowski, Zhen-Qiang Yin, Guang-Can Guo, and Zheng-Fu Han. "Semi-device-independent randomness certification using $n \to 1$ quantum random access codes". Phys. Rev. A **85**, 052308 (2012).

[9] Tommaso Lunghi, Jonatan Bohr Brask, Charles Ci Wen Lim, Quentin Lavigne, Joseph Bowles, Anthony Martin, Hugo Zbinden, and Nicolas Brunner. "Self-testing quantum random number generator". Phys. Rev. Lett. **114**, 150501 (2015).

[10] Armin Tavakoli, Jędrzej Kaniewski, Tamás Vértesi, Denis Rosset, and Nicolas Brunner. "Self-testing quantum states and measurements in the prepare-and-measure scenario". Phys. Rev. A **98**, 062307 (2018).

[11] Máté Farkas and Jędrzej Kaniewski. "Self-testing mutually unbiased bases in the prepare-and-measure scenario". Phys. Rev. A **99**, 032316 (2019).

[12] Armin Tavakoli. "Semi-device-independent certification of independent quantum state and

measurement devices". Phys. Rev. Lett. **125**, 150503 (2020).

[13] Miguel Navascués, Károly F. Pál, Tamás Vértesi, and Mateus Araújo. "Self-testing in prepare-and-measure scenarios and a robust version of wigner's theorem". Phys. Rev. Lett. **131**, 250802 (2023).

[14] Sophie Egelhaaf, Jef Pauwels, Marco Túlio Quintino, and Roope Uola. "Certifying measurement incompatibility in prepare-and-measure and bell scenarios" (2024). arXiv:2407.06787.

[15] Armin Tavakoli, Alastair A. Abbott, Marc-Olivier Renou, Nicolas Gisin, and Nicolas Brunner. "Semi-device-independent characterization of multipartite entanglement of states and measurements". Phys. Rev. A **98**, 052333 (2018).

[16] George Moreno, Ranieri Nery, Carlos de Gois, Rafael Rabelo, and Rafael Chaves. "Semi-device-independent certification of entanglement in superdense coding". Phys. Rev. A **103**, 022426 (2021).

[17] Pharnam Bakhshinezhad, Mohammad Mehboudi, Carles Roch i Carceller, and Armin Tavakoli. "Scalable entanglement certification via quantum communication" (2024). arXiv:2401.00796.

[18] Armin Tavakoli, Jef Pauwels, Erik Woodhead, and Stefano Pironio. "Correlations in entanglement-assisted prepare-and-measure scenarios". PRX Quantum **2**, 040357 (2021).

[19] Jef Pauwels, Armin Tavakoli, Erik Woodhead, and Stefano Pironio. "Entanglement in prepare-and-measure scenarios: many questions, a few answers". NJPq **24**, 063015 (2022).

[20] Carlos Vieira, Carlos de Gois, Lucas Pollyceno, and Rafael Rabelo. "Interplays between classical and quantum entanglement-assisted communication scenarios". NJP **25**, 113004 (2023).

[21] Jef Pauwels, Stefano Pironio, Erik Woodhead, and Armin Tavakoli. "Almost qudits in the prepare-and-measure scenario". Phys. Rev. Lett. **129**, 250504 (2022).

[22] Thomas Van Himbeeck, Erik Woodhead, Nicolas J. Cerf, Raúl García-Patrón, and Stefano Pironio. "Semi-device-independent framework based on natural physical assumptions". Quantum **1**, 33 (2017).

[23] Thomas Van Himbeeck and Stefano Pironio. "Correlations and randomness generation based on energy constraints" (2019). arXiv:1905.09117.

[24] Gabriel Senno and Antonio Acín. "Semi-device-independent full randomness amplification based on energy bounds" (2021). arXiv:2108.09100.

[25] Davide Rusca, Thomas van Himbeeck, Anthony Martin, Jonatan Bohr Brask, Weixu Shi, Stefano Pironio, Nicolas Brunner, and Hugo Zbinden. "Self-testing quantum random-number generator based on an energy bound". Phys. Rev. A **100**, 062338 (2019).

[26] Davide Rusca, Hamid Tebyanian, Anthony Martin, and Hugo Zbinden. "Fast self-testing quantum random number generator based on homodyne detection". Appl. Phys. Lett **116**, 264004 (2020).

[27] Hamid Tebyanian, Mujtaba Zahidy, Marco Avesani, Andrea Stanco, Paolo Villoresi, and Giuseppe Vallone. "Semi-device independent randomness generation based on quantum state's indistinguishability". QST **6**, 045026 (2021).

[28] Marco Avesani, Hamid Tebyanian, Paolo Villoresi, and Giuseppe Vallone. "Semi-device-independent heterodyne-based quantum random-number generator". Phys. Rev. Appl. **15**, 034034 (2021).

[29] Jonatan Bohr Brask, Anthony Martin, William Esposito, Raphael Houlmann, Joseph Bowles, Hugo Zbinden, and Nicolas Brunner. "Megahertz-rate semi-device-independent quantum random number generators based on unambiguous state discrimination". Phys. Rev. Appl. **7**, 054018 (2017).

[30] Yukun Wang, Ignatius William Primaatmaja, Emilien Lavie, Antonios Varvitsiotis, and Charles Ci Wen Lim. "Characterising the correlations of prepare-and-measure quantum networks". npj Quantum Inf. **5**, 17 (2019).

[31] Marie Ioannou, Maria Ana Pereira, Davide Rusca, Fadri Grünenfelder, Alberto Boaron, Matthieu Perrenoud, Alastair A. Abbott, Pavel Sekatski, Jean-Daniel Bancal, Nicolas Maring, Hugo Zbinden, and Nicolas Brunner. "Receiver-Device-Independent Quantum Key Distribution". Quantum **6**, 718 (2022).

[32] Marie Ioannou, Pavel Sekatski, Alastair A Abbott, Denis Rosset, Jean-Daniel Bancal, and Nicolas Brunner. "Receiver-device-independent quantum key distribution protocols". NJP **24**, 063006 (2022).

[33] Carles Roch i Carceller, Kieran Flatt, Hanwool Lee, Joonwoo Bae, and Jonatan Bohr Brask. "Quantum vs noncontextual semi-device-independent randomness certification". Phys. Rev. Lett. **129**, 050501 (2022).

[34] Weixu Shi, Yu Cai, Jonatan Bohr Brask, Hugo Zbinden, and Nicolas Brunner. "Semi-device-independent characterization of quantum measurements under a minimum overlap assumption". Phys. Rev. A **100**, 042108 (2019).

[35] Qin Fan, Meng-Yun Ma, Yong-Nan Sun, Qi-Ping Su, and Chui-Ping Yang. "Experimental certification of nonprojective quantum measurements under a minimum overlap assumption". Opt. Express **30**, 34441–34452 (2022).

[36] Armin Tavakoli. "Semi-device-independent framework based on restricted distrust in

prepare-and-measure experiments". Phys. Rev. Lett. **126**, 210503 (2021).

[37] Ivan Šupić, Paul Skrzypczyk, and Daniel Cavalcanti. "Measurement-device-independent entanglement and randomness estimation in quantum networks". Phys. Rev. A **95**, 042340 (2017).

[38] Armin Tavakoli, Emmanuel Zambrini Cruzeiro, Jonatan Bohr Brask, Nicolas Gisin, and Nicolas Brunner. "Informationally restricted quantum correlations". Quantum **4**, 332 (2020).

[39] Armin Tavakoli, Emmanuel Zambrini Cruzeiro, Erik Woodhead, and Stefano Pironio. "Informationally restricted correlations: a general framework for classical and quantum systems". Quantum **6**, 620 (2022).

[40] Anubhav Chaturvedi and Debashis Saha. "Quantum prescriptions are more ontologically distinct than they are operationally distinguishable". Quantum **4**, 345 (2020).

[41] Robert Konig, Renato Renner, and Christian Schaffner. "The operational meaning of min- and max-entropy". IEEE Trans. Inf. Theory **55**, 4337–4347 (2009).

[42] Armin Tavakoli, Massimiliano Smania, Tamás Vértesi, Nicolas Brunner, and Mohamed Bourennane. "Self-testing nonprojective quantum measurements in prepare-and-measure experiments". Sci. Adv. **6**, eaaw6664 (2020).

[43] Daniel Martínez, Esteban S. Gómez, Jaime Cariñe, Luciano Pereira, Aldo Delgado, Stephen P. Walborn, Armin Tavakoli, and Gustavo Lima. "Certification of a non-projective qudit measurement using multiport beamsplitters". Nat. Phys. **19**, 190–195 (2023).

[44] Lan-Tian Feng, Xiao-Min Hu, Ming Zhang, Yu-Jie Cheng, Chao Zhang, Yu Guo, Yu-Yang Ding, Zhibo Hou, Fang-Wen Sun, Guang-Can Guo, Dao-Xin Dai, Armin Tavakoli, Xi-Feng Ren, and Bi-Heng Liu. "Higher-dimensional symmetric informationally complete measurement via programmable photonic integrated optics" (2023). arXiv:2310.08838.

[45] Yu Guo, Hao Tang, Jef Pauwels, Emmanuel Zambrini Cruzeiro, Xiao-Min Hu, Bi-Heng Liu, Yu-Feng Huang, Chuan-Feng Li, Guang-Can Guo, and Armin Tavakoli. "Experimental higher-dimensional entanglement advantage over qubit channel" (2023). arXiv:2306.13495v2.

[46] Sander Gribling, David de Laat, and Monique Laurent. "Bounds on entanglement dimensions and quantum graph parameters via noncommutative polynomial optimization". Math. Program. **170**, 5–42 (2018).

[47] Armin Tavakoli, Emmanuel Zambrini Cruzeiro, Roope Uola, and Alastair A. Abbott. "Bounding and simulating contextual correlations in quantum theory". PRX Quantum **2**, 020334 (2021).

[48] Carles Roch i Carceller, Jef Pauwels, Stefano Pironio, and Armin Tavakoli. "Prepare-and-measure scenarios with photon-number constraints" (2024). arXiv:2412.13000.

[49] A. Nayak. "Optimal lower bounds for quantum automata and random access codes". In 40th Annual Symposium on Foundations of Computer Science (Cat. No.99CB37039). Pages 369–376. (1999).

[50] Michele Dall'Arno, Sarah Brandsen, Alessandro Tosini, Francesco Buscemi, and Vlatko Vedral. "No-hypersignaling principle". Physical Review Letters **119**, 020401 (2017).

[51] Péter E. Frenkel and Mihály Weiner. "Classical information storage in an n-level quantum system". Communications in Mathematical Physics **340**, 563–574 (2015).

[52] Charles H. Bennett and Stephen J. Wiesner. "Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states". Phys. Rev. Lett. **69**, 2881–2884 (1992).

[53] Carl W. Helstrom. "Quantum detection and estimation theory". J. Stat. Phys. **1**, 231–252 (1969).

[54] Hari Krovi, Saikat Guha, Zachary Dutton, and Marcus P. da Silva. "Optimal measurements for symmetric quantum states with applications to optical communication". Phys. Rev. A **92**, 062333 (2015).

[55] Ashley Montanaro. "On the distinguishability of random quantum states". Comm. Math. Phys. **273**, 619–636 (2007).

[56] Matthew McKague, Michele Mosca, and Nicolas Gisin. "Simulating quantum systems using real Hilbert spaces". Phys. Rev. Lett. **102**, 020505 (2009).

[57] Armin Tavakoli. "Quantum steering with imprecise measurements". Physical Review Letters **132**, 070204 (2024).

[58] "The matlab script that was used to verify this can be found on `https://github.com/jefpauwels/SDISeesaw`.".